

Top 10 OWASP

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

BeeBox [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Applications Places System

bee@bee-box: ~

File Edit View Terminal Tabs Help

Database changed

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

| id | login | password | activated | reset_code | admin | email | secret | activation_code |
|----|--------|--|-----------|------------|-------|--------------------------|-------------------------------------|---|
| 1 | A.I.M. | 6885858486f31043e5839c735d99457f045affd0 | 1 | NULL | 1 | bwapp-aim@mailinator.com | A.I.M. or Authentication Is Missing | NULL |
| 2 | bee | 6885858486f31043e5839c735d99457f045affd0 | 1 | NULL | 1 | bwapp-bee@mailinator.com | Any bugs? | NULL |
| 3 | geeks | 6885858486f31043e5839c735d99457f045affd0 | 1 | NULL | 1 | geeks@test.com | secret test | 3a9088512a3d2132c537ffail13261b1d10b8cb34 |

3 rows in set (0.00 sec)

mysql>

bwAPP covers all major known web vulnerabilities, including all risks from the OWASP Top 10 project!
It is for security-testing and educational purposes only.

Which bug do you want to hack today? :

bwAPP v2.2

- / A1 - Injection
- HTML Injection - Reflected (GET)
- HTML Injection - Reflected (POST)
- HTML Injection - Reflected (Current URL)
- HTML Injection - Stored (Blog)
- iFrame Injection
- LDAP Injection (Search)
- Mail Header Injection (SMTP)

Hack

bwAPP is licensed under © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet containing all solutions

Done

bee@bee-box: ~ | bwAPP - Portal - Mozi... | bee@bee-box: ~

Applications Places System

bwAPP - Insecure DOR - Mozilla Firefox

File Edit View History Bookmarks Tools Help

bee@bee-box: ~

File Edit View Terminal Tabs Help

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

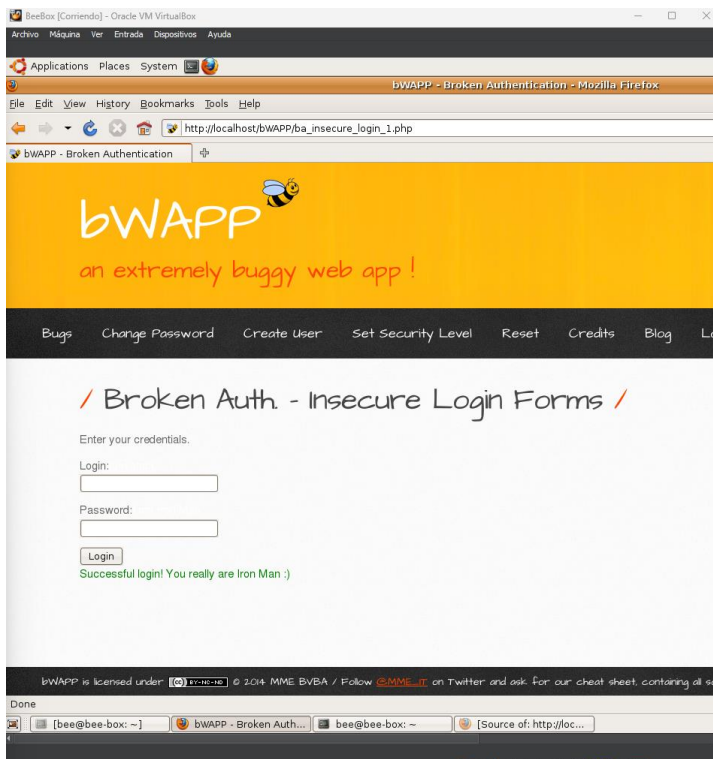
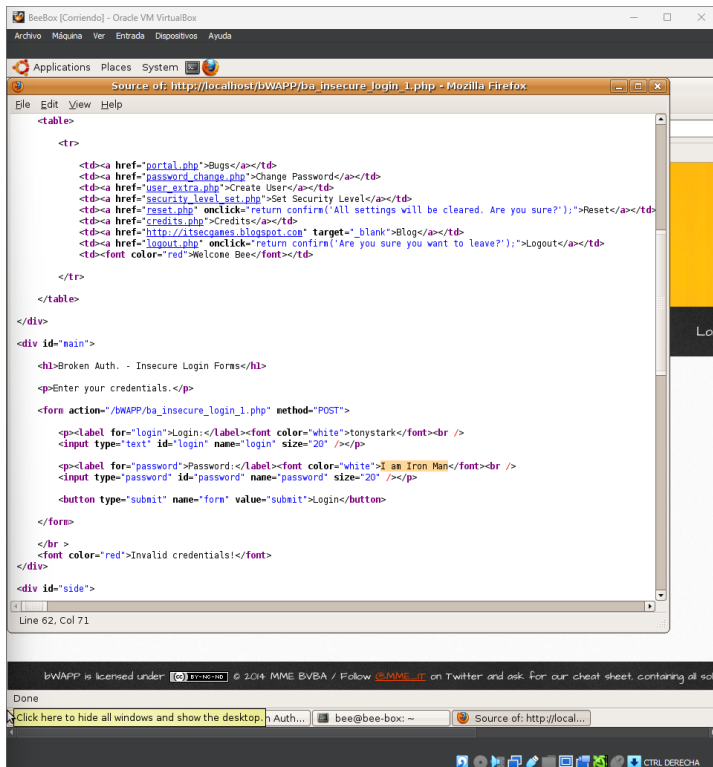
| id | login | password | activated | reset_code | admin | email | secret | activation_code |
|----|--------|--|-----------|------------|-------|--------------------------|-------------------------------------|---|
| 1 | A.I.M. | 6885858486f31043e5839c735d99457f045affd0 | 1 | NULL | 1 | bwapp-aim@mailinator.com | A.I.M. or Authentication Is Missing | NULL |
| 2 | bee | 6885858486f31043e5839c735d99457f045affd0 | 1 | NULL | 1 | bwapp-bee@mailinator.com | Any bugs? | NULL |
| 3 | geeks | 6885858486f31043e5839c735d99457f045affd0 | 1 | NULL | 1 | geeks@test.com | Hello geeks | 3a9088512a3d2132c537ffail13261b1d10b8cb34 |

