

Desenvolvimento Web Seguro - Plano de Aula

Semana 2 - Autenticação e Autorização

Prof. Jefferson O. Andrade

[2024-05-15 qua]

1 Objetivos da Aula

- Compreender os diferentes métodos de autenticação e autorização.
- Identificar e resolver problemas comuns relacionados à autenticação e autorização.
- Analisar estudos de caso para entender a aplicação prática de métodos seguros de autenticação e autorização.

2 Estrutura da Aula

1. Introdução (5 minutos)

- Breve introdução sobre a importância da autenticação e autorização em segurança de aplicações web.

2. Apresentações dos Grupos (40-60 minutos)

- **A02:2021 - Cryptographic Failures (10-15 minutos)**
 - Apresentação por Murilo e Rafael.
- **A03:2021 - Injection (10-15 minutos)**
 - Apresentação por Marcio e Ana.
- **A07:2021 - Identification and Authentication Failures (10-15 minutos)**
 - Apresentação por Anderson e Hericca.
- **A10:2021 - Server-Side Request Forgery (10-15 minutos)**
 - Apresentação por Felipe, Fabrício e Carlos.

3. Discussão sobre Apresentações (10 minutos)

- Perguntas e respostas.
- Feedback sobre as apresentações.

4. Autenticação e Autorização: Conceitos Básicos (20 minutos)

- Definições e diferenças entre autenticação e autorização.
- Métodos comuns de autenticação (senhas, tokens, biometria, MFA).
- Mecanismos de autorização
 - Controle de acesso baseado em funções (RBAC – *Rule Based Access Control*)
 - Controle de acesso baseado em atributos (ABAC – *Attribute Based Access Control*)

5. Estudos de Caso (20 minutos)

- Análise de estudos de caso reais onde falhas na autenticação e autorização levaram a violações de segurança.
- Discussão sobre como esses problemas poderiam ter sido evitados.

6. Atividade Prática (30 minutos)

- Resolução de problemas comuns relacionados à autenticação e autorização.
- Implementação de um sistema simples de autenticação e autorização em um ambiente de desenvolvimento (exemplo prático).

7. Conclusão e Próximos Passos (10 minutos)

- Recapitulação dos pontos chave da aula.
- Introdução ao conteúdo da próxima aula.
- Tarefas pós-aula: Leitura recomendada e exercícios para praticar.

3 Recursos Necessários:

- Slides de apresentação.
- Exemplos de código para a atividade prática.
- Links para vídeos e leituras recomendadas.
- Acesso à plataforma de videoconferência (Google Meet) para ministrar a aula síncrona.