UNIVERSIDADE SÃO JUDAS TADEU – USJT

GERÊNCIA E SEGURANÇA DE REDES

VICTOR GONÇALVES VOLPI **/ RA: 825117218**

Ferramentas de Detecção de Vulnerabilidades em Aplicação Web

"Análise dos funcionamento, vantagens e tipos de falhas detectadas"

SÃO PAULO – SP

2025

ATIVIDADE 1

Pergunta 1 – Primeiro, familiarize-se com as principais vulnerabilidades do OWASP para entender quais tipos de vulnerabilidades devem ser procurados. Você pode encontra-las no site oficial do OWASP.

R: Apenas uma análise no site da OWASP.

Pergunta 2 – Descreva as vulnerabilidades (2021) mais recente e comente cada uma dela.

R:

A01:2021 – Controle de Acesso Quebrado (Broken Access Control): é uma vulnerabilidade onde usuários conseguem acessar dados ou funções que não deveriam.
Comentário: Ele é muito comum, pode permitir que invasores vejam informações privadas ou alterem dados de outros usuários.

A02:2021 – Falhas Criptográficas (Cryptographic Failures): ela é mais relacionadas a senhas fracas, dados sensíveis sem criptografia adequada ou protocolos inseguros.
Comentário: Basicamente ela compromete a confidencialidade e integridade das informações.

A03:2021 – Injeção (Injection): Quando os dados maliciosos são enviados para comandos SQL, NoSQL, OS ou LDAP.
Comentário: Na minha visão é um dos ataques mais perigosos, podendo expor e manipular bancos de dados.

A04:2021 – Design Inseguro (Insecure Design): São praticamente falhas de arquitetura ou lógica de negócio mal planejada.
Comentário: Elas são muito difícil de serem corrigidas, pois exige rever todo o projeto de segurança do sistema.

A05:2021 – Configuração de Segurança Incorreta (Security Misconfiguration): Eles ocorrem por falhas em permissões, serviços expostos ou configurações padrão inseguras.
Comentário: Ele é muito comum, e geralmente explorada facilmente por atacantes.

A06:2021 – Componentes Vulneráveis e Desatualizados (Vulnerable and Outdated Components): Uma falta de atualização constante obtendo o uso de bibliotecas, frameworks e softwares sem atualização.
Comentário: Facilita os invasores atacarem facilmente, pois exploram falhas já documentadas.

A07:2021 – Identificação e Autenticação Quebradas (Identification and Authentication Failures): Basicamente eles Inclui senhas fracas, falta de MFA e tokens inseguros.
Comentário: E isso permite que invasores assumam a identidade de usuários legítimos.

A08:2021 – Falhas em Software e Integridade de Dados (Software and Data Integrity Failures): Quando os códigos, bibliotecas ou atualizações não são verificadas quanto à integridade.
Comentário: Levam facilmente ataques de supply chain (cadeia de suprimentos).

A09:2021 – Falhas de Registro e Monitoramento de Segurança (Security Logging and Monitoring Failures): Eles obtém uma ausência grande em logs, dificultando a detecção de ataques.
Comentário: Sem monitoramento, um ataque pode ficar “invisível” por meses.

A10:2021 – SSRF (Server-Side Request Forgery): Quando o servidor é enganado para fazer requisições para locais internos ou externos.
Comentário: Eles exporem serviços internos e informações críticas da infraestrutura.

ATIVIDADE 2

Identificar ferramentas de detecção de vulnerabilidades em um site web.

Pergunta 1 – Qual o objetivo da ferramenta?

R: Bom vou utilizar a OWASP ZAP, o principal objetivo é identificar vulnerabilidades em aplicações web, ajudando os desenvolvedores e analistas identificar as falhas antes dos ataques.

Pergunta 2 – Como a ferramenta funciona?

R: Funciona mais ou menos assim. Ela seria tipo um Proxy entre um usuário e a aplicação web, interceptando e analisando o trafego nos protocolos do HTTP/HTTPS. E ela basicamente simula alguns ataques, como injeção de banco de dados e outros.

Pergunta 3 – Quais são as principais vantagens e desvantagens da ferramenta?

R: As vantagens são mais por ele ser gratuito e ser um item de código aberto, com uma facilidade de integração em testes e eles detectam uma ampla gama de vulnerabilidades.

R: As desvantagens ela principalmente não substitui totalmente testes manuais, ela requer também um conhecimento técnico para interpretar corretamente os resultados e ela também pode gerar falsos positivos e isso pode complicar no futuro.

Pergunta 4 – A ferramenta é fácil de usar? Por que?

R: Sim, pois ela possui uma interface gráfica intuitiva e tutoriais disponíveis. Porém, para aproveitar todo o potencial, é necessário ter noções de segurança e redes.

Pergunta 5 – Quais são os tipos de vulnerabilidades que a ferramenta pode detectar?

R: Bom acho que ela identifica pontos cruciais.

Injeção de banco de dados com o principal sendo o SQL.

Quebras de autenticação em sessões.

Configurações de segurança incorretas.

Inclusão de arquivos inseguros.

Uma exposição sobre dados sensíveis.

Ela também identifica vulnerabilidades em APIS.

VICTOR GONÇALVES VOLPI **/ RA: 825117218**

Ferramentas de Detecção de Vulnerabilidades em Aplicação Web

"Análise dos funcionamento, vantagens e tipos de falhas detectadas"

Trabalho apresentado a Universidade São Judas Tadeu – USJT como requisito para conclusão do trabalho de Gerência e Segurança de redes.

Orientador: Prof. Jorge Werner

SÃO PAULO - SP

2025