



Navegação do questionário



[Terminar revisão](#)

Iniciado em
quarta-feira, 2 out. 2024, 17:50

Estado
Finalizada

Concluída em
quarta-feira, 2 out. 2024, 18:27

Tempo
empregado 36 minutos 39 segundos

QUESTÃO 1

Incorreto

Vale 1,00 ponto(s).

A melhor maneira de se testar condições de corrida consiste em:

Escolha uma opção:

- ☒ a. Usar uma ferramenta automatizada. ✖
- ☐ b. Executar manual e repetidamente as operações da aplicação em busca de inconsistências.
- ☐ c. Fornecer valores grandes às entradas da aplicação.
- ☐ d. Variar as URLs das requisições em busca de recursos escondidos.
- ☐ e. Analisar código fonte.



Sua resposta está incorreta.

Condições de corrida são difíceis de serem encontradas a partir de uma análise dinâmica do código (não é impossível, mas improvável). Para localizar este tipo de vulnerabilidade o recomendável é analisar o código fonte da aplicação, num primeiro momento utilizando ferramentas automatizadas.

A resposta correta é: Analisar código fonte.


QUESTÃO 2

Correto

Vale 1,00 ponto(s).

O que uma aplicação deve fazer para evitar acesso direto a recursos?

Escolha uma opção:

- ☒ a. Implementar corretamente um monitor de referências. 
- ☐ b. Usar o cabeçalho HTTP Referer.
- ☐ c. Ofuscar as referências aos recursos da aplicação.
- ☐ d. Verificar logo após a autenticação as opções que o usuário pode acessar.
- ☐ e. Não há como evitar este tipo de ataque.



Sua resposta está correta.

Um monitor de referência é um componente que pode ser utilizado para controlar o acesso direto a recursos de uma aplicação.

A resposta correta é: Implementar corretamente um monitor de referências.

QUESTÃO 3

Correto

Vale 1,00 ponto(s).

Considere o seguinte trecho de código vulnerável o qual usa somente variáveis inteiras:

```
if (limiteUsado + valorEmprestimo <= limiteMaximo) {  
    // Concede o empréstimo  
    valorConta = valorConta + valorEmprestimo;  
} else {  
    // Exibe mensagem de erro  
}
```

Como ele pode ser explorado?

Escolha uma opção:

- ☐ a. Fornecendo um valor de empréstimo negativo.
- ☐ b. Explorando uma injeção de SQL.
- ☐ c. Explorando o servidor para modificação do limite máximo armazenado em banco de dados.
- ☒ d. Fornecendo um valor de empréstimo que cause um extravasamento de inteiro ao se realizar "limiteUsado + valorEmprestimo". ✓
- ☐ e. O código não possui vulnerabilidades.



Sua resposta está correta.

Uma forma de explorar este código seria fornecer um valor de empréstimo maior que a capacidade de um inteiro para a linguagem de programação utilizada. No caso de Java, por exemplo, basta que este valor não esteja na faixa de -2147483648 a 2147483647

A resposta correta é: Fornecendo um valor de empréstimo que cause um extravasamento de inteiro ao se realizar "limiteUsado + valorEmprestimo".



QUESTÃO 4

Correto

Vale 1,00 ponto(s).

Ao implementar um sistema computacional seu desenvolvedor optou por um método de controle de acesso do tipo mandatório - MAC. Com isso o dono de um objeto:

Escolha uma opção:

- ☒ a. Não pode atribuir permissão de acesso para qualquer outro usuário e depende de um administrador para isso. ✓
- ☐ b. Pode atribuir permissão de acesso ao objeto para qualquer outro usuário, já que ele é o dono portanto o seu criador.
- ☐ c. Pode atribuir permissão de acesso desde que o sistema tenha uma regra para tal.
- ☐ d. Pode atribuir permissão de acesso desde que esteja escrito em uma determinada ACL



Sua resposta está correta.

No controle de acesso do tipo mandatório o usuário criador não tem permissão automática para dar acesso aos arquivos que criou. Apenas no modelo DAC isso é possível.

O sistema baseado em regra é conhecido como RBAC e baseado em listas seria o ACL.

QUESTÃO 5

Correto

Vale 1,00 ponto(s).

A resposta correta é: Não pode atribuir permissão de acesso para qualquer outro usuário e depende de um administrador para isso.

Qual dos itens abaixo NÃO é uma maneira viável a ser utilizada por um usuário malicioso para descobrir URLs das operações de um sistema às quais não têm acesso:

Escolha uma opção:

- ☐ a. avaliar registros de trilhas de auditoria.
- ☐ b. inspecionar tráfego capturado.
- ☒ c. realizar uma varredura de vulnerabilidades. ✓
- ☐ d. interagir com outros usuários do sistema.



Sua resposta está correta.

Realizar uma varredura de vulnerabilidades não irá permitir a identificação de URLs que não estejam disponíveis ao usuário autenticado.

A resposta correta é: realizar uma varredura de vulnerabilidades.

◀ Tarefa 8

Conteúdo do Módulo ▶