3 rows in set (0.00 sec)

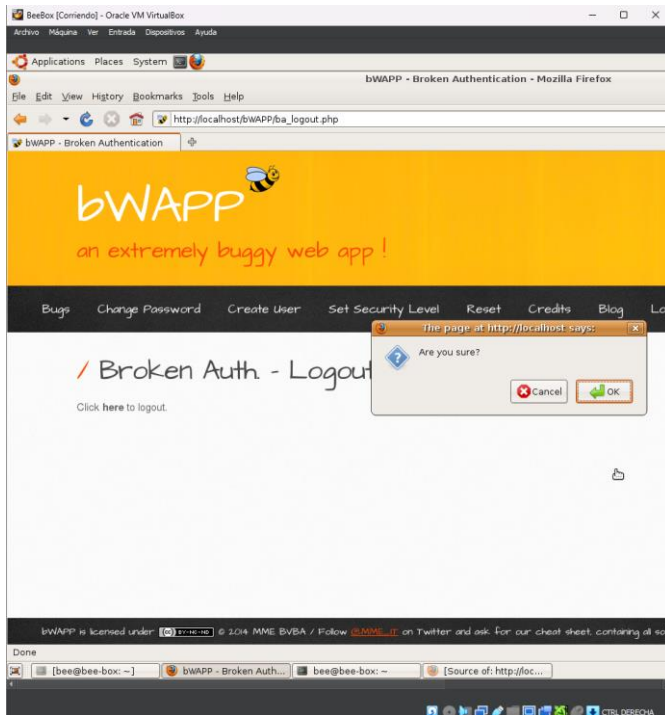
mysql>

Top 10 OWASP

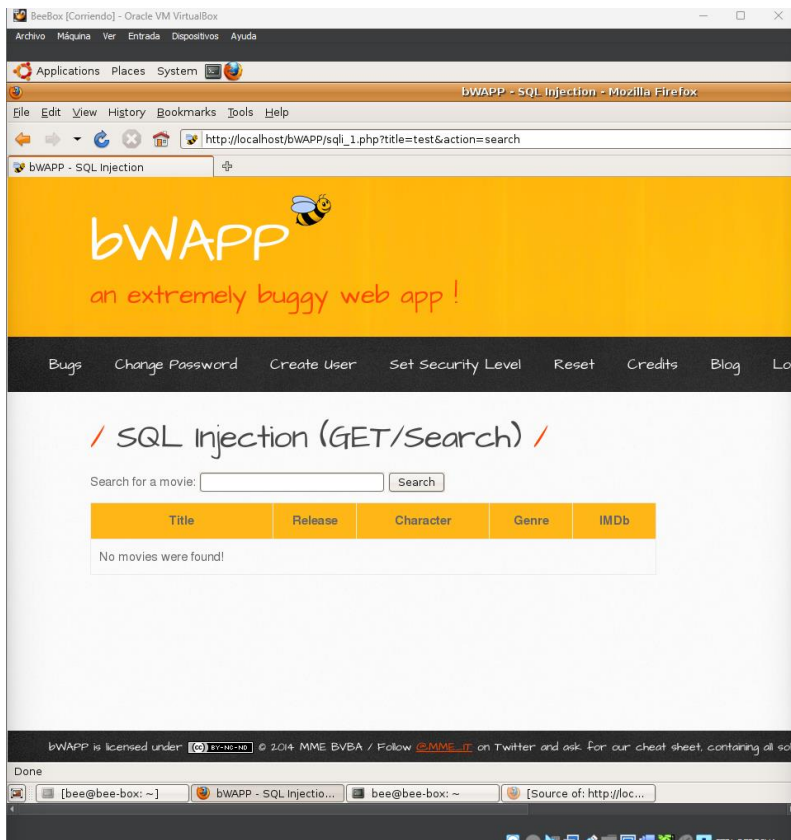
2.- Identification & authentication failures - Broken Authentication



