ESCOLA SUPERIOR DE REDES

Navegação do questionário

1 2 3 4 5

Terminar revisão

Iniciado em	domingo, 29 set. 2024, 09:38
Estado	Finalizada
Concluída em	domingo, 29 set. 2024, 09:52
Tempo empregado	13 minutos 49 segundos

QUESTÃO 1

Correto

Vale 1,00 ponto(s).

Qual a principal técnica que pode ser utilizada para evitar os diversos tipos de ataques de injeção?

Escolha uma opção:

a. Usar token anti-CSRF.

b. Codificar os caracteres que possuem sentido especial em HTML.

c. Cifrar a base de dados.

d. Utilizar um firewall na borda da infraestrutura e implantar antivírus no servidor de aplicação.

e. Validar, imediatamente antes do uso, todas as entradas da aplicação por meio de listas brancas. ✓

Sua resposta está correta.

Ataques de injeção podem ser evitados com a implementação de ferramentas que valide a entrada de dados substituindo caracteres que podem ser manipulados por códigos HTML bem como a implementação de listas brancas.

A resposta correta é: Validar, imediatamente antes do uso, todas as entradas da aplicação por meio de listas brancas.

QUESTÃO 2

Correto

Vale 1,00 ponto(s).

Ao testar se uma aplicação é vulnerável à injeção de comandos na shell, supondo que o resultado do comando injetado não possa ser visualizado, qual a melhor maneira de saber se a fraqueza está presente?

Escolha uma opção:

a. Injetando um comando para remoção de todos os arquivos, para verificar se a aplicação fica indisponível.

b. Injetando um script escrito em Javascript.

c. Injetando um comando que reinicie o servidor.

d. Injetando um comando que consuma alguns segundos de processamento. ✓

e. Injetando um comando SQL.

Sua resposta está correta.

Para identificar se uma aplicação é vulnerável à injeção de comandos na Shell o recomendável é injetar um comando simples, como cat, e observar a resposta do servidor.

A resposta correta é: Injetando um comando que consuma alguns segundos de processamento.

QUESTÃO 3

Correto

Vale 1,00 ponto(s).

XPath é uma linguagem utilizada para acessar elementos de um documento XML a partir de um modelo de dados representado em formato de árvore.

Sendo assim, uma consulta XPath pode devolver:

Escolha uma opção:

- a. um conjunto de nós do modelo ou valores atômicos. ✓
- b. uma lista com todos os objetos manipulados pela DOM.
- c. uma lista hierarquizada de classes CSS, mostrando a precedência de cada elemento.
- d. uma lista contendo todas as requisições realizadas pelo servidor para carregar uma determinada página.

Sua resposta está correta.

Uma consulta XPath pode devolver um conjunto de nós do modelo ou valores atômicos de um arquivo XML.

A resposta correta é: um conjunto de nós do modelo ou valores atômicos.

QUESTÃO 4

Correto

Vale 1,00 ponto(s).

Para testar se uma aplicação é vulnerável à poluição de parâmetros HTTP, um dos passos iniciais seria:

Escolha uma opção:

a. Remover parâmetros da requisição.

b. Inserir um parâmetro de requisição com mesmo nome de um existente, mas com valor diferente. ✓

c. Inserir um parâmetro de requisição não existente.

d. Transpor parâmetros do corpo da requisição para a query string.

e. Nenhum dos itens anteriores.

Sua resposta está correta.

Ao inserir um parâmetro de requisição com o mesmo nome de um existente, mas como valor diferente, você conseguirá avaliar como funciona o sistema de precedência e, dependendo do resultado, identificar se o sistema é vulnerável a este tipo de ataque. Por isso esse seria o primeiro passo para explorar esta vulnerabilidade.

Os demais passos citados nesta questão serão executados após este.

A resposta correta é: Inserir um parâmetro de requisição com mesmo nome de um existente, mas com valor

diferente.

QUESTÃO 5

Correto

Vale 1,00 ponto(s).

Uma contramedida para ataques de injeção de auditoria seria:

Escolha uma opção:

a. usar funções da linguagem na qual a aplicação é desenvolvida, que sejam específicas para o propósito desejado.

b. enviar múltiplas instâncias do mesmo elemento verificando se ele foi encaminhado pelo canal correto.

c. calcular e armazenar uma assinatura digital ou um código de autenticação de mensagem para cada registro recebido. ✓

d. estabelecer o máximo de elementos que podem ser recuperados por meio de uma consulta.

Sua resposta está correta.

Cada item representa um método de proteção para ataques de injeção, ou seja:

- Injeção LDAP - estabelecer o máximo de elementos que podem ser recuperados por meio de uma consulta.
- Injeção de Comandos - usar funções da linguagem

na qual a aplicação é desenvolvida, que sejam específicas para o propósito desejado.

- Poluição de HTTP - enviar múltiplas instâncias do mesmo elemento verificando se ele foi encaminhado pelo canal correto.

Injeção de Auditoria - calcular e armazenar uma assinatura digital ou um código de autenticação de mensagem para cada registro recebido.

A resposta correta é: calcular e armazenar uma assinatura digital ou um código de autenticação de mensagem para cada registro recebido.

◄ Tarefa 7

Conteúdo do Módulo ►