

# ELABORATO S6 – L2

## Sfruttamento delle vulnerabilità XSS Reflected e SQL Injection su DVWA

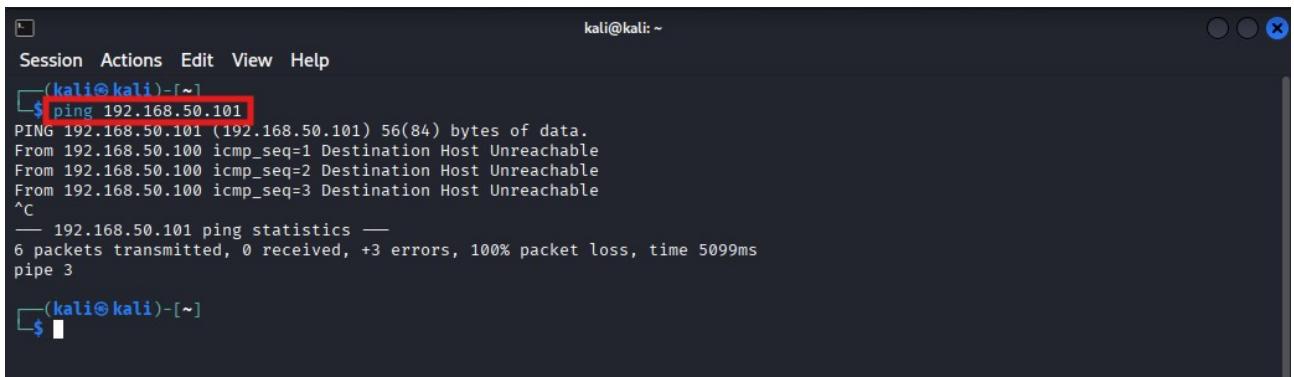
### Introduzione

Il presente elaborato descrive la configurazione di un laboratorio di test e lo sfruttamento controllato delle vulnerabilità XSS Reflected e SQL Injection non blind presenti nella Damn Vulnerable Web Application (DVWA).

Le attività sono state svolte dalla macchina Kali Linux verso la macchina target, applicando esclusivamente le tecniche illustrate.

### 1 – Ping Metasploitable

Verifica della raggiungibilità della macchina target DVWA dalla macchina attaccante Kali Linux tramite ping.

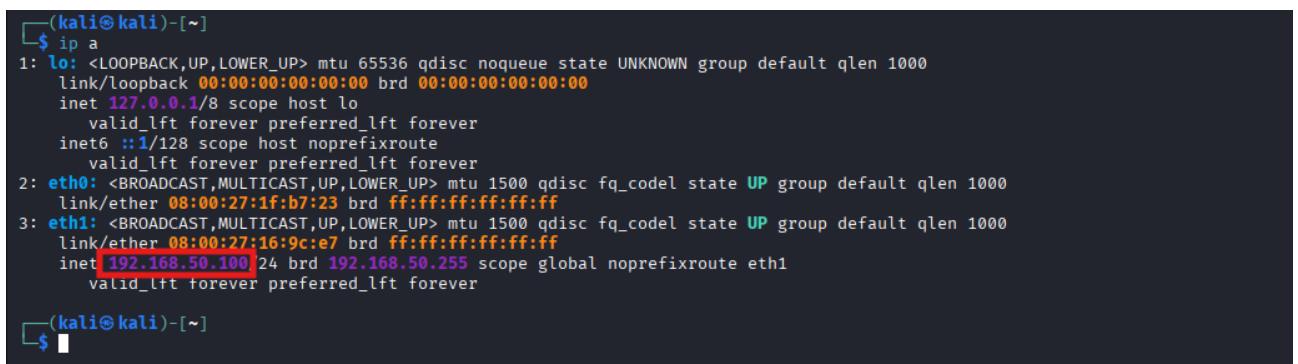


```
(kali㉿kali)-[~]
$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
From 192.168.50.100 icmp_seq=1 Destination Host Unreachable
From 192.168.50.100 icmp_seq=2 Destination Host Unreachable
From 192.168.50.100 icmp_seq=3 Destination Host Unreachable
^C
--- 192.168.50.101 ping statistics ---
6 packets transmitted, 0 received, +3 errors, 100% packet loss, time 5099ms
pipe 3

(kali㉿kali)-[~]
```

### 2 – IP Kali

Identificazione dell’indirizzo IP assegnato alla macchina Kali Linux all’interno del laboratorio.