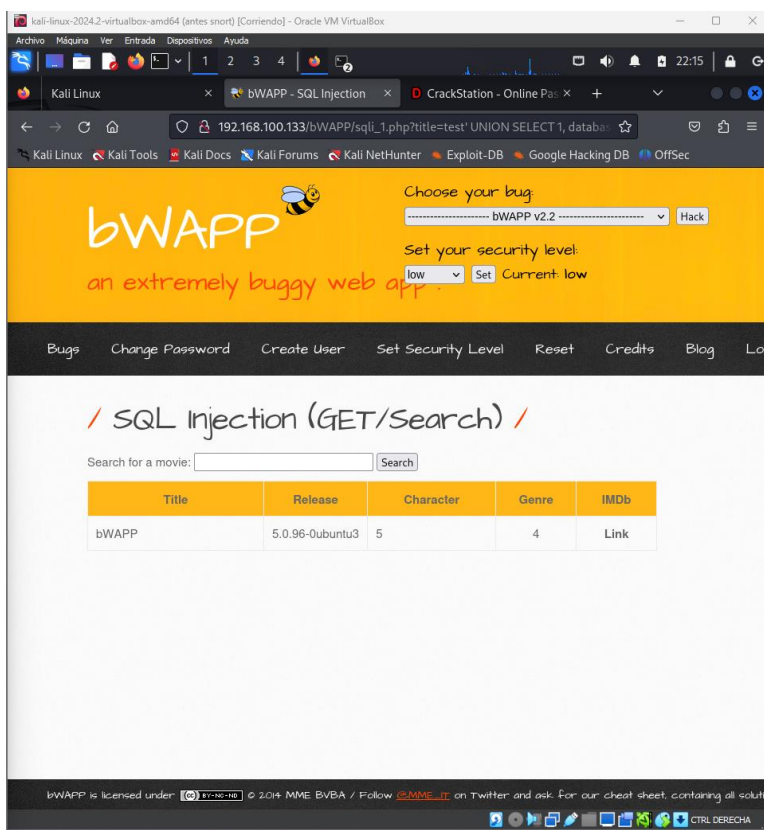
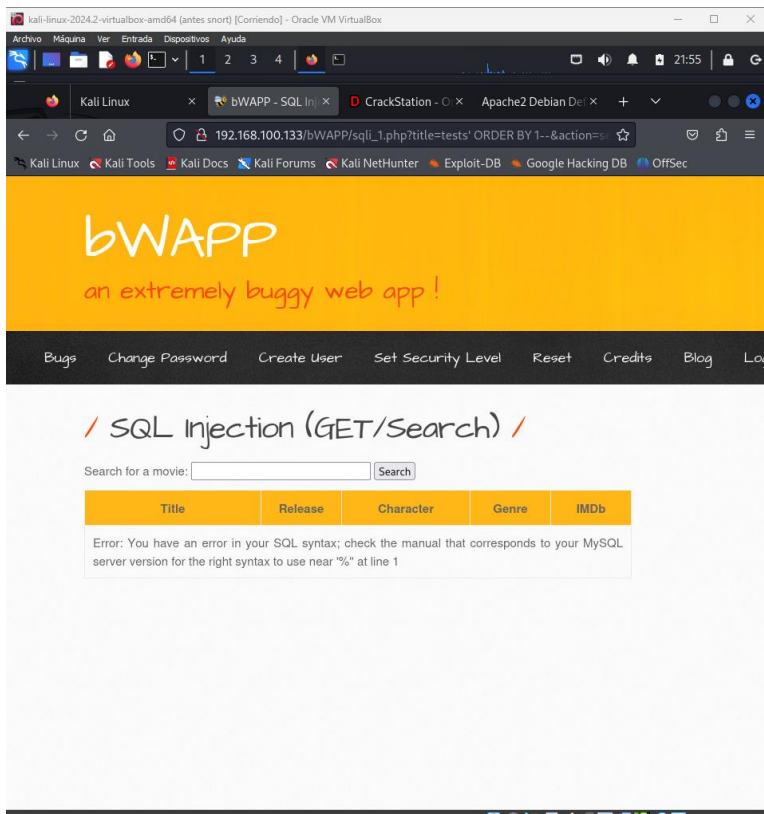
Top 10 OWASP



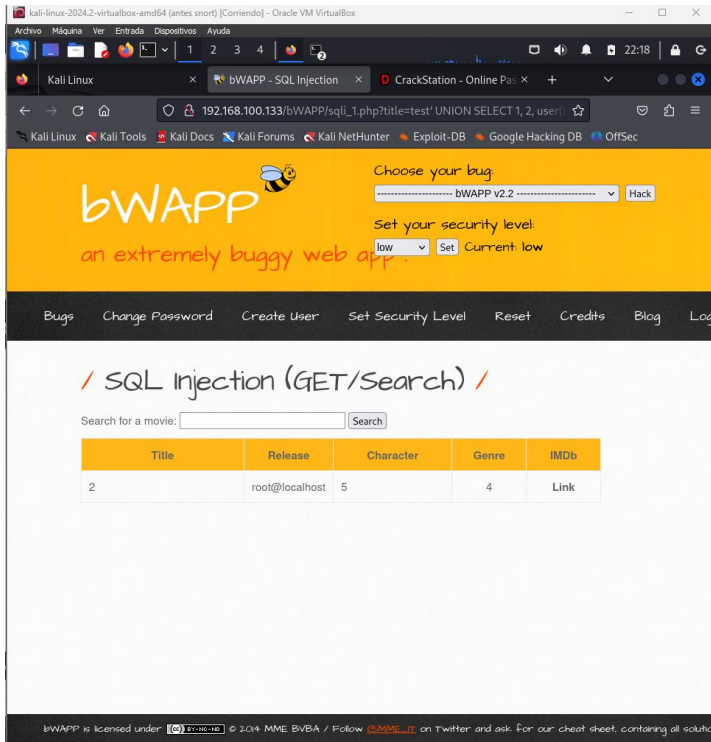
3.- Injection - SQL injection



Top 10 OWASP



Top 10 OWASP



Choose your bug
bWAPP v2.2 Hack

Set your security level:
low Set Current: low

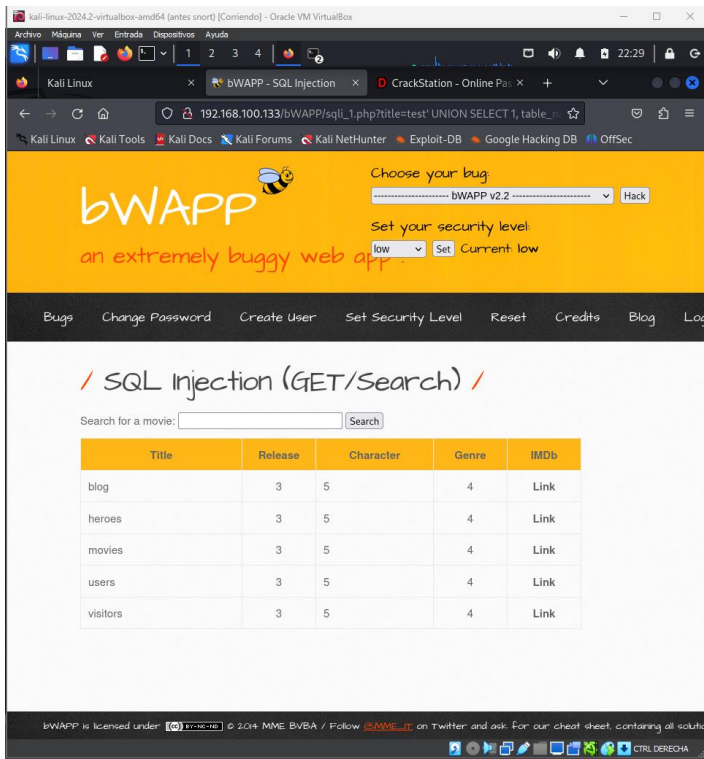
Bugs Change Password Create User Set Security Level Reset Credits Blog Log

/ SQL Injection (GET/Search) /

Search for a movie: Search

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

bWAPP is licensed under © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions



