Plano de Estudo

Headers de Segurança e Política de Segurança de Conteúdo (CSP)

Prof. Jefferson O. Andrade

2024-06-19

1 Objetivo

- Capacitar os alunos a compreender a importância dos headers de segurança e da Política de Segurança de Conteúdo (CSP) na proteção de aplicações web.
- Ensinar os alunos a configurar headers de segurança em servidores web e implementar uma CSP eficaz.

2 Formato

- Estudo dirigido com atividades práticas e entrega de trabalho individual.

3 Materiais

- Roteiro de estudo (fornecido abaixo)
- Documentação sobre os principais headers de segurança (disponível online)
- Tutoriais sobre como criar e implementar uma CSP (disponível online)
- Ambiente de desenvolvimento web (local ou online)
- Ferramentas de desenvolvimento web (browser, editor de código, etc.)

4 Pré-requisitos

- Conhecimento básico de HTML, CSS e JavaScript
- Familiaridade com o funcionamento de servidores web (Apache, Nginx, etc.)
- Conhecimentos das semanas anteriores sobre segurança web

5 Duração

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

6 Atividades

1. **Estudo dos Headers de Segurança (1 hora)**
    - Os alunos deverão ler a documentação sobre os principais headers de segurança, incluindo:
        - `X-XSS-Protection`
        - `X-Frame-Options`
        - `Strict-Transport-Security` (HSTS)
        - `X-Content-Type-Options`
        - `Referrer-Policy`
        - `Content-Security-Policy` (CSP)
    - Para cada header, os alunos devem entender:
        - O propósito e a funcionalidade do header.
        - Como o header ajuda a proteger contra ataques específicos.
        - Como configurar o header em diferentes servidores web (Apache, Nginx, etc.).
    - Os alunos devem fazer anotações e tirar dúvidas sobre os headers de segurança.
2. **Estudo da Política de Segurança de Conteúdo (CSP) (1 hora)**
    - Os alunos deverão ler tutoriais sobre como criar e implementar uma CSP, incluindo:
        - As diferentes diretivas da CSP e seus significados.
        - Como construir uma política CSP eficaz para diferentes tipos de aplicações web.
        - Como testar e depurar uma CSP.
    - Os alunos devem criar uma CSP básica para um site simples, utilizando as diretivas mais comuns.
    - Os alunos devem testar a CSP no navegador e verificar se ela está funcionando corretamente.
3. **Atividade Prática: Configuração de Headers e Implementação de CSP (1 hora)**
    - Os alunos deverão configurar os headers de segurança em um servidor web local ou online.
    - Os alunos deverão implementar a CSP criada na etapa anterior no site simples.
    - Os alunos deverão testar a configuração dos headers e a implementação da CSP, utilizando ferramentas online e o console do navegador.

7 Trabalho em Grupo

- Os alunos deverão entregar um relatório contendo:
    - Uma descrição detalhada da configuração dos headers de segurança no servidor web.
    - O código da CSP implementada no site simples.
    - Uma análise dos resultados dos testes realizados, incluindo capturas de tela do console do navegador e de ferramentas online.
    - Uma reflexão sobre a importância dos headers de segurança e da CSP na proteção de aplicações web.

8 Avaliação

- Qualidade do relatório entregue, incluindo a clareza das explicações, a correção da configuração dos headers e da implementação da CSP, e a profundidade da análise dos resultados dos testes.

9 Recursos de Aprendizado

- OWASP Secure Headers Project: `https://owasp.org/www-project-secure-headers/`
- MDN Web Docs - Content Security Policy: `https://developer.mozilla.org/pt-BR/docs/Web/HTTP/CSP`
- Google CSP Evaluator: `https://csp-evaluator.withgoogle.com/`