ESCOLA SUPERIOR DE REDES

Navegação do questionário

1 2 3 4 5 6 7 8 9 10

Mostrar uma página por vez

Terminar revisão

Iniciado em	sábado, 5 out. 2024, 12:29
Estado	Finalizada
Concluída em	sábado, 5 out. 2024, 12:57
Tempo empregado	28 minutos 31 segundos
Avaliar	9,00 de um máximo de 10,00(90%)

QUESTÃO 1

Correto

Atingiu 1,00 de 1,00

O padrão PCI DSS sugeria, erroneamente, que a proteção do número de cartão poderia ser protegido por meio de funções de hash criptográficas, quando armazenados. Um erro semelhante afetou a proteção de códigos prioritários de cinco caracteres do Mac World Expo 2007, mantidos no lado cliente da aplicação. Como o uso de funções de hash criptográficas na proteção de valores pertencentes a domínios de baixa cardinalidade pode ser quebrado?

Escolha uma opção:

a. Através do cálculo de Rainbow Tables e aplicação aos hashes encontrados.

b. Aplicando a função de hash a todos os elementos do domínio e comparando com os valores armazenados. ✓

c. Realizando a criptoanálise da função de hash criptográfica empregada.

d. Só é possível atacar a solução se uma função fraca for utilizada.

e. Não é possível atacar esta construção.

Sua resposta está correta.

Quando a função hash é aplicada a um domínio com baixa cardinalidade significa que o domínio tem muitos poucos valores (em termos de variedade) o que facilita um processo de quebra por for uta, já que o espaço de todas as combinações possíveis a serem testadas é menor.

A resposta correta é: Aplicando a função de hash a todos os elementos do domínio e comparando com os valores armazenados.

QUESTÃO 2

Correto

Atingiu 1,00 de 1,00

A utilização criteriosa dos atributos de cabeçalho do HTTP é um importante mecanismo para o gerenciamento de sessões. Qual dos atributos abaixo define uma lista de destinos que o navegador está autorizado a enviar o cookie de um determinado usuário, como parte da requisição?

a. Domain ✓

b. Path

c. Secure

d. HttpOnly

Sua resposta está correta.

O atributo “domain” estipula para quais domínios o navegador web deve enviar o cookie, como parte da requisição.

O atributo “path” permite especificar um caminho diferente para os domínios que irão receber o cookie.

O atributo “secure” informa ao navegador web que o cookie contém informações sensíveis e, por isso, não deve ser enviado, por meio de conexões desprotegidas.

O atributo “HttpOnly”, introduzido pela Microsoft, tem por objetivo impedir que cookies sejam manipulados por scripts no lado cliente da aplicação.

A resposta correta é:

Domain

QUESTÃO 3

Correto

Atingiu 1,00 de 1,00

Por que é recomendável utilizar o atributo HttpOnly em cookies que carregam identificadores de sessão?

Escolha uma opção:

- a. Evitar ataques CSRF
- b. Evitar a obtenção do identificador de sessão por meio de um XSS. ✓
- c. Decifrar o cookie somente quando for manipulado por scripts.
- d. Proteger o identificador de sessão em trânsito.
- e. Proteger a aplicação contra clickjacking.

Sua resposta está correta.

Para se prevenir de ataques cross-site scripting (XSS) os cookies marcados com HttpOnly são inacessíveis para a API JavaScript local Document.* podendo, apenas, ser enviados ao servidor.

A resposta correta é: Evitar a obtenção do identificador de sessão por meio de um XSS.

QUESTÃO 4

Incorreto

Atingiu 0,00 de 1,00

Um teste inicial e simples que pode ser usado para detectar se uma informação foi cifrada com um algoritmo clássico ou muito fraco consiste em:

Escolha uma opção:

- a. Tentar comprimir o texto cifrado. Se a taxa obtida for alta, o algoritmo é fraco. Se não, nada é possível afirmar.
- b. Tentar comprimir o texto cifrado. Se a taxa obtida for alta, o algoritmo é fraco. Se não, um algoritmo forte foi empregado. ✕
- c. Tentar comprimir o texto cifrado. Se ocorrer expansão, o algoritmo é fraco. De outro modo, é seguro.
- d. Verificar se o texto cifrado está codificado em BASE64.
- e. Executar busca exaustiva de chaves.

