Instituto Brasileiro de Tecnologia
Curso de Pós-Graduação em Segurança da Informação

Segurança de Aplicações WEB: Hardening nos Servidores baseados em software livre

por
ALBERTO LUIS VIEGAS
alviegas@gmail.com

Recife
2008

Alberto Luis Viegas

Segurança de Aplicações WEB:
Hardening nos Servidores baseados em software livre

Monografia de conclusão do Curso de Pós-Graduação Latto Sensu, apresentada ao Instituto Brasileiro de Tecnologia como requisito à obtenção do título de especialista em segurança da Informação.

Orientador: M.S.c. Márcio Luiz Machado Nogueira

RECIFE

2008

AGRADECIMENTOS

Agradeço ao Prof. Marcio Nogueira, pelo apoio durante a realização desse trabalho.

A Arte da guerra nos ensina a confiar, não na possibilidade de o inimigo não vir, mas sim, na nossa prontidão para recebê-lo; não na probabilidade de ele não atacar, mas preferivelmente no fato de termos tornado nossa posição inexpugnável. (Sun Tzu)

RESUMO

Quando se encontra uma falha numa aplicação Web já em produção, às vezes se torna inviável sua correção, pois a empresa geralmente não tem o devido suporte contratado ou não dispõe de corpo técnico suficientemente para corrigir o problema em tempo hábil.

O objetivo deste trabalho é demonstrar técnicas de fortalecimento (*hardening)* nos servidores, para executar aplicações web, com o objetivo de minimizar a possibilidade de ter seu ambiente comprometido por atacantes.

Este trabalho,trata-se de um estudo na área de segurança da informação, com ênfase das melhores práticas de hardening em servidores baseados em software livre. Realizamos uma análise prática de uma aplicação web, com algumas falhas de seguraça, explorando suas vulnerabilidades, e relacionando com as melhores práticas de proteção deste ambiente.

Os resultados apontaram uma melhoria efetiva no sistema, ao bloquear vulnerabilidades antes expostas, simulando um sevidor e uma aplicação web com falhas de segurança.

Foram utilizadas algumas práticas já conhecidas, mas com objetivos específicos entre elas, destacamos o Scan de Rede, Análise de Vulnerabilidades e utilização de Técnicas de Intrusões.

Palavras-Chave: Hardening, Aplicações Web, Fortalecimento da Segurança em servidores.

LISTA DE ILUSTRAÇÕES

Figura 01 – Modelo de aplicação web 11
Figura 02 – Incidentes reportados pela CERT.br em 2008 19
Figura 03 – Comando “Nmap” aplicado no experimento 23
Figura 04 – Tela inicial do Nessus 27
Figura 05 – Tela Final do Relatório do Nessus 27
Figura 06 – Esquema do Cenário 1 33
Figura 07 – Resultado do Nmap do laboratório 1 34
Figura 08 – Tela inicial do Nessus do Cenário 1 34
Figura 09 – Resultado do Scan de vulnerabilidade do Cenário 1 35
Figura 10 – Acunetix: Configurando URL da aplicação do cenário 1 36
Figura 11 – Acunetix: Informações levantadas do cenário 1 36
Figura 12 – Acunetix: opções para rastrear do cenário 1 37
Figura 13 – Acunetix: opções para scan do cenário 1 38
Figura 14 – Acunetix: Informações de autenticações do cenário 1 39
Figura 15 – Acunetix: Sumário para realizar scan do cenário 1 39
Figura 16 – Acunetix: Resultado do scan do cenário 1 40
Figura 17 – Tela de SQL injection do Laboratório 1 40
Figura 18 – Tela do sucesso da SQL Injection do laboratório 1 41
Figura 19 - Esquema do Cenário 2 42
Figura 20 - Resultado do Nmap do Cenário 2 43
Figura 21 – Nessus: configuração inicial do Cenário 2 43
Figura 22 – Nessus: Relatório do Cenário 2 44
Figura 23 – Acunetix: Configurando a URL da aplicação do cenário 2 45
Figura 24 – Acunetix: Informações levantadas do cenário 2 45
Figura 25 – Acunetix: opções para rastrear do cenário 2 46
Figura 26 – Acunetix: opções para scan do cenário 2 47
Figura 27 – Acunetix: Informações de autenticações do cenário 2 48
Figura 28 – Acunetix: Sumário para realizar scan do cenário 2 48
Figura 29 – Acunetix: Resultado do scan do cenário 2 49
Figura 30 – Tela de SQL injection do Cenário 2 50
Figura 31 – Tela da falha da SQL Injection do Cenário 2 50

LISTA DE TABELAS

Tabela 01 – Relação entre principais problemas de segurança e Técnicas de *Hardening*.....31
Tabela 02 – Análise do ambiente: Antes do *hardening* 41
Tabela 03 – Análise do ambiente: Após as práticas *hardening* 51

SUMÁRIO

Introdução 9

Capítulo 1 10

1.1 Contextualização 10
1.2 Problemática 13
1.3 Objetivos 13
1.3.1 Objetivo Geral 13
1.3.2 Objetvo Específico 13

Capitulo 2 15

2.1 Levantamento Histórico Sobre Hardening 15
2.2 Levantamento Histórico Sobre Aplicações Web 16
2.3 Principais problemas de segurança web 16

Capitulo 3 22

3. Características técnicas de fortalecimento para servidores 22
3.1 Ferramentas de Scan de rede 22
3.1.1 Nmap 22
Algumas opções: 25
3.2 Ferramentas de Análise de Vulnerabilidade 25
3.2.1 Nessus 25
3.1.3 Acunetix 28

3.2. Técnicas de Hardening 28

3.2.1 Segurança no sistema de arquivos 28

3.2.2 Utilização de Quota 29
3.2.3 Remoção de programas desnecessários 29
3.2.4 Permissões especiais de arquivos 29
3.2.5 Segurança no Terminal 29
3.2.6 Regras de utilização de serviços de rede e serviços ativos do sistema 29
3.2.7 Firewall 30
3.2.8 Tunning do Kernel 30
3.2.9 Firewall de aplicação Web 30
3.2.10 Análise de vulnerabilidades 30
3.3 Relação entre as principais vulnerabilidades e técnicas de hardening 30

Capitulo 4 33

4. Experimento dos conceitos levantados sobre uma aplicação insegura 33
4.1 Cenário 1 33
4.2 Cenário 2 42

Capitulo 5 52

5. Conclusão 52

Referências Bilbliográficas 54

ANEXO I 56

ANEXO II 61

ANEXO III 74

ANEXO IV 110

ANEXO V 118

Introdução

Um estudo realizado pela empresa de segurança Acunetix, (ACUNETIX, 2006), apontou que 70% dos sites têm problemas de segurança. O estudo revela que 7 em cada 10 sites possui vulnerabilidades de segurança que permitiriam ataques de crackers, nos casos mais extremos com brechas para roubo de informações confidenciais. A Acunetix verificou 3,2 mil sites pertencentes a companhias e organizações não-comerciais que se ofereceram como voluntárias para o teste de segurança. Segundo a Acunetix, 2006, os resultados foram assustadores: um total de 210 mil vulnerabilidades, representando uma média de 66 falhas de segurança em cada aplicação online. Metade dos perigos encontrados diz respeito a vulnerabilidades em bancos de dados SQL. Enquanto outros 42% a falhas de Cross-Scripting, em que crackers inserem códigos em sites e serviços que são posteriormente executados nos computadores dos visitantes. Esta relação entre as vulnerabiliades em SQL e Cross- Scripting, acontece devido a falha de validação de entradas, que não é tratada na aplicação web.

Com o uso de aplicações web no mundo cada vez maior, cresce também os problemas de validação de entradas dos sistemas que comprometem as máquinas que hospedam estes serviços. Nosso trabalho apresenta alguns dos principais problemas de segurança existentes, em servidores web baseados em software livre, e as técnicas de segurança mais utilizadas atualmente, que possibilita a redução dos riscos associados a estes serviços.

Capítulo 1

1.1 Contextualização

Para Tanenbaum,(2003), muitas empresas possuem um número significativo de computadores distribuídos nos mais distintos departamentos organizacionais. As redes de computadores permitiram a interligação desses computadores e subsidiou o desenvolvimento de sistemas. Assim, como o compartilhamento de recursos e informações. Essa descentralização constituiu uma arquitetura Cliente/Servidor e gerou a necessidade de mecanismos de segurança aos usuários e aplicações, tais como, sistemas de autenticação.

A arquitetura Cliente/Servidor é amplamente utilizada e constituí a base da grande utilização da rede. Há dois processos envolvidos: um na máquina cliente e um na máquina servidor. A comunicação utiliza o processo cliente enviando uma mensagem pela rede ao processo servidor, nesse caso, o processo cliente espera por uma mensagem em resposta. Quando o processo servidor recebe a solicitação, executa o trabalho ou procura pelos dados solicitados, enviando de volta uma resposta.

As aplicações web, se utilizam do protocolo http. Definido por Assunção (2008), o protocolo http é usado pela *World Wide Web*, a rede mundial de websites da Internet. O http é um protocolo chamado de “sem estado”, pois cada comando é executado independente, sem nenhum conhecimento dos comandos que vieram antes dele. Por isso, é difícil implementar sites web que reajam de modo inteligente à entrada de dados de um usuário.

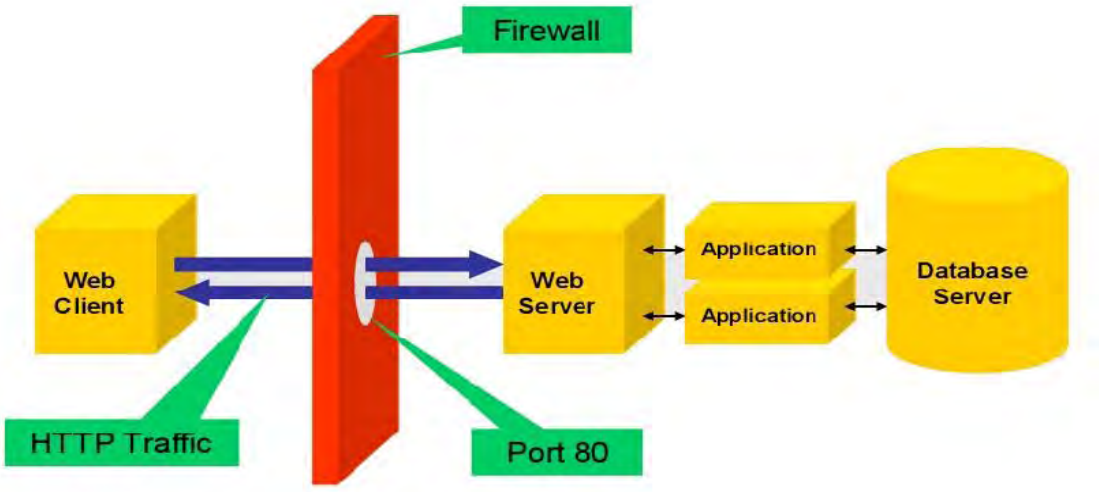

Figura 01 – Modelo de aplicação web

Para Horton (2004), não é nenhuma surpresa que as empresas estão cada vez mais realizando seus negócios através da Internet, como também oferecendo uma maior funcionalidade e lidando com dados mais importantes através de serviços Web. As aplicações Web estão sendo usadas para melhorar a interação com o cliente e aumentar a funcionalidade comercial. Para o publico mundial, Internet tem ajudado as empresas a aumentarem consideravelmente seus negócios, mas, ao mesmo tempo, trouxe uma série de falhas de seguranças nas aplicações web, que podem comprometer os servidores.

Não é nenhuma surpresa que as empresas estão cada vez mais realizando seus negócios através da Internet, como também oferecendo uma maior funcionalidade e lidando com dados mais importantes através de serviços Web. As aplicações Web são usadas para melhorar a interação com o cliente e aumentar a funcionalidade comercial. Para o público mundial, a Internet tem ajudado as empresas a aumentarem consideravelmente seus negócios, entretanto ao mesmo tempo vem trazendo uma série de falhas de seguranças em suas aplicações, comprometem os servidores. (HORTON, 2004)

A Associação Profissional de Risco, (APRISCO, 2006), afirma que, a segurança das aplicações, principalmente aquelas conectadas a uma rede Internet é bastante complexa. Essa complexidade advém do fato que as aplicações web, e-commerce, Internet bank, na realidade são agrupamentos bastante heterogêneos de plataformas, bancos de dados, servidores de aplicação entre outros.

Uma mesma aplicação, geralmente, está distribuída em vários servidores, rodando diversos aplicativos e, para funcionar na velocidade adequada, a aplicação precisa que as interfaces entre os diversos sistemas sejam construídas com a premissa de que os dados passados através da mesma, sejam confiáveis e não inseguras, pois não há tempo hábil para duplas verificações.

O “Ponto fraco” destas aplicações é a insegurança, pois há uma necessidade de “confiança” entre os diversos subsistemas, é atráves dessa vulnerabilidade que os hackers e outros cibercriminosos agem.

Segundo a SecurityFocus, as vulnerabilidades são classificadas em:

a) Input Validation Error – Erro de validação de entrada, ocorre quando um programa falhou ao reconhecer sintaticamente uma entrada incorreta, o modulo

aceita campos de entrada estranhos, um modulo falha, ao tratar campos e entrada não preenchidos.

b) Boundary Condition Error – Condição de erro limite ocorre quando um processo tenta ler ou escrever além de um endereço limite válido; um recurso de sistema é esgotado.

c) Design Error – Erro de planejamento ocorre durante o planejamento / desenho da solução.

d) Access Validation Error – Erro de validação de acesso ocorre quando alguém invoca uma operação ou um objeto fora do domínio de acesso; Um objeto aceita entrada de algo não autorizado; O sistema falhou ao autenticar algo / alguém.

e) Atomicity Error – Errors de atomicidade ocorrem quando o código terminou com dados modificados apenas parcialmente, oriundo de alguma operação que deveria ter sido atômica.

f) Enviroment Error – Erros de ambiente é o resultado da interação em um ambiente específico entre módulos funcionalmente corretos ocorrem quando um programaé executado em uma máquina específica, em uma configuração particular; O sistema operacional é diferente daquele para o qual o software foi escrito.

g) Race Condition Error – Erros de condição de corrida ocorrem durante uma janela de tempo entre dias operações, Em um ambiente multitarefas, vários processos estão em execução pseudo-simultânea e isto dá margem a uma classe de ataques que exploram as condições de disputa.

h) Serialization Error – Erro d serialização resulta da serialização inadequada ou imprópria de operações / informações.

i) Origin Validation – Erro de validação de origem ocorre quando o sistema falha ao autenticar alguém antes de executar operações provilegiadas; O objeto aceita uma entrada de alguém não autorizado, pressupondo que alguém já o aceitou antes.

j) Failure to Handle exceptions condicions – Falha de tratamento de exceções ocorre quando o sistema falha ao tratar exceções geradas por um módulo, dispositivo ou entrada do usuário.

Estas classes de vulnerabilidades citadas, fazem parte da taxonomia de vulnerabilidades descritas pela securityfocus, onde possue um grande banco de informações referente as vulnerabilidades publicadas e devidamente classificadas, informando a data da publicação da falha, autor e sugestões para solucionar o problema encontrado.

1.2 Problemática

Avaliar as propostas técnicas de fortalecimento de servidores web e verificar se de fato, estas possibilitam um ambiente mais seguro, e em qual proporção, para os usuários.

1.3 Objetivos

1.3.1 Objetivo Geral

Avaliar as medidas de segurança oferecida a aplicações web, através das técnicas de fortalecimento de servidores.

1.3.2 Objetvo Específico

- Levantamento Histórico sobre Hardening e Aplicações web
- Características técnicas de fortalecimento para servidores
- Experimento dos conceitos levantados sobre uma aplicação web insegura

1.4 Metodologia Científica

A norma OSSTMM, desenvolvida inicialmente por Herzog em 2001, descreve a necessidade de realização de testes de segurança, entre as quais destacamos: Varredura (Network Scanning), Análise de Vulnerabilidade (Vulnerability Scanning).

Baseado nestas informações nosso experimento se propõe a demonstrar,

utilizando uma aplicação de web com falhas de segurança já conhecidas e dentro de um laboratório simulando a internet. Nosso experimento será feito com base nas recomendações da OSSTMM.

Capitulo 2

2.1 Levantamento Histórico Sobre Hardening

Turnbull, (2005), enfatiza que a segurança do seu sistema depende da vasta variedade de elementos de configurações, tanto no nível do sistema operacional, quanto no nível da aplicação. Destacamos a complexidade do kernel do Linux e a importância de sua customização. Algumas vulnerabilidades de segurança nem sempre são perceptíveis podendo conduzir a uma exposição involuntária.

> *"Well, as the old saying goes, "The devil is in the details." The security of your system depends on awide variety of configuration elements both at the operating system level and the application level. Additionally, the Linux operating system and kernel are complex and not always easy to configure. In fact, Linux systems are nearly infinitely configurable, and subtle configuration changes can have significant security implications. Thus, some security exposures and vulnerabilities are not always immediately obvious, and alack of understanding about the global impact of changing configuration elements can lead to inadvertent exposures".* (Turnbull, (2005).

Ele recomenda ainda algumas práticas simples para instalar de forma segura o sistema operacional:

- Instalar somente o necessário
- Segurança no Boot do Sistema
- Seqüência de inicialização de serviços
- Controle das consoles virtuais
- Administração Usuários e Grupos
- Políticas de Senha
- Integridade dos arquivos do sistema
- Atualização dos pacotes e Patches
- Remoção de Compiladores e pacotes de desenvolvimentos
- Implementar segurança no Kernel
- Aplicar filtro de pacotes (Firewall)

As técnicas de Hardening, são recomendações sugeridas pela BS7799,

criada pelo British Standard Institution (BSI) com objetivo de ajudar as empresas a construir políticas de segurança concisas e efetivas para todos os ativos da empresa a partir de uma contextualização, tendo como base os princípios da segurança da informação.

Muitos administradores sem experiência em segurança preparam seus servidores com a instalação básica e convencional, sem qualquer configuração extra a fim de alterar o padrão disponibilizado pelo fabricante.

Melo (2006), reforça que o sistema operacional torna-se bastante seguro uma vez devidamente trabalhado. É por causa disso que se deve aperfeiçoar suas configurações padrões. As técnicas de *Hardening* embora sejam muito boas, porém não se aplicam em todas as situações, devendo ser observada as características da aplicação web em questão.

2.2 Levantamento Histórico Sobre Aplicações Web

Aplicação Web é o termo utilizado para designar de forma geral, sistemas de informática projetados para utilização através de um navegador, na internet ou em redes privadas (Intranet). Trata-se de um conjunto de programas que é executado em um servidor de web. O desenvolvimento da tecnologia web está relacionado, entre outros fatores, a necessidade de simplificar a atualização e manutenção mantendo o código-fonte em um mesmo local de onde ele é acessado pelos diferentes usuários. Podemos definir uma aplicação web como um sistema de software que utiliza a web, através de um browser, como ambiente de execução.

2.3 Principais problemas de segurança web

Os ataques que hoje conhecemos são baseados em vulnerabilidades típicas de aplicações web complexas independente do sistema operacional utilizado.

Existêm vulnerabilidades que são periodicamente descobertas por hackers e só se transformam em atualizações depois que os mesmos já exploraram algumas vezes.

