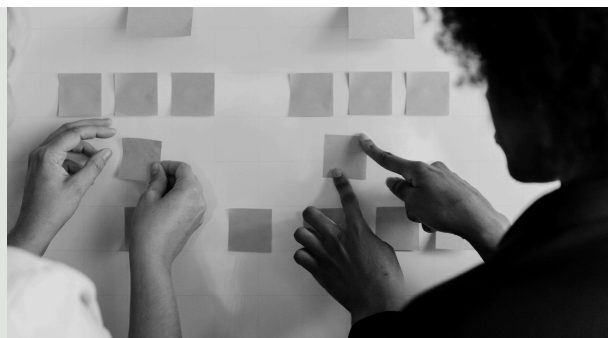


# S6L1



Data: 04/11/24

## INFORMAZIONI PRINCIPALI

L'esercizio consiste nel configurare Metasploitable e Kali Linux per caricare ed eseguire una shell PHP tramite DVWA, quindi analizzare le richieste HTTP/HTTPS con BurpSuite per identificare vulnerabilità.

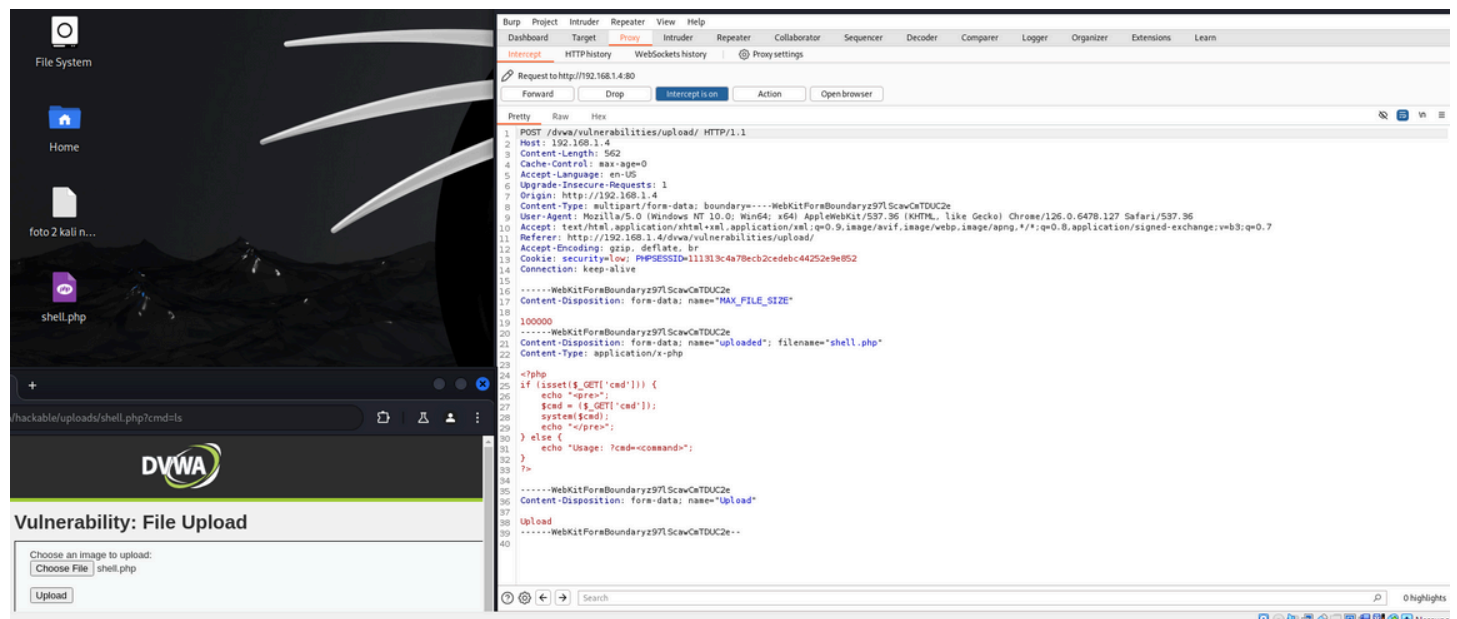
# Sviluppo Dell'esercizio

Per prima cosa ho confermato la connessione tra le due macchine tramite accesso al sito (e ping) e ho impostato la DVWA su Low Security.

