

[da Cibersegurança](#) > QUIZ Fundamentos da Segurança Cibernética

Iniciado em	quinta, 22 Dez 2022, 12:44
Estado	Finalizada
Concluída em	quinta, 22 Dez 2022, 12:52
Tempo empregado	7 minutos 39 segundos
Avaliar	10,00 de um máximo de 10,00(100%)

Questão 1

Correto

Atingiu 2,00 de 2,00

Um criminoso virtual utiliza de diversas técnicas para obter sucesso em uma tentativa de invasão ou em um roubo de informações. Em um processo de hacking, um termo muito utilizado é o de "Exploitar" uma aplicação.

Assinale a alternativa que corresponde corretamente ao significado do termo Exploitar:

- a. Exploitar uma aplicação significa expor e explorar as vulnerabilidades mais críticas de uma aplicação ou sistema, para que o atacante consiga alcançar maior impacto em sua invasão.
- b. Exploitar é a ação mais danosa que um criminoso virtual pode executar em um ataque cibernético, pois é a ação de exclusão ou quebra do funcionamento da aplicação que foi vitimada no ataque.
- c. Exploitar é uma etapa do processo de hacking que segue a etapa de port scan, permitindo que uma aplicação seja explorada a partir da execução de uma sequência grande de tentativas de executar login e senha a partir de dicionários de senhas mais comuns.
- d. Exploitar é o mesmo que vazar dados, quando um ataque cibernético é bem-sucedido.

Sua resposta está correta.

A resposta correta é:

Exploitar uma aplicação significa expor e explorar as vulnerabilidades mais críticas de uma aplicação ou sistema, para que o atacante consiga alcançar maior impacto em sua invasão.

Questão 2

Correto

Atingiu 2,00 de 2,00

O modelo STRIDE foi desenvolvido para ajudar na identificação e classificação de ameaças à segurança cibernética de sistemas. Assinale a alternativa que corresponde corretamente ao significado do acrônimo STRIDE:

- a. SPOOFING
TAMPERING
REPUDIATION
INTEGRITY
DENIAL OF SERVICE
ELEVATION
- b. SPOOFING
TRUSTED INFORMATION
REPUDIATION
INTEGRITY
DENIAL OF SERVICE
ELEVATION
- c. SPANING TREE
TAMPERING
REPUDIATION
INTEGRITY
DENIAL OF SERVICE
ELEVATION
- d. SPOOFING ✓
TAMPERING
REPUDIATION
INFORMATION DISCLOSURE
DENIAL OF SERVICE
ELEVATION

Sua resposta está correta.

A resposta correta é:

SPOOFING
TAMPERING
REPUDIATION
INFORMATION DISCLOSURE
DENIAL OF SERVICE
ELEVATION

Questão 3

Correto

Atingiu 2,00 de 2,00

Quando se fala em padrões de segurança adotados para setores específicos, existem diversos padrões que devem ser adotados, obrigatoriamente, pelas empresas pertencentes àquele setor.

De acordo com estas informações, considere a lista de leis, normas, organizações e padrões de segurança apresentada a seguir:

- I. OWASP
- II. SANS
- III. MITRE
- IV. NIST
- V. PCI-DSS
- VI. SOX

Assinale a alternativa que corresponde corretamente às leis, normas, organizações e padrões relacionadas com as empresas do setor financeiro:

- a. III e IV
- b. II e III
- c. I e II
- d. V e VI✓

Sua resposta está correta.

A resposta correta é:

V e VI

Questão 4

Correto

Atingiu 2,00 de 2,00

Sobre a segurança de páginas WEB, existem diversos desafios para definir um modelo seguro para o acesso às páginas. Sobre os métodos de requisição e resposta do protocolo HTTP, assinale a alternativa correta:

- a. O método GET é mais seguro que o POST, pois ele utiliza certificados digitais em suas requisições, gerando a navegação HTTPS.
- b. O método POST é mais seguro que o GET, pois ele utiliza certificados digitais em suas requisições, gerando a navegação HTTPS.
- c. O método POST é mais seguro que o GET, pois ele não traz informações de sua requisição diretamente na URL do navegador.
- d. O método GET é mais seguro que o POST, pois ele não traz informações de sua requisição diretamente na URL do navegador.

Sua resposta está correta.

A resposta correta é:

O método POST é mais seguro que o GET, pois ele não traz informações de sua requisição diretamente na URL do navegador.

Questão 5

Correto

Atingiu 2,00 de 2,00

Existem diversos projetos que auxiliam os profissionais de Segurança Cibernética e Desenvolvimento Seguro de Software a descobrir e reduzir a incidência de vulnerabilidades e problemas de segurança relacionados ao desenvolvimento de aplicações.

Assinale a alternativa que corresponde corretamente ao principal projeto de segurança em aplicações:

- a. SANS CVE
- b. NIST CWE
- c. OWASP TOP 10✓
- d. MITRE ATT@CK

Sua resposta está correta.

A resposta correta é:

OWASP TOP 10