Um dos ataques mais comuns em aplicações web, é a exploração da validação de dados, através da Injeção de SQL. Esta técnica consiste na inserção de

comandos SQL – *Structured Query Language* – nas entradas de dados dos clientes. Algumas aplicações fazem consultas a banco de dados baseadas nas informações recebidas dos clientes. Assim, se os dados recebidos não forem validados corretamente, será possível a concatenação de comandos SQL à informação desejada pela aplicação. Dessa maneira, o atacante poderá executar comandos no banco de dados da aplicação. Os possíveis danos provenientes de ataques de injeção de SQL são a visualização, a alteração e a exclusão dos registros presentes em uma base de dados por uma pessoa não autorizada. A depender do Sistema Gerenciador de Banco de Dados utilizado, todas as operações comuns em um acesso legítimo a uma base de dados podem ser efetuadas por um atacante utilizando a técnica de Injeção de SQL (OWASP, 2007b).

Segundo a OWASP em 2007, obtidas através do estudo de Tendências de Vulnerabilidades para 2006 do MITRE, foram extraídos 10 vulnerabilidades conhecidas, relativas a aplicações WEB.

I) Cross Site Scripting (XSS)

Os furos XSS ocorrem sempre que uma aplicação obtém as informações fornecidas pelo usuário e as envia de volta ao navegador sem realizar validação ou codificação daquele conteúdo. O XSS permite aos atacantes executarem scripts no navegador da vítima, o qual pode roubar sessões de usuário, pichar sites Web, introduzir worms entre outros.

II) Injeção de SQL

As falhas de injeção, em especial SQL Injection, são comuns em aplicações Web. A injeção ocorre quando os dados fornecidos pelo usuário são enviados a um interpretador com parte do comando ou consulta. A informação maliciosa fornecida pelo atacante engana o interpretador que irá executar comandos mal intencionados ou manipular informações.

III) Execução maliciosa de Arquivos

Os códigos vulneráveis à inclusão remota de arquivos (RFI) permitem ao atacante incluir código e dados maliciosos, resultando em ataques devastadores, como o comprometimento total do servidor. Os ataques de execução de arquivos maliciosos afetam PHP, XML e todos os frameworks que aceitem nomes de

arquivo ou arquivos dos usuários.

IV) Referência Insegura Direta a Objetos

Uma referência direta a objeto ocorre quando um desenvolvedor expõe a referência a um objeto implementado internamente. É o caso de arquivos, diretórios, registros da base de dados ou chaves, na forma de uma URL ou parâmetro de formulário. Os atacantes podem manipular estas referências para acessar outros objetos sem autorização.

V) Cross Site Request Forgery (CSRF)

Um ataque CSRF força o navegador da vítima, que esteja autenticado em uma aplicação, a enviar uma requisição pré-autenticada a um servidor Web vulnerável, que por sua vez força o navegador da vítima a executar uma ação maliciosa em prol do atacante. O CSRF pode ser tão poderoso quanto à aplicação Web que ele ataca.

VI) Vazamento de Informações e Tratamento de Erros Inapropriado

As aplicações podem divulgar informações sobre suas configurações, processos internos ou violar a privacidade por meio de uma série de problemas na aplicação sem haver qualquer intenção. Os atacantes podem usar esta fragilidade para roubar informações consideradas sensíveis ou conduzir ataques mais estruturados.

VII) Autenticação Falha e Gerenciamento de Sessão

As credenciais de acesso e token de sessão não são protegidas apropriadamente com bastante freqüência. Atacantes comprometem senhas, chaves ou tokens de autenticação de forma a assumir a identidade de outros usuários.

VIII) Armazenamento Criptográfico Inseguro

As aplicações Web raramente utilizam funções criptográficas de forma adequada para proteção de informações e credenciais. Os atacantes se aproveitam de informações mal protegidas para realizar roubo de identidade e outros crimes, como fraudes de cartões de crédito.

IX) Comunicações inseguras

As aplicações freqüentemente falham em criptografar tráfego de rede quando se faz necessário proteger comunicações críticas/confidenciais.

X) Falha de Restrição de Acesso à URL

Frequentemente, uma aplicação protege suas funcionalidades críticas somente pela supressão de informações como links ou URLs para usuários não autorizados. Os atacantes podem fazer uso desta fragilidade para acessar e realizar operações não autorizadas por meio do acesso direto às URLs.

Segundo a CERT.br (2008), os ataques de Fraude e Scan, permanecem no topo da lista dos incidentes reportados, veja o gráfico abaixo:

Figura 02 – Incidentes reportados pela CERT.br em 2008

Podemos definir scan, como programas que percorrem as principais portas e serviços do sistema em busca de respostas. Basicamente estão divididos em dois grupos, Port Scanning e Scanning de vulnerabilidades.

a) **Port Scanning**

Verifica as portas abertas de um sistema. O objetivo de um port scan é detectar as portas de serviços de um sistema, fazendo-as responder cada vez que forem consultadas. Existem algumas técnicas de portscanning utilizadas. São elas:

- TCP CONNECT SCAN - Este tipo de scanner se conecta a porta e executa os três handshakes básicos (SYN, SYN/ACK e ACK). Ele é facilmente detectável.
- TCP SYN SCAN - Conhecido como half-open scanning, devido a conexão total TCP durante a operação. Dessa forma, evita que o log da operação fique no sistema. Normalmente, o programa envia um pacote SYN para a porta-alvo. Se recebi um SYN/ACK do alvo, o programa deduz que a porta está no modo de escuta; caso seja um RST/ACK, significa que a porta não está ativa naquele momento.
- UDP SCAN - Trata-se de um dos processos mais lentos de scanning, pois depende de fatores de utilização da rede e de recursos de sistema. O scanner envia um pacote UDP para a porta-alvo: se a resposta for ICMP port unreachable, a porta encontra-se fechada; casocontrário, o scanner deduz que a porta está aberta.
- TCP NULL SCAN - Neste caso, o scanner desativa todos os flags e aguarda do alvo um RST para identificar todas as portas fechadas. Baseado na RFC 793.
- TCP FIN SCAN - O scanner envia pacotes FIN para a porta-alvo e espera o retorno de um RST para as portas fechadas. Baseado em RFC 793.
- TCP XMAS TREE SCAN - Neste caso, o scanner envia pacotes FIN, URG e Push para a porta-alvo e espera o retorno de um RST para as portas fechadas. Baseado também na RFC 793.

b) **Scanner de Vulnerabilidade**

Utilizado para detecção de vulnerabilidades em softwares executados em um sistema. Esse tipo de scanner é muito útil para o hacker, já que, através dele, o atacante pode escolher qual o exploit a ser utilizado para a invasão. Existem diversos scanners de vulnerabilidade, mas muitos crackers desenvolvem scanners private (scanner de uso pessoal não divulgado), e os utilizam para fins não éticos. Basicamente a idéia do scanner de vulnerabilidade é, através de uma lista, checar se o sistema está ou não executando um serviço com problemas. Estes scanners são facilmente desatualizados, pois existe uma quantidade enorme de descobertas

hoje lançadas em sites de segurança.

Agora que conhecemos os principais problemas de segurança em aplicações web, veremos no próximo capítulo quais as técnicas para identificar estas falhas, e formas de nos protegemos dos ataques.

Capitulo 3

3. Características técnicas de fortalecimento para servidores

Com a grande quantidade de aplicações web disponível no mundo, nos diversos tipos de sistemas operacionais e serviços, tecnicamente se tornam inviáveis a realização destes testes manualmente. Neste trabalho, destacamos algumas ferramentas que vão fornecer relatórios necessários, para que seja levantado o nível de segurança dos nossos servidores. Entre elas destacamos: o Nmap (insecure.org) para realizar a varredura de portas abertas na rede, o Nessus (Tenable Network Security), para a análise de vulnerabilidades e o Acunetix Vulnerability Scanner (Acunetix), para análise dos serviços web. Estas ferramentas estão no Top 100 da insecure.org, (2008).

3.1 Ferramentas de Scan de rede

3.1.1 Nmap

Criada por Fyodor, o Nmap (Network Mapper) é uma ferramenta free e open source sob licença GPL. É um utilitário de exploração de redes a procura de portas tcp e udp abertas. Muitos administradores de redes a utilizam para mostrar como levantar um inventário da rede, gerenciar atualizações e monitorar hosts ou tempo de serviços ativos. O NMAP usa o IP puro e através de tipos de pacotes pode determinar quais hosts estão disponíveis na rede; quais os serviços (nome das aplicações e versões) estes hosts estão oferecendo; qual o sistema operacional (e versões) eles estão rodando; qual tipo de filtro de pacotes/firewalls está em uso, e dezenas de outras características. Com o Nmap é possível levantar informações de uma rede grande. Funciona na maioria dos sistemas operacionais, e está disponível em cersão console e ambiente gráfico.

Métodos de Varredura do NMAP:

No experimento, foi utilizada a seguinte técnica de Port Scan, com o NMAP:

Figura 03 – Comando “Nmap” aplicado no experimento

Onde as opções utilizadas no nmap, para o host 192.168.220.129, foi:

-sS

TCP SYN scan: Técnica também conhecida como “half-open”, pois não abre uma conexão TCP completa. É enviado um pacote SYN, como se ele fosse uma conexão real e aguardasse uma resposta. Caso um pacote SYN-ACK seja recebido, a porta será aberta, enquanto uma outra resposta indica que a porta está fechada. A vantagem dessa abordagem é que poucos irão detectar esse scanning de portas.

-T4

Método de Scan, agressivo.

-A

Habilita o modo de detecção do Sistema Operacional e as versões dos serviços identificados.

Seguem outras opções do Nmap que podemos combinar a fim de obter diversos resultados:

-sP

Ping scan: Algumas vezes é necessário saber se um determinado host ou rede está no ar. Nmap pode enviar pacotes ICMP “echo request” para verificar se determinado host ou rede está ativa. Hoje em dia, existem muitos filtros que rejeitam os pacotes ICMP “echo request”, por esse motivo, ele envia um pacote TCP ACK para a porta 80 (default) e caso receba RST o alvo está ativo. Uma terceira técnica envia um pacote SYN e espera um RST ou SYN-ACK.

-sR

RCP scan: Este método trabalha em conjunto com várias técnicas do Nmap. Ele considera todas as portas TCP e UDP abertas e envia comandos NULL SunRPC, para determinar se realmente são portas RPC. É como se o comando “rpcinfo -p” estivesse sendo utilizado, mesmo através de um firewall ou protegido por TCP wrappers.

-sT

TCP connect() scan: É a técnica mais básica de TCP scanning. Utiliza a chamada de um sistema (system call) “connect()” que envia um sinal as portas ativas. Caso a porta esteja aberta recebe como resposta “connect()”. Podemos dizer que é um dos scan mais rápidos, porém fácil de ser detectado.

-sU

UDP scan: Este método é utilizado para determinar qual porta UDP está aberta em um host. A técnica consiste em enviar um pacote UDP de 0 byte para cada porta do host. Se for recebida uma mensagem ICMP “port unreachable” então a porta está fechada, de outro modo a porta provalvelmente pode estará aberta. A Microsoft, por exemplo, ignorou a sugestão da RFC e com isso a varredura de máquinas Windows é muito rápida.

-sV

Version detection: Após as portas TCP e/ou UDP serem descobertas por algum dos métodos, o nmap irá determinar qual o serviço estará rodando no momento. O arquivo nmap-service-probes é utilizado para determinar tipos de protocolos, nome da aplicação, número da versão entre outros detalhes.

-sF, -sX, -sN

Stealth FIN, Xmas Tree ou Null: Alguns firewalls e filtros de pacotes detectam pacotes SYN's em portas restritas, então é necessário utilizar métodos avançados para atravessar esses softwares.

FIN: Portas fechadas enviam um pacote RST como resposta a pacotes FIN, enquanto portas abertas ignoram esses pacotes. (Esse método não funciona com a plataforma Windows, uma vez que a Microsoft não seguiu RFC 973)

Xmas Tree: Portas fechadas enviam um pacote RST como resposta a pacotes FIN, enquanto portas abertas ignoram esses pacotes. As flags FIN, URG e PUSH são utilizados nos pacotes FIN que é enviado ao alvo. (Esse método não funciona com a plataforma Windows, uma vez que a Microsoft não seguiu RFC 973)

Null: Portas fechadas enviam um pacote RST como resposta a pacotes FIN, enquanto portas abertas ignoram esses pacotes. Nenhuma flag é ligada no pacote FIN. (Esse método não funciona com a plataforma Windows, uma vez que a Microsoft não seguiu RFC 973)

Algumas opções:

-O

Ativa a identificação do host remoto via TCP/IP. Irá apresentar versão do Sistema Operacional e tempo ativo.

-p <lista_de_portas>

Especifica quais portas devem ser verificadas na varredura. Por default, todas as portas entre 1 e 1024 são varridas.

-P0

Não tenta pingar o host antes de iniciar a varredura. Isto permite varrer alvos que bloqueiam ICMP “echo request (ou responses)” através de firewall.

-v

Modo verbose. Mostra tudo o que está se passando.

3.2 Ferramentas de Análise de Vulnerabilidade

3.2.1 Nessus

O Nessus é uma ferramenta designada para testar e descobrir falhas de segurança (portas, vulnerabilidades, exploits) de uma ou mais máquinas. Estas

falhas ou problemas podem ser descobertos por um grupo hacker (ou um único hacker), uma empresa de segurança ou pelo próprio fabricante, podendo ser de maneira acidental ou proposital, O Nessus ajuda a identificar e resolver estes problemas antes que alguém tire vantagem destas falhas com propósitos maliciosos.

O Nessus foi incialmente distribuído sob os termos da Licença Pública Geral GNU. O suporte técnico pago para o Nessus pode ser visto no site http://www.tenablesecurity.com. Atualmente está livre para download. A subscrição de updates de vulnerabilidades da Tenable está disponível de duas maneiras: Home Users e Professional Users.

Uma das principais características do Nessus é a sua tecnologia cliente-servidor, onde os servidores podem ser alocados em pontos estratégicos da rede permitindo testes de vários pontos diferentes. Um cliente central ou múltiplos clientes podem controlar todos os servidores. O Nessus está disponível para a maioria das plataformas *nix, roda no MAC OS X, IBM/AIX e Windows. Uma parte (Servidor) executa os testes enquanto a outra parte (cliente) permite a configuração e emissão de relatórios.

Ele realiza uma varredura de portas, detectando servidores ativos e simulando invasões para detectar vulnerabilidades. Uma característica importante é que o Nessus procura por servidores ativos não apenas nas portas padrão, mas em todas as portas TCP. Pode ser obtido em http://www.nessus.org/nessus.

Nos testes realizados nos servidores, utilizamos os plugins padrões, sem prescisar alterar as configurações originais. Apenas fizemos referências aos respectivos IPs. Já para fins de testes no experimento, foram utilizados configurações padõres no NESSUS, sem qualquer alteração em suas configurações, como mostram as figuras abaixo:

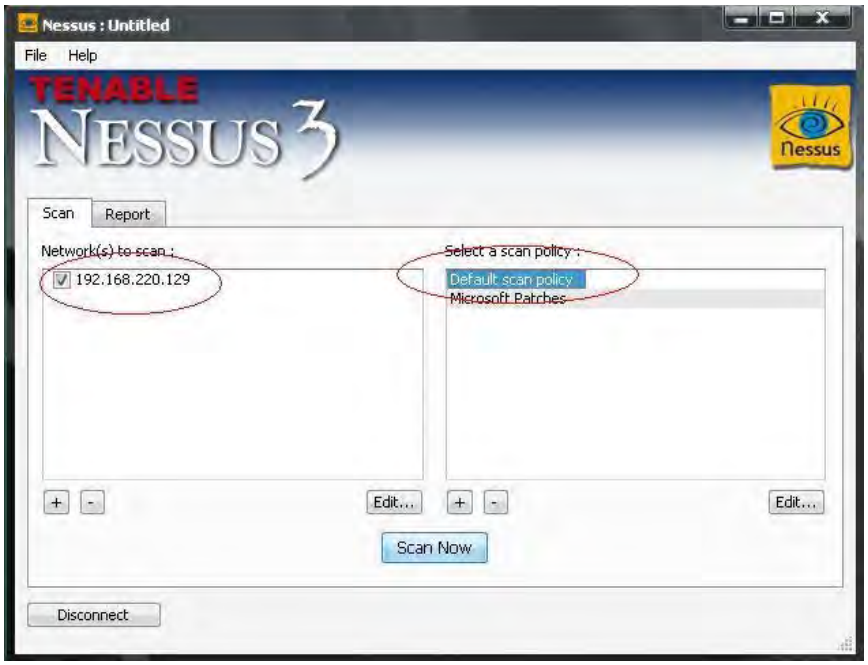

Figura 04 – Tela inicial do Nessus

"Nesta tela, adicionamos o host *192.168.220.129*, que será analisado pela ferramenta. Selecionamos a política de scan, definida por padrão, pela ferramenta, *Default policy*", para mostrar que a política padrão pode trazer informações valiosas.

Figura 05 – Tela Final do Relatório do Nessus

"Nesta tela, temos o resultado da análise de segurança do host, onde podemos

exportar para outros formatos, entre eles, o html”.

3.1.3 Acunetix

O Scanner de Vulnerabilidade Acunetix é uma ferramenta automatizada para a segurança da Web. Ela examina suas aplicações verificando se há Vulnerabilidades exploráveis com a técnica de exploit hacking. As varreduras automatizadas podem ser mais completas como SQL Injection e Cross Site Scripting (XSS).

Acunetix foi fundada com o propósito definido de combater a pirataria na web site. Foi desenvolvida uma ferramenta automatizada tendo como função principal ajudar as empresas a verificarem a segurança de suas aplicações web.

Em julho de 2005 a Acunetix Web Vulnerability Scanner foi liberada. Ela usa uma ferramenta que rastreia o site para vulnerabilidades de injeção SQL, cross site scripting e outros ataques na web feitos pelos hackers.

O time de desenvolvimento do Acunetix é composta pelos melhores desenvolvedores de segurança todos com larga experiência nesse tipo de empreendimento.

Para esse experimento, foram utilizados configurações padrões do Acunetix, sem qualquer alteração em suas configurações nos ambiente, mais detalhes veremos no capítulo 4.

3.2. Técnicas de Hardening

Como fator determinante para obter sucesso na implementação de um servidor de aplicações web seguro, devemos analisar os tópicos aqui relacionados e adaptar-los de acordo com as nossas necessidades.

Segundo Melo (2006), são destacadas as seguintes técnicas de hardening:

3.2.1 Segurança no sistema de arquivos

É aconselhável particionar o disco e colocar os principais diretórios em partições diferentes. Isso proporcionará uma maior segurança, pois cada partição tem sua tabela separada (man 5 fstab.) Verificar ANEXO I, sobre o item.

3.2.2 Utilização de Quota

Deve-se usar o recurso de quota, pois é o meio pelo qual se pode controlar a utilização dos sistemas de arquivos entre todos os usuários, *man 1 quota*.

3.2.3 Remoção de programas desnecessários

Após a instalação do sistema Linux, devemos nos preocupar se todos os programas que foram instalados são realmente necessários. Mesmo que tenha sido feita a instalação mais básica possível. Verificar os programas é sempre uma boa escolha, *man 8 rpm ; man 8 dpkg*. Verificar ANEXO I, sobre o item.

3.2.4 Permissões especiais de arquivos

A permissão “Suid bit” possibilita que um determinado binário que só possa ser executado, por exemplo, pelo usuário root seja executado por qualquer outro usuário comum do sistema. Muitos binários no sistema já vêm com a permissão do Suid bits, pois alguns binários que, somente o root pode executar precisam ser utilizados por um usuário. O administrador tem que observar essas coisas, *man 1 chmod*. Verificar ANEXO I, sobre o item.

3.2.5 Segurança no Terminal

Neste item, a preocupação é com a segurança local do sistema. São elas: como reiniciar o sistema com a junção das teclas CTRL+ALT+DEL, logar direto como root nas consoles virtuais, autenticação, limite de usuários, entre outros, *man 5 inittab*. Verificar ANEXO I, sobre o item.