Sua resposta está incorreta.

O que o compactador de arquivos faz é simplesmente eliminar redundâncias no arquivo encontrando sequências de bits que podem ser simplificadas, ou seja, sempre que encontrar uma palavra contendo "aba" troque "aba" por "a" (esse é um exemplo hipotético apenas para ilustrar o processo).

Ao criptografar um arquivo cifrado se a taxa de compressão obtida for alta significa que o algoritmo tem baixa entropia portanto ele é fraco já que foi possível encontrar sequências de bits redundante a isso não se pode afirmar mais nada sobre o algoritmo.

A resposta correta é: Tentar comprimir o texto cifrado. Se a taxa obtida for alta, o algoritmo é fraco. Se não, nada é possível afirmar.

QUESTÃO 5

Correto

Atingiu 1,00 de 1,00

Quando Carlos navega na Internet com o uso do protocolo HTTPS é comum aparecer em seu browser, na barra de endereços, o ícone de um cadeado ao lado da URL. Considerando esse fato, atente às seguintes afirmações:

I. O cadeado informa que a comunicação entre o computador de Carlos e o site em questão está fazendo uso criptografado do protocolo seguro SSH.

II. A figura do cadeado procura assegurar que a troca de informações entre o navegador de Carlos e o site está protegida contra a leitura em casos de interceptação telemática.

III. O protocolo TLS, bastante usado nesses casos, é instalado somente no PC de Carlos e também em seu smartphone.

Está correto o que se afirma em

Escolha uma opção:

a. II apenas ✓

b. III apenas

c. II e III

d. I e II

Sua resposta está correta.

O protocolo utilizado em cliente e servidor é o SSL ou o TLS, e não o SSH. A figura do cadeado protege a comunicação em casos de interceptação. O protocolo TLS é configurado normalmente nos servidores Web apenas portanto o navegador do usuário apenas faz uso do protocolo.

A resposta correta é: II apenas

QUESTÃO 6

Correto

Atingiu 1,00 de 1,00

Quando se fala em vulnerabilidades considerando o fator humano, a falta de preparo para lidar com as ameaças recentes é um dos mais importantes tópicos em qualquer política de segurança corporativa. Nesse sentido, marque a alternativa que contenha ao menos um tipo de ataque em que os usuários precisam ser ludibriados a "clicarem" em arquivos e links suspeitos:

Escolha uma opção:

- a. Phishing ✓
- b. SQL Injection
- c. Buffer Overflow
- d. Remote Code Execution (RCE)

Sua resposta está correta.

O único tipo de ameaça/ataque em que os usuários precisam ter uma interação direta e voluntária é o ataque de Phishing. Os demais ataques não necessariamente precisam de uma interação direta do usuário porque o atacante tem a possibilidade de executá-los remotamente sem a intervenção humana.

A resposta correta é: Phishing

QUESTÃO 7

Correto

Atingiu 1,00 de 1,00

Para realizar um teste de invasão, o analista irá utilizar várias ferramentas como: navegador web, web spiders, varredores de portas, proxies de interceptação, fuzzers e varredores de vulnerabilidades. Qual destas ferramentas pode ser utilizada para alterar, em tempo real, o comando HTTP de um navegador antes deste comando ser enviado para ser processado por um servidor WEB no destino?

a. proxy de interceptação ✓

b. fuzzers

c. varredores de vulnerabilidades

d. web spiders

Sua resposta está correta.

Os proxies de interceptação permitem inspecionar requisições e respostas HTTP e alterá-las conforme desejado, em tempo real, antes de serem enviadas para o servidor.

Web spiders, também conhecido como web crawlers, têm por objetivo montar automaticamente o mapa da aplicação, visitando cada página disponível e realizando uma cópia local de cada recurso encontrado, para fins de análise posterior.