Choose your bug
bWAPP v2.2 Hack

Set your security level:
low Set Current: low

Bugs Change Password Create User Set Security Level Reset Credits Blog Log

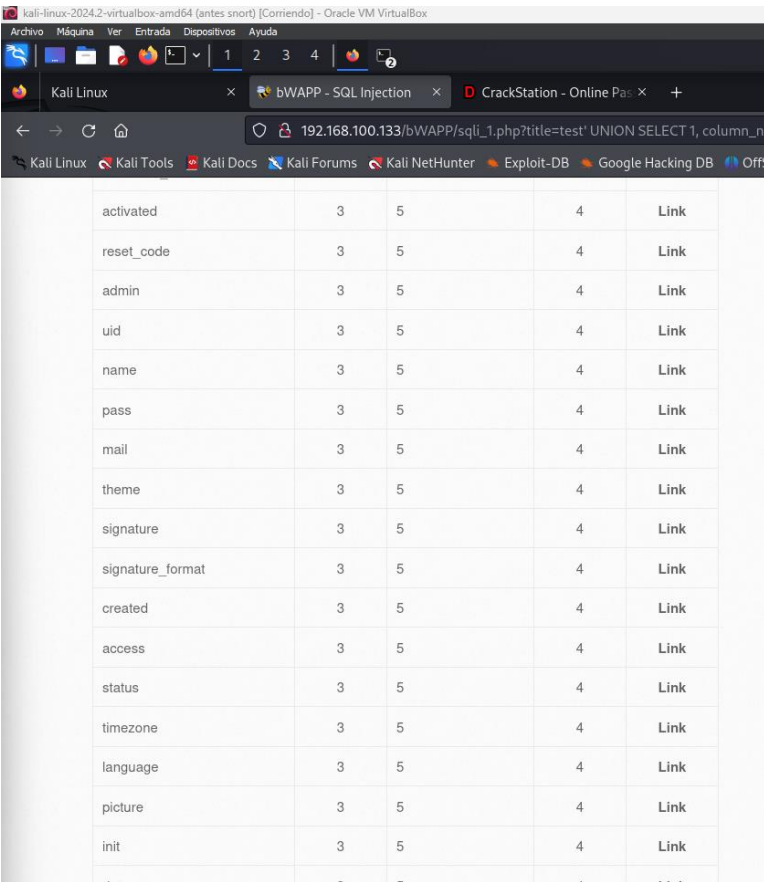
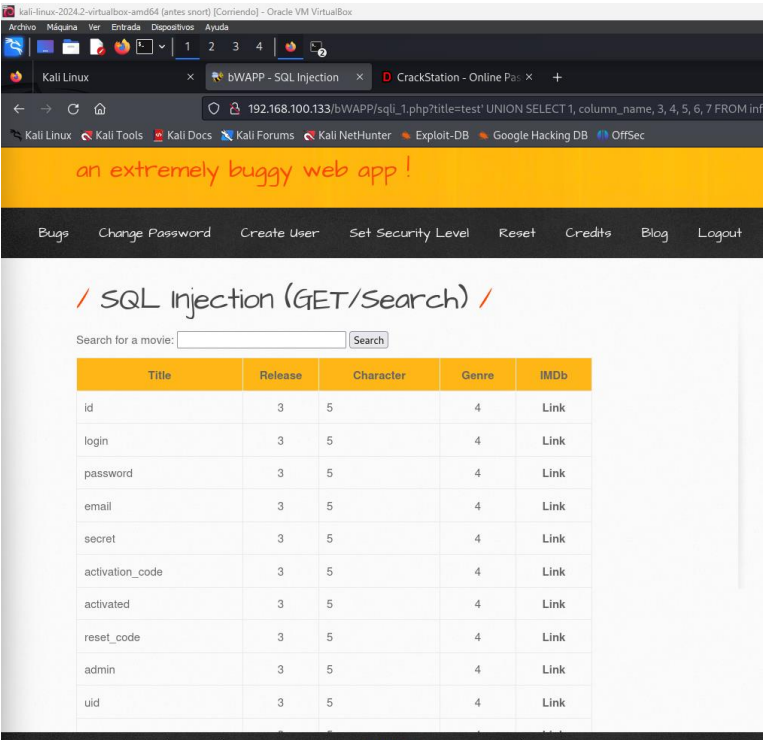
/ SQL Injection (GET/Search) /

Search for a movie: Search

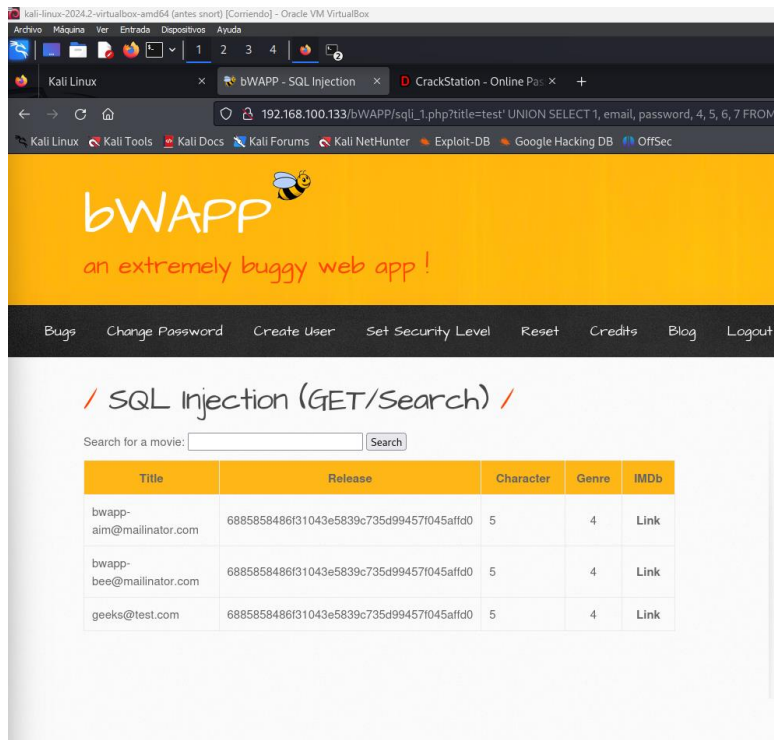
| Title | Release | Character | Genre | IMDb |
|----------|---------|-----------|-------|------|
| blog | 3 | 5 | 4 | Link |
| heroes | 3 | 5 | 4 | Link |
| movies | 3 | 5 | 4 | Link |
| users | 3 | 5 | 4 | Link |
| visitors | 3 | 5 | 4 | Link |

bWAPP is licensed under © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions

Top 10 OWASP

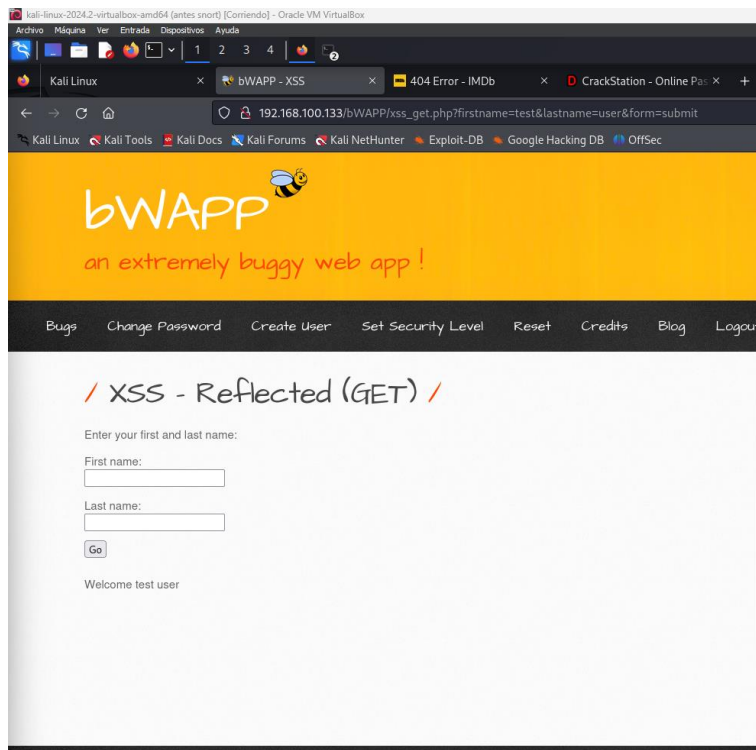


Top 10 OWASP

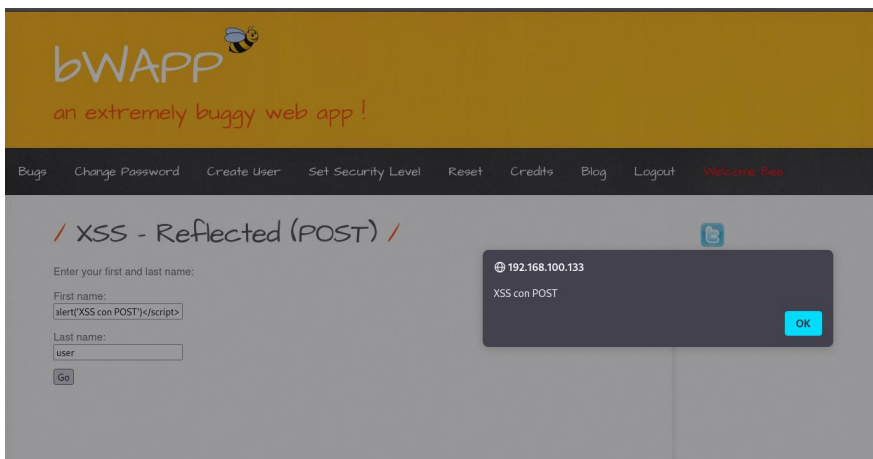
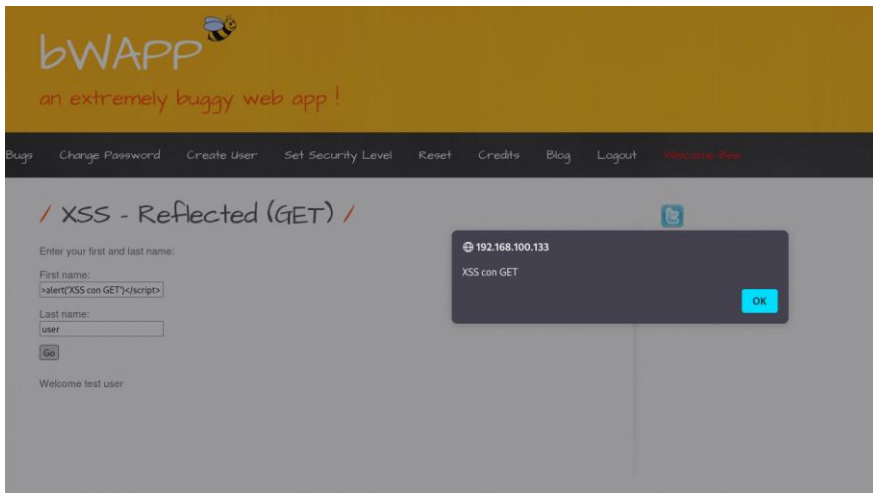


4.- Injection - Cross-site scripting (XSS) Reflected GET and POST

Cross-Site Scripting (XSS) Reflected (GET)