3.2.6 Regras de utilização de serviços de rede e serviços ativos do sistema

As Redes facilitam a transferência e o compartilhamento de arquivos para todos os computadores da rede web. Todas essas conexões de computadores feitas ao mesmo tempo pode ser prático, entretanto, ao mesmo tempo podem trazem vulnerabilidades e brechas de segurança. Se não soubermos limitar o uso e restringir o acesso, usuários comuns podem ter uma liberdade indevida, *man 8 xinetd; man 5 hosts_access*. Verificar ANEXO I, sobre o item.

3.2.7 Firewall

Sistemas de firewall são importantes num projeto de segurança, todavia sozinhos não tem como garantir a segurança de uma rede de computadores. O firewall utilizado no Linux com kernel 2.4 e superior, será o iptables, capaz de manipular as “capacidades” do Netfilter, que utiliza tecnologia State Full, *man 8 iptables*. ANEXO I, sobre o item.

3.2.8 Tunning do Kernel

Customizaçãodo Kernel, para o administrador de sistemas Linux, ao pensar em implementar um firewall, tem que ter em mente que ele é fundamental em um projeto de rede. Pois ele é um elemento que, combinado com outros, irá melhorar a segurança proposta. Os parâmetros de kernel podem ser alterados através do sistema de arquivos “proc” ou mesmo da ferramenta sysctl, *man 5 proc ; man 8 sysctl*.

3.2.9 Firewall de aplicação Web

É parte de um novo conceito, que é a defesa na camada de aplicação. Estas são defesas nas aplicações dos clientes, não padronizadas, heterogêneas e distribuídas em vários sistemas operacionais e, que usa diversos servidores de aplicação e de bancos de dados, *man mod_security*.

3.2.10 Análise de vulnerabilidades

Um administrador de rede não pode ficar esperendo por novos problemas de segurança, um novo bug ou mesmo uma nova técnica e/ou ferramenta que prove um conceito de vulnerabilidade. Devido aos riscos eminentes que existe em toda web, o administrador deve se antecipar na busca por vulnerabilidades na rede e desse modo resolvê-las antes que os atacantes desculbram essas vulnerabilidades.

3.3 Relação entre as principais vulnerabilidades e técnicas de hardening

a) Prinicpais Vulnerabilidades
CSS – Cross Site Scripting (XSS)
FI – Falhas de Injeção
EMA – Execução maliciosa de Arquivos

RIDO – Referência Insegura Direta à Objetos
CSRF – Cross Site Request Forgery (CSRF)
VITE – Vazamento de Informações e Tratamento de Erros Inapropriado
AFGS – Autenticação falha e Gerenciamento de Sessão
ACI – Armazenamento Criptográfico Inseguro
CI – Comunicações inseguras
FRAU – Falha de Restrição de Acesso à URL
SC – Scan

b) Técnicas de Hardening
SSA - Segurança no Sistema de Arquivos
UQ - Utilização de Quotas
RPD - Remoção de Programas desnecessários
PEA - Permissões especiais de arquivos
ST - Segurança no Terminal
RUSRSAS - Regras de utilização de serviços de rede e serviços ativos do sistema
FW - Firewall
TK - Tunning do Kernel
FAW - Firewall de aplicação Web

	Principais problemas de segurança										
Técnicas de Hardening	CSS	FI	EMA	RIDO	CSRF	VITE	AFGS	ACI	CI	FRAU	SC
SSA			**x**								
UQ			**x**								
RPD			**x**			**x**					
PEA			**x**								
ST											
RUSRSAS						**x**			**X**		
FW			**x**								**x**
TK											**x**
FAW	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**X**	**x**	**x**

Tabela 01 – Relação entre principais problemas de segurança e Técnicas de *Hardening*

- A técnica de segurança nos sistemas de arquivos e a utilização de quotas podem evitar a execução maliciosa de arquivos. É possível limitar as criações de arquivos em número e tamanho, as permissões dos arquivos nas partições do Sistema Operacional instalado, entre outros recursos. Para maiores detalhes, ver ANEXO I.

- A remoção de programas desnecessários pode evitar: a execução maliciosa de arquivos, vazamento de informações e tratamento de erros inapropriado. Nesse caso os arquivos que não vão ser usados, podem trazer informações desnecessárias a respeito do servidor e possuir algum tipo de vulnerabilidade conhecida. Para maiores detalhes, ver ANEXO I.

- As permissões especiais de arquivos devem ser revisadas, pois podem permitir a execução maliciosa de arquivos. Entre os arquivos a serem revisados destacamos: Arquivos do Sistema Operacional, arquivos dos

serviços instalados e também aplicações desenvolvidas por terceiros. Para maiores detalhes, ver ANEXO I.

- As regras de utilizações de serviços de rede e serviços ativos do sistema devem ser analisadas e revisadas. Isso é importante para evitar comunicações inseguras e vazamento de Informações, como também o tratamento de erros inapropriado. Para maiores detalhes, ver ANEXO I.

- A utilização de um bom Firewall é crucial para evitar a prática de PortScans. Utilizabndo uma Ferramenta Firewall de qualidade podemos minimizar a execução maliciosa de códigos, desde que este possa analisar o conteúdo dos pacotes trafegados. Para maiores detalhes, ver ANEXO I.

- A prática do Tunning no Kernel do sistema permite alterar o comportamento padrão do sistema operacional. Essa prática apóia a implantação do firewall, minimizando o impacto realizado pelo Postcan. Para maiores detalhes, ver ANEXO I.

- O Firewall de aplicação Web é sem dúvida uma das melhores práticas de segurança para se implementar nos servidores. Principalmente se o intuito for roteger aplicações web. Ele praticamente minimiza o impacto de todas as vulnerabilidades descritas neste documento. Para maiores detalhes, ver ANEXO I.

Capitulo 4

4. Experimento dos conceitos levantados sobre uma aplicação insegura

Neste capítulo pretendemos descrever as técnicas utilizadas em dois cenários. No primeiro vamos disponibilizar o ambiente para testes (sem qualquer alteração na sua estrutura). No segundo a sua topologia será alterada, ficando a mesma, por trás de uma máquina que passou por técnicas de “hardening” e que filtrará as requisições web solicitadas.

4.1 Cenário 1

Neste cenário, tendo como base a Figura 6, o servidor de aplicação está exposto de forma direta na Internet. Trata-se de um ambiente comum e muito usado por administradores de rede. É uma maneira mais simples de disponibilizar seus servidores. Podemos observer que o IP 192.168.220.129 está com um serviço na escuta, na porta 8080.

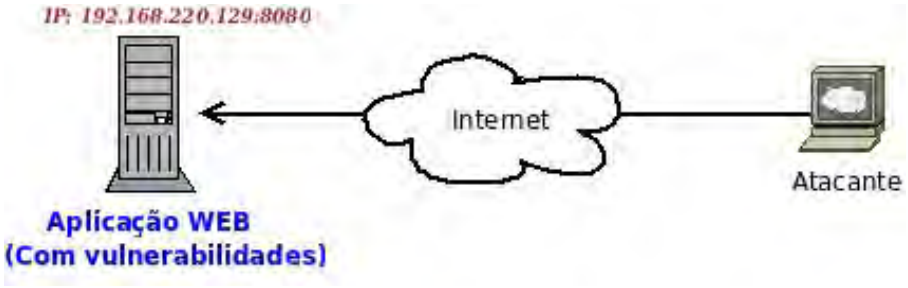

Figura 06 – Esquema do Cenário 1

Sistema Operacional do servidor de aplicação web inseguro: Linux Debian 4.0r0
Aplicação Web: Desenvolvida em Java, com banco de dados MySQL, com servidor web TomCAT.

a) Testes Preliminares

a.1) Análise com o NMAP

Para levantarmos informações a respeito do servidor, utilizaremos o NMAP, para realizar um *port scan* , e tentar levantar o maior numero de informações

possíveis tais como: serviços disponíveis com suas respectivas portas e versões.

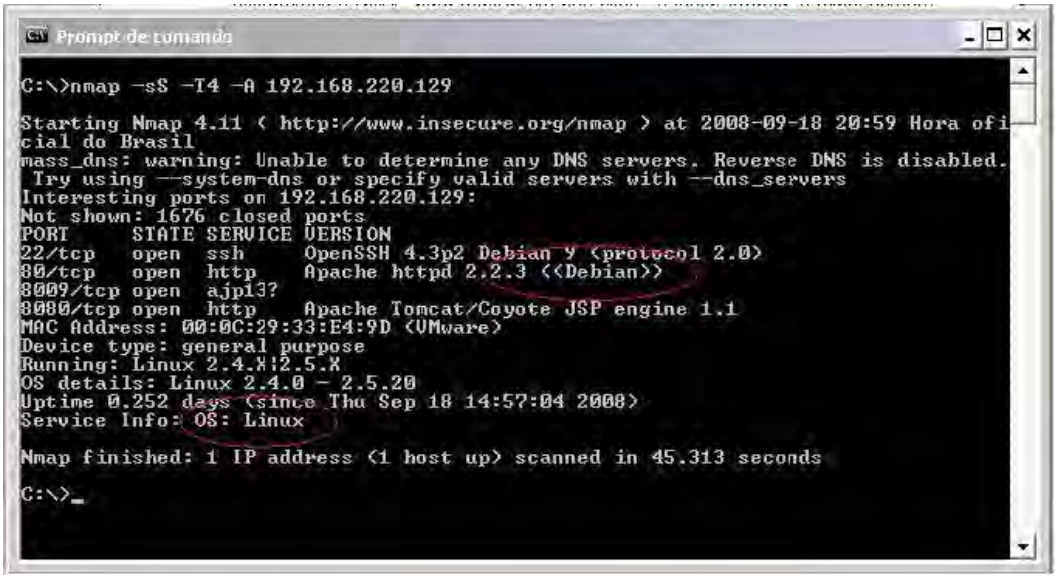

Figura 07 – Resultado do Nmap do laboratório 1

Conforme a figura 2, podemos observar que através do Nmap, conseguimos obter informações relevantes tais como: serviços remotos disponíveis, versão do web Server, e que o Sistema Operacional, que neste caso é um kernel Linux, possivelmente Debian, devido banner, disponibilizado na porta 80 (HTTP).

a.2) Análise com o Nessus

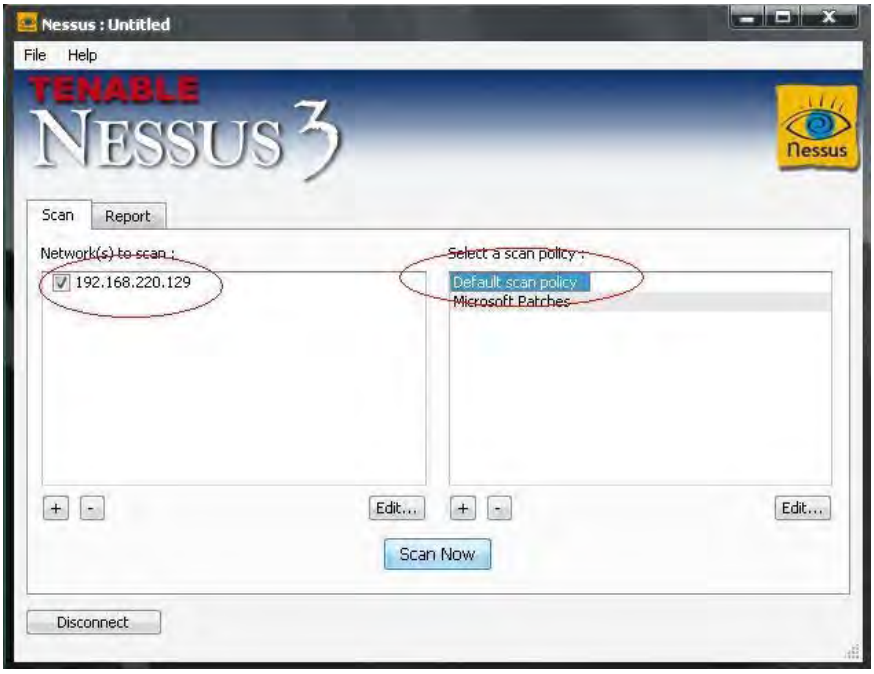

Figura 08 – Tela inicial do Nessus do Cenário 1

Conforme a Figura 6, podemos ver a configuração do IP do host, e a política de testes a ser aplicada na aplicação web.

Figura 09 – Resultado do Scan de vulnerabilidade do Cenário 1

Na figura 7, podemos ver o resultado obtido na análise de vulnerabilidades do host, no Cenário 1.

De acordo com o relatório gerado pelo Nessus, no ANEXO II, resultado exportado em HTML. Podemos observar uma séria de informações relevantes. Estas podem fornecer informações necessárias para que um possível atacante comprometa o sistema. Entre as informações levantadas, destacamos informações e versões dos serviços nos servidores e a vulnerabilidades no protocolo http, descritas na Tabela 1.

a.3) Análise como Acunetix

Iremos verificar a prática de análise de vunerabilidades específica dos serviços web, no servidor do cenário 1, utilizando a ferramenta Acunetix.

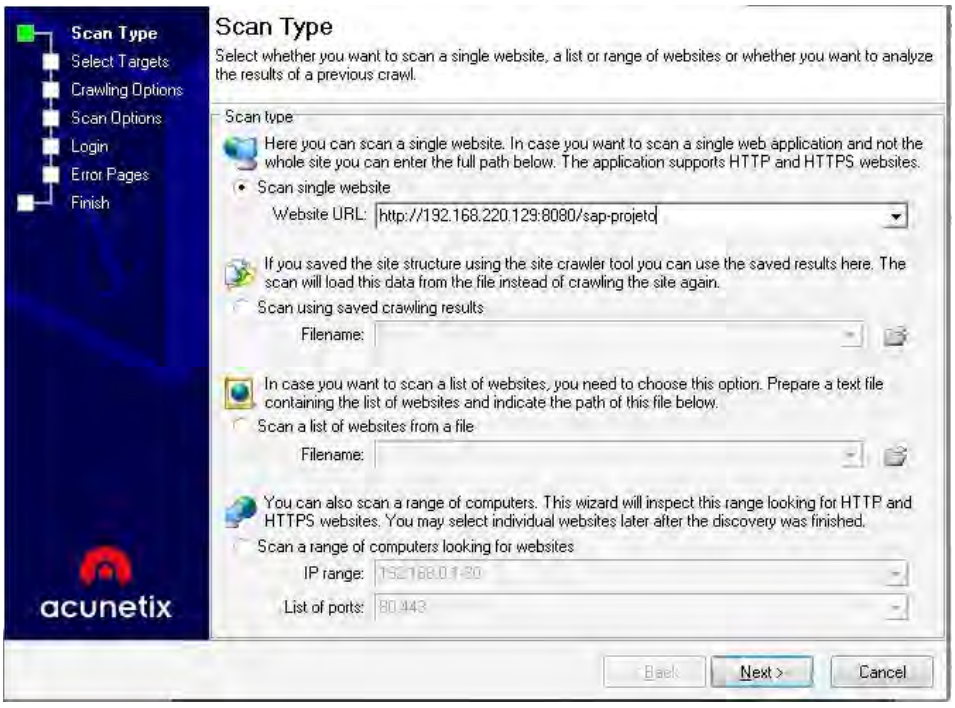

Figura 10 – Acunetix: Configurando URL da aplicação do cenário 1

Configuração da URL para realizar os testes de análise de vulnerabilidades no servidor e aplicações Web.

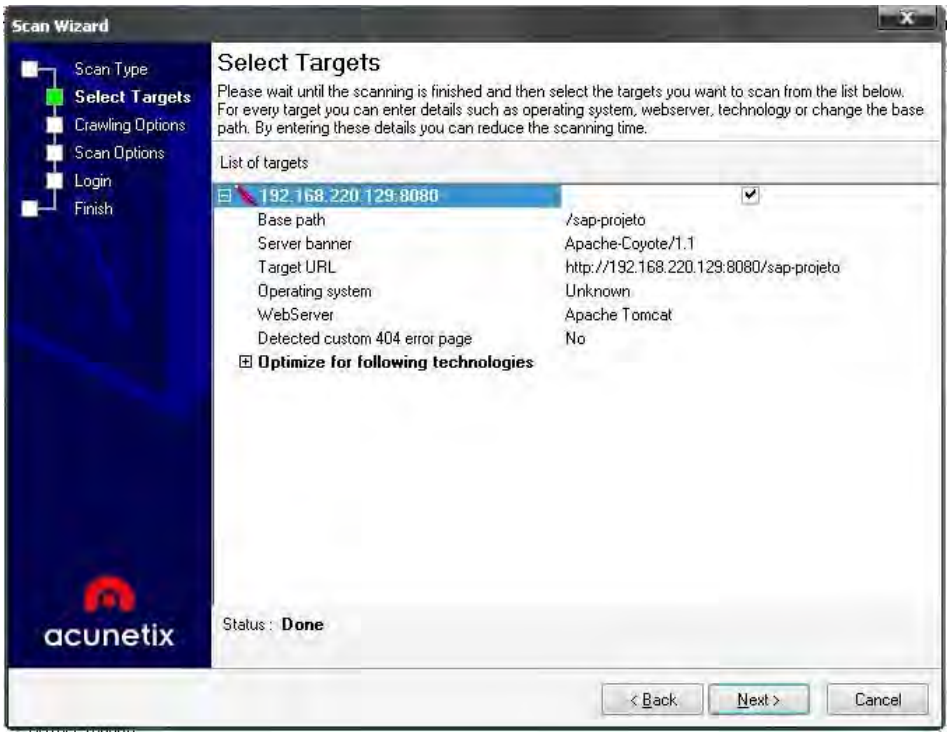

Figura 11 – Acunetix: Informações levantadas do cenário 1

Nesta tela, podemos destacar algumas tecnologias extrar para aplicar no servidor web, como por exemplo: PHP, ASP, ASP.NET, RUBY, Perl, Mod_ssl, FrontPage, OpenSSL etc.

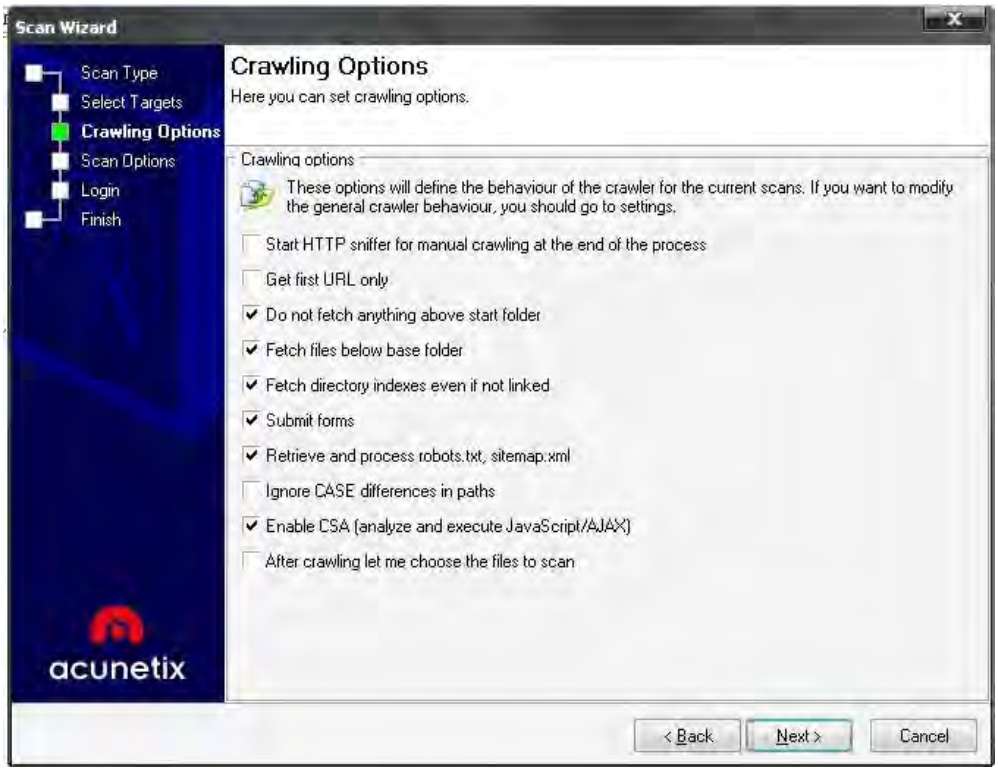

Figura 12 – Acunetix: opções para rastrear do cenário 1

Já nesta tela, podemos selecionar opções extras para realizar o restreamento no servidor web, como por exemplo: Ignorar caixa alta nos nosmes dos arquivos e caminhos de diretórios, analisar de forma recursiva dos diretórios, selecionar manualmente os arquivops a serem analisados entre outras coisas.