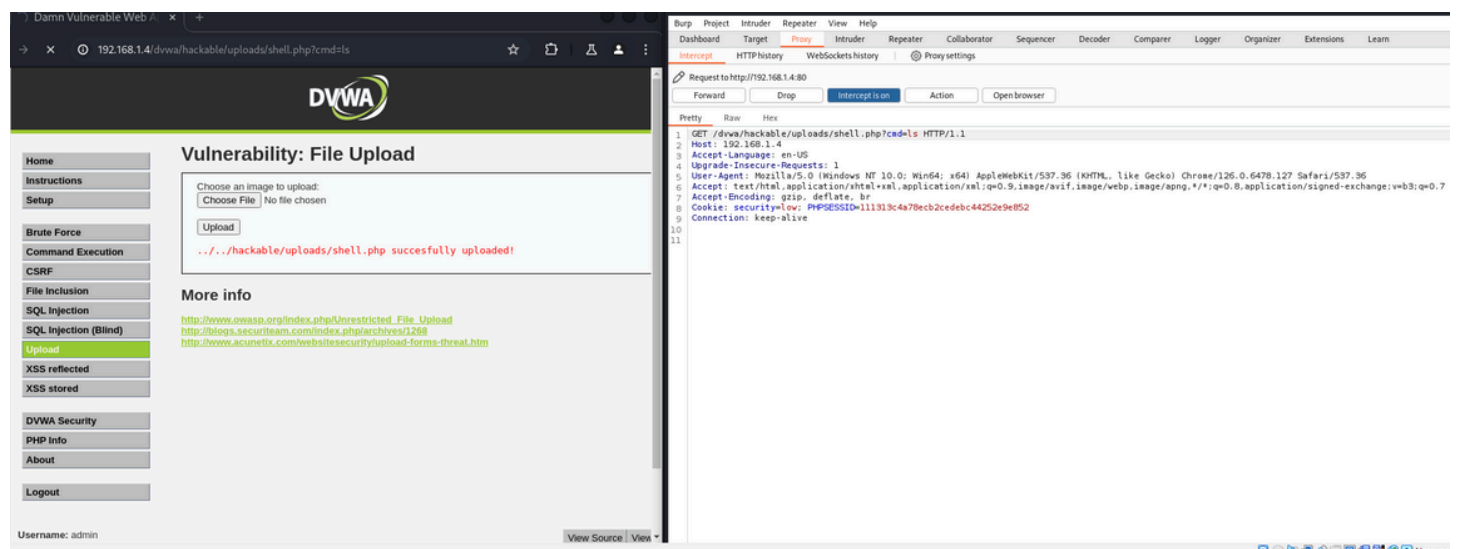
The screenshot shows a Kali Linux desktop environment. In the foreground, a web browser window displays the DVWA (Damn Vulnerable Web Application) interface. The browser's address bar shows the URL `192.168.1.4/dvwa/security.php`. The DVWA interface includes a sidebar with navigation links: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, and XSS stored. The main content area shows the 'Script Security' section, where the security level is currently set to 'low'. Below this, there is a 'PHPIDS' section with a version number of 0.0.6 and a status of 'disabled'. In the background, a terminal window is open, displaying the output of a ping command to `192.168.1.4`. The terminal output shows 20 packets transmitted, 20 received, and 0% packet loss, with a total time of 19582ms. The terminal prompt is `root@kali: /home/kali/Desktop`.

```
File Actions Edit View Help
64 bytes from 192.168.1.4: icmp_seq=2 ttl=64 time=0.183 ms
64 bytes from 192.168.1.4: icmp_seq=3 ttl=64 time=0.269 ms
64 bytes from 192.168.1.4: icmp_seq=4 ttl=64 time=0.212 ms
64 bytes from 192.168.1.4: icmp_seq=5 ttl=64 time=0.175 ms
64 bytes from 192.168.1.4: icmp_seq=6 ttl=64 time=0.193 ms
64 bytes from 192.168.1.4: icmp_seq=7 ttl=64 time=0.219 ms
64 bytes from 192.168.1.4: icmp_seq=8 ttl=64 time=0.276 ms
64 bytes from 192.168.1.4: icmp_seq=9 ttl=64 time=0.250 ms
64 bytes from 192.168.1.4: icmp_seq=10 ttl=64 time=0.371 ms
64 bytes from 192.168.1.4: icmp_seq=11 ttl=64 time=0.208 ms
64 bytes from 192.168.1.4: icmp_seq=12 ttl=64 time=0.244 ms
64 bytes from 192.168.1.4: icmp_seq=13 ttl=64 time=0.196 ms
64 bytes from 192.168.1.4: icmp_seq=14 ttl=64 time=0.226 ms
64 bytes from 192.168.1.4: icmp_seq=15 ttl=64 time=0.189 ms
64 bytes from 192.168.1.4: icmp_seq=16 ttl=64 time=0.209 ms
64 bytes from 192.168.1.4: icmp_seq=17 ttl=64 time=0.274 ms
64 bytes from 192.168.1.4: icmp_seq=18 ttl=64 time=0.192 ms
64 bytes from 192.168.1.4: icmp_seq=19 ttl=64 time=0.227 ms
64 bytes from 192.168.1.4: icmp_seq=20 ttl=64 time=0.195 ms
^C
— 192.168.1.4 ping statistics —
20 packets transmitted, 20 received, 0% packet loss, time 19582ms
rtt min/avg/max/mdev = 0.175/0.225/0.371/0.044 ms
(root@kali)~[/home/kali/Desktop]
```