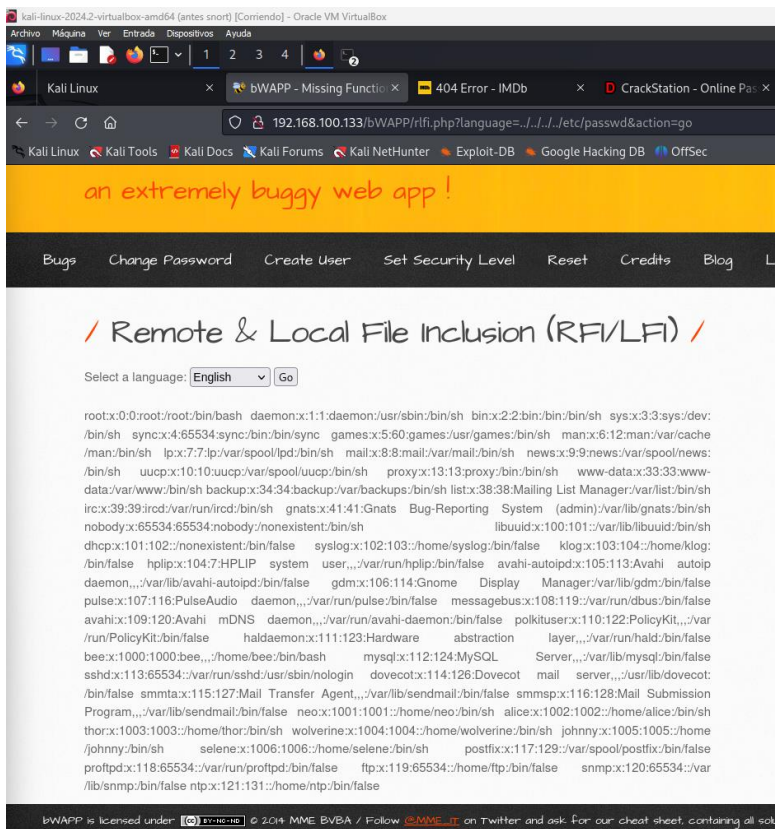
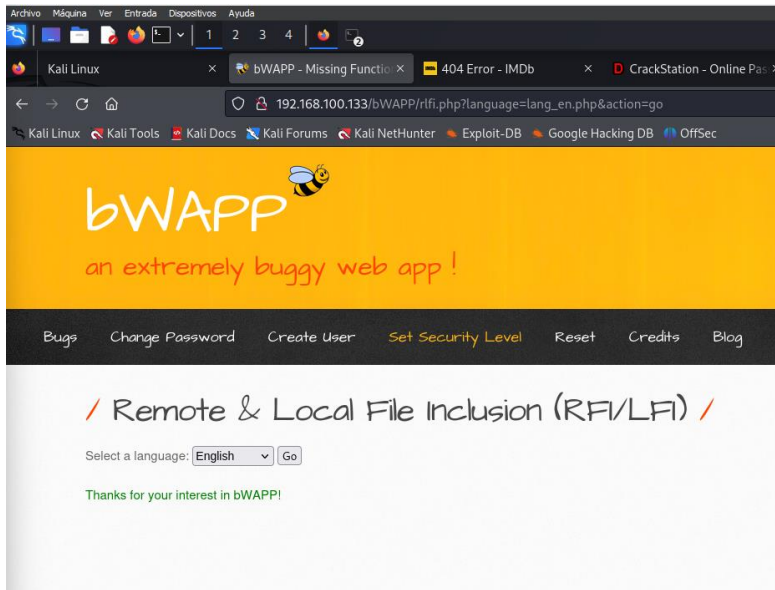


Top 10 OWASP

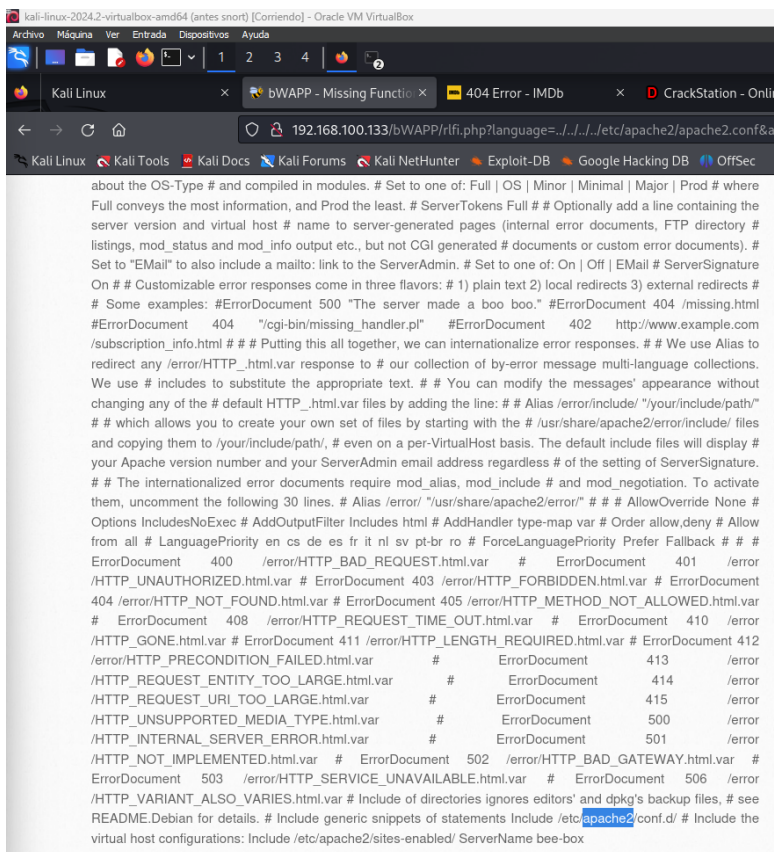
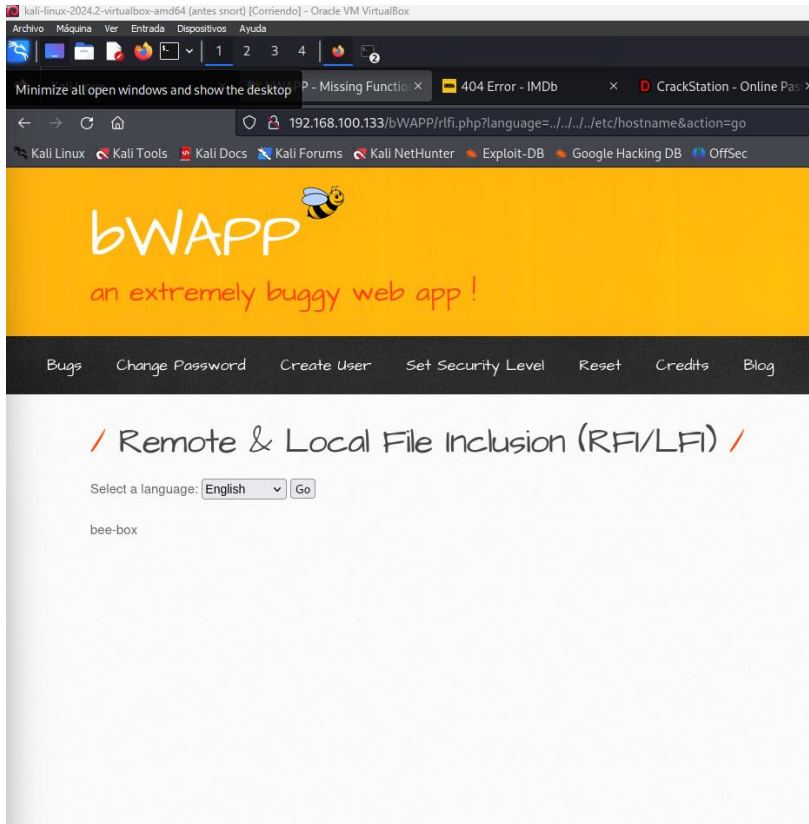