A técnica de fuzzing consiste em fornecer automaticamente valores para campos e parâmetros que aceitam dados de usuário, em uma aplicação, serviço ou protocolo, com o objetivo de descobrir v ıbilidades que possam ser exploradas.

Varredores de vulnerabilidades têm por objetivo encontrar, de maneira automatizada, o maior número possível de vulnerabilidades em um ativo.

A resposta correta é:
proxy de interceptação

QUESTÃO 8

Correto

Atingiu 1,00 de 1,00

Você está testando um aplicativo da Web como parte de sua campanha do Pentest. Enquanto você realiza o ataca, insere o seguinte código no formulário de pesquisa do seu destino::

//////////////////////////

<script> alert ("Muito Vulnerável!")</script>

//////////////////////////

Por fim, você clicou no botão de pesquisa e uma caixa pop-up aparece no seu navegador com o "Muito Vulnerável!".

Selecione a resposta que descreve o ataque que você realizou:

Escolha uma opção:

a. SQL Injection

b. Buffer overflow

c. DoS

d. XSS ✓

Sua resposta está correta.

Cross-Site Scripting (XSS) permite que invasores injetem scripts do lado do cliente em páginas da web, neste caso, JavaScript. As injeções de SQL consistem em inserir comandos SQL maliciosos em um campo de entrada para execução, isso não era um comando SQL. O estouro de buffer ocorre quando um programa ultrapassa o limite do buffer e sobrescreve a memória adjacente local enquanto grava dados em um buffer. O DoS é um ataque de disponibilidade.

A resposta correta é: XSS

QUESTÃO 9

Correto

Atingiu 1,00 de 1,00

A realização de um teste de invasão tem como objetivo verificar a segurança de um ambiente, plataforma ou sistema, por meio da simulação de ataques reais explorando as vulnerabilidades encontradas. Para realização destes testes podemos utilizar diversas abordagens que, em resumo, implicam na quantidade de informações que a organização repassa ao analista responsável por executar o teste. Em qual tipo de teste um invasor recebe informações parciais sobre o ambiente da organização?

a. Caixa Preta
b. Caixa Branca
c. Caixa Verde
d. Caixa Cinza ✓

Sua resposta está correta.

No teste "Caixa Branca" o analista responsável pelo pentest recebe da empresa todas as informações essenciais para realizar o trabalho, como topografia, senhas, IPs, logins e todos os outros dados que dizem respeito à rede, servidores, estrutura, potenciais medidas de segurança, firewalls etc.

No teste "Caixa Preta" o analista não recebe nenhuma informação da empresa da, é bem comum que a equipe de não seja avisada que o teste irá acontecer.

No teste "Caixa Cinza" o analista recebe informações parciais sobre o ambiente, não tão detalhada como o "Caixa Branca", porém informações consideradas mínimas sobre o ambiente.

Não existe teste Caixa Verde.

A resposta correta é:
Caixa Cinza

QUESTÃO 10

Correto

Atingiu 1,00 de 1,00

Um modelo de controle de acesso é um arcabouço responsável por definir quais recursos podem ser acessados pelas diversas entidades do sistema. No modelo de controle de acesso discricionário (DAC), compete ao usuário:

a. seguir as permissões definidas por um administrador da rede.

b. associar-se a um perfil de acesso antes de tentar acessar qualquer arquivo.

c. estabelecer horários e locais onde os arquivos podem ser acessados.

d. Estabelecer as permissões nos arquivos que for dono. ✓

Sua resposta está correta.

Um modelo de controle de acesso é um arcabouço responsável por definir quais recursos podem ser acessados pelas diversas entidades do sistema. Os tipos mais comuns de controle de acesso são:

- Controle de acesso discricionário (DAC): o usuário é proprietário do recurso e compete a ele atribuir a permissão que desejar.
- Controle de acesso mandatório (MAC): as permissões são atribuídas por um administrador central

Controle de acesso baseado em papéis (RBAC): as permissões dos objetos são atribuídas a uma função e os usuários, então, associados a esta função.

A resposta correta é:
Estabelecer as permissões nos arquivos que for dono.

◄ Questionário de Fixação 10