5ª. Lista de Exercícios de Segurança de Sistemas
Prof. Manoel Ribeiro

1) A Open Web Application Security Project (OWASP) mantém um documento que lista os 10 ataques a segurança de aplicações web mais críticos. Dentre esses ataques descritos na versão mais recente do documento estão:

   I. Injection Flaws.
   II. Cross-site Scripting (XSS).
   III. Malicious File Execution.
   IV. Cross-site Request Forgery (CSRF).

   Está correto o que se afirma em
   a) I, II e IV, apenas.
   b) I, II, III e IV.
   c) II e III, apenas.
   d) II, III e IV, apenas.
   e) I e II, apenas.

2) Um ataque de XSS (cross site script) não permite a injeção de código em formulários HTTP.

   a) Errado
   b) Certo

3) A melhor forma para descobrir se uma aplicação está vulnerável a este tipo de ataque é verificar se todos os usos dos interpretadores separam claramente os dados não confiáveis do comando ou consulta. Para chamadas em linguagem estruturada de consulta, isso significa utilizar variáveis de ligação em todas as instruções preparadas e procedimentos armazenados, e evitar consultas dinâmicas.

   O tipo de ataque citado no texto é conhecido como
   A Key Logging.
   B Buffer overflow.
   C SQL Injection.
   D Cross-Site Scripting (XSS).
   E Cross-Site Request Forgery (CSRF).

4) A melhor maneira de evitar ataques de Cross-Site Scripting (XSS) em aplicações web é
   A validar adequadamente as entradas de dados dos usuários.
   B criar sessões nos processos de autenticação de usuários.
   C utilizar linguagens de programação orientadas a objeto para garantir o encapsulamento dos dados.
   D criptografar dados nas transações entre cliente e servidor.
   E utilizar, nos formulários, nomes de variáveis diferentes dos nomes dos campos da tabela do banco de dados.

5) Em um ataque em que o Cracker injeta códigos JavaScript em um campo texto de uma página Web já existente e este JavaScript é apresentado para outros usuários, este JavaScript poderia, por exemplo, simular a página de login do site, capturar os valores digitados e enviá-los a um site que os armazene. Este ataque é denominado
   A XSS.
   BSpyware de Web.
   CBackdoor JavaScript.
   D Cross-site Request Forgery.
   E CSRF de Java.

6) O Cross-Site Scripting (XSS)
   I. executa no cliente web um código malicioso que, necessariamente, está armazenado no servidor acessado;
   II. explora vulnerabilidades relacionadas à falta de validação dos dados de entrada do usuário em uma página web;
   III. serve de base técnica para a realização de ataques como o SQL Injection e Script Injection.

   Está correto o que se afirma em
   A I, apenas.
   B I e II, apenas.
   C I e III, apenas.
   D II e III, apenas.
   E I, II e III.

7) O ataque cross-site scripting, executado quando um servidor web inclui, nos dados de uma página web enviada para um usuário legítimo, um conjunto de dados que tenham sido previamente recebidos de um usuário malicioso, permite que se roube de um usuário legítimo senhas, identificadores de sessões e cookies.
   C Certo
   E Errado

8) Considere o exemplo escrito em HTML:

```
<ul>
 <li><a href="message.cgi?say=Ola">Ola</a>
 <li><a href="message.cgi?say=Bem Vindo">Bem Vindo</a>
</ul>
```

   Se a mensagem for simplesmente exibida ao usuário sem efetuar a validação (escaping), a seguinte URL poderia ser criada:

```
http://example.com/message.cgi?say=%3Cscript%3Ealert%28%27Oh%20no%21%27%29%3C/script%3E
```

   Causando um problema de vulnerabilidade conhecido como
   A SQL Injection.
   B buffer overfun.
   C buffer overflow.
   D cross-site scripting attack.
   E DDoS.