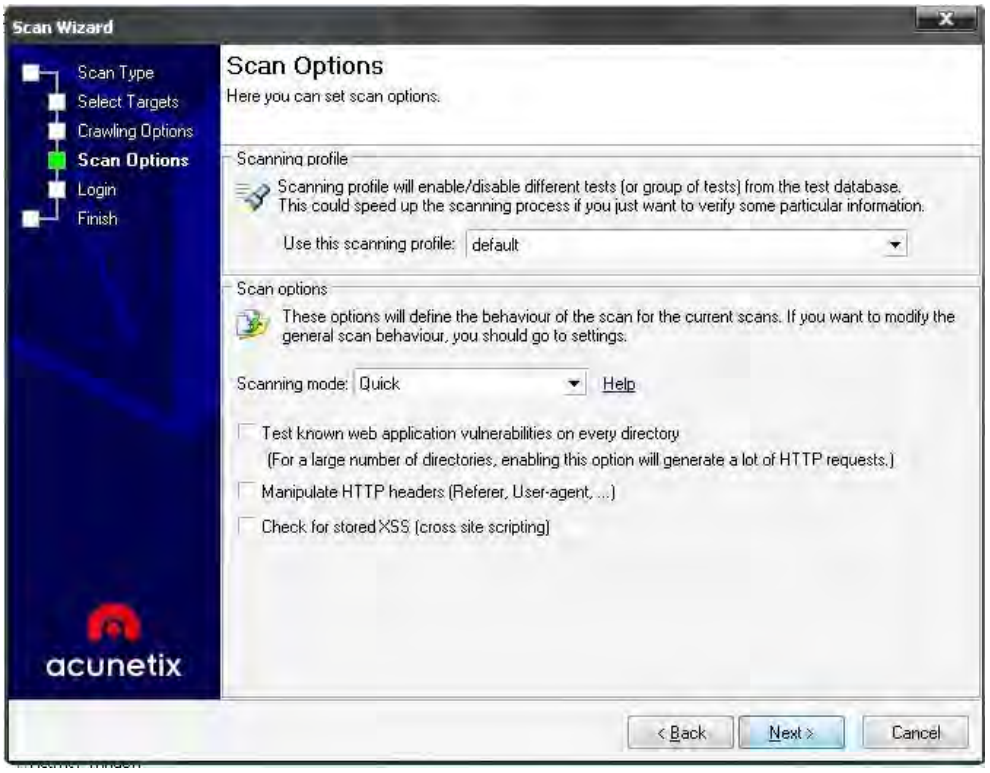

Figura 13 – Acunetix: opções para scan do cenário 1

Nesta parte da configuração, podemos selecionar o tipo de perfil de teste a ser analisado no servidor web, por exemplo, testes de SQL Injection, Bind injection, testes de CGIs entre outros.

Figura 14 – Acunetix: Informações de autenticações do cenário 1

Nesta tela podemos selecionar, se desejarmos, informações de credenciais de acesso, como login e senhas.

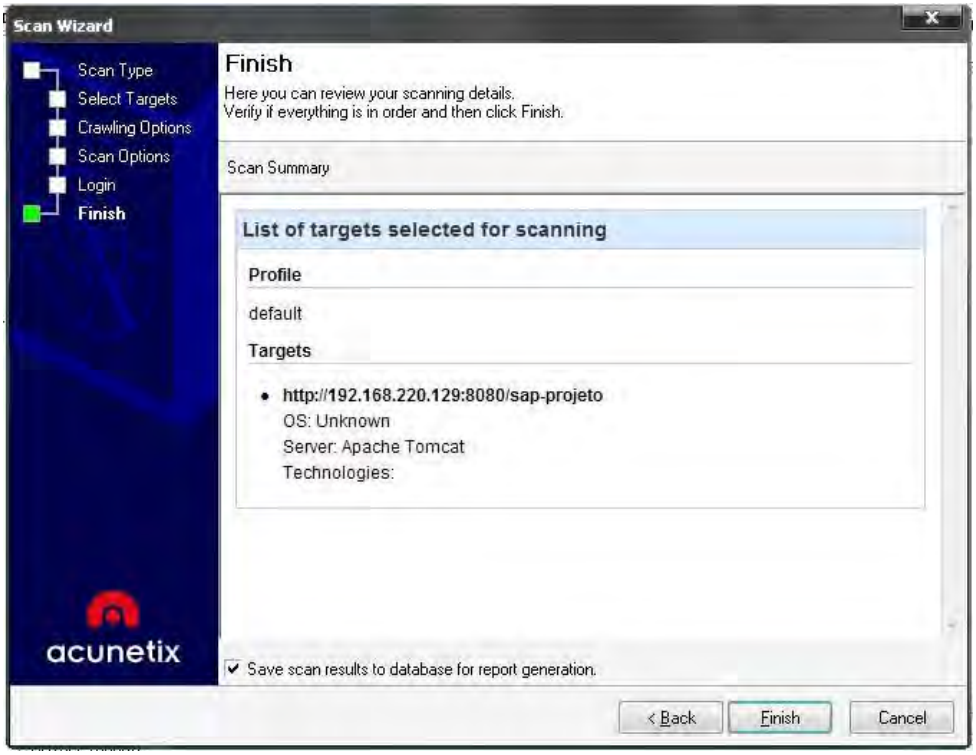

Figura 15 – Acunetix: Sumário para realizar scan do cenário 1

Esta tela, mostra o sumário a ser realizado pelo Acunetix.

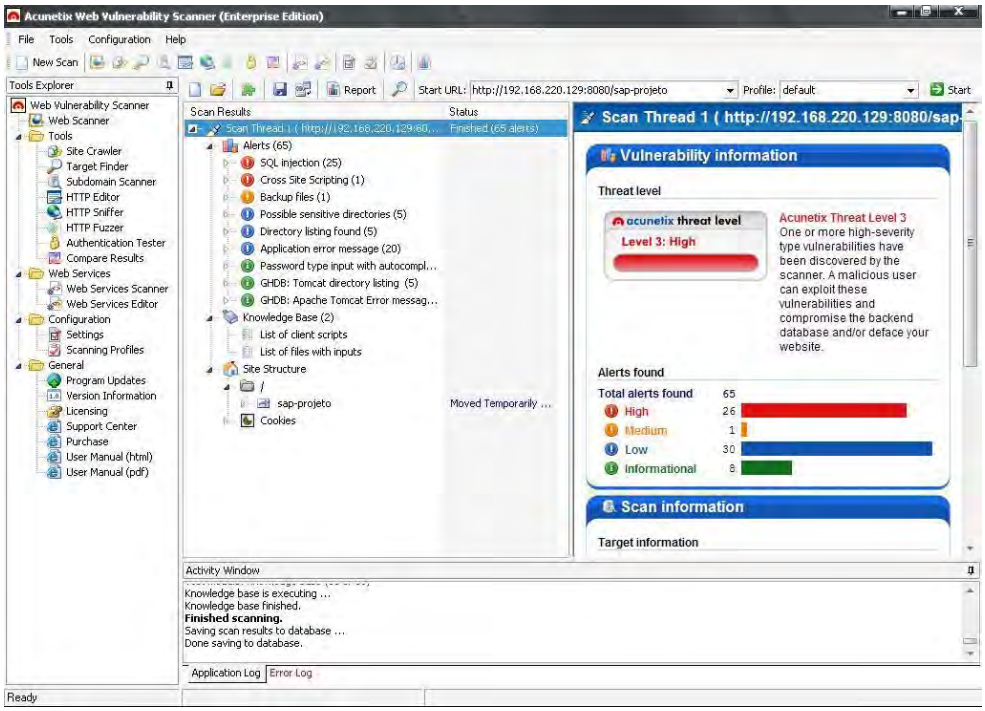

Figura 16 – Acunetix: Resultado do scan do cenário 1

De acordo com o relatório gerado pelo Acunetix, na figura 14, podemos observar que os níveis de informações a respeito da aplicação web são mais aprofundados, foram encontrados 65 alertas, entre eles 26 críticos e que merecem soluções imediatas. Para maiores detalhes, ver resultado em HTML, no ANEXO III.

b) Testes Aprofundados

Nesta parte dos testes, verificamos a possibilidade de falhas de validação de entrada, através da técnica de SQL Injection.

Nessa aplicação modelo está inserindo um código de SQL Injection comum, no campo referente ao Login do usuário.

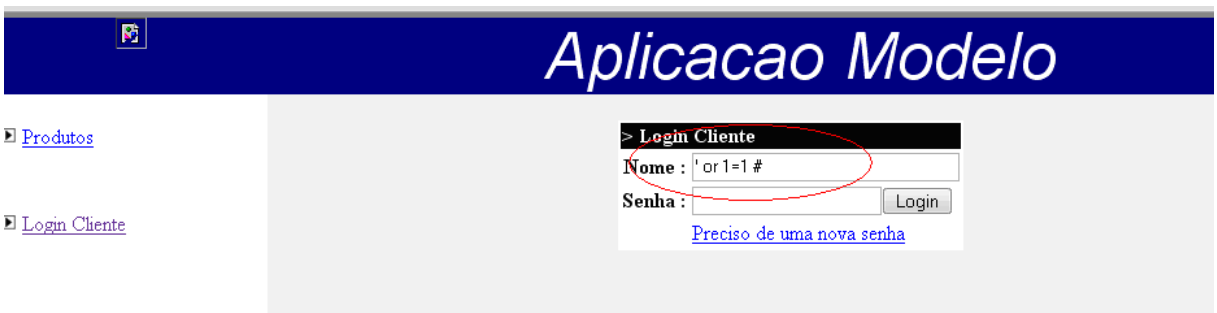

Figura 17 – Tela de SQL injection do Laboratório 1

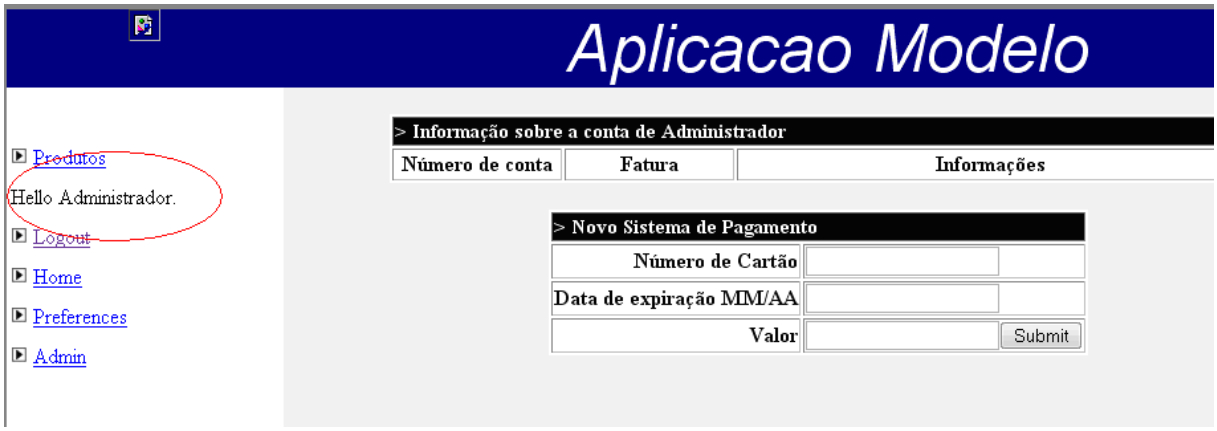

Figura 18 – Tela do sucesso da SQL Injection do laboratório 1

Podemos observar na Figura 4, que a aplicação não foi capaz de tratar a validação de entrada do usuário, permitindo que o atacante, conseguisse obter login do usuário, sem a necessidade de se autenticar com uma senha.

O resultado obtido neste laboratório conseguiu explorar através das técnicas II e VI do capítulo 2, a possibilidade de comprometimento do sistema, alteração de informação, destruição de dados e violação de privacidade.

Análise do ambiente: Antes do *hardening*

Vulnerabilidades	Nmap	Nessus	Acunetix
Cross Site Scripting (XSS)		**P**	**P**
Falhas de Injeção		**P**	**P**
Execução maliciosa de Arquivos		**P**	**P**
Referência Insegura Direta à Objetos		**P**	**P**
Cross Site Request Forgery (CSRF)		**P**	**P**
Vazamento de Informações e Tratamento de Erros Inapropriado		**P**	**P**
Autenticação falha e Gerenciamento de Sessão		**N**	**P**
Armazenamento Criptográfico Inseguro		**N**	**P**
Comunicações inseguras		**N**	**P**
Falha de Restrição de Acesso à URL		**P**	**P**
SCAN	**P**	**P**	**P**

Tabela 02 – Análise do ambiente: Antes do *hardening*

P – Positivo: ferramenta consegue detectar falha.

N – Negativo: ferramenta não consegue detectar falha.

4.2 Cenário 2

No experimento do Cenário 2, conforme apresentado na Figura 15, o servidor de aplicação, está disponível por trás de uma máquina, que passou por *hardening,* que irá realizar a função de tratar as requisições para o servidor de aplicação web inseguro, impedindo, dessa forma, que o atacante tenha acesso direto a mesma.

A máquina, denominada de “www.faw.net”, é um domínio fictício, que faz o papel de firewall de aplicação web, no qual recebem as requisições web pela porta padrão 80 e redireciona para a aplicação web na porta 8080.

Figura 19 - Esquema do Cenário 2

Sistema Operacional do servidor com Hardening aplicado: GNU/Linux CentOS 5.0

Técnicas de Hardening Aplicadas: Tunning do Kernel, Firewall, permissões de arquivos especiais, remoção de serviços desnecessários, firewall de aplicação web, segurança no sistema de arquivos.

a) Testes Preliminares

Para levantarmos informações a respeito do servidor, utilizamos o NMAP, para realizar um *port scan* , e tentar levantar o maior numero de informações possíveis tais como: serviços disponíveis com suas respectivas portas e versões.

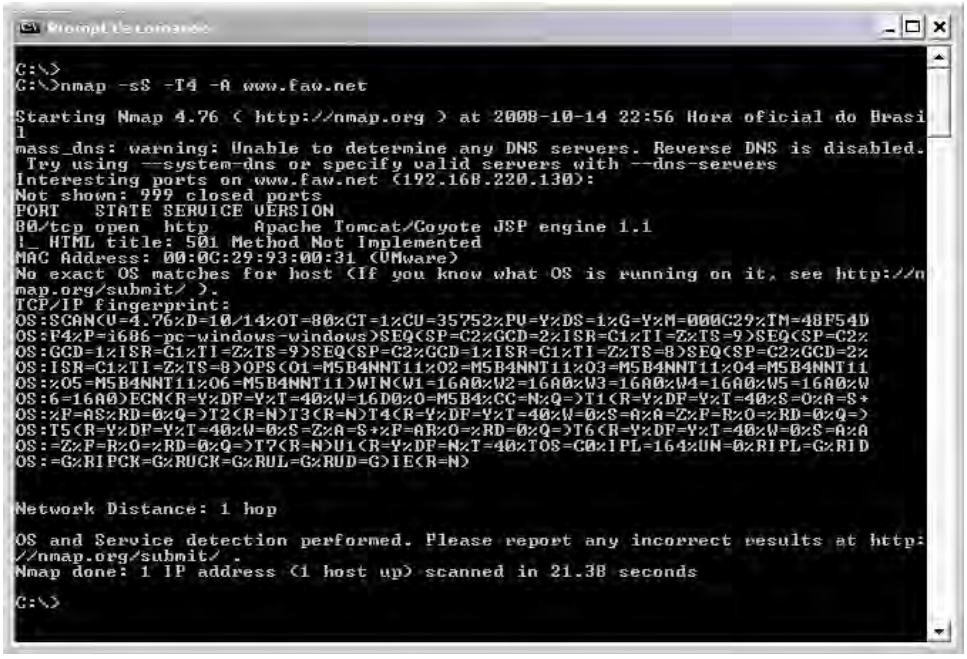

Figura 20 - Resultado do Nmap do Cenário 2

Podemos observar que o resultado obtido pelo Nmap, não conseguiu trazer informações precisas sobre o servidor, não foi capaz de mostrar com maior precisão qual o sistema operacional que está sendo executado, nem encontrou outra porta TCP ou UDP na escuta, além da porta 80, padrão da web.

a.2) Análise com o Nessus

Figura 21 – Nessus: configuração inicial do Cenário 2

Figura 22 – Nessus: Relatório do Cenário 2

De acordo com o relatório, gerado pelo Nessus, no ANEXO IV, podemos observar que os níveis de informações geradas, foram reduzidas drasticamente, não publicando qualquer tipo de informação desnecessária.

a.3) Análise como Acunetix

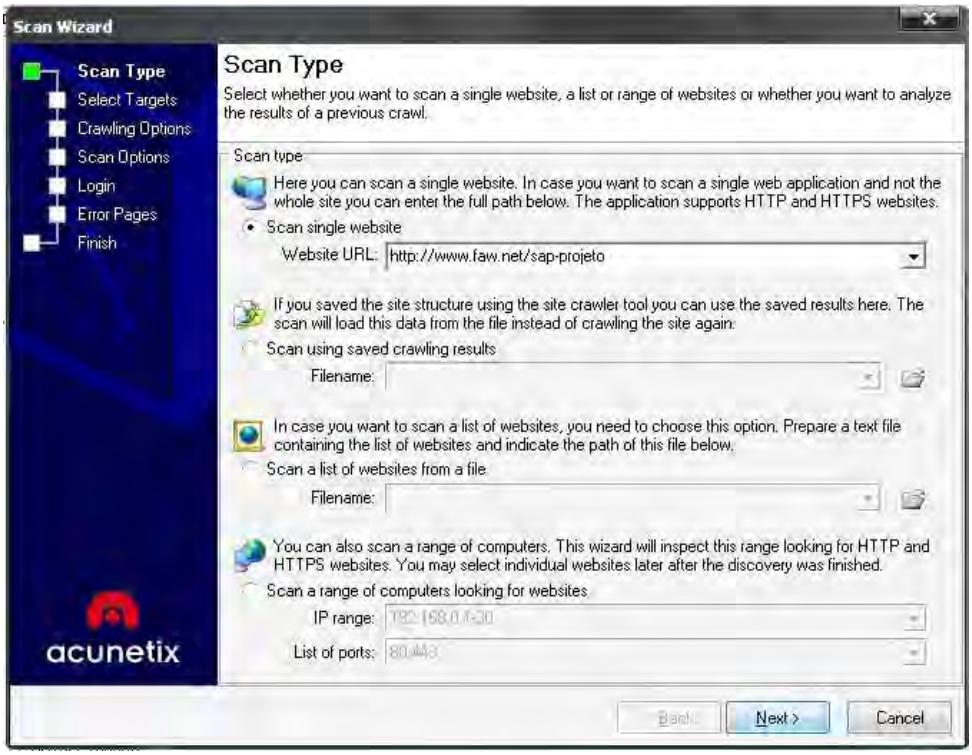

Figura 23 – Acunetix: Configurando a URL da aplicação do cenário 2

Configuração da URL para realizar os testes de análise de vulnerabilidades no servidor e aplicações Web.