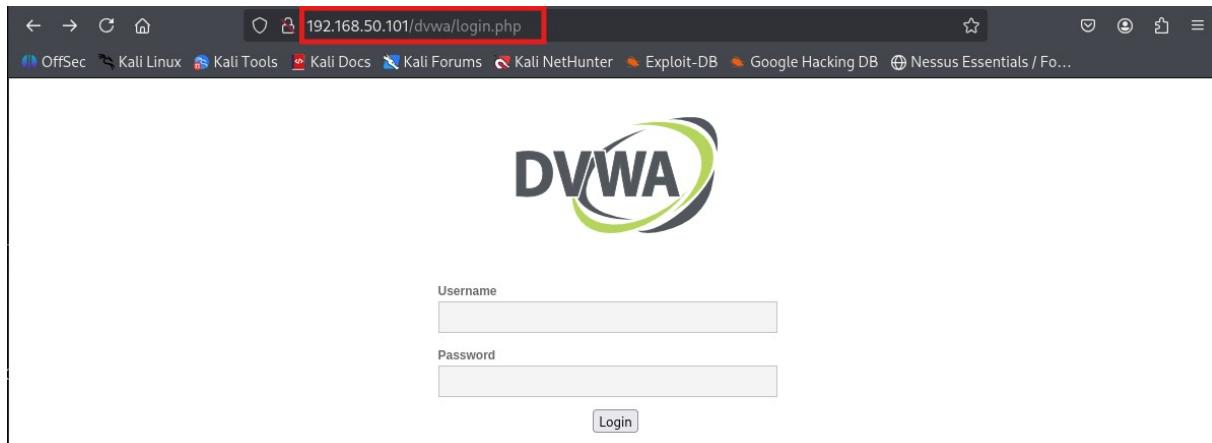


```
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:1f:b7:23 brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:16:9c:e7 brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.100/24 brd 192.168.50.255 scope global noprefixroute eth1
        valid_lft forever preferred_lft forever

(kali㉿kali)-[~]
```

### 3 – Accesso a DVWA

Accesso all'applicazione DVWA tramite browser Firefox dalla macchina Kali Linux.



