Iniciado em	sábado, 24 Dez 2022, 08:39
Estado	Finalizada
Concluída em	sábado, 24 Dez 2022, 09:00
Tempo empregado	21 minutos 12 segundos
Avaliar	**9,83** de um máximo de 10,00(**98,33**%)

Questão 1

Correto

Atingiu 0,50 de 0,50

Um ataque cibernético permitiu que um criminoso virtual tivesse acesso a uma conta de usuário na rede da empresa. Este criminoso virtual conseguiu escalar o privilégio da conta, virou administrador no servidor e alterou o conteúdo do website da empresa. Quando isso ocorre, qual pilar da segurança da informação é quebrado?

a. Integridade

b. Privacidade

c. Confidencialidade ✔

d. Não-repúdio

e. Disponibilidade

Sua resposta está correta.

A resposta correta é:
Confidencialidade

Questão 2

Correto

Atingiu 0,50 de 0,50

Quando se fala em incidente cibernético, existem termos que são importantes. Desde a prevenção, detecção e resposta, muitas ações são fundamentais para evitar ou conter um incidente. Um destes termos é a MITIGAÇÃO. Assinale a alternativa que corresponde corretamente ao significado deste termo:

a. É um modelo para a identificação de ameaças de segurança, utilizado para ajudar a encontrar ameaças em um sistema.

b. São as medidas tomadas para reduzir o impacto de uma ameaça. ✔

c. É uma atualização disponibilizada que visa tratar ou remover uma vulnerabilidade ou falha de um sistema.

d. É algum ponto fraco da aplicação ou da infraestrutura que pode ser explorado.

e. É uma consequência potencial, caso um determinado fato ocorra.

Sua resposta está correta.

A resposta correta é:
São as medidas tomadas para reduzir o impacto de uma ameaça.

Questão 3

Correto

Atingiu 0,50 de 0,50

Um sistema de mensageria foi desenvolvido sem o uso de certificado digital para validar os usuários. O usuário A enviou uma mensagem para o usuário B, mas depois afirmou que não mandou essa mensagem. O suporte técnico foi acionado e não pôde concluir se quem mandou a mensagem foi realmente o usuário A. Quando isso ocorre, estamos quebrando qual pilar da segurança da informação?

a. Privacidade

b. Disponibilidade

c. Integridade

d. Confidencialidade

e. Não-repúdio ✔

Sua resposta está correta.

A resposta correta é:
Não-repúdio

Questão 4

Correto

Atingiu 1,00 de 1,00

[OWASP TOP 10 - 2021]

Que tipo de falha acontece quando dados fornecidos pelo usuário são enviados a um interpretador ou inseridos como parte a consulta de banco de dados, sem validação?

a. Falha de autorização

b. Falhas da injeção ✔

c. Ataque de Cross-site request forgery

d. Falhas de quebra de controle de acesso

Sua resposta está correta.

A resposta correta é:
Falhas da injeção

Questão 5

Correto

Atingiu 1,00 de 1,00

[OWASP TOP 10 - 2021]

Uma empresa está desenvolvendo uma nova aplicação e precisa decidir qual a melhor opção para proteger as credenciais dos usuários armazenadas pela empresa:

a. Nunca armazenar senhas de usuários

b. Combinar as senhas com SALT e utilizar um algoritmo de HASH considerado seguro ✔

c. Encriptar as senhas usando criptografia assimétrica de 4098 bits

d. Encriptar as senhas usando criptografia simétrica

Sua resposta está correta.

A resposta correta é:
Combinar as senhas com SALT e utilizar um algoritmo de HASH considerado seguro

Questão 6

Correto

Atingiu 1,00 de 1,00

[OWASP TOP 10 - 2021]

Que tipo de falha acontece quando uma aplicação renderiza dados de usuário como parte do código HTML enviado ao lado cliente sem validação?

- a. Cross-site scripting (XSS) ✔
- b. Injeção SQL
- c. Falha de controle de acesso
- d. Cross-site request forgery (CSRF)

Sua resposta está correta.

A resposta correta é:
Cross-site scripting (XSS)

Questão 7

Correto

Atingiu 1,00 de 1,00

[OWASP TOP 10 - 2021]

Qual das categorias de risco abaixo foi adicionada ou renomeada na lista de principais riscos da OWASP TOP 10 2021?

