Graduação em Análise e Desenvolvimento de Sistemas

Segurança em Desenvolvimento de Sistemas

Prof.º: Plinio Marcos Mendes Carneiro

Hardening

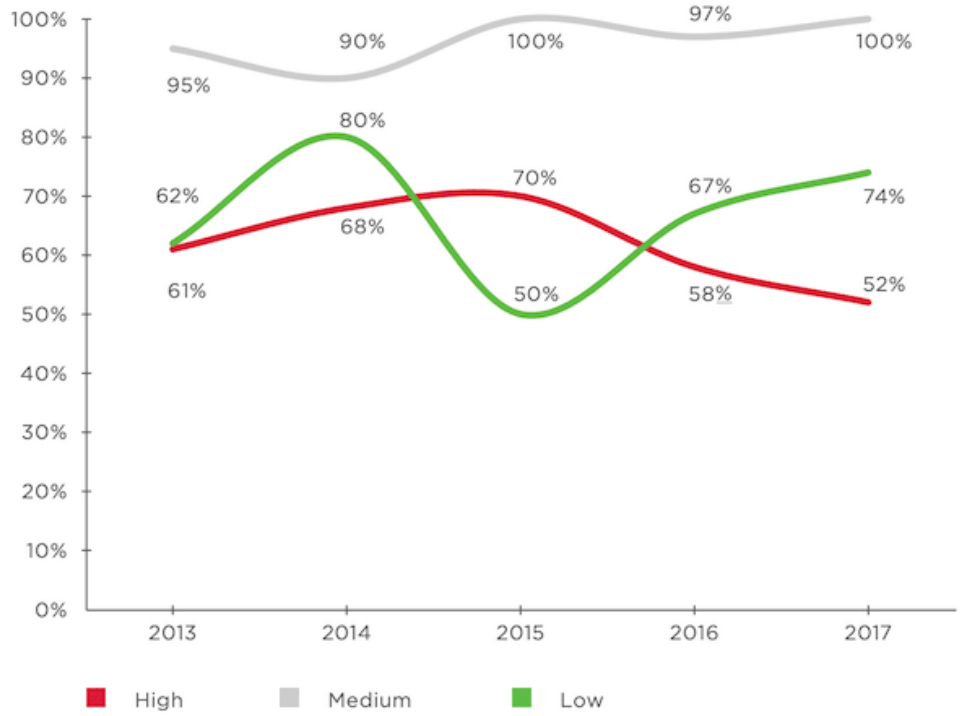
É um processo de mapeamento das ameaças, mitigação dos riscos e execução das atividades corretivas, com foco na infraestrutura e objetivo principal de torná-la preparada para enfrentar tentativas de ataque.

Hardening Servidor Web Apache

- O servidor da Web é uma parte crucial dos aplicativos baseados na Web.
- O servidor da Web Apache geralmente é colocado na borda da rede, tornando-se um dos serviços mais vulneráveis a ataques.
- A configuração padrão fornece muitas informações confidenciais que podem ajudar o hacker a se preparar para um ataque aos aplicativos.

Hardening Servidor Web Apache

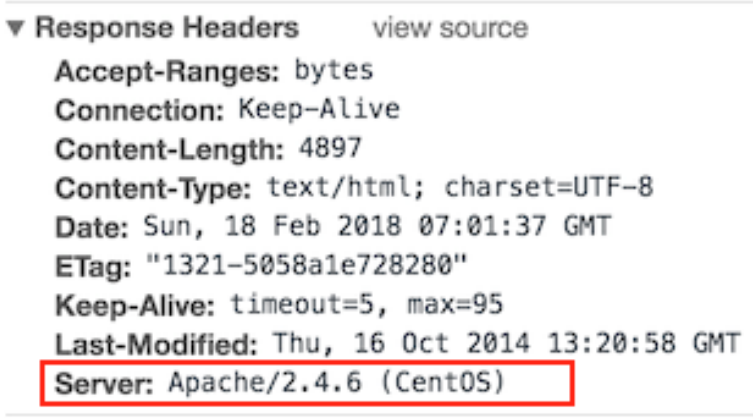
- Uma pesquisa interessante da **Positive Technologies** revela que 52% dos aplicativos digitalizados tinham altas vulnerabilidades.



