Trabalho Prático 1: Introdução à Segurança em Aplicações Web (PHP ou Python)

Valor: 2 pontos

Objetivo

Este trabalho visa introduzir conceitos básicos de segurança em aplicações web, focando em vulnerabilidades comuns e suas correções teóricas. O aluno deverá pesquisar e explicar as falhas de segurança presentes em um dos relatórios dos sistemas **PHP** ou **Python**, sem a necessidade de implementação prática.

Enunciado

Você é um analista de segurança e recebeu dois relatórios de vulnerabilidades:

1. Sistema em PHP (aplicação web tradicional).

2. Sistema em Python (usando Flask).

Sua tarefa é **pesquisar e explicar** as vulnerabilidades encontradas em cada um, descrevendo:

- **O que é a vulnerabilidade?** (Definição teórica).
- **Quais os riscos?** (Impacto se explorada).
- **Como corrigir?** (Medidas preventivas, sem código).

ATENÇÃO:

Pontos para pesquisa se a escolha for o Sistema PHP:

1. Política de Segurança de Conteúdo (CSP) Ausente ou Insegura

🔷 O que é?

🔷 Riscos:

🔷 Correção:

2. Cookies sem HttpOnly, Secure e SameSite

🔷 O que é?

🔷 Riscos:

🔷 Correção:

3. Vazamento de Informações no Cabeçalho HTTP (X-Powered-By, Server)

🔷 O que é?

🔷 Riscos:

🔷 Correção:

4. Falta de Tokens Anti-CSRF

🔷 O que é?

🔷 Riscos:

🔷 Correção:

5. Ausência de X-Frame-Options (Clickjacking)

🔷 O que é?

🔷 Riscos:

🔷 Correção:

Pontos para pesquisa se a escolha for o Sistema PYTHON:

1. CSP Não Configurado
🔷 O que é?
🔷 Riscos:
🔷 Correção:

2. Cookies Inseguros
🔷 O que é?
🔷 Riscos:
🔷 Correção:

3. Falta de Proteção Anti-CSRF
🔷 O que é?
🔷 Riscos:
🔷 Correção:

4. Vazamento de Informações (Server Headers)
🔷 O que é?
🔷 Riscos:
🔷 Correção:

5. Falta de Sanitização de Entradas
🔷 O que é?
🔷 Riscos:
🔷 Correção:

Entrega
📌 **Relatório Teórico** (Documento ou apresentação) contendo:
1. Explicação das vulnerabilidades em **PHP** ou **Python**.
2. Riscos associados a cada uma.
3. Medidas de correção (sem código, apenas conceitos).

Formato:
- Texto claro e objetivo.
- Pode incluir exemplos genéricos (ex: "Um token CSRF é um valor único gerado para cada sessão...").

Prazo final para envio: 16/04/2025.

Forma de envio: via e-mail professorjdefora@gmail.com com as seguintes informações:
ASSUNTO: Trabalho 1
CONTEÚDO: a escolha do sistema e os nomes completos de até 5 integrantes do grupo
ANEXO: qualquer formato desde que acessível sem necessidade de confirmação.

Critérios de Avaliação:
- Clareza na explicação.
- Precisão técnica.

- Organização do conteúdo.

Bom trabalho! 🔒