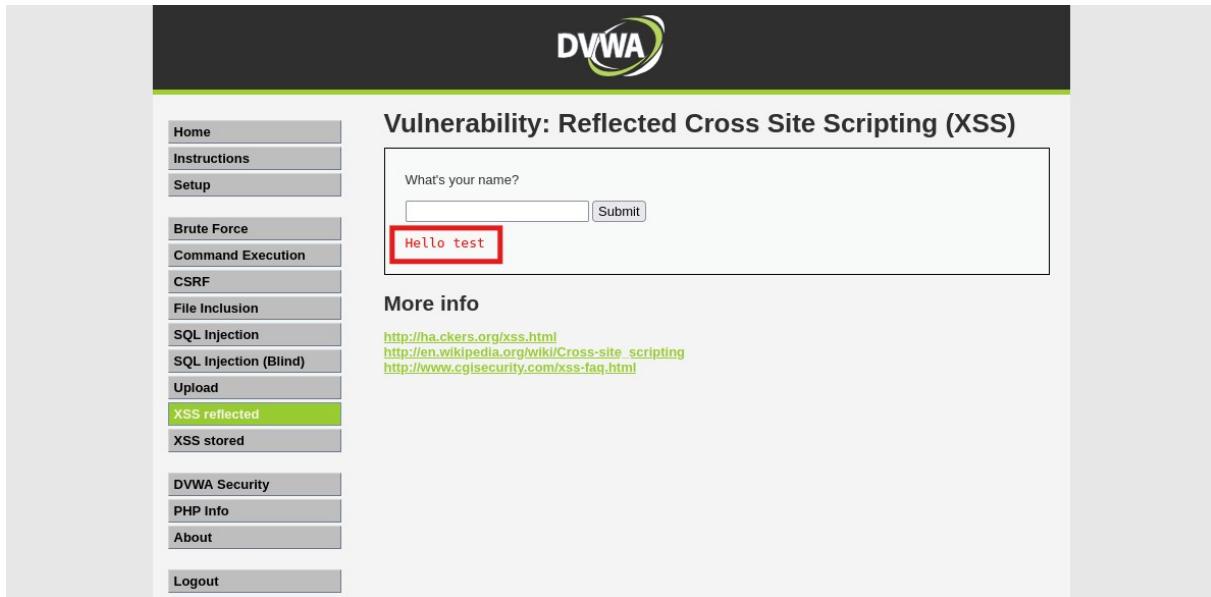
### 4 – Security Level LOW

Impostazione del livello di sicurezza di DVWA su LOW per consentire lo sfruttamento delle vulnerabilità.

A screenshot of the DVWA security configuration page. The DVWA logo is at the top. On the left is a sidebar with various links: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security (which is highlighted in green), PHP Info, About, and Logout. The main content area has a heading 'DVWA Security' with a lock icon. It says 'Script Security' and 'Security Level is currently low.' Below that, it says 'The security level changes the vulnerability level of DVWA.' There is a dropdown menu set to 'low' with a 'Submit' button next to it, both of which are enclosed in a red box. The 'low' selection is also highlighted with a red box. The 'PHPIDS' section follows, with a note about PHPIDS being a security layer for PHP-based web applications, and a link to enable it. There is another red box around the message 'Security level set to low' in the PHPIDS section.

## 5 – XSS Reflected (test riflessione input)

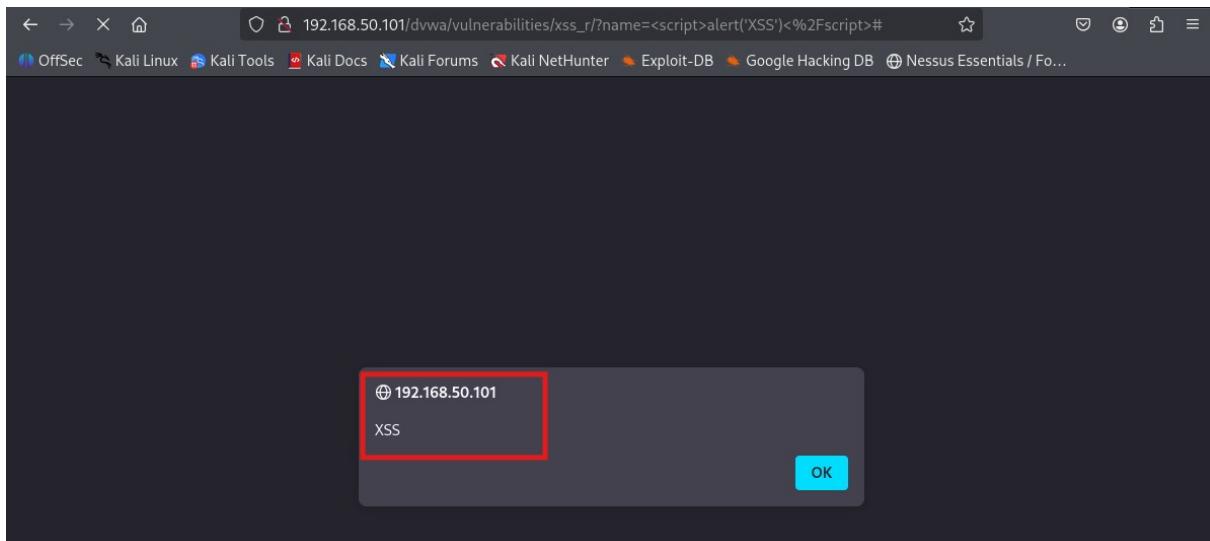
Individuazione del reflection point tramite inserimento di input utente riflesso nell'output della pagina.