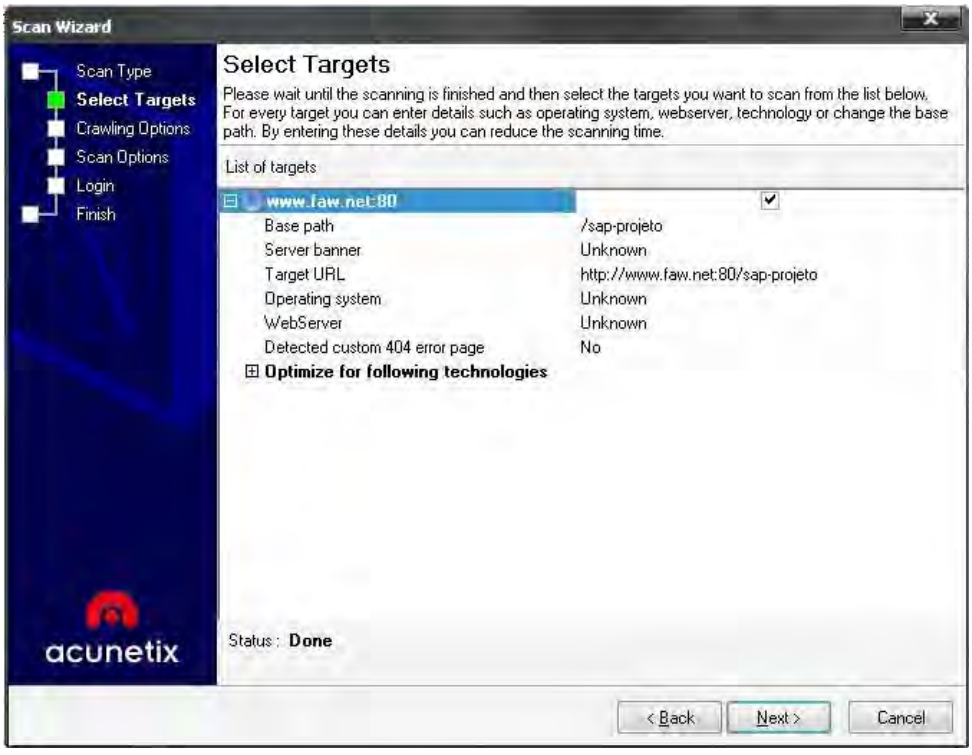

Figura 24 – Acunetix: Informações levantadas do cenário 2

Nesta tela, podemos selecionar algumas tecnologias extras para aplicar no servidor web, como por exemplo: PHP, ASP, ASP.NET, RUBY, Perl, Mod_ssl, FrontPage, OpenSSL etc.

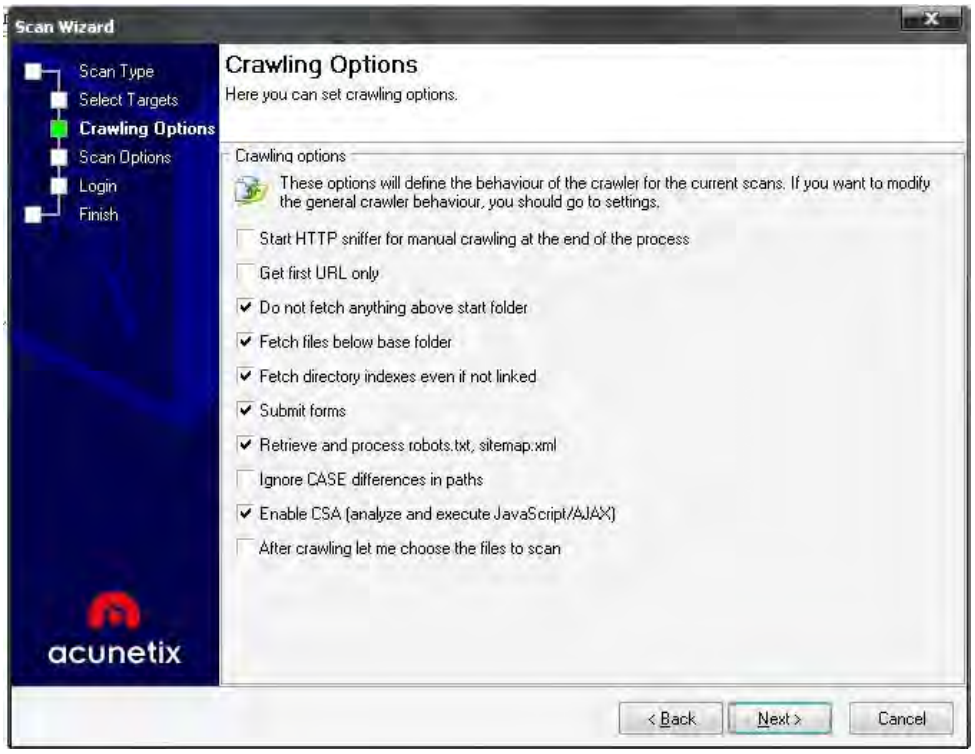

Figura 25 – Acunetix: opções para rastrear do cenário 2

Nesta tela, podemos selecionar opções extras para realizar o restreamento no servidor web, como por exemplo: Ignorar caixa alta nos nosmes dos arquivos e caminhos de diretórios, analisar de forma recursiva nos diretórios, selecionar manualmente os arquivops a serem analisados entre outras coisas.

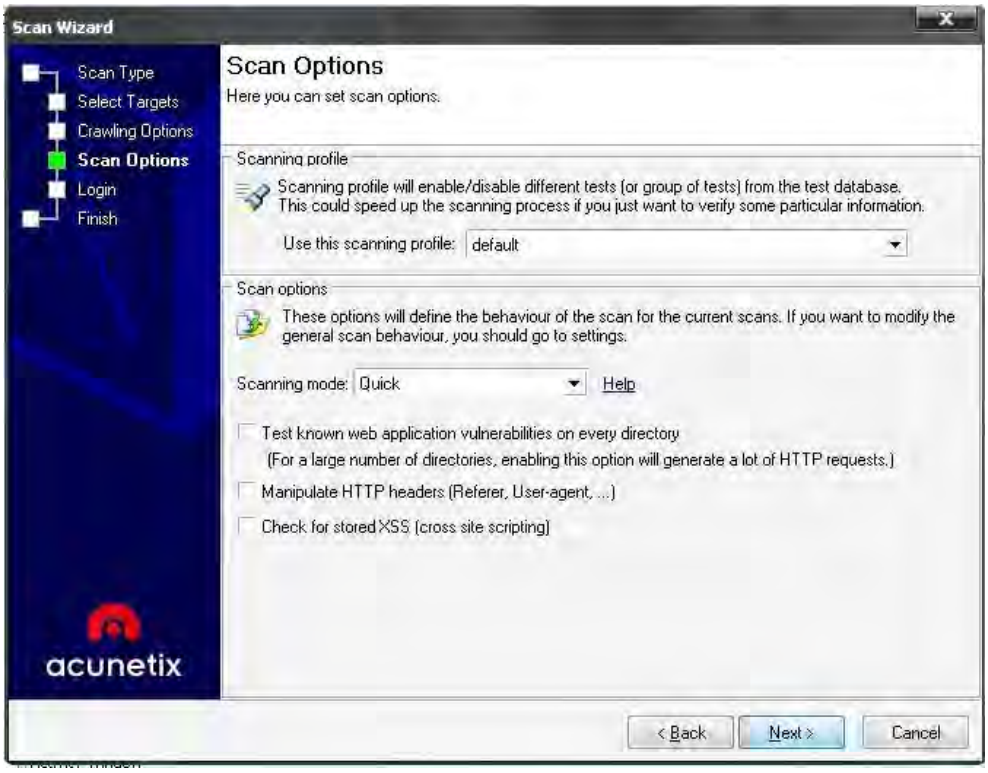

Figura 26 – Acunetix: opções para scan do cenário 2

Nesta parte da configuração, podemos selecionar o tipo de perfil de testesa ser analisado no servidor web, por exemplo, testes de SQL Injection, Bind injection, testes de CGIs.

Figura 27 – Acunetix: Informações de autenticações do cenário 2

Nesta tela podemos selecionar, se desejar, informações de credenciais de acesso, como login e senhas, para que os testes sejam mais aprofundados.

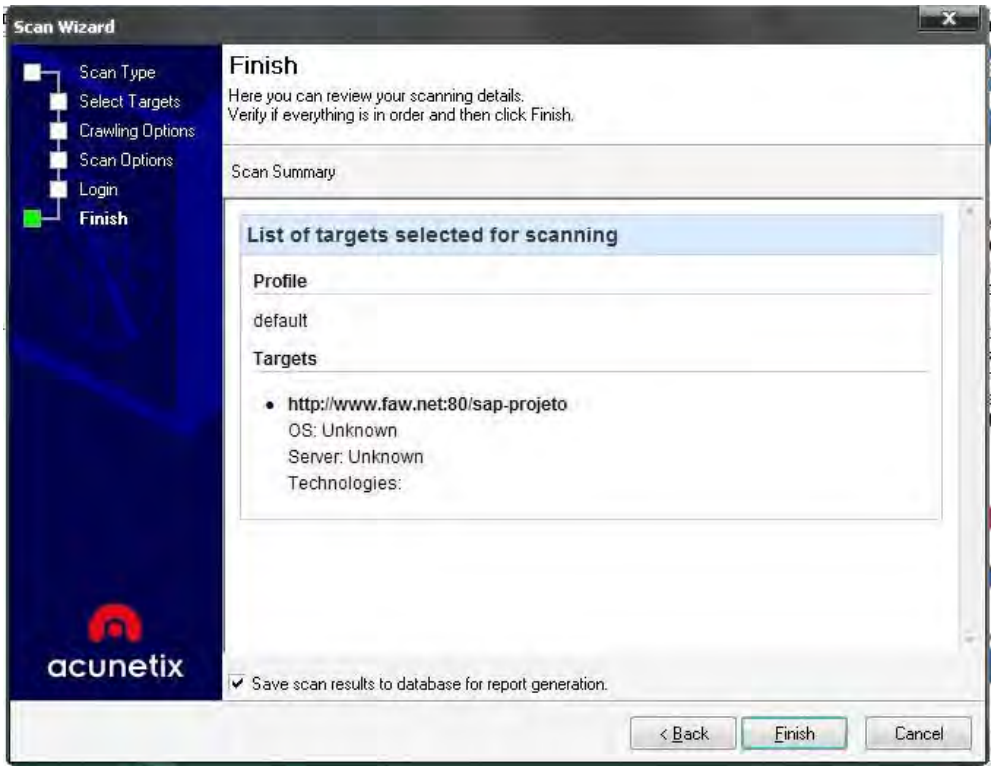

Figura 28 – Acunetix: Sumário para realizar scan do cenário 2

Nesta tela, mostra o sumário a ser realizado pelo Acunetix.

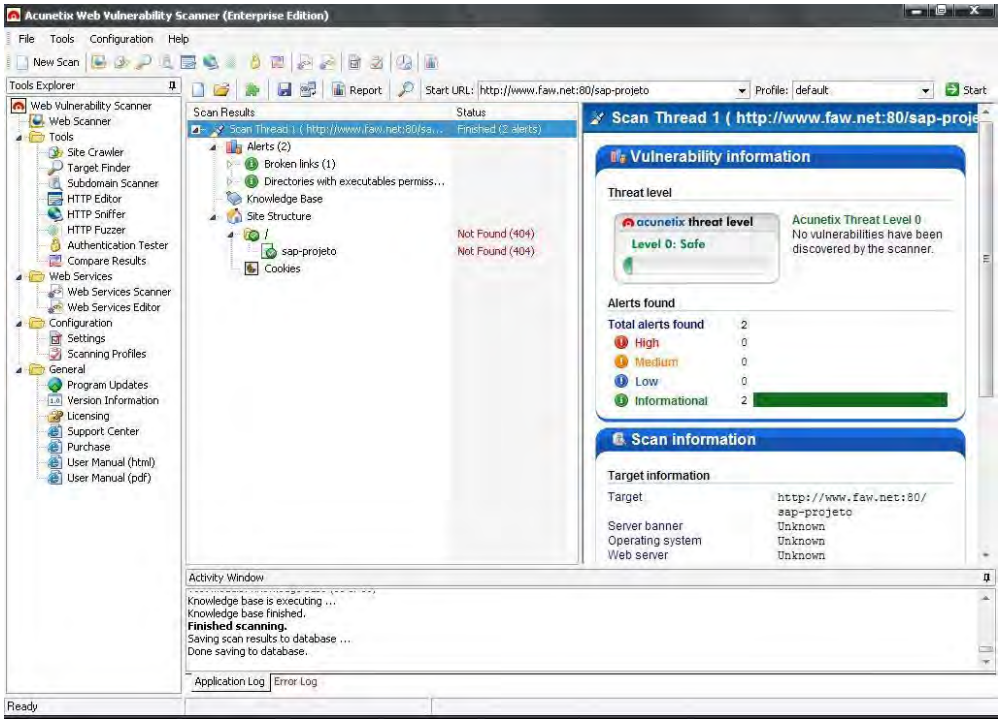

Figura 29 – Acunetix: Resultado do scan do cenário 2

De acordo com o relatório, gerado pelo Acunetix, no ANEXO V, podemos observar que o nível de informações praticamente desapareceu, inclusive as informações das falhas da aplicação web, pois teve todas as suas requisições tratadas pelo Firewall de aplicação Web.

b) Testes Aprofundados

Nesta parte dos testes, vamos verificar a possibilidade de falhas de validação de entrada, através da técnica de SQL Injection.

Nesta aplicação modelo, estamos inserindo um código de SQL Injection comum, no campo referente ao Login do usuário.

Figura 30 – Tela de SQL injection do Cenário 2

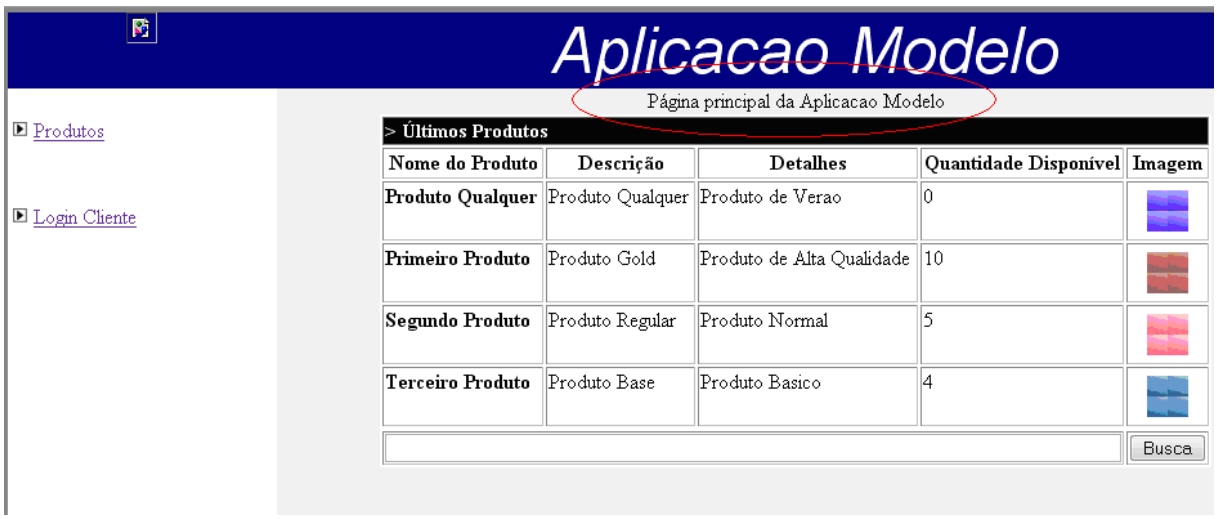

Figura 31 – Tela da falha da SQL Injection do Cenário 2

Diferente o resultado obtido da SQL Injection aplicada no cenário 1, neste experimento a técnica não foi bem sucedida, após receber a entrada da SQL Injection, o servidor responsável pelo redirecionamento, tratou a entrada da requisição e identificando que se tratava de uma técnica de ataque, carregou novamente a página principal do da aplicação, comprovando assim a eficácia do Hardening. As regras do tratamento das técnicas deste tipo de ataque, podem ser configuradas de várias maneiras. Ver ANEXO I, item j .

Análise do ambiente: Após as práticas do *hardening*

Vulnerabilidades	Nmap	Nessus	Acunetix
Cross Site Scripting (XSS)		**N**	**N**
Falhas de Injeção		**N**	**N**
Execução maliciosa de Arquivos		**N**	**N**
Referência Insegura Direta à Objetos		**N**	**N**
Cross Site Request Forgery (CSRF)		**N**	**N**
Vazamento de Informações e Tratamento de Erros Inapropriado		**N**	**N**
Autenticação falha e Gerenciamento de Sessão		**N**	**N**
Armazenamento Criptográfico Inseguro		**N**	**N**
Comunicações inseguras		**N**	**N**
Falha de Restrição de Acesso à URL		**N**	**N**
SCAN	**N**	**N**	**N**

Tabela 03 – Análise do ambiente: Após as práticas *hardening*

P – Positivo: ferramenta consegue detectar falha.

N – Negativo: ferramenta não consegue detectar falha.

Capitulo 5

5. Conclusão

A OWASP enfatiza que embora a terminologia utilizada comumente combine vulnerabilidades e ataques, e se organizações usam este documento para tornar suas aplicações seguras, consequientemente reduzem o risco para seus negócios. Observamos uma redução direta nos seguintes pontos:

a) **Ataques de phishing** - Podem explorar qualquer uma dessas vulnerabilidades, particularmente, XSS e problemas de autenticação e autorização.

b) **Violação de privacidade** – Ocorre devido à validação fraca, regras de negócio e verificações de autorização fracas.

c) **Roubo de identidade** – Acontece por meio de controles de criptografia fraca ou inexistente, inclusão de arquivo remoto e autenticação, regras de negócio e verificação de autorização.

d) **Comprometimento de sistema** – Ocorre por ataques de injeção e inclusão de arquivo remoto.

e) **Alteração de informação** – Ocorre por meio de transações não autorizadas e ataques.

f) **Destruição de dados** – Ocorre por meio de transações não autorizadas e ataques.

g) **Perda de reputação** – Ocorre devido à exploração de qualquer uma das vulnerabilidades acima.

Podemos observar a eficiência de usar práticas de *Hardening,* para elevar o nível de segurança dos servidores. As técnicas utilizadas neste trabalho, são práticas recomendadas pelos principais órgãos que seguem as normas da BS17799 e estudiosos especialistas em segurança da informação. As ferramentas para análise do ambiente, são de licença pública, baseadas em software livre, exceto a ferramenta Acunetix que possui licença proprietária.

A importância de ter um ambiente o mais seguro possível, não está relacionado apenas a vulnerabilidade do sistema. Para as empresas um ambiente seguro representa uma grande credibilidade dentro do mercado. Se uma empresa tiver seu sistema invadido or atacantes, sua imagem será ofuscada,tendo esta uma

enorme dificuldade no resgate de sua credibilidade.

Os administradores de segurança da informação não devem acomodar-se, e pensar que seu ambiente sempre estará seguro, a criatividade dos atacantes cresce de forma exponencial e requer que estejamos sempre atualizados com as novas formas de ataques.

Referências Bilbliográficas

APPU, A. **Administering and Securing the Apache Server**, 2002 Premier Press
ISBN: 1592000037.

ASSUNÇÃO, M. F. A. **Segredos do hacker ético.** 2ª Edição, 2008 Visual Books
ISBN: 978-85-7502-235-1.