Websites by vulnerability severity

Remover banner da versão do servidor

- É uma das primeiras coisas a considerar, pois você não deseja expor qual versão do servidor web está usando.
- Expor a versão significa que você está ajudando o hacker a acelerar o processo de reconhecimento.
- A configuração padrão irá expor a versão do Apache e o tipo de SO, conforme mostrado abaixo.



Laboratório Hardening Servidor WEB Apache

INSTALANDO O APACHE

apt-get install apache2 -y

ACESSANDO O APACHE VIA BROWSER

http://IP_DO_SERVIDOR

VERIFICANDO A VERSÃO DO APACHE

cd /var/www/html

mv index.html index.html.old

http://IP_DO_SERVIDOR

DESABILITANDO A VISUALIZAÇÃO DA VERSÃO DO APACHE

cd /etc/apache2/conf-available

nano security.conf

ServerSignature Off

/etc/init.d/apache2 restart

ACESSANDO O APACHE VIA BROWSER

http://IP_DO_SERVIDOR

Mod Security – WAF (Web Aplication Firewall)

- firewall de aplicativos da Web de código aberto, que você pode usar com o Apache.
- Ele vem como um módulo que você precisa compilar e instalar. Se você não puder pagar por um firewall comercial de aplicativos da web , essa seria uma excelente opção.
- Para fornecer proteção genérica a aplicativos da Web, as Regras Principais usam as seguintes técnicas:
- Proteção HTTP - detecção de violações do protocolo HTTP e uma política de uso definida localmente
- Pesquisas na lista negra em tempo real - utiliza reputação IP de terceiros
- Detecção de malware com base na Web - identifica conteúdo malicioso da Web, verificando a API de Navegação segura do Google.
- Proteções de negação de serviço HTTP - defesa contra inundações HTTP e ataques lentos de HTTP DoS.
- Proteção comum contra ataques da Web - detecção de ataques comuns à segurança de aplicativos da Web
- Detecção de automação - detecção de bots, rastreadores, scanners e outra atividade superficial maliciosa
- Integração com o AV Scanning for Uploads de arquivos - identifica arquivos maliciosos enviados por meio do aplicativo Web.
- Rastreando dados confidenciais - rastreia o uso do cartão de crédito e bloqueia vazamentos.
- Proteção contra Trojan - Detectando o acesso a cavalos de Troia.
- Identificação de defeitos do aplicativo - alerta sobre configurações incorretas do aplicativo.
- Detecção e ocultação de erros - Disfarçando mensagens de erro enviadas pelo servidor.

Instalação Apache Mod Security

apt-get install libapache2-mod-security2

/etc/init.d/apache2 restart

apachectl -M |grep security

cp /etc/modsecurity/modsecurity.conf-recommended /etc/modsecurity/modsecurity.conf

nano /etc/modsecurity/modsecurity.conf

SecRuleEngine = on

systemctl restart apache2

mv /usr/share/modsecurity-crs /usr/share/modsecurity-crs.bk

git clone https://github.com/SpiderLabs/owasp-modsecurity-crs.git /usr/share/modsecurity-crs

cp /usr/share/modsecurity-crs/crs-setup.conf.example /usr/share/modsecurity-crs/crs-setup.conf

nano /etc/apache2/mods-enabled/security2.conf

IncludeOptional /usr/share/modsecurity-crs/*.conf

IncludeOptional "/usr/share/modsecurity-crs/rules/*.conf

systemctl restart apache2

http://IP-SERVIDOR-WEB/index.html?exec=/bin/bash