ESCOLA SUPERIOR DE REDES

Navegação do questionário

1 2 3 4 5

Terminar revisão

Iniciado em	sexta-feira, 20 set. 2024, 15:49
Estado	Finalizada
Concluída em	sexta-feira, 20 set. 2024, 16:08
Tempo empregado	19 minutos 23 segundos

QUESTÃO 1

Correto

Vale 1,00 ponto(s).

Que tipo de ataque NÃO pode ser realizado por meio de um XSS?

Escolha uma opção:

a. Adulteração da página da aplicação vulnerável.

b. Modificação diretamente na base de dados. ✓

c. Varredura de redes privadas.

d. Quebra de token anti-CSRF.

e. Descoberta de histórico de navegação.

Sua resposta está correta.

A modificação direta na base de dados só pode ser realizada por ataques de injeção SQL.

A resposta correta é: Modificação diretamente na base de dados.

QUESTÃO 2

Correto

Vale 1,00 ponto(s).

Qual dos itens abaixo não é um possível ponto de injeção do código submetido por meio de um ataque XSS?

Escolha uma opção:

a. Corpo da página.

b. Dentro de um script.

c. Dentro de um marcador HTML.

d. Dentro de um arquivo de imagem. ✓

e. No título da página.

Sua resposta está correta.

Não é possível implementar ataques de XSS a partir do conteúdo de uma imagem pois neste tipo de mídia o navegador apenas mostra o conteúdo, sem processar nenhuma informação que eventualmente seja inserida dentro da imagem.

A resposta correta é: Dentro de um arquivo de imagem.

QUESTÃO 3

Correto

Vale 1,00 ponto(s).

Quais as contramedidas mais eficazes contra um XSS?

Escolha uma opção:

a. Utilização de HTTPS para proteção das informações trocadas entre navegador e aplicação.

b. Remoção não recursiva de caracteres perigosos e palavras reservadas de HTML para toda entrada obtida de fontes não confiáveis.

c. Desabilitar javascript nos navegadores web.

d. Validação de entrada por meio de listas brancas.

e. Validação de entrada por meio de listas brancas e aplicação de codificação HTML aos caracteres reservados presentes na página gerada. ✓

Sua resposta está correta.

Utilização de HTTPs irá apenas garantir o sigilo do ataque durante o trânsito dos dados entre cliente e servidor.

Uma remoção não recursiva de caracteres não confiáveis deixaria de lado variáveis internas e tags HTML que não estejam associadas diretamente a página principal (document.*)

Desabilitar javascript no navegador faz com que nenhuma validação funcione.

A validação de entrada por meio de listas brancas apenas poderia permitir a execução de scripts se o atacante conseguir descobrir quais são as regras implementadas pela lista branca.

A resposta correta é: Validação de entrada por meio de listas brancas e aplicação de codificação HTML aos caracteres reservados presentes na página gerada.

QUESTÃO 4

Correto

Vale 1,00 ponto(s).

O vetor abaixo pode ser utilizado para implementar que tipo de ataque XSS?

http://victim.site/welcome.php?name=</h4><script>alert('XSS'); </ script>

Escolha uma opção:

- a. XSS refletido ✓
- b. XSS persistente
- c. XSS baseado em DOM
- d. XCS

Sua resposta está correta.

O vetor apresentado refere-se a um link que o usuário precisaria clicar para ser direcionado a página victim.site que não realiza qualquer tipo de validação para o campo “name”. Este é um exemplo de XSS refletido.

A resposta correta é: XSS refletido

QUESTÃO 5

Incorreto

Vale 1,00 ponto(s).

Que ferramenta pode ser utilizada para controlar máquinas remotamente?

Escolha uma opção:

- a. netcat ✗
- b. Nessus
- c. nmap
- d. BeeF
- e. Wireshark

Sua resposta está incorreta.

O BeEF é uma ferramenta desenvolvida em Ruby que suporta diversas plataformas diferentes. A arquitetura geral é composta por um único servidor, que realiza a interface com o usuário e controla os navegadores web escravizados.

netcat é utilizado para testes de conexão pois permite abrir portas em um servidor.

Nessus é um scanner de vulnerabilidades

nmap um scanner de rede

wireshark um capturador e analisador de pacotes (sniffer)

A resposta correta é: BeeF

◄ Tarefa 5

Conteúdo do Módulo ►