The screenshot shows the DVWA application interface. On the left is a sidebar menu with various security test categories: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected (which is highlighted in green), XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area has a title "Vulnerability: Reflected Cross Site Scripting (XSS)". Below the title is a form field labeled "What's your name?" containing the value "Hello test". A red box highlights the "Hello test" text. Below the form is a section titled "More info" with three links: <http://ha.ckers.org/xss.html>, [http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting), and <http://www.cgisecurity.com/xss-faq.html>.

## 6 – JavaScript (PoC XSS riflesso)

Esecuzione di codice JavaScript riflesso nel browser che conferma la presenza di una vulnerabilità XSS Reflected.



The screenshot shows a browser window with the URL "192.168.50.101/dvwa/vulnerabilities/xss\_r/?name=<script>alert('XSS')<%2Fscript>#". The browser toolbar includes icons for back, forward, search, and refresh. Below the toolbar is a navigation bar with links to OffSec, Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and Nessus Essentials / Fo... The main content area displays a modal dialog box. The dialog has a red border and contains the text "192.168.50.101" and "XSS". A blue "OK" button is visible at the bottom right of the dialog.

## 7 – SQL Injection (baseline)

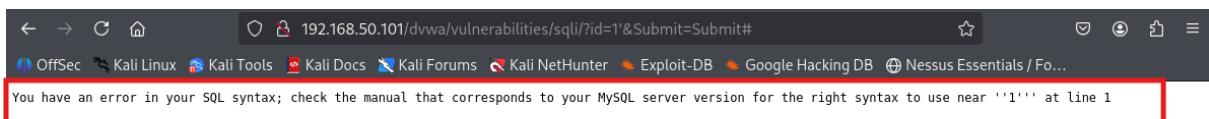
Comportamento normale dell'applicazione con input valido, utilizzato come baseline di confronto.



The screenshot shows the DVWA application interface. The main title is "Vulnerability: SQL Injection". On the left, there's a sidebar menu with various security modules: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection (highlighted in green), SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The "SQL Injection" item is currently selected. The main content area has a form labeled "User ID:" with a red box around the output field showing "ID: 1 First name: admin Surname: admin". Below the form, there's a "More info" section with three links: <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>, [http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection), and <http://www.unixwiz.net/tchtips/sql-injection.html>.

## 8 – SQL Injection (test terminatore)

Identificazione dell'injection point tramite inserimento di un terminatore che provoca un errore SQL.



The screenshot shows a browser window with the URL "192.168.50.101/dvwa/vulnerabilities/sqli/?id=1'&Submit=Submit#". The status bar indicates the page is from Kali Linux. The main content area displays an error message: "You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''1'' at line 1". This error is highlighted with a red box.

## 9 – SQL Injection Boolean-Based (non blind)

Alterazione della logica della query SQL tramite condizione booleana che produce output visibile, confermando una SQL Injection non blind.

The screenshot shows the DVWA application interface. On the left is a sidebar with various vulnerability categories: Home, Instructions, Setup, Bruteforce, Command Execution, CSRF, File Inclusion, SQL Injection (the current category, highlighted in green), SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area has a title 'Vulnerability: SQL Injection'. Below it, there's a form with a 'User ID:' label and a text input field containing '1 OR 1=1'. A 'Submit' button is next to it. To the right of the input field, the application's response is displayed in a red-bordered box:  
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

## Conclusione

L'esercizio ha dimostrato come un'applicazione web con adeguate misconfigurazioni di sicurezza (**Configurazione errata o non sicura di un sistema, applicazione o servizio, che introduce vulnerabilità sfruttabili**) sia vulnerabile ad attacchi XSS e SQL Injection.

**I test effettuati hanno confermato** l'esecuzione di codice riflesso e la manipolazione della logica delle query SQL con output visibile, evidenziando **l'importanza di una corretta validazione degli input e di misure di sicurezza adeguate**.