Plano de Aula

Semana 4: Injeção de SQL e Gerenciamento de Sessão Segura (Estudo Dirigido)

Prof. Jefferson O. Andrade

2024-06-05

1 Objetivo

- Capacitar os alunos a compreender os riscos da injeção de SQL e da má gestão de sessões, bem como aplicar técnicas de prevenção em aplicações Flask.

2 Formato

- Estudo dirigido com atividades práticas e discussões em grupo.

3 Materiais

- Roteiro de estudo (fornecido abaixo)
- Ambiente de desenvolvimento com Flask (local ou online)
- Ferramentas de desenvolvimento web (browser, editor de código, etc.)
- Acesso a um banco de dados SQL (SQLite, MySQL, PostgreSQL, etc.)
- Tutoriais em vídeo e/ou texto sobre os temas da semana

4 Pré-requisitos

- Conhecimento básico de SQL
- Familiaridade com o framework Flask
- Conhecimentos da semana anterior sobre XSS e CSRF

5 Duração

- 3 horas (tempo estimado para realização das atividades de forma autônoma)

6 Atividades

1. **Introdução e Contextualização (30 minutos)**
    - Os alunos deverão assistir a um vídeo introdutório sobre injeção de SQL e gerenciamento de sessão.
        - SQL Injections: The Full Course
        - SQL Injection Hacking Tutorial (Beginner to Advanced)

- Após o vídeo, os alunos devem ler um breve resumo sobre os temas da semana, também disponível no AVA.
- O professor deve estar disponível para tirar dúvidas e promover uma breve discussão online sobre a importância da segurança em relação a bancos de dados e sessões.

2. **Estudo Dirigido: Injeção de SQL (1 hora)**
    - Os alunos, em grupos, seguirão o roteiro de estudo, que inclui:
        - Leitura de tutoriais sobre diferentes tipos de injeção de SQL (SQLi).
        - Discussão em grupo, utilizando ferramentas de comunicação online (fórum, chat, etc.), sobre as descobertas e os desafios encontrados.
3. **Estudo Dirigido: Gerenciamento de Sessão Segura (1 hora)**
    - Os alunos, em grupos, continuarão o estudo dirigido, abordando:
        - Leitura de materiais sobre práticas de gerenciamento de sessão segura (cookies seguros, tempo de expiração, regeneração de ID, etc.).
        - Discussão em grupo, utilizando ferramentas de comunicação online, sobre as melhores práticas e os desafios de garantir a segurança das sessões.
4. **Apresentação e Discussão dos Resultados (30 minutos)**
    - Cada grupo deverá entregar um vídeo com suas descobertas e aprendizado.
    - O professor fará um feedback geral sobre os vídeos, destacando os pontos positivos e os pontos a serem melhorados.
    - Discussão online sobre as diferentes abordagens e as melhores práticas para prevenir SQLi e garantir a segurança das sessões.
    - O professor complementa a discussão, esclarece dúvidas e apresenta exemplos adicionais.

7 Roteiro de Estudo

7.1 Injeção de SQL

1. Leia os tutoriais sobre os diferentes tipos de injeção de SQL:
    - Injeção de SQL baseada em União (Union-based SQLi)
    - Injeção de SQL baseada em Erro (Error-based SQLi)
    - Injeção de SQL baseada em Booleano (Boolean-based SQLi)
    - Injeção de SQL baseada em Tempo (Time-based SQLi)
    - **Fontes:**
        - OWASP SQL Injection: `https://owasp.org/www-community/attacks/SQL_Injection`
        - Portswigger SQL Injection: `https://portswigger.net/web-security/sql-injection`
2. Discuta com seu grupo as descobertas e aprendizados encontrados.
3. Pesquise e apresente as principais técnicas de prevenção contra SQLi:
    - Prepared Statements
    - Object-Relational Mappers (ORMs)
    - Validação e sanitização de entradas
    - Mínimos privilégios no banco de dados

7.2 Gerenciamento de Sessão Segura

1. Leia os materiais sobre práticas de gerenciamento de sessão segura:
    - Uso de cookies seguros (HttpOnly, Secure flags)
    - Configuração adequada do tempo de expiração da sessão
    - Regeneração do ID da sessão após ações sensíveis (login, logout, etc.)
    - Proteção contra ataques de fixação de sessão
    - **Fontes:**
        - OWASP Session Management Cheat Sheet: `https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html`
2. Discuta com seu grupo as melhores práticas e os desafios de garantir a segurança das sessões.

8 Avaliação

- Qualidade do relatório (vídeo) entregue pelo grupo, incluindo a análise das vulnerabilidades e as soluções propostas.
- Participação ativa nas discussões online e contribuição para o aprendizado do grupo (auto-avaliação).

9 Recursos Adicionais

- OWASP Top 10: `https://owasp.org/www-project-top-ten/`