GAFINKEL, S**. Web Security, Privacy & Commerce** 2a Edição O´Reilly
ISBN: 0-596-00045-6.

HORTON, M. ET AL. **Hack Notes: Segurança de Redes** , 2004 Campus
ISBN: 85-3521351-1.

MELO, Sandro ET AL. **BS7799: Da tática à prática em servidores Linux.** 1ª Edição, 2006 Alta Books
ISBN: 857608126-1.

MOBILY, T. **Hardening Apache**, 2004 Apress
ISBN: 1590593782

RISTIC, I **Apache Security: The Complete Guide to Securing**, 2005 O´Reilly
ISBN: 0-596-00724-8.

SCAMBRAY, J**. Hacking Exposed:Web Applications**. 2**a Edição** OSBORNE - MCGRAW-HIL, 2006
ISBN: 0072262990.

TANENBAUM, A. S. **Redes de Computadores**. 4. ed. , 2003 Campus.
ISBN: 8535211853.

TURNBULL, J. **Hardening Linux. Apress**, 2006 Apress
ISBN (pbk): 1-59059-444-4.

BREACH **ModSecurity Reference Manual**
Version 2.1.7 (April 2,2008)
Obtido no Site: < http://www.modsecurity.org/documentation/modsecurity-apache/2.5.6/modsecurity2-apache-reference.pdf >

BREACH **The Core Rule Set: Generic detection of Application layer attacks**
Obtido no Site:
<http://www.modsecurity.org/documentation/ModSecurity_Core_Rules.pdf >

BREACH **Best Practices: Use of Web Application Firewalls**
Obitido no site: < http://blog.modsecurity.org/2008/09/best-practices.html>

OWASP
Obtido no site: < http://www.owasp.org/index.php/OWASP_Spring_Of_Code_2007>

ACUNETIX
Obtido no site: < http://www.acunetix.com/news/security-audit-results.htm>

A Guide to Building Secure Web Applications
Obtido no site: < http://www.cgisecurity.com/owasp/html/ >

APRISCO
Obtido no site:
<http://www.clm.com.br/resourcecenter/watchguard/Firewall_de_Aplicacao-WP.pdf>

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br)
Obtido em: <http://www.cert.br >

Clube do Hacker
Obtido em: < http://www.clubedohacker.com.br/tutoriaisartigos-mainmenu-31/26-pilha-tcpip/218-scanners-ferramentas-de-ataque-ou-defesa >

ISECOM
OSSTMM - Open Source Security Testing Methodology Manual, 2001
Peter Herzog
Obtido no site: < http://www.isecom.org/osstmm/ >

Metasploit
Obtido no site: <http://www.metasploit.com/framework>

NMAP
Obtido no site: < HTTP://insegure.org>

SECURITYFOCUS
Obtido no site: < http://www.securityfocus.com/columnists/395 >

Tenable Network Security - NESSUS
Obtido no site: < http://www.nessus.org>

TERRA Tecnologia
Obtido no site: < http://tecnologia.terra.com.br/interna/0,,OI1410595-EI4805,00.html>

WEBSENSE
Obtido no site:
http://www.sosni.com.br/html/modules.php?name=News&file=article&sid=3705

WIRESHARK
Obtido em: < http://www.wireshark.org/ >

ANEXO I

Técnicas de Hardening no servidor GNU/Linux

a) Configuração dos Pontos de Montagens

- Padronização dos pontos de montagens no /etc/fstab

[dispositivo] /boot ext3 defaults,nosuid,nodev 0 2

No ponto de montagem “/boot”, não será possível criar dispositivos do sistema nem utilizar executáveis com o suid bit habilita.

[dispositivo] / ext3 defaults 0 1

[dispositivo] /home ext3 defaults,nosuid,nodev,async,noexec,usrquota,grpquota 0 2

No ponto de montagem “/home”, não será possível criar dispositivos do sistema,na será possível utilizar executáveis com o suid bit habilita, sem possibilidades de criar arquivos executáveis, sincronizar a escrita dos asquivos e habilitar suporte a cota de usuários e grupos do sistema.

[dispositivo] /tmp ext3 defaults,nosuid,nodev,noexec 0 2

No ponto de montagem “/tmp”, não será possível criar dispositivos do sistema nem utilizar executáveis com o suid bit habilita, sem possibilidades de criar arquivos executáveis.

[dispositivo] /usr ext3 defaults,nosuid 0 2

No ponto de montagem “/usr”, não será possível utilizar executáveis com o suid bit habilita.

[dispositivo] /var ext3 defaults,nosuid,noexec 0 2

No ponto de montagem “/var”, sem suporte a suid bit e executáveis.

[dispositivo] /var/log ext3 defaults,nosuid,noexec,noatime 0 2

No ponto de montagem “/var/log”, sem suporte a suid bit, executáveis, e atualizações do time stamp dos LOGs, permintindo assim melhor performance de I/O do disco rígido.

b) Remoção de Pacotes desnecessários

Neste ítem, foi retirado os pacotes “realmente” desnecessários, ou seja se não será utilizado, por exemplo: gcc, make, wget.

c) Customizar o OpenSSH server

Neste Ítem é importante pois foi customizado o acesso remoto, de forma mais segura.
Baixar a ultima versão do openssh-server em : http://www.openssh.com/ e compilar.

Segue o processo:

compilação do openssh-server :

tar -zxpvf openssh-XX.tgz

cd openssh-XX

- *Editar o arquivo "version.h" , e retirar as informações do banner ...*

./configure

make && make install

adduser --home /var/run/sshd --shell /usr/sbin/nologin --uid 103 --gid 65534 sshd

- *Colocar na inicialização do sistema a camado do OpenSSH.*

echo "/usr/local/sbin/sshd" >> /etc/rc.local

- *Customizar o arquivo de configuração do openssh "/usr/local/etc/sshd_config"*

Port 33456 # Alterando a porta do SSHD

PermitRootLogin no # Nao permitir login como root

UsePrivilegeSeparation yes # Usar separacao de privilegios

Protocol 2 # Usar a versao 2 do protocolo

AllowTcpForwarding no # Desabilitar o Forward de Portas (Importante !!!)

X11Forwarding no # Desabilitar exportacao do grafico

StrictModes yes # Checar as permissoes dos arquivos e donos ao mesmo tempo

#Subsystem # Desabilitar o sftp

IgnoreRhosts yes # Desabilitar autenticacoes baseadas em confianca entre os hosts

HostbasedAuthentication no # Desabilitar autenticacoes baseadas em confianca entre os hosts

d) Tuning no Kernel

(Alterar no /etc/sysctl.conf)

Esta opção deve ser 0 (Zero), caso esta máquina não funcione como Gateway, Firewall, Roteador ou coisa parecida, caso contrário colocar 1 (um) !!!

net.ipv4.ip_forward = 0
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.default.accept_source_route = 0
kernel.sysrq = 0
kernel.core_uses_pid = 1
net.ipv4.tcp_syncookies = 1
net.ipv4.icmp_echo_ignore_all = 1
net.ipv4.icmp_echo_ignore_broadcasts = 1

kernel.printk = 4 4 1 7
net.ipv4.icmp_ignore_bogus_error_responses = 1
net.ipv4.ip_default_ttl = 255

# valores recomendados para tratamento DOS e DDOS
net.ipv4.tcp_window_scaling = 0
net.ipv4.tcp_sack = 0
net.ipv4.tcp_fin_timeout = 30
net.ipv4.tcp_keepalive_time = 7200
net.ipv4.conf.all.accept_redirects = 0

- Ao final de tudo executar o bom e velho: # ***sysctl -p***

e) Remoção dos Bits Especiais

- Removendo os SUIDs e GIDs do sistema ...

- Mantendo o SU e passwd ...

- Lista dos arquivos atuais com os SUIDs e SGIDs do sistema, depois remove as BITs especiais e habilita para o SU e o PASSWD (Por motivos óbvios)

#find / -type f -perm -4000 -o -perm -2000 > /tmp/suids_gids.log

#chmod a-s `find / -type f -perm -4000 -o -perm -2000`

#chmod a+s /usr/bin/passwd

#chmod a+s /bin/su

- Remove os STICKs dos diretorios, Liberando apenas para /vat/tmp e /tmp

- Checar lista de arquivos com STICKs em /tmp/sticks.txt

#find / -path /proc -prune -o -perm -2 ! -type l > /tmp/sticks.txt

#chmod o-t `find / -path /proc -prune -o -perm -2 ! -type l`

#chmod o+t /tmp

#chmod o+t /var/tmp

f) Variáveis de Ambiente

Configuração de algumas variáveis de ambiente especiais, declara no arquivos (/etc/profile)

HISTSIZE=25

TMOUT=3600

export TMOUT

HISTSIZE

#source /etc/profile

g) Banner dos Logins

- Alteração no Banner de apresentação do Sistema, altere os arquivo:

/etc/issue

/etc/issue.net

/etc/motd

/etc/motd.tail (Nas distros baseadas em Debian)

h) Compilação do Kernel

Ré-compile seu Kernel, retire os recursos que você não usa, se possível aplique o patch de segurança disponível em http://grsecurity.net *certamente vai elevar o nível de segurança do seu sistema.*

i) Filtros de Pacotes

Entre as regras existentes, devemos bloquear portscan, é interessante colocar a seguinte linha nas regras do Iptables.

```
#!/bin/bash
IPTABLES='/sbin/iptables'
# Protege contra os "Ping of Death"
```

```
$IPTABLES -A FORWARD -p icmp --icmp-type echo-request -m limit --limit 1/s -j ACCEPT

# Protege contra os ataques do tipo "Syn-flood, DoS, etc"
$IPTABLES -A FORWARD -p tcp -m limit --limit 1/s -j ACCEPT

# Permitir repassamento (NAT,DNAT,SNAT) de pacotes etabilizados e os relatados ...
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

# Logar os pacotes mortos por inatividade ...
$IPTABLES -A FORWARD -m limit --limit 3/minute --limit-burst 3 -j LOG

# Protege contra port scanners avanÃ§os (Ex.: nmap)
$IPTABLES -A FORWARD -p tcp --tcp-flags SYN,ACK,FIN,RST RST -m limit --limit 1/s -j ACCEPT

# Protege contra pacotes que podem procurar e obter informaÃ§s daarede interna ...
$IPTABLES -A FORWARD --protocol tcp --tcp-flags ALL SYN,ACK -j DROP

# Protecoes contra ataques
$IPTABLES -A INPUT -m state --state INVALID -j DROP
```

j) Firewall de Aplicação Web - Instalar e configurar o ModSecurity

Esta é a ferramente que vai realizar o tratamento de validação de entrada entre outras coisas, na aplicação web.

Instalar o mod_security-2.1.4-1

No arquivo "/etc/httpd/modsecurity.d/modsecurity_crs_40_generic_attacks.conf" ajustar para:

SecDefaultAction "log,drop,redirect:http://[IP da aplicacao]/sap-projeto/public,phase:2,status:500,t:none"

Esta entrada, vai fazer com que qualquer tipo de ataque conhecido nas assinaturas do ModSecurity, serão: Armazenados em LOG, Negar a continuação do acesso e ré-direcionado para um local definido, no caso recomendado, o início da aplicação web.

No arquivo "/etc/httpd/modsecurity.d/modsecurity_crs_10_config.conf"

SecServerSignature "IIS/5.0 (Microsoft Widnows 2003 Server SP3)"

Esta entrada, faz com que informações a respeito do servidor que está hospedando a aplicação web, forneça uma falsa informação ao atacante.

ANEXO II

Relatório do Nessus: Antes do Hardening

List of hosts

192.168.220.129	High Severity problem(s) found

[^] Back

192.168.220.129

Scan time :

Start time :	Mon Oct 13 13:38:07 2008
End time :	Mon Oct 13 13:42:41 2008

Number of vulnerabilities :

Open ports :	4
Low :	19
Medium :	2
High :	1

Information about the remote host :

Operating system :	Linux Kernel 2.6 on Debian 4.0 (etch)
NetBIOS name :	(unknown)
DNS name :	(unknown)

[^] Back to 192.168.220.129

Port ssh (22/tcp)

Service Identification (2nd pass)

An SSH server seems to be running on this port

Nessus ID : 11153

SSH Server type and version

Synopsis :

An SSH server is listening on this port.

Description :

It is possible to obtain information about the remote SSH
server by sending an empty authentication request.

Risk factor :

None

Plugin output :

SSH version : SSH-2.0-OpenSSH_4.3p2 Debian-9
SSH supported authentication : publickey,password

Nessus ID : 10267

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Synopsis :

The remote SSH host keys are weak.

Description :

The remote SSH host key has been generated on a Debian
or Ubuntu system which contains a bug in the random number
generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all
sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote
key and use this to set up decipher the remote session or
set up a man in the middle attack.

Solution :

Consider all cryptographic material generated on the remote host
to be guessable. In particuliar, all SSH, SSL and OpenVPN key
material should be re-generated.

See also :

http://www.nessus.org/u?5d01bdab (Debian)
http://www.nessus.org/u?f14f4224 (Ubuntu)

Risk factor :

Critical / CVSS Base Score : 10.0
(AV:R/AC:L/Au:NR/C:C/A:C/I:C/B:C)
CVE : CVE-2008-0166

BID : 29179

Nessus ID : 32314

SSH protocol versions supported

Synopsis :

An SSH server is running on the remote host.

Description :

This plugin determines the versions of the SSH protocol supported by
the remote SSH daemon.

Risk factor :

None

Plugin output :

The remote SSH daemon supports the following versions of the
SSH protocol :

- 1.99
- 2.0

SSHv2 host key fingerprint : b5:c5:01:02:15:a1:ed:20:63:99:b3:86:22:79:18:2a

Nessus ID : 10881

[^] Back to 192.168.220.129

Port general/udp

Traceroute

For your information, here is the traceroute from 192.168.220.1 to 192.168.220.129 :
192.168.220.1
?
192.168.220.129

Nessus ID : 10287

[^] Back to 192.168.220.129

Port general/tcp

Ping the remote host

The remote host is up

Nessus ID : 10180

TCP timestamps

Synopsis :

The remote service implements TCP timestamps.

Description :

The remote host implements TCP timestamps, as defined by RFC1323.
A side effect of this feature is that the uptime of the remote
host can sometimes be computed.

See also :

http://www.ietf.org/rfc/rfc1323.txt

Risk factor :

None

Nessus ID : 25220

Linux Distribution Detection

Using the remote HTTP banner, it is possible to guess that the
Linux distribution installed on the remote host is :
- Debian 4.0 (etch)

Nessus ID : 18261

OS Identification

Remote operating system : Linux Kernel 2.6 on Debian 4.0 (etch)
Confidence Level : 95
Method : SSH

The remote host is running Linux Kernel 2.6 on Debian 4.0 (etch)

Nessus ID : 11936

Information about the scan

Information about this scan :

Nessus version : 3.2.1.1
Plugin feed version : 200810040934
Type of plugin feed : HomeFeed (Non-commercial use only)
Scanner IP : 192.168.220.1
Port scanner(s) : synscan
Port range : default

Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Max hosts : 20
Max checks : 5
Recv timeout : 5
Backports : Detected
Scan Start Date : 2008/10/13 13:38
Scan duration : 273 sec

Nessus ID : 19506

[^] Back to 192.168.220.129

Port http-alt (8080/tcp)

Service detection

A web server is running on this port.

Nessus ID : 22964

HTTP Server type and version

Synopsis :

A web server is running on the remote host.

Description :

This plugin attempts to determine the type and the version of
the remote web server.

Risk factor :

None

Plugin output :

The remote web server type is :

Coyote HTTP/1.1 Connector

Nessus ID : 10107

HyperText Transfer Protocol Information

Synopsis :

Some information about the remote HTTP configuration can be extracted.

Description :

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem

Risk factor :

None

Plugin output :

Protocol version : HTTP/1.1
SSL : no
Pipelining : yes
Keep-Alive : no
Options allowed : GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS
Headers :

Server: Apache-Coyote/1.1
Content-Type: text/html;charset=UTF-8
Content-Length: 1130
Date: Mon, 10 Mar 2008 12:03:50 GMT

Nessus ID : 24260

[^] Back to 192.168.220.129

Port http (80/tcp)

Service detection

A web server is running on this port.

Nessus ID : 22964

Directory Scanner

Synopsis :

It is possible to enumerate web directories.

Description :

This plugin attempts to determine the presence of various common dirs on the remote web server.

Risk factor :

None

Plugin output :

The following directories were discovered:
/cgi-bin, /icons

While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards

Other references : OWASP:OWASP-CM-006

Nessus ID : 11032

HTTP Server type and version

Synopsis :

A web server is running on the remote host.

Description :

This plugin attempts to determine the type and the version of the remote web server.

Risk factor :

None

Plugin output :

The remote web server type is :

Apache/2.2.3 (Debian)

Solution : You can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.

Nessus ID : 10107

HyperText Transfer Protocol Information

Synopsis :

Some information about the remote HTTP configuration can be extracted.

Description :

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem

Risk factor :

None

Plugin output :

Protocol version : HTTP/1.1
SSL : no
Pipelining : yes
Keep-Alive : yes
Options allowed : GET,HEAD,POST,OPTIONS,TRACE
Headers :

Date: Mon, 10 Mar 2008 12:03:51 GMT
Server: Apache/2.2.3 (Debian)
Location: http://192.168.220.129/apache2-default/
Content-Length: 303
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

Nessus ID : 24260

HTTP TRACE / TRACK Methods

Synopsis :

Debugging functions are enabled on the remote web server.

Description :

The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

In addition, it has been shown that servers supporting the TRACE method are subject to cross-site scripting attacks, dubbed XST for "Cross-Site Tracing", when used in conjunction with various weaknesses in browsers. An attacker may use this flaw to trick your legitimate

web users to give him their credentials.

See also :

http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf
http://www.apacheweek.com/issues/03-01-24
http://www.kb.cert.org/vuls/id/867593

Solution :

Disable these methods.

Risk factor :

Medium / CVSS Base Score : 5.0
(CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)
Solution :

Add the following lines for each virtual host in your configuration file :

RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2
support disabling the TRACE method natively via the 'TraceEnable'
directive.

Plugin output :

The server response from a TRACE request is :

TRACE /Nessus14015.html HTTP/1.1
Connection: Close
Host: 192.168.220.129
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

CVE : CVE-2004-2320
BID : 9506, 9561, 11604
Other references : OSVDB:877, OSVDB:3726

Nessus ID : 11213

Apache < 2.2.9 Multiple Vulnerabilities (DoS, XSS)

Synopsis :

The remote web server may be affected by several issues.

Description :

According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.9. Such versions may be affected by several issues, including :

- Improper handling of excessive forwarded interim responses may cause denial-of-service conditions in mod_proxy_http (CVE-2008-2364).

- A cross-site request forgery vulnerability in the balancer-manager interface of mod_proxy_balancer (CVE-2007-6420).

Note that the remote web server may not actually be affected by these vulnerabilities. Nessus did not try to determine whether the affected modules are in use or to check for the issues themselves.

See also :

http://www.apache.org/dist/httpd/CHANGES_2.2.9
http://httpd.apache.org/security/vulnerabilities_22.html

Solution :

Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.9 or later.

Risk factor :

Medium / CVSS Base Score : 5.0
(CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

Plugin output :

According to its banner, Apache version 2.2.3 is installed on the remote host.

CVE : CVE-2007-6420, CVE-2008-2364
BID : 27236, 29653
Other references : OSVDB:42937, Secunia:30621

Nessus ID : 33477

Apache < 2.2.8 Multiple Vulnerabilities (XSS, DoS)

Synopsis :

The remote web server may be affected by several issues.

Description :

According to its banner, the version of Apache 2.2 installed on the
remote host is older than 2.2.8. Such versions may be affected by
several issues, including :

- A cross-site scripting issue involving mod_imagemap
(CVE-2007-5000).