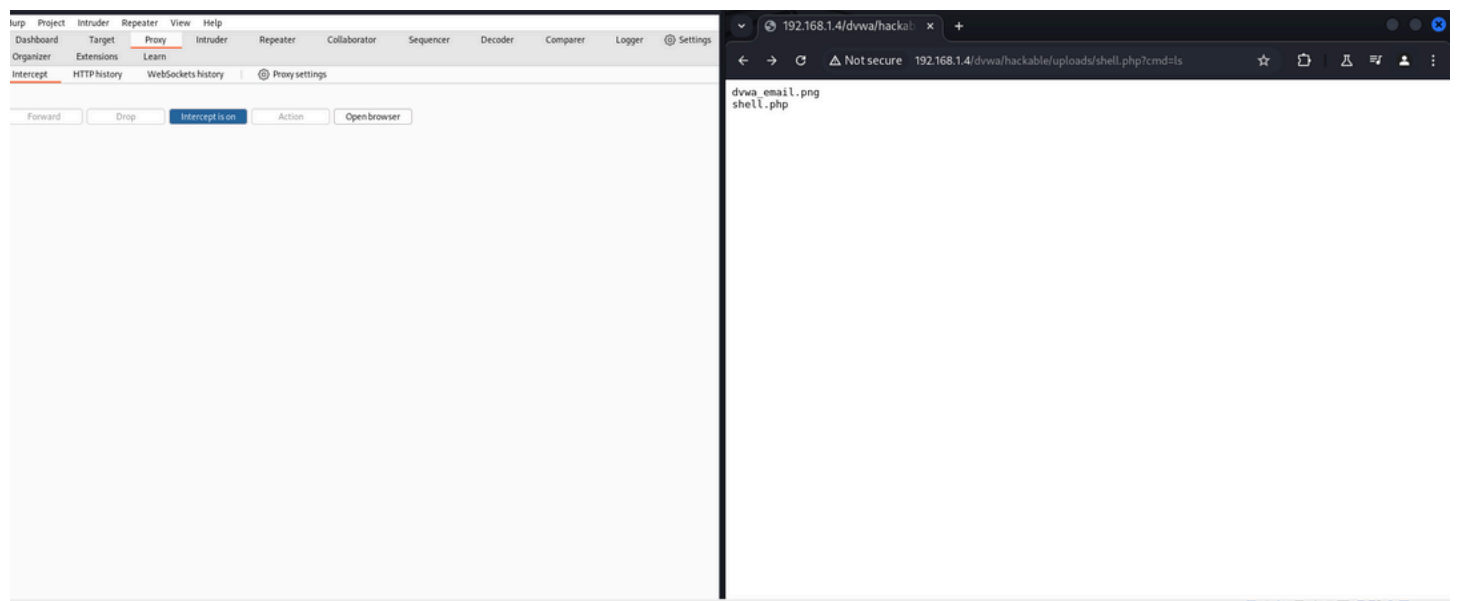
Ho avviato burpsuite e intercettato tutto il traffico da qui in poi. Ho Fatto l'upload dell'exploit e analizzato il "post" di burpsuite.



