

# *XSS reflected e SQL injection*



# Avvio Meta

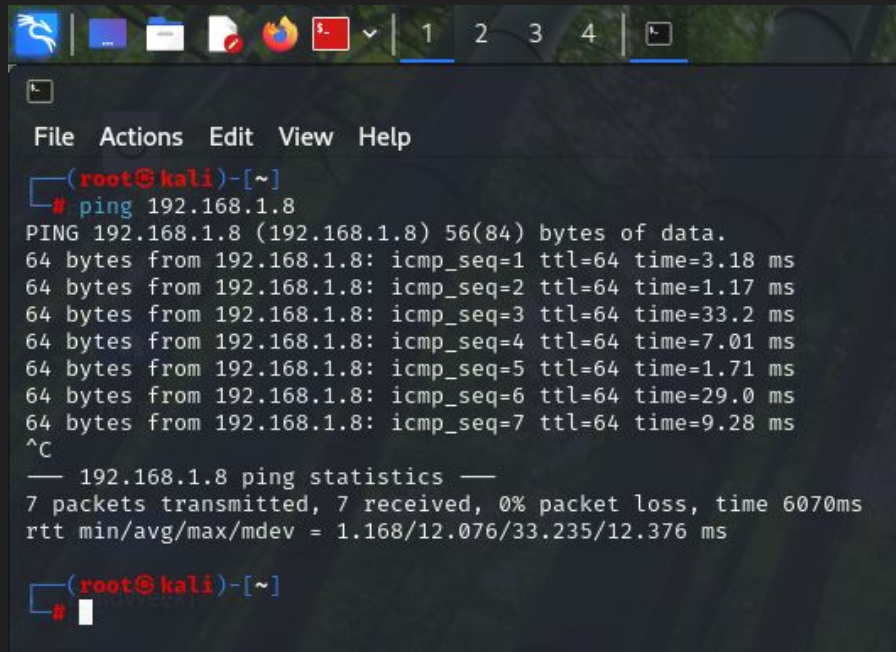
```
Metasploitable2 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:4a:ad:67
          inet addr:192.168.1.8  Bcast:192.168.1.255  Mask:255.255.255.
          inet6 addr: fe80::a00:27ff:fe4a:ad67/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:99 errors:0 dropped:0 overruns:0 frame:0
          TX packets:101 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9928 (9.6 KB)  TX bytes:10104 (9.8 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:33 errors:0 dropped:0 overruns:0 frame:0
          TX packets:33 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:14613 (14.2 KB)  TX bytes:14613 (14.2 KB)

msfadmin@metasploitable:~$ _
```

Verifico la comunicazione tra le due macchine



A screenshot of a terminal window on a Kali Linux system. The window has a dark theme and a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal shows a root user at the kali machine in the home directory. The user enters the command 'ping 192.168.1.8'. The output shows seven successful ping packets with varying response times. After pressing Ctrl-C, the terminal displays the ping statistics, indicating 7 packets transmitted, 7 received, 0% packet loss, and a total time of 6070ms. The average, maximum, and minimum round-trip times are also listed.

```
(root@kali)-[~]  
# ping 192.168.1.8  
PING 192.168.1.8 (192.168.1.8) 56(84) bytes of data.  
64 bytes from 192.168.1.8: icmp_seq=1 ttl=64 time=3.18 ms  
64 bytes from 192.168.1.8: icmp_seq=2 ttl=64 time=1.17 ms  
64 bytes from 192.168.1.8: icmp_seq=3 ttl=64 time=33.2 ms  
64 bytes from 192.168.1.8: icmp_seq=4 ttl=64 time=7.01 ms  
64 bytes from 192.168.1.8: icmp_seq=5 ttl=64 time=1.71 ms  
64 bytes from 192.168.1.8: icmp_seq=6 ttl=64 time=29.0 ms  
64 bytes from 192.168.1.8: icmp_seq=7 ttl=64 time=9.28 ms  
^C  
— 192.168.1.8 ping statistics —  
7 packets transmitted, 7 received, 0% packet loss, time 6070ms  
rtt min/avg/max/mdev = 1.168/12.076/33.235/12.376 ms  
  
(root@kali)-[~]  
#
```

Mi collego alla DVWA



Username


admin

Password

••••••••

Login

# Entro



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

Username: admin  
Security Level: high  
PHPIDS: disabled

## Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

### WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing [XAMPP](#) onto a local machine inside your LAN which is used solely for testing.

### Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

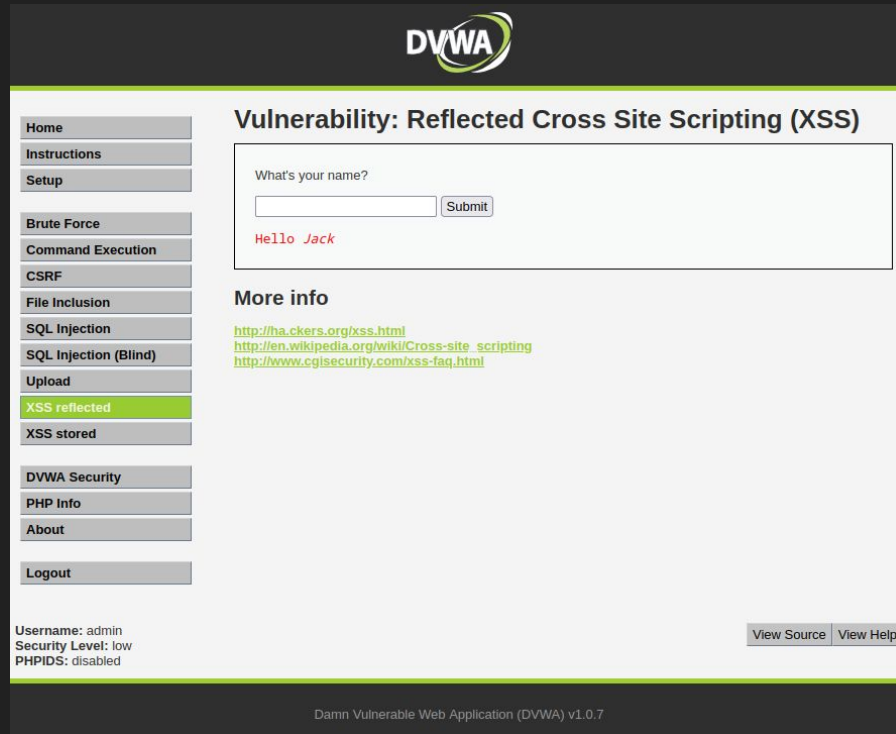
### General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

You have logged in as 'admin'

Damn Vulnerable Web Application (DVWA) v1.0.7

Mi reco sull'interfaccia all'interno della quale posso testare l'XSS reflected e inserisco *Jack* che mi restituirà "Jack" scritto in corsivo, ovvero il codice viene eseguito 'di riflesso' dal server web al client, proprio come avviene in un attacco di questo tipo.



The screenshot displays the DVWA web application interface. At the top, the DVWA logo is visible. On the left, a sidebar contains a list of navigation links: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected (highlighted in green), XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area is titled 'Vulnerability: Reflected Cross Site Scripting (XSS)'. It features a form with the label 'What's your name?' and a 'Submit' button. Below the form, the output 'Hello Jack' is displayed in red text. Under the 'More info' section, three links are provided: <http://hackers.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>. At the bottom left, the user information is shown: Username: admin, Security Level: low, and PHPIDS: disabled. At the bottom right, there are links for 'View Source' and 'View Help'. The footer at the very bottom reads 'Damn Vulnerable Web Application (DVWA) v1.0.7'.

**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: Reflected Cross Site Scripting (XSS)**

What's your name?

Hello Jack

**More info**  
<http://hackers.org/xss.html>  
[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)  
<http://www.cgisecurity.com/xss-faq.html>

Username: admin  
Security Level: low  
PHPIDS: disabled

[View Source](#) [View Help](#)

Damn Vulnerable Web Application (DVWA) v1.0.7

Testo anche l'SQL injection inserendo "5" come id, e ciò mi restituirà la riga di record corrispondente.

In generale, l'SQL injection è un attacco che sfrutta le vulnerabilità delle applicazioni web per eseguire comandi SQL arbitrari sui database relazionali.



The screenshot displays the DVWA (Damn Vulnerable Web Application) interface. At the top, the DVWA logo is visible. Below it, a sidebar contains a list of application features: 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 main content area is titled "Vulnerability: SQL Injection". It features a "User ID:" label, an input field containing the value "5", and a "Submit" button. Below the input field, the output is displayed in red text: "ID: 5", "First name: Bob", and "Surname: Smith". Under the "More info" section, three links are provided: <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/techtips/sql-injection.html>. At the bottom left, the user information is shown: "Username: admin", "Security Level: low", and "PHPIDS: disabled". At the bottom right, there are "View Source" and "View Help" buttons. The footer at the very bottom reads "Damn Vulnerable Web Application (DVWA) v1.0.7".