- A cross-site scripting issue involving 413 error pages
via a malformed HTTP method (PR 44014 / CVE-2007-6203).

- A cross-site scripting issue in mod_status involving
the refresh parameter (CVE-2007-6388).

- A cross-site scripting issue in mod_proxy_balancer
involving the worker route and worker redirect
string of the balancer manager (CVE-2007-6421).

- A denial of service issue in the balancer_handler
function in mod_proxy_balancer can be triggered by
an authenticated user when a threaded Multi-
Processing Module is used (CVE-2007-6422).

- A cross-site scripting issue using UTF-7 encoding
in mod_proxy_ftp exists because it does not
define a charset (CVE-2008-0005).

Note that the remote web server may not actually be affected by these
vulnerabilities. Nessus did not try to determine whether the affected
modules are in use or to check for the issues themselves.

See also :

http://www.apache.org/dist/httpd/CHANGES_2.2.8
http://httpd.apache.org/security/vulnerabilities_22.html

Solution :

Either ensure that the affected modules are not in use or upgrade to
Apache version 2.2.8 or later.

Risk factor :

Low / CVSS Base Score : 2.6
(CVSS2#AV:N/AC:H/Au:N/C:N/I:N/A:P)

Plugin output :

According to its banner, Apache version 2.2.3 is installed on the
remote host.

CVE : CVE-2007-5000, CVE-2007-6203, CVE-2007-6388, CVE-2007-6421, CVE-2007-6422, CVE-2008-0005
BID : 26663, 26838, 27234, 27236, 27237
Other references : OSVDB:39003, OSVDB:39134, OSVDB:40262, OSVDB:40263, OSVDB:40264,
OSVDB:42214, OSVDB:42937

Nessus ID : 31118

[^] Back to 192.168.220.129

Port general/icmp

ICMP Timestamp Request

Synopsis :

It is possible to determine the exact time set on the remote host.

Description :

The remote host answers to an ICMP timestamp request. This allows an
attacker to know the date which is set on your machine.

This may help him to defeat all your time based authentication
protocols.

Solution :

Filter out the ICMP timestamp requests (13), and the outgoing ICMP
timestamp replies (14).

Risk factor :

None

Plugin output :

The difference between the local and remote clocks is 16578 seconds

CVE : CVE-1999-0524, CVE-1999-0524

Nessus ID : 10114

[^] Back to 192.168.220.129

Port ajp13 (8009/tcp)

AJP Connector Detection

Synopsis :

There is an AJP connector listening on the remote host.

Description :

The remote host is running an AJP (Apache JServ Protocol) connector, a service by which a standalone web server such as Apache communicates over TCP with a Java servlet container such as Tomcat.

See also :

http://tomcat.apache.org/connectors-doc/
http://tomcat.apache.org/connectors-doc/common/ajpv13a.html

Risk factor :

None

Plugin output :

The connector listing on this port supports the ajp13 protocol.

Nessus ID : 21186

ANEXO III

Relatório do Acunetix – Antes do Hardening

Scan of http://192.168.220.129:8080/sap-projeto

Scan details

Scan information	
Starttime	13/10/2008 12:55:37
Finish time	13/10/2008 12:56:53
Scan time	1 minutes, 16 seconds
Profile	default

Server information	
Responsive	True
Server banner	Apache-Coyote/1.1
Server OS	Unknown
Server technologies	

Threat level

Acunetix Threat Level 3
One or more high-severity type vulnerabilities have been discovered by
scanner. A malicious user can exploit these vulnerabilities and comprom
the backend database and/or deface your website.

Alerts distribution

Total alerts found	**65**
High	26
Medium	1
Low	30
Informational	8

Knowledge base

List of client scripts

- **/sap-projeto/common/script/custom.js**

List of files with inputs

- **/sap-projeto/public** - **1** inputs
- **/sap-projeto/public/index.jsp** - **1** inputs
- **/sap-projeto/public/Login.jsp** - **2** inputs
- **/sap-projeto/public/ForgotLogin.jsp** - **1** inputs
- **/sap-projeto/admin/activateAccount.jsp** - **2** inputs

Alerts summary

Cross Site Scripting

Affects	Vari
/sap-projeto/public/ForgotLogin.jsp	1

SQL injection

Affects	Vari
/sap-projeto/admin/activateAccount.jsp	16
/sap-projeto/public/ForgotLogin.jsp	3
/sap-projeto/public/Login.jsp	6

Backup files

Affects	Vari
/sap-projeto/public/Login.jsp.old	1

Application error message

Affects	Vari
/sap-projeto/admin/activateAccount.jsp	20

Directory listing found

Affects	Vari
/sap-projeto/admin	1
/sap-projeto/common	1
/sap-projeto/common/art	1
/sap-projeto/common/script	1
/sap-projeto/common/theme	1

Possible sensitive directories

Affects	Vari
/sap-projeto/admin	1
/sap-projeto/common	1
/sap-projeto/public	2
/sap-projeto/secure	1

GHDB: Apache Tomcat Error message

Affects	Vari
/sap-projeto/admin/activateAccount.jsp	1

GHDB: Tomcat directory listing

Affects	Vari
/sap-projeto/admin	1
/sap-projeto/common	1
/sap-projeto/common/art	1
/sap-projeto/common/script	1
/sap-projeto/common/theme	1

Password type input with autocomplete enabled

Affects	Vari
/sap-projeto/public/Login.jsp	1
/sap-projeto/public/Login.jsp.old	1

Alert details

Cross Site Scripting

Severity	**High**
Type	Validation
Reported by module	Parameter manipulation

Description

This script is possibly vulnerable to Cross Site Scripting (XSS) attacks.

Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. Because a browser cannot know if the script should be trusted or not, it will execute the script in the user context allowing the attacker to access any cookies or session tokens retained by the browser.

Impact

Malicious users may inject JavaScript, VBScript, ActiveX, HTML or Flash into a vulnerable application to fool a user in order to gather data from them. An attacker can steal the session cookie and take over the account, impersonating the user. It is also possible to modify the content of the page presented to the user.

Recommendation

Your script should filter metacharacters from user input.

Affected items

/sap-projeto/public/ForgotLogin.jsp

Details

The GET variable **email** has been set to **"+onmouseover=alert(404835389583)+** .

Request

```
GET /sap-projeto/public/ForgotLogin.jsp?email="+onmouseover=alert(404835389583)+ HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 2214
Date: Mon, 10 Mar 2008 11:46:32 GMT
Connection: close
```

SQL injection

Severity	**High**
Type	Validation
Reported by module	Parameter manipulation

Description

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter backend SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable

Impact

An attacker may execute arbitrary SQL statements on the vulnerable system. This may compromise the integrity of your database and/or expose sensitive information.

Depending on the back-end database in use, SQL injection vulnerabilities lead to varying levels of data/system access for the attacker. It may be possible to not only manipulate existing queries, but to UNION in arbitrary data, use subselects, or append additional queries. In some cases, it may be possible to read in or write out to files, or to execute shell commands on the underlying operating system.

Certain SQL Servers such as Microsoft SQL Server contain stored and extended procedures (database server functions). If an attacker can obtain access to these procedures it may be possible to compromise the entire machine.

Recommendation

Your script should filter metacharacters from user input.
Check detailed information for more information about fixing this vulnerability.

Affected items

/sap-projeto/admin/activateAccount.jsp

Details

The GET variable **accountId** has been set to **acunetix'"** .

Request

```
GET /sap-projeto/admin/activateAccount.jsp?updateActivation=0&accountId=acunetix'"
HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2750
Date: Mon, 10 Mar 2008 11:46:47 GMT
Connection: close
```

/sap-projeto/admin/activateAccount.jsp

Details

The GET variable **accountId** has been set to **%00'** .

Request

```
GET /sap-projeto/admin/activateAccount.jsp?updateActivation=0&accountId=%00' HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
```


Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2737
Date: Mon, 10 Mar 2008 11:46:47 GMT
Connection: close
```

/sap-projeto/admin/activateAccount.jsp

Details

The GET variable **accountId** has been set to **'** .

Request

```
GET /sap-projeto/admin/activateAccount.jsp?updateActivation=0&accountId=' HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2736
Date: Mon, 10 Mar 2008 11:46:47 GMT
Connection: close
```

/sap-projeto/admin/activateAccount.jsp

Details

The GET variable **accountId** has been set to **%2527** .

Request

```
GET /sap-projeto/admin/activateAccount.jsp?updateActivation=0&accountId=%2527 HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2738
Date: Mon, 10 Mar 2008 11:46:47 GMT
Connection: close
```

/sap-projeto/admin/activateAccount.jsp

Details

The GET variable **accountId** has been set to **0.01** .

Request

```
GET /sap-projeto/admin/activateAccount.jsp?updateActivation=0&accountId=0.01 HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
```



```
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2739
Date: Mon, 10 Mar 2008 11:46:47 GMT
Connection: close
```

/sap-projeto/admin/activateAccount.jsp

Details

The GET variable **accountId** has been set to **JyI%3D** .

Request

```
GET /sap-projeto/admin/activateAccount.jsp?updateActivation=0&accountId=JyI%3D HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2739
Date: Mon, 10 Mar 2008 11:46:47 GMT
Connection: close
```

/sap-projeto/admin/activateAccount.jsp

Details

The GET variable **accountId** has been set to **\'** .

Request

```
GET /sap-projeto/admin/activateAccount.jsp?updateActivation=0&accountId=\' HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2737
Date: Mon, 10 Mar 2008 11:46:47 GMT
Connection: close
```


/sap-projeto/admin/activateAccount.jsp

Details

The GET variable **accountId** has been set to **\"** .

Request

```
GET /sap-projeto/admin/activateAccount.jsp?updateActivation=0&accountId=\" HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2742
Date: Mon, 10 Mar 2008 11:46:47 GMT
Connection: close
```

/sap-projeto/admin/activateAccount.jsp

Details

The GET variable **updateActivation** has been set to **%00'** .

Request

```
GET /sap-projeto/admin/activateAccount.jsp?updateActivation=%00'&accountId=111-222-
1933email@address.tst HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2764
Date: Mon, 10 Mar 2008 11:46:47 GMT
Connection: close
```

/sap-projeto/admin/activateAccount.jsp

Details

The GET variable **updateActivation** has been set to **acunetix'"** .

Request

```
GET /sap-projeto/admin/activateAccount.jsp?updateActivation=acunetix'"&accountId=111-222-
1933email@address.tst HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
```



```
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2764
Date: Mon, 10 Mar 2008 11:46:47 GMT
Connection: close
```

/sap-projeto/admin/activateAccount.jsp

Details

The GET variable **updateActivation** has been set to **'** .

Request

```
GET /sap-projeto/admin/activateAccount.jsp?updateActivation='&accountId=111-222-
1933email@address.tst HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2764
Date: Mon, 10 Mar 2008 11:46:47 GMT
Connection: close
```

/sap-projeto/admin/activateAccount.jsp

Details

The GET variable **updateActivation** has been set to **%2527** .

Request

```
GET /sap-projeto/admin/activateAccount.jsp?updateActivation=%2527&accountId=111-222-
1933email@address.tst HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2764
Date: Mon, 10 Mar 2008 11:46:47 GMT
Connection: close
```

/sap-projeto/admin/activateAccount.jsp

Details

The GET variable **updateActivation** has been set to **JyI%3D** .

Request

```
GET /sap-projeto/admin/activateAccount.jsp?updateActivation=JyI%3D&accountId=111-222-
1933email@address.tst HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2764
Date: Mon, 10 Mar 2008 11:46:47 GMT
Connection: close
```

/sap-projeto/admin/activateAccount.jsp

Details

The GET variable **updateActivation** has been set to **0.01** .

Request

```
GET /sap-projeto/admin/activateAccount.jsp?updateActivation=0.01&accountId=111-222-
1933email@address.tst HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2764
Date: Mon, 10 Mar 2008 11:46:47 GMT
Connection: close
```

/sap-projeto/admin/activateAccount.jsp

Details

The GET variable **updateActivation** has been set to **\'** .

Request

```
GET /sap-projeto/admin/activateAccount.jsp?updateActivation=\'&accountId=111-222-
1933email@address.tst HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2764
Date: Mon, 10 Mar 2008 11:46:47 GMT
Connection: close
```

/sap-projeto/admin/activateAccount.jsp

Details

The GET variable **updateActivation** has been set to **\"** .

Request

```
GET /sap-projeto/admin/activateAccount.jsp?updateActivation=\"&accountId=111-222-
1933email@address.tst HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2764
Date: Mon, 10 Mar 2008 11:46:47 GMT
Connection: close
```

/sap-projeto/public/ForgotLogin.jsp

Details

The GET variable **email** has been set to **'** .

Request

```
GET /sap-projeto/public/ForgotLogin.jsp?email=' HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2632
Date: Mon, 10 Mar 2008 11:46:32 GMT
Connection: close
```

/sap-projeto/public/ForgotLogin.jsp

Details

The GET variable **email** has been set to **%00'** .

Request

```
GET /sap-projeto/public/ForgotLogin.jsp?email=%00' HTTP/1.0
Accept: */*
```



```
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2630
Date: Mon, 10 Mar 2008 11:46:32 GMT
Connection: close
```

/sap-projeto/public/ForgotLogin.jsp

Details

The GET variable **email** has been set to **acunetix'"** .

Request

```
GET /sap-projeto/public/ForgotLogin.jsp?email=acunetix'" HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2636
Date: Mon, 10 Mar 2008 11:46:32 GMT
Connection: close
```

/sap-projeto/public/Login.jsp

Details

The GET variable **login** has been set to **'** .

Request

```
GET /sap-projeto/public/Login.jsp?login='&pass=111-222-1933email@address.tst HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2642
Date: Mon, 10 Mar 2008 11:46:31 GMT
Connection: close
```


/sap-projeto/public/Login.jsp

Details

The GET variable **login** has been set to **%00'** .

Request

```
GET /sap-projeto/public/Login.jsp?login=%00'&pass=111-222-1933email@address.tst HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2642
Date: Mon, 10 Mar 2008 11:46:31 GMT
Connection: close
```

/sap-projeto/public/Login.jsp

Details

The GET variable **login** has been set to **acunetix'"** .

Request

```
GET /sap-projeto/public/Login.jsp?login=acunetix'"&pass=111-222-1933email@address.tst
HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2678
Date: Mon, 10 Mar 2008 11:46:31 GMT
Connection: close
```

/sap-projeto/public/Login.jsp

Details

The GET variable **pass** has been set to **acunetix'"** .

Request

```
GET /sap-projeto/public/Login.jsp?login=111-222-1933email@address.tst&pass=acunetix'"
HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```


Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2596
Date: Mon, 10 Mar 2008 11:46:31 GMT
Connection: close
```

/sap-projeto/public/Login.jsp

Details

The GET variable **pass** has been set to **%00'** .

Request

```
GET /sap-projeto/public/Login.jsp?login=111-222-1933email@address.tst&pass=%00' HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2584
Date: Mon, 10 Mar 2008 11:46:31 GMT
Connection: close
```

/sap-projeto/public/Login.jsp

Details

The GET variable **pass** has been set to **'** .

Request

```
GET /sap-projeto/public/Login.jsp?login=111-222-1933email@address.tst&pass=' HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2588
Date: Mon, 10 Mar 2008 11:46:31 GMT
Connection: close
```

Backup files

Severity	**Medium**
Type	Validation
Reported by module	File checks

Description

A possible backup file has been found on your webserver. These files are usually created by developers to backup their

Impact

Backup files can contain script sources, configuration files or other sensitive information that may help an malicious user to prepare more advanced attacks.

Recommendation

Remove the file(s) if they are not required on your website. As an additional step, it is recommended to implement a security policy within your organization to disallow creation of backup files in directories accessible from the web.

Affected items

/sap-projeto/public/Login.jsp.old

Details

No details are available.

Request

```
GET /sap-projeto/public/Login.jsp.old HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
ETag: W/"1403-1204034028000"
Last-Modified: Tue, 26 Feb 2008 13:53:48 GMT
Content-Length: 1403
Date: Mon, 10 Mar 2008 11:46:35 GMT
Connection: close
```

Application error message

Severity	**Low**
Type	Validation
Reported by module	Parameter manipulation

Description

This page contains an error/warning message that may disclose the sensitive information.The message can also contain the location of the file that produced the unhandled exception.

This may be a false positive if the error message is found in documentation pages.

Impact

The error messages may disclose sensitive information. This information can be used to launch further attacks.

Recommendation

Review the source code for this script.

Affected items

/sap-projeto/admin/activateAccount.jsp

Details

The GET variable **accountId** has been set to **NULL** .

Request

```
GET /sap-projeto/admin/activateAccount.jsp?updateActivation=0&accountId=NULL HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2739
Date: Mon, 10 Mar 2008 11:46:48 GMT
Connection: close
```

/sap-projeto/admin/activateAccount.jsp

Details

The GET variable **accountId** has been set to .

Request

```
GET /sap-projeto/admin/activateAccount.jsp?updateActivation=0&accountId= HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2735
Date: Mon, 10 Mar 2008 11:46:48 GMT
Connection: close
```

/sap-projeto/admin/activateAccount.jsp

Details

The GET variable **accountId** has been set to **\'\");|]*{%0d%0a<%00** .

Request

```
GET /sap-
projeto/admin/activateAccount.jsp?updateActivation=0&accountId=\'\");|]*{%0d%0a<%00
HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
```



```
Content-Length: 2757
Date: Mon, 10 Mar 2008 11:46:48 GMT
```

/sap-projeto/admin/activateAccount.jsp

Details

The GET variable **accountId** has been set to **0xffffffff** .

Request

```
GET /sap-projeto/admin/activateAccount.jsp?updateActivation=0&accountId=0xffffffff
HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2745
Date: Mon, 10 Mar 2008 11:46:48 GMT
Connection: close
```

/sap-projeto/admin/activateAccount.jsp

Details

The GET variable **accountId** has been set to **-1.0** .

Request

```
GET /sap-projeto/admin/activateAccount.jsp?updateActivation=0&accountId=-1.0 HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2739
Date: Mon, 10 Mar 2008 11:46:48 GMT
Connection: close
```

/sap-projeto/admin/activateAccount.jsp

Details

The GET variable **accountId** has been set to **0x7fffffff** .

Request

```
GET /sap-projeto/admin/activateAccount.jsp?updateActivation=0&accountId=0x7fffffff
HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
```



```
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2745
Date: Mon, 10 Mar 2008 11:46:48 GMT
Connection: close
```

/sap-projeto/admin/activateAccount.jsp

Details

The GET variable **accountId** has been set to **0x3fffffff** .

Request

```
GET /sap-projeto/admin/activateAccount.jsp?updateActivation=0&accountId=0x3fffffff
HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2745
Date: Mon, 10 Mar 2008 11:46:48 GMT
Connection: close
```

/sap-projeto/admin/activateAccount.jsp

Details

The GET variable **accountId** has been set to **0x80000000** .

Request

```
GET /sap-projeto/admin/activateAccount.jsp?updateActivation=0&accountId=0x80000000
HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2745
Date: Mon, 10 Mar 2008 11:46:48 GMT
Connection: close
```

/sap-projeto/admin/activateAccount.jsp

Details

The GET variable **updateActivation** has been set to **0x3fffffff** .

Request

```
GET /sap-projeto/admin/activateAccount.jsp?updateActivation=0x3fffffff&accountId=111-222-
1933email@address.tst HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2764
Date: Mon, 10 Mar 2008 11:46:48 GMT
Connection: close
```

/sap-projeto/admin/activateAccount.jsp

Details

The GET variable **updateActivation** has been set to **NULL** .

Request

