Estrutura da Aula Prática

1. Introdução (19:30 - 19:40)

- Boas-vindas e visão geral da aula.
- Breve revisão sobre a importância da segurança da informação.
- Explicação do objetivo da aula: entender e corrigir vulnerabilidades.

2. Discussão dos Resultados dos Scans (19:40 - 20:00)

- Os alunos, em grupos, apresentam as vulnerabilidades encontradas em casa.
- Cada grupo discute brevemente como identificou cada vulnerabilidade.

3. Análise de Vulnerabilidades (20:00 - 20:30)

- Discussão guiada sobre o que é uma vulnerabilidade.
- Identificar tipos comuns de vulnerabilidades (SQL Injection, XSS, etc.).
- Análise das vulnerabilidades mais comuns encontradas pelos grupos.

4. Laboratório Prático: Correção de Vulnerabilidades (20:30 - 21:00)

- **Correção na aplicação/servidor:**
  - ✓ Demonstrações práticas de como corrigir vulnerabilidades no código ou configuração.
  - ✓ Os alunos tentam aplicar correções sob supervisão.
- **Correção no usuário:**
  - ✓ Discussão sobre como práticas de segurança podem prevenir certas vulnerabilidades.
  - ✓ Simulações de ataques phishing para ensinar reconhecimento e prevenção.

5. Documentação de Segurança (21:00 - 21:20)

- Importância da documentação no processo de segurança.
- Como documentar uma vulnerabilidade e a correção aplicada.
- Exemplo de documentação eficaz.

6. Conclusão e Dúvidas (21:20 - 21:30)

- Recapitulação dos pontos principais da aula.
- Sessão de perguntas e respostas.
- Orientações para atividades futuras e encerramento.