ESCOLA SUPERIOR DE REDES

Navegação do questionário

1 2 3 4 5

Terminar revisão

Iniciado em	sábado, 21 set. 2024, 09:10
Estado	Finalizada
Concluída em	sábado, 21 set. 2024, 09:34
Tempo empregado	23 minutos 58 segundos

QUESTÃO 1

Correto

Vale 1,00 ponto(s).

Em um ataque de injeção de SQL qual seria a razão de adicionar comentários no meio do comando injetado?

Escolha uma opção:

a. Realizar um ataque de injeção de SQL às cegas.

b. Realizar um ataque de injeção de SQL de segunda ordem.

c. Obter informações do dicionário de dados.

d. Evadir filtros de entrada mal escritos. ✓

e. Efetuar partição e balanceamento.

Sua resposta está correta.

Ao inserir o caractere de comentário em uma entrada o atacante busca evitar a execução de um determinado pedaço do código no servidor ou a geração de erros que possa lhe repassar alguma informação. Com isso ele irá evadir eventuais filtros de entrada que estejam mal implementados.

A resposta correta é: Evadir filtros de entrada mal escritos.

QUESTÃO 2

Correto

Vale 1,00 ponto(s).

Considere uma aplicação vulnerável à injeção de SQL cujo ponto de injeção é um SELECT utilizado pela aplicação para exibição de informações textuais. Qual a melhor técnica para extração de informações a partir de outras tabelas que não as usadas pelo SELECT problemático?

Escolha uma opção:

- a. Técnica baseada em UNION. ✓
- b. Injeção de SQL às cegas baseada em tempo.
- c. Injeção de SQL de segunda ordem.
- d. Partição e balanceamento.
- e. Injeção de SQL às cegas baseada no método bit-a-bit.

Sua resposta está correta.

Para poder unir o resultado de uma consulta com registros de outras tabelas é necessário utilizar a função UNION do PL/SQL

A resposta correta é: Técnica baseada em UNION.

QUESTÃO 3

Correto

Vale 1,00 ponto(s).

Em injeção de SQL, a técnica de partição e balanceamento serve para:

Escolha uma opção:

a. Acelerar a obtenção de informações por meio de uma estratégia “dividir para conquistar”.

b. Evadir filtros de entrada mal escritos.

c. Permitir a injeção sem causar um erro sintático no comando original. ✓

d. Empilhar comandos.

e. Nenhuma das anteriores.

Sua resposta está correta.

A técnica de partição e balanceamento permite injetar consultas e expressões SQL, no meio de valores fornecidos à aplicação, sem se preocupar com o número de aspas e parênteses presentes no comando original.

É importante salientar que expressões escritas, desse jeito, podem ser injetadas em qualquer ponto de um comando sendo esta a principal vantagem desta técnica.

A resposta correta é: Permitir a injeção sem causar um erro sintático no comando original.

QUESTÃO 4

Incorreto

Vale 1,00 ponto(s).

Qual das funções abaixo não poderia ser feita a partir de um ataque de injeção SQL em uma determinada aplicação Web?

Escolha uma opção:

- a. realizar a varredura de rede. ✗
- b. executar comandos no shell da máquina.
- c. visualizar informações de tabelas utilizadas direta ou indiretamente pelo sistema.
- d. Obter os números de identificador de sessão dos usuários conectados ao sistema.
- e. Executar funções específicas do SGBD.

Sua resposta está incorreta.

O número de identificação de sessão dos usuários conectados não poderia ser visualizado a partir de um ataque de injeção de SQL.

Obs.: cabe destacar que o servidor Web Apache, por exemplo, pode ser configurado para armazenar os identificadores de sessão gerados em uma tabela no SGDB. Esta configuração, embora possível, é pouco usual sendo, inclusive, não recomendada.

A resposta correta é: Obter os números de identificador de sessão dos usuários conectados ao sistema.

QUESTÃO 5

Correto

Vale 1,00 ponto(s).

Em um ataque a uma aplicação Web vulnerável a injeção SQL e cujo o SGGB seja o MySQL, qual seria a consequência da execução do vetor:

' and 1=2 union select table_rows,null,table_schema, null,table_name,null from information_schema.tables where table_schema<>'information_schema' order by 3#

Escolha uma opção:

a. realizar um sleep no banco de dados.

b. listar informações sobre todas as tabelas de um determinado sistema. ✓

c. realizar uma varredura na rede buscando outros servidores ativos.

d. inserir informações em uma determinada tabela.

e. listar dados de uma tabela acessória que poderia conter, por exemplo, a lista de usuários ativos no sistema.

Sua resposta está correta.

O vetor em questão é específico para banco de dados MySQL e tem como objetivo listar todas as tabelas que podem ser acessadas pelo

usuário utilizado pela aplicação para acesso aos dados.

A resposta correta é: listar informações sobre todas as tabelas de um determinado sistema.

◄ Tarefa 6

Conteúdo do Módulo ►