```
GET /sap-projeto/admin/activateAccount.jsp?updateActivation=NULL&accountId=111-222-
1933email@address.tst HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2764
Date: Mon, 10 Mar 2008 11:46:48 GMT
Connection: close
```

/sap-projeto/admin/activateAccount.jsp

Details

The GET variable **updateActivation** has been set to **\'\");|]*{%0d%0a<%00** .

Request

```
GET /sap-
projeto/admin/activateAccount.jsp?updateActivation=\'\");|]*{%0d%0a<%00&accountId=111-
222-1933email@address.tst HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2764
Date: Mon, 10 Mar 2008 11:46:48 GMT
Connection: close
```

/sap-projeto/admin/activateAccount.jsp

Details

The GET variable **updateActivation** has been set to **0** .

Request

```
GET /sap-projeto/admin/activateAccount.jsp?updateActivation=0&accountId=111-222-
1933email@address.tst HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2764
Date: Mon, 10 Mar 2008 11:46:48 GMT
Connection: close
```

/sap-projeto/admin/activateAccount.jsp

Details

The GET variable **updateActivation** has been set to **0x80000000** .

Request

```
GET /sap-projeto/admin/activateAccount.jsp?updateActivation=0x80000000&accountId=111-222-
1933email@address.tst HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2764
Date: Mon, 10 Mar 2008 11:46:48 GMT
Connection: close
```

/sap-projeto/admin/activateAccount.jsp

Details

The GET variable **updateActivation** has been set to **-1.0** .

Request

```
GET
```



```
/sap-projeto/admin/activateAccount.jsp?updateActivation=-1.0&accountId=111-222-
1933email@address.tst HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2764
Date: Mon, 10 Mar 2008 11:46:48 GMT
Connection: close
```

/sap-projeto/admin/activateAccount.jsp

Details

The GET variable **updateActivation** has been set to **0xffffffff** .

Request

```
GET /sap-projeto/admin/activateAccount.jsp?updateActivation=0xffffffff&accountId=111-222-
1933email@address.tst HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2764
Date: Mon, 10 Mar 2008 11:46:48 GMT
Connection: close
```

/sap-projeto/admin/activateAccount.jsp

Details

The GET variable **updateActivation** has been set to **0x7fffffff** .

Request

```
GET /sap-projeto/admin/activateAccount.jsp?updateActivation=0x7fffffff&accountId=111-222-
1933email@address.tst HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
```



```
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2764
Date: Mon, 10 Mar 2008 11:46:48 GMT
```

/sap-projeto/admin/activateAccount.jsp

Details

The GET variable **updateActivation** has been set to **65536** .

Request

```
GET /sap-projeto/admin/activateAccount.jsp?updateActivation=65536&accountId=111-222-
1933email@address.tst HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2764
Date: Mon, 10 Mar 2008 11:46:48 GMT
Connection: close
```

/sap-projeto/admin/activateAccount.jsp

Details

The GET variable **updateActivation** has been set to **-268435455** .

Request

```
GET /sap-projeto/admin/activateAccount.jsp?updateActivation=-268435455&accountId=111-222-
1933email@address.tst HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2764
Date: Mon, 10 Mar 2008 11:46:48 GMT
Connection: close
```

/sap-projeto/admin/activateAccount.jsp

Details

The GET variable **updateActivation** has been set to .

Request

```
GET /sap-projeto/admin/activateAccount.jsp?updateActivation=&accountId=111-222-
1933email@address.tst HTTP/1.0
```



```
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2764
Date: Mon, 10 Mar 2008 11:46:48 GMT
Connection: close
```

/sap-projeto/admin/activateAccount.jsp

Details

The GET variable **updateActivation** has been set to **268435455** .

Request

```
GET /sap-projeto/admin/activateAccount.jsp?updateActivation=268435455&accountId=111-222-
1933email@address.tst HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2764
Date: Mon, 10 Mar 2008 11:46:48 GMT
Connection: close
```

Directory listing found

Severity	**Low**
Type	Information
Reported by module	Text search

Description

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

Impact

A user can view a list of all files from this directory possibly exposing sensitive information.

Recommendation

You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration.

Affected items

Acunetix Website Audit 23

/sap-projeto/admin

Details

We found
<body><h1>Directory Listing For /admin/ - Up To /</h1>

Request

```
GET /sap-projeto/admin/ HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Referer: http://192.168.220.129:8080/sap-projeto/admin/
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=UTF-8
Content-Length: 1655
Date: Mon, 10 Mar 2008 11:46:47 GMT
Connection: close
```

/sap-projeto/common

Details

We found
<body><h1>Directory Listing For /common/ - Up To /</h1>

Request

```
GET /sap-projeto/common/ HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=UTF-8
Content-Length: 2783
Date: Mon, 10 Mar 2008 11:46:21 GMT
Connection: close
```

/sap-projeto/common/art

Details

We found
<body><h1>Directory Listing For /common/art/ - Up To /common</h1>

Request

```
GET /sap-projeto/common/art/ HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
```

```
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
```

Response

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=UTF-8
Content-Length: 2634
Date: Mon, 10 Mar 2008 11:46:21 GMT
Connection: close
```

/sap-projeto/common/script

Details

We found
<body><h1>Directory Listing For /common/script/ - Up To /common</h1>

Request

```
GET /sap-projeto/common/script/ HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=UTF-8
Content-Length: 1439
Date: Mon, 10 Mar 2008 11:46:21 GMT
Connection: close
```

/sap-projeto/common/theme

Details

We found
<body><h1>Directory Listing For /common/theme/ - Up To /common</h1>

Request

```
GET /sap-projeto/common/theme/ HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=UTF-8
Content-Length: 2138
Date: Mon, 10 Mar 2008 11:46:21 GMT
Connection: close
```

Severity	**Low**
Type	Validation
Reported by module	Directory checks

Description

A possible sensitive directory has been found. This directory is not directly linked from the website.This check looks for known sensitive directories like: backup directories, database dumps, administration pages, temporary directories. Each of those directories may help an attacker to learn more about his target.

Impact

This directory may expose sensitive information that may help an malicious user to prepare more advanced attacks.

Recommendation

Restrict access to this directory or remove it from the website.

Affected items

/sap-projeto/admin

Details

No details are available.

Request

```
GET /sap-projeto/admin HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 302 Moved Temporarily
Server: Apache-Coyote/1.1
Location: http://192.168.220.129:8080/sap-projeto/admin/
Date: Mon, 10 Mar 2008 11:46:36 GMT
Connection: close
```

/sap-projeto/common

Details

No details are available.

Request

```
GET /sap-projeto/common HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 302 Moved Temporarily
Server: Apache-Coyote/1.1
Location: http://192.168.220.129:8080/sap-projeto/common/
Date: Mon, 10 Mar 2008 11:46:36 GMT
Connection: close
```


/sap-projeto/public

Details

No details are available.

Request

```
GET /sap-projeto/public HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 302 Moved Temporarily
Server: Apache-Coyote/1.1
Location: http://192.168.220.129:8080/sap-projeto/public/
Date: Mon, 10 Mar 2008 11:46:36 GMT
Connection: close
```

/sap-projeto/public

Details

No details are available.

Request

```
GET /sap-projeto/public HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 302 Moved Temporarily
Server: Apache-Coyote/1.1
Location: http://192.168.220.129:8080/sap-projeto/public/
Date: Mon, 10 Mar 2008 11:46:36 GMT
Connection: close
```

/sap-projeto/secure

Details

No details are available.

Request

```
GET /sap-projeto/secure HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 302 Moved Temporarily
Server: Apache-Coyote/1.1
```



```
Location: http://192.168.220.129:8080/sap-projeto/secure/
Date: Mon, 10 Mar 2008 11:46:36 GMT
```

GHDB: Apache Tomcat Error message

Severity	**Informational**
Type	Informational
Reported by module	GHDB - Google hacking database

Description

The description for this alert is contributed by the GHDB community, it may contain inappropriate language.

Category : Error Messages

Apache Tomcat Error messages. These can reveal various kinds information depending on the type of error.

The Google Hacking Database (GHDB) appears courtesy of the Google Hacking community.

Impact

Not available. Check description.

Recommendation

Not available. Check description.

Affected items

/sap-projeto/admin/activateAccount.jsp

Details

We found
intitle:"Apache Tomcat" "Error Report"

Request

```
GET /sap-projeto/admin/activateAccount.jsp?updateActivation=0&accountId= HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Referer: http://192.168.220.129:8080/sap-projeto/admin/activateAccount.jsp
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2735
Date: Mon, 10 Mar 2008 11:46:47 GMT
Connection: close
```

GHDB: Tomcat directory listing

Severity	**Informational**
Type	Informational
Reported by module	GHDB - Google hacking database

Description

The description for this alert is contributed by the GHDB community, it may contain inappropriate language.

Category : Sensitive Directories

The Google Hackers Guide explains how to find Apache directory indexes, which are the most common found on the Internet. There are other ways however. This query is a generic search for servers using Tomcat with directory listings enabled. They are a bit more fancy than Apache's default lists and more importantly they will not be found using "index.of".

The Google Hacking Database (GHDB) appears courtesy of the Google Hacking community

Impact

Not available. Check description.

Recommendation

Not available. Check description.

Affected items

/sap-projeto/admin

Details

We found
intitle:"Directory Listing For" intext:Tomcat -int

Request

```
GET /sap-projeto/admin/ HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Referer: http://192.168.220.129:8080/sap-projeto/admin/
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=UTF-8
Content-Length: 1655
Date: Mon, 10 Mar 2008 11:46:47 GMT
Connection: close
```

/sap-projeto/common

Details

We found
intitle:"Directory Listing For" intext:Tomcat -int

Request

```
GET /sap-projeto/common/ HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```


Response

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=UTF-8
Content-Length: 2783
Date: Mon, 10 Mar 2008 11:46:21 GMT
Connection: close
```

/sap-projeto/common/art

Details

We found
intitle:"Directory Listing For" intext:Tomcat -int

Request

```
GET /sap-projeto/common/art/ HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=UTF-8
Content-Length: 2634
Date: Mon, 10 Mar 2008 11:46:21 GMT
Connection: close
```

/sap-projeto/common/script

Details

We found
intitle:"Directory Listing For" intext:Tomcat -int

Request

```
GET /sap-projeto/common/script/ HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=UTF-8
Content-Length: 1439
Date: Mon, 10 Mar 2008 11:46:21 GMT
Connection: close
```

/sap-projeto/common/theme

Details

We found
intitle:"Directory Listing For" intext:Tomcat -int

Request

```
GET /sap-projeto/common/theme/ HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=UTF-8
Content-Length: 2138
Date: Mon, 10 Mar 2008 11:46:21 GMT
Connection: close
```

Password type input with autocomplete enabled

Severity	**Informational**
Type	Informational
Reported by module	Crawler

Description

When a new name and password is entered in a form and the form is submitted, the browser asks if the password be saved. Thereafter when the form is displayed, the name and password are filled in automatically or are comple the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.

Impact

Possible sensitive information disclosure

Recommendation

The password autocomplete should be disabled in sensitive applications.
To disable autocomplete, you may use a code similar to:

```
<INPUT TYPE="password" AUTOCOMPLETE="off">
```

Affected items

/sap-projeto/public/Login.jsp

Details

Password type input named **pass** from **unnamed form** with action **Login.jsp** has autocomplete enabled.

Request

```
GET /sap-projeto/public/Login.jsp HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Referer: http://192.168.220.129:8080/sap-projeto/public/index.jsp
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
```

Acunetix Website Audit

```
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 2255
Date: Mon, 10 Mar 2008 11:46:21 GMT
```

/sap-projeto/public/Login.jsp.old

Details

Password type input named **pass** from **unnamed form** with action **Login.jsp** has autocomplete enabled.

Request

```
GET /sap-projeto/public/Login.jsp.old HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.220.129:8080
Cookie: JSESSIONID=DFA45074C81085C749605D14CBC588A4
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
ETag: W/"1403-1204034028000"
Last-Modified: Tue, 26 Feb 2008 13:53:48 GMT
Content-Length: 1403
Date: Mon, 10 Mar 2008 11:46:35 GMT
Connection: close
```

ANEXO IV

Relatório do Nessus – Depois do Hardening

List of hosts

192.168.220.130	Medium Severity problem(s) found

[^] Back

192.168.220.130

Scan time :

Start time :	Mon Oct 13 13:47:59 2008
End time :	Mon Oct 13 13:53:54 2008

Number of vulnerabilities :

Open ports :	2
Low :	14
Medium :	1
High :	0

Information about the remote host :

Operating system :	(unknown)
NetBIOS name :	(unknown)
DNS name :	www.faw.net.

[^] Back to 192.168.220.130

Port general/udp

Traceroute

For your information, here is the traceroute from 192.168.220.1 to 192.168.220.130 :
192.168.220.1
192.168.220.130

Nessus ID : 10287

[^] Back to 192.168.220.130

Port general/tcp

Ping the remote host

The remote host is up

Nessus ID : 10180

TCP timestamps

Synopsis :

The remote service implements TCP timestamps.

Description :

The remote host implements TCP timestamps, as defined by RFC1323.
A side effect of this feature is that the uptime of the remote
host can sometimes be computed.

See also :

http://www.ietf.org/rfc/rfc1323.txt

Risk factor :

None

Nessus ID : 25220

Host FQDN

192.168.220.130 resolves as www.faw.net.

Nessus ID : 12053

Information about the scan

Information about this scan :

Nessus version : 3.2.1.1
Plugin feed version : 200810131134
Type of plugin feed : HomeFeed (Non-commercial use only)
Scanner IP : 192.168.220.1
Port scanner(s) : synscan
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Max hosts : 20
Max checks : 5
Recv timeout : 5
Backports : None
Scan Start Date : 2008/10/13 13:48
Scan duration : 354 sec

Nessus ID : 19506

[^] Back to 192.168.220.130

Port https (443/tcp)

Service detection

A TLSv1 server answered on this port.

Nessus ID : 22964

Service detection

A web server is running on this port through TLSv1.

Nessus ID : 22964

Supported SSL Ciphers Suites

Synopsis :

The remote service encrypts communications using SSL.

Description :

This script detects which SSL ciphers are supported by the remote
service for encrypting communications.

See also :

http://www.openssl.org/docs/apps/ciphers.html

Risk factor :

None

Plugin output :

Here is the list of SSL ciphers supported by the remote server :

Medium Strength Ciphers (>= 56-bit and < 112-bit key)
SSLv3
EDH-RSA-DES-CBC-SHA Kx=DH Au=RSA Enc=DES(56) Mac=SHA1
DES-CBC-SHA Kx=RSA Au=RSA Enc=DES(56) Mac=SHA1
TLSv1
EDH-RSA-DES-CBC-SHA Kx=DH Au=RSA Enc=DES(56) Mac=SHA1
DES-CBC-SHA Kx=RSA Au=RSA Enc=DES(56) Mac=SHA1

High Strength Ciphers (>= 112-bit key)
SSLv3

EDH-RSA-DES-CBC3-SHA Kx=DH Au=RSA Enc=3DES(168) Mac=SHA1
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
TLSv1
EDH-RSA-DES-CBC3-SHA Kx=DH Au=RSA Enc=3DES(168) Mac=SHA1
DHE-RSA-AES128-SHA Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
DHE-RSA-AES256-SHA Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
AES128-SHA Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
AES256-SHA Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}

Nessus ID : 21643

SSL Certificate Expiry

Synopsis :

The remote server's SSL certificate has already expired or will expire shortly.

Description :

This script checks expiry dates of certificates associated with SSL-enabled services on the target and reports whether any have already expired or will expire shortly.

Solution :

Purchase or generate a new SSL certificate to replace the existing one.

Risk factor :

None

Plugin output :

The SSL certificate of the remote service expired Jul 25 21:38:58 2008 GMT!

Nessus ID : 15901

HTTP Server type and version

Synopsis :

A web server is running on the remote host.

Description :

This plugin attempts to determine the type and the version of
the remote web server.

Risk factor :

None

Plugin output :

The remote web server type is :

Coyote HTTP/1.1 Connector

Nessus ID : 10107

HyperText Transfer Protocol Information

Synopsis :

Some information about the remote HTTP configuration can be extracted.

Description :

This test gives some information about the remote HTTP protocol - the
version used, whether HTTP Keep-Alive and HTTP pipelining are enabled,
etc...

This test is informational only and does not denote any security
problem

Risk factor :

None

Plugin output :

Protocol version : HTTP/1.1
SSL : yes
Pipelining : no

Keep-Alive : no
Options allowed : GET,HEAD,POST,OPTIONS,TRACE
Headers :

Date: Fri, 19 Oct 2007 19:57:36 GMT
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=UTF-8
Content-Length: 1130
Connection: close

Nessus ID : 24260

[^] Back to 192.168.220.130

Port http (80/tcp)

Service detection

A web server is running on this port.

Nessus ID : 22964

HTTP Server type and version

Synopsis :

A web server is running on the remote host.

Description :

This plugin attempts to determine the type and the version of
the remote web server.

Risk factor :

None

Plugin output :

The remote web server type is :

Coyote HTTP/1.1 Connector

Nessus ID : 10107

HyperText Transfer Protocol Information

Synopsis :

Some information about the remote HTTP configuration can be extracted.

Description :

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem

Risk factor :

None

Plugin output :

Protocol version : HTTP/1.1
SSL : no
Pipelining : no
Keep-Alive : no
Options allowed : GET,HEAD,POST,OPTIONS,TRACE
Headers :

Date: Fri, 19 Oct 2007 19:57:36 GMT
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=UTF-8
Content-Length: 1130
Connection: close

Nessus ID : 24260

[^] Back to 192.168.220.130

Port general/icmp

ICMP Timestamp Request

Synopsis :

It is possible to determine the exact time set on the remote host.

Description :

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine.

This may help him to defeat all your time based authentication protocols.

Solution :

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk factor :

None

Plugin output :

The difference between the local and remote clocks is -11247 seconds

CVE : CVE-1999-0524, CVE-1999-0524

Nessus ID : 10114

ANEXO V

Relatório do Acunetix – Depois do Hardening

Scan of http://www.faw.net:80/sap-projeto

Scan details

Scan information	
Starttime	13/10/2008 13:05:31
Finish time	13/10/2008 13:05:36
Scan time	5 seconds
Profile	default

Server information	
Responsive	True
Server banner	Unknown
Server OS	Unknown
Server technologies	

Threat level

Acunetix Threat Level 0
No vulnerabilities have been discovered by the scanner.

Alerts distribution

Total alerts found	**2**
High	0
Medium	0
Low	0
Informational	2

Alerts summary

Broken links

Affects	Vari
/sap-projeto	1

Directories with executables permission enabled

Affects	Vari
/	1

Alert details

Broken links

Severity	**Informational**
Type	Informational
Reported by module	Crawler

Description

A broken link refers to any link that should take you to a document, image or webpage, that actually results in ar
This page was linked from the website but it is inaccessible.

Impact

Problems navigating the site.

Recommendation

Remove the links to this file or make it accessible.

Affected items

/sap-projeto
Details
No details are available.
Request

```
GET /sap-projeto HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: www.faw.net
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 404 Not Found
Date: Fri, 19 Oct 2007 19:39:58 GMT
Content-Length: 285
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

Directories with executables permission enabled

Severity	**Informational**
Type	Validation
Reported by module	Directory checks

Description

This directory has Executables enabled from Execute permissions. This check is only related to Microsoft IIS server

Impact

It's possible to run executables (.EXE, .DLL, .BAT, ...) in this directory.

Recommendation

Verify directory permissions and check if Executables access is required.

Affected items

Acunetix Website Audit

/

Details

No details are available.

Request

```
GET /Web_Scanner_Test.dll HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: www.faw.net
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/5.5 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 500 Internal Server Error
Date: Fri, 19 Oct 2007 19:40:00 GMT
Content-Length: 610
Connection: close
Content-Type: text/html; charset=iso-8859-1
```