Top 10 OWASP

5.- Security Misconfiguration - Local File Inclusion (LFI)

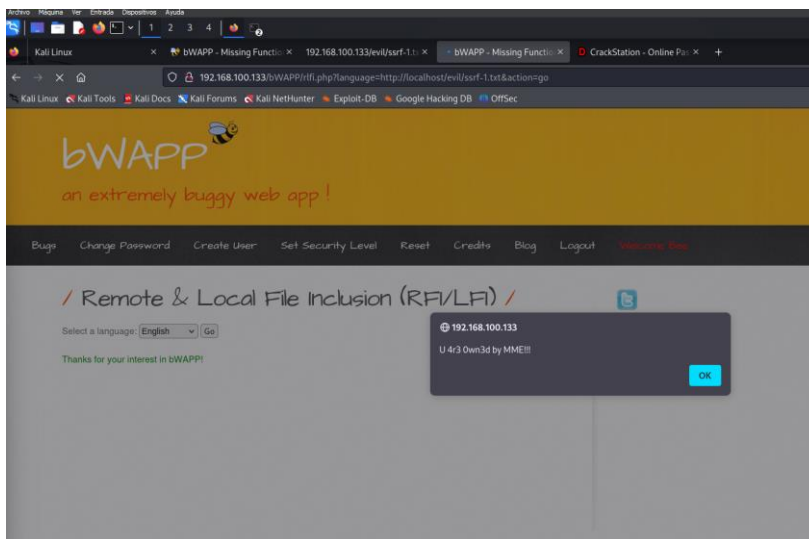
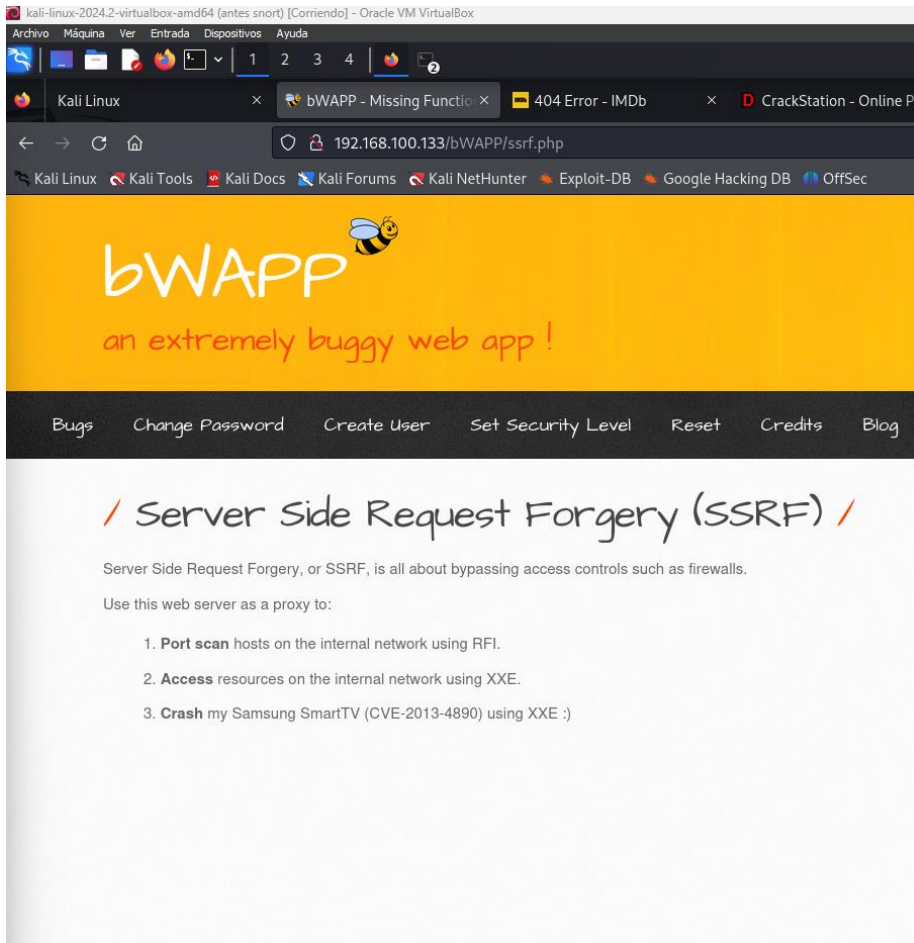