- a. A4:2021 - Design Inseguro ✔
- b. A5:2021 - Configuração de Segurança Incorreta
- c. A9:2021 - Falhas de Registro e Monitoramento
- d. A3:2021 - Injeção

Sua resposta está correta.

A resposta correta é:
A4:2021 - Design Inseguro

Questão 8

Correto

Atingiu 1,00 de 1,00

[OWASP TOP 10 - 2021]

O trecho de código a seguir contém uma vulnerabilidade que pode ser classificada como qual das categorias de risco da OWASP TOP 10 2021?

Trecho:

```
$search_query = $GET['q'];
echo '<h1> search results for: ' . $search_query . '</h1>;'
```

a. A3:2021 - Injeção ✔
semana

b. A2:2021 - Falhas criptográficas

c. A7:2021 - Falhas de Identificação e autenticação

d. A8:2021 - Falhas de Integridade de software e dados

Sua resposta está correta.

A resposta correta é:
A3:2021 - Injeção
semana

Questão 9

Correto

Atingiu 1,00 de 1,00

[OWASP TOP 10 - 2021]

Que tipo de falha pode ser explorada para que um atacante execute código malicioso como sendo código de uma dependência de sua aplicação?

a. A10:2021 - Server Side Request orgery (SSRF)

b. A6:2021 - Componentes Desatualizados e Vulneráveis

c. Nenhuma das listadas pois este cenário não é possível

d. A8:2021 - Falhas de integridade de software e dados ✔

Sua resposta está correta.

A resposta correta é:
A8:2021 - Falhas de integridade de software e dados

Questão 10

Correto

Atingiu 1,00 de 1,00

No que consiste o risco Broken User Authentication em APIs?

- a. Na falta de habilidade do sistema em identificar e validar a identidade do usuário/cliente requisitante comprometendo a segurança do sistema. ✔
- b. Na manipulação de informações em massa que usuário/cliente não deveria ter conhecimento e/ou acesso.
- c. Na exposição e endpoint que manipulam objetos internos sem o controle adequado de autorização.
- d. Na falta de habilidade do sistema em identificar e validar a identidade do atacante, comprometendo a segurança do sistema.

Sua resposta está correta.

A resposta correta é:
Na falta de habilidade do sistema em identificar e validar a identidade do usuário/cliente requisitante comprometendo a segurança do sistema.

Questão 11

Parcialmente correto

Atingiu 0,33 de 0,50

Cite algumas boas práticas para remediar o risco Insufficient Logging & Monitoring.

- a. Implementar LOGs nas aplicações e EndPoints ✔
- b. Realizar monitoramento e triagem dos log para identificar comportamentos suspeitos ✔
- c. Avaliar a criticidade das APIs para definir o nível ideal de monitoramento e registro de log
- d. Verificar a autorização no nível das funções.
- e. Gerenciar o ciclo de vida da API, desative endpoint antigos que não necessitem estar em funcionamento

Sua resposta está parcialmente correta.

Você selecionou corretamente 2.
As respostas corretas são:
Implementar LOGs nas aplicações e EndPoints,

Realizar monitoramento e triagem dos log para identificar comportamentos suspeitos,

Avaliar a criticidade das APIs para definir o nível ideal de monitoramento e registro de log

Questão 12

Correto

Atingiu 0,50 de 0,50

No que consiste o risco Lack of Resources & Rate Limiting ?

a. Na manipulação de informações em massa que usuário/cliente não deveria ter conhecimento e/ou acesso.

b. na falta de habilidade do sistema em identificar e validar a identidade do usuário/cliente requisitante comprometendo a segurança do sistema.

c. Na falta de definição do limites computacionais que a API pode utilizar. ✔

d. Na exposição e endpoint que manipulam objetos internos sem o controle adequado de autorização.

Sua resposta está correta.

A resposta correta é:
Na falta de definição do limites computacionais que a API pode utilizar.

Questão 13

Correto

Atingiu 0,50 de 0,50

Cite algumas boas práticas para remediar o risco Lack of Resources & Rate Limiting em APIs.

a. Implementar um limite na frequência com que um usuário/cliente pode chamar a API dentro de um período de tempo definido.

b. Monitorar o serviço para identificar acessos suspeitos e IPs com reputação ruim.

c. Ter cuidado com serviços escaláveis, pois eles podem mascarar ataques DoS.

d. Todas as demais. ✔

e. Impor limites de utilização de recursos computacionais baseado na necessidade do negócio.

Sua resposta está correta.

A resposta correta é:
Todas as demais.