

Roteiro análise servidor web

Objetivo: Evidenciar o aprendizado e a metodologia adotada pelo aluno para avaliação de vulnerabilidade de sistemas WEB e a produção de um relatório de testes.

Tarefa

Orientações:

- Consulte os materiais disponibilizados;
- Todas as evidencias registradas deverão estar acompanhadas de print das telas (evidências).
- A entrega deverá ser feita via BlackBoard até o dia 30 de maio de 2022.
- Faça a instalação do Wordpress na maquina Metasploitable (talvez seja necessário atualizar o PHP) e realize um PENTEST registrando os resultados e suas considerações em um relatório.

Relatório Pentest

Os relatórios de teste de penetração é uma parte muito importante e fornece a você a estrutura detalhada do pentest após a conclusão dos testes. No entanto, muitas vezes esta documentação crítica carece de aspectos-chave do que deve ser incluído, e os clientes começam a questionar o valor prático de suas avaliações. O relatório é o reflexo da qualidade de seu teste.

A seguir algumas dicas para um bom relatório de Pentest:

Resumo executivo para a direção estratégica: O resumo executivo serve como uma visão de alto nível do risco e do impacto nos negócios. O objetivo é ser conciso e claro. Deve ser algo que os leitores não técnicos possam revisar e obter informações sobre as questões de segurança destacadas no relatório.

Embora a equipe de TI possa precisar de todos os detalhes técnicos, os executivos não precisam entender a *tecnologia*. Eles precisam entender os riscos do negócio,

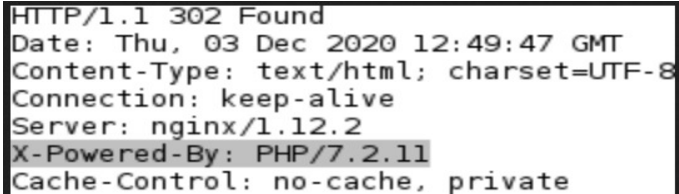
algo que um bom resumo executivo comunicará com eficácia. É imperativo que os líderes de negócios entendam o que está em jogo para tomar decisões informadas para suas empresas, e o resumo executivo é essencial para fornecer esse entendimento.

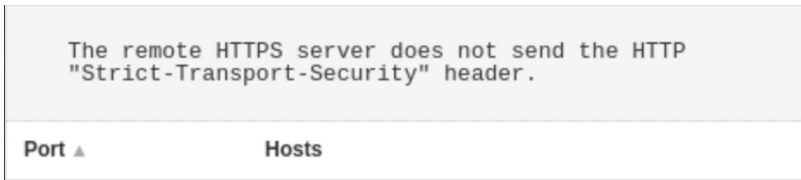
A comunicação visual também pode ser útil para esclarecer pontos complexos. Procure gráficos, tabelas e recursos visuais semelhantes ao comunicar os dados de resumo fornecidos aqui.

Calculando os riscos técnicos: A maioria dos relatórios usa algum tipo de sistema de classificação para medir o risco, mas raramente se dá ao trabalho de *explicar* o risco. A utilização do CVSS para qualificar e avaliar vulnerabilidades nos sistemas é uma boa prática. É necessário que os riscos sejam apresentados de forma clara, pois apenas afirmar que algo é perigoso não transmite risco adequadamente.

Várias recomendações para a correção da vulnerabilidade: A maioria dos relatórios de teste de penetração incluirá uma descrição genérica de alto nível de como lidar com as correções de vulnerabilidades. No entanto, essas recomendações genéricas muitas vezes ficam aquém do contexto exclusivo das necessidades do cliente. Busque apresentar algumas possibilidades quando possível.

A seguir seguem dois exemplos de apontamento de vulnerabilidades em um teste.

Vulnerabilidade:	Identificação versão aplicação em cabeçalho de resposta http
Risco:	baixo
Descrição:	Durante à execução dos testes, por meio dos Headers da aplicação, foi possível identificar a versão da linguagem de programação utilizado pela aplicação. Com esta informação, um atacante pode realizar um ataque focado diretamente neste servidor, tendo assim, uma maior chance de sucesso em seu ataque.
Evidência:	 <pre>HTTP/1.1 302 Found Date: Thu, 03 Dec 2020 12:49:47 GMT Content-Type: text/html; charset=UTF-8 Connection: keep-alive Server: nginx/1.12.2 X-Powered-By: PHP/7.2.11 Cache-Control: no-cache, private</pre>
Correções:	Recomenda-se que as informações sejam retiradas do cabeçalho HTTP através de configurações no servidor web.

Vulnerabilidade:	Strict Transport Security Not Enforced
Risco:	médio
Descrição:	<p>"O aplicativo falha ao impedir que os usuários se conectem a ele através de conexões não criptografadas. Um invasor capaz de modificar o tráfego de rede de um usuário legítimo pode ignorar o uso da criptografia SSL / TLS do aplicativo e usar o aplicativo como uma plataforma para ataques contra seus usuários. Esse ataque é realizado reescrevendo os links HTTPS como HTTP, para que, se um usuário de destino siga um link para o site a partir de uma página HTTP, o navegador nunca tente usar uma conexão criptografada. A ferramenta sslstrip automatiza esse processo. Para explorar esta vulnerabilidade, o invasor deve estar posicionado para interceptar e modificar o tráfego de rede da vítima. Esse cenário geralmente ocorre quando um cliente se comunica com o servidor por uma conexão insegura."</p>
Evidência:	
Correções:	<p>O aplicativo deve instruir os navegadores da Web a acessarem o aplicativo apenas usando HTTPS. Para fazer isso, ative o HSTS (HTTP Strict Transport Security) adicionando um cabeçalho de resposta com o nome 'Strict-Transport-Security' e o valor 'max-age = expireTime', em que expireTime é o tempo em segundos que os navegadores devem lembrar que o site só deve ser acessado usando HTTPS. Considere adicionar o sinalizador 'includeSubDomains', se apropriado.</p>