Top 10 OWASP



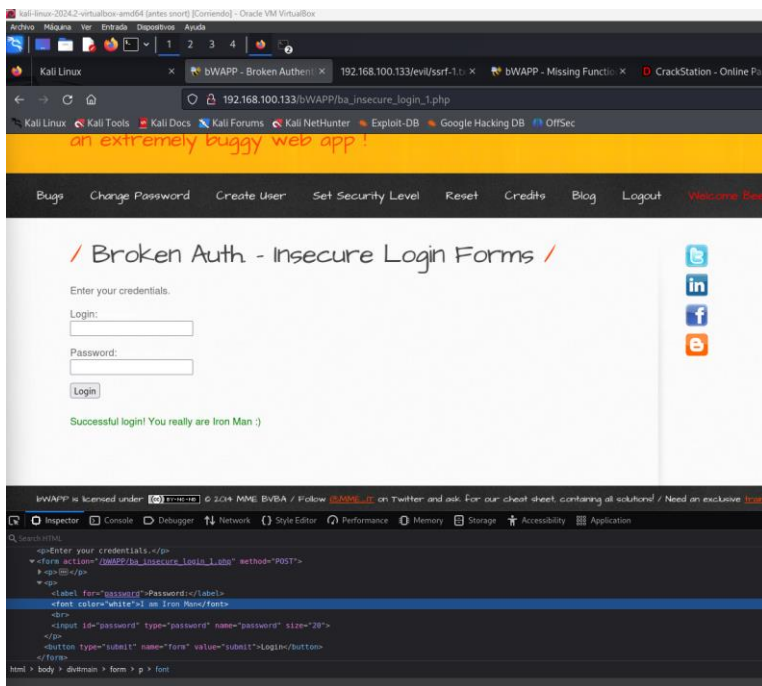
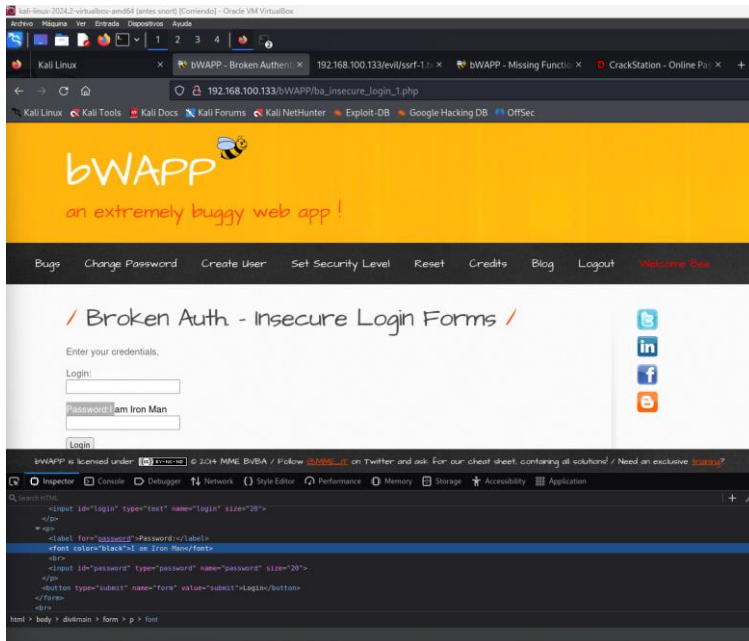
Top 10 OWASP

6.- Server side request forgery - port scan



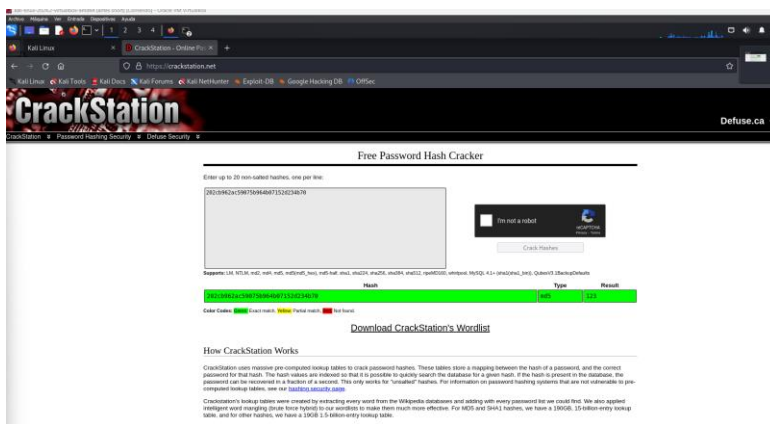
Top 10 OWASP

7.- Security Logging and Monitoring Failures



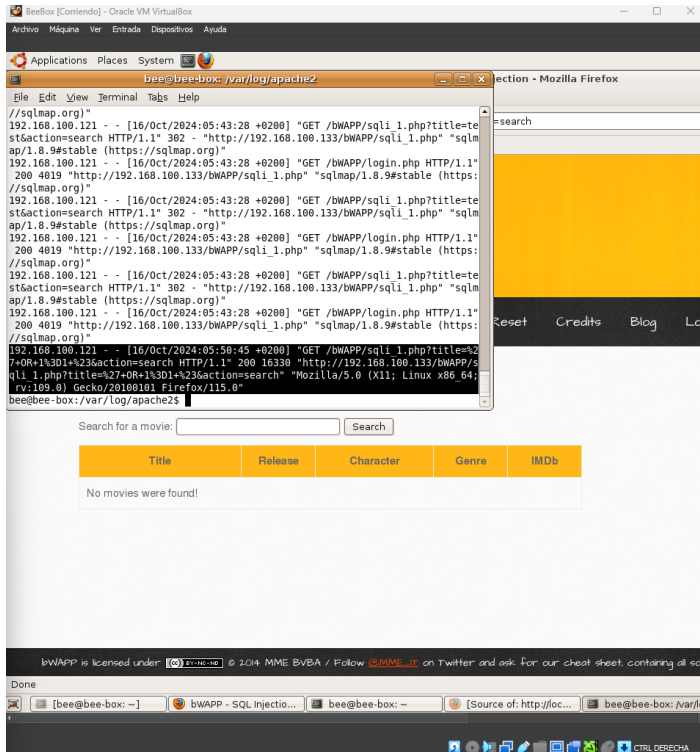
Top 10 OWASP

8.- Fallos de criptografía - Hashing Débil de Contraseñas



Top 10 OWASP

9.- Security Logging and Monitoring Failures



10.- Vulnerable and outdated components

