

DESENV. WEB SEGURO

INTRODUÇÃO À SEGURANÇA DE DESENVOLVIMENTO

WEB

JEFFERSON O. ANDRADE

OBJETIVOS DA AULA

- Introduzir os conceitos básicos de desenvolvimento web seguro.
- Identificar as principais ameaças e vulnerabilidades em aplicativos web.
- Compreender a importância da segurança no desenvolvimento web.

PLANO DE AULA

- Discussão sobre Segurança de Aplicativos Web
- Princípios de Desenvolvimento Web Seguro
- Os 10 Maiores Riscos de Segurança em Aplicações Web
- Exemplos Práticos e Estudos de Caso
- Encerramento e Próximos Passos

SEGURANÇA DE APLICATIVOS WEB

- O que é desenvolvimento web seguro?
- Quais são as principais ameaças e vulnerabilidades enfrentadas pelos aplicativos web?
- Como as vulnerabilidades podem ser exploradas por invasores?

O QUE É DESENVOLVIMENTO WEB SEGURO?

Desenvolvimento web seguro (DWS) é uma disciplina que se concentra em proteger os aplicativos e sistemas web contra ameaças, ataques e vulnerabilidades que possam comprometer a segurança dos dados e a integridade do sistema.

DWS envolve a implementação de práticas, técnicas e medidas de segurança durante o ciclo de vida do desenvolvimento de software, desde o planejamento e a concepção até a implantação e a manutenção.

PRINCÍPIOS DE DESENVOLVIMENTO WEB SEGURO

- Autenticação e autorização
- Proteção contra injeção de código
- Validação de entrada de dados
- Gerenciamento de sessão
- Configuração segura do servidor
- Auditoria e monitoramento

AUTENTICAÇÃO E AUTORIZAÇÃO

Garantir que os usuários sejam quem dizem ser e que tenham permissões adequadas para acessar recursos específicos dentro do sistema.

PROTEÇÃO CONTRA INJEÇÃO DE CÓDIGO

Prevenir ataques de injeção de código, como injeção de SQL e injeção de scripts, que podem permitir que um invasor execute comandos maliciosos no sistema.

VALIDAÇÃO DE ENTRADA DE DADOS

Garantir que os dados fornecidos pelos usuários sejam válidos e seguros, prevenindo assim ataques de XSS (Cross-Site Scripting) e CSRF (Cross-Site Request Forgery), entre outros.

GERENCIAMENTO DE SESSÃO

Manter a segurança das sessões de usuário, protegendo-as contra roubo de sessão e outras formas de ataques de sessão.

CONFIGURAÇÃO SEGURA DO SERVIDOR

Garantir que o servidor web e outros componentes do sistema estejam configurados de maneira segura e adequada para minimizar as vulnerabilidades.

AUDITORIA E MONITORAMENTO

Implementar ferramentas e práticas para auditar e monitorar o sistema em busca de atividades suspeitas e anomalias de segurança.

OS 10 MAIORES RISCOS (OWASP TOP TEN)

- A01:2021 - Broken Access Control
- A02:2021 - Cryptographic Failures
- A03:2021 - Injection
- A04:2021 - Insecure Design
- A05:2021 - Security Misconfiguration
- A06:2021 - Vulnerable and Outdated Components
- A07:2021 - Identification and Authentication Failures
- A08:2021 - Software and Data Integrity Failures
- A09:2021 - Security Logging and Monitoring Failures
- A10:2021 - Server-Side Request Forgery

A01:2021 - BROKEN ACCESS CONTROL

- Falhas na implementação de controle de acesso, permitindo acesso não autorizado a recursos protegidos.
- Permite exploração de falhas na implementação de controle de acesso para acessar recursos não autorizados, como URLs restritas ou dados confidenciais.

A02:2021 - CRYPTOGRAPHIC FAILURES

- Falhas na implementação de criptografia, levando à exposição de dados sensíveis ou comprometimento do sistema.
- Permite exploração de falhas na criptografia para interceptar comunicações, decifrar senhas ou manipular dados sensíveis.

A03:2021 - INJECTION

- Vulnerabilidades que permitem a inserção de código malicioso em campos de entrada, como SQL injection e XSS.
- Permite inserção de código malicioso em campos de entrada para executar comandos no banco de dados (SQL injection) ou no navegador do usuário (XSS).

A04:2021 - INSECURE DESIGN

- Riscos relacionados a falhas de design que tornam os sistemas suscetíveis a ataques.
- Explorado pela identificação de falhas de design para explorar brechas de segurança, como acesso não autorizado a áreas do sistema ou manipulação de funcionalidades.

A05:2021 - SECURITY MISCONFIGURATION

- Configurações inadequadas de segurança que deixam o sistema vulnerável a ataques.
- Explorado pela identificação de configurações inadequadas para acessar informações sensíveis, como arquivos de configuração não protegidos ou servidores mal configurados.

A06:2021 - VULNERABLE AND OUTDATED COMPONENTS

- Uso de componentes desatualizados ou com vulnerabilidades conhecidas que podem ser exploradas por invasores.
- Permite exploração de vulnerabilidades conhecidas em componentes desatualizados ou com falhas de segurança para acessar o sistema ou comprometer os dados.

A07:2021 - IDENTIFICATION AND AUTHENTICATION FAILURES

- Falhas no processo de identificação e autenticação, permitindo acesso não autorizado a contas de usuário.
- Permite acesso não autorizado a contas de usuário, explorando falhas na autenticação, como senhas fracas ou tokens de sessão vulneráveis.

A08:2021 - SOFTWARE AND DATA INTEGRITY FAILURES

- Falhas na garantia da integridade dos dados e do software, permitindo alterações não autorizadas ou corrupção de dados.
- Manipulação de dados ou software para alterar informações sensíveis ou comprometer a integridade do sistema.

A09:2021 - SECURITY LOGGING AND MONITORING FAILURES

- Falhas na implementação de logs de segurança e monitoramento, dificultando a detecção de atividades suspeitas.
- Realização de atividades maliciosas sem ser detectado devido à falta de registros ou monitoramento adequado das atividades do sistema.

A10:2021 - SERVER-SIDE REQUEST FORGERY

- Vulnerabilidades que permitem que um invasor faça solicitações para outros sistemas a partir do servidor, explorando a confiança indevida em solicitações internas.
- Exploração de falhas que permitem a um invasor fazer solicitações de servidor para servidor, como acessar informações confidenciais ou explorar vulnerabilidades em sistemas internos.

EXEMPLOS PRÁTICOS E ESTUDOS DE CASO

- Demonstração de vulnerabilidades em aplicativos web.
- Análise de estudos de caso de ataques bem-sucedidos.

DÚVIDAS?

- Estou à disposição para responder às suas perguntas!

OBRIGADO!

- Obrigado por participar da aula de hoje. Nos vemos na próxima semana!