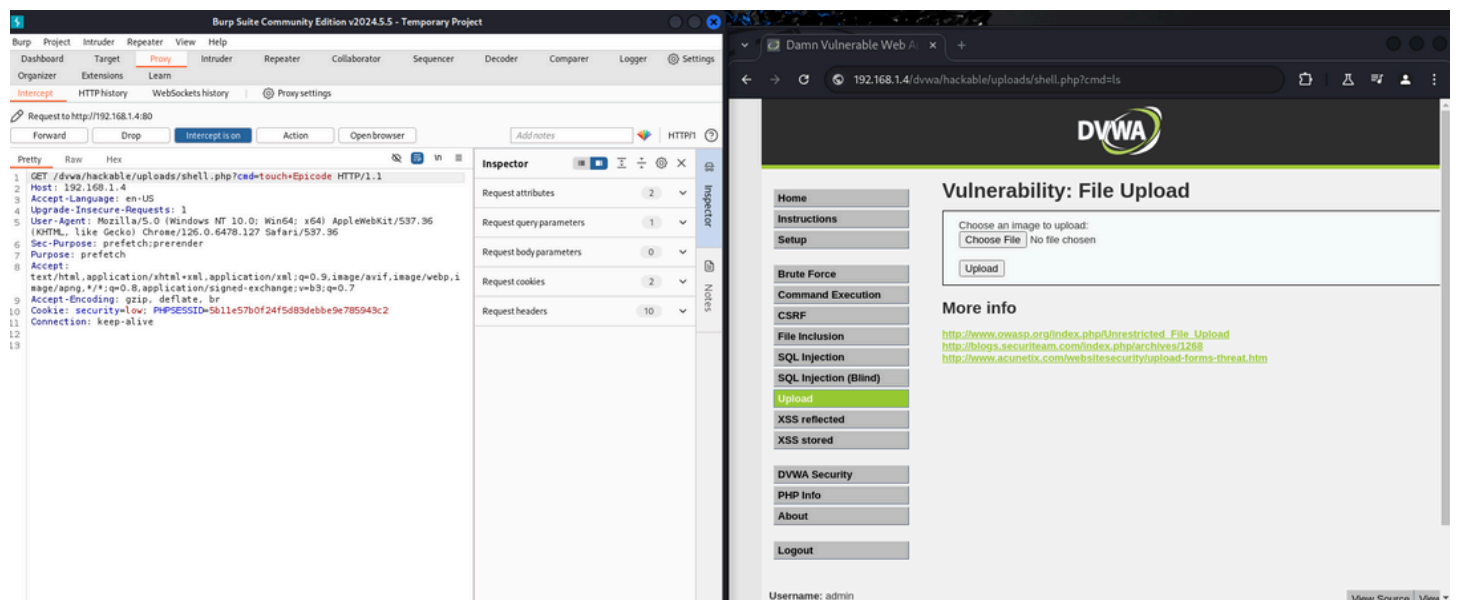
Usando il comando ipmeta/dvwa/hackable/uploads/shell.php?cmd=ls consente di eseguire il comando ls (list) sulla macchina Metasploitable tramite la shell PHP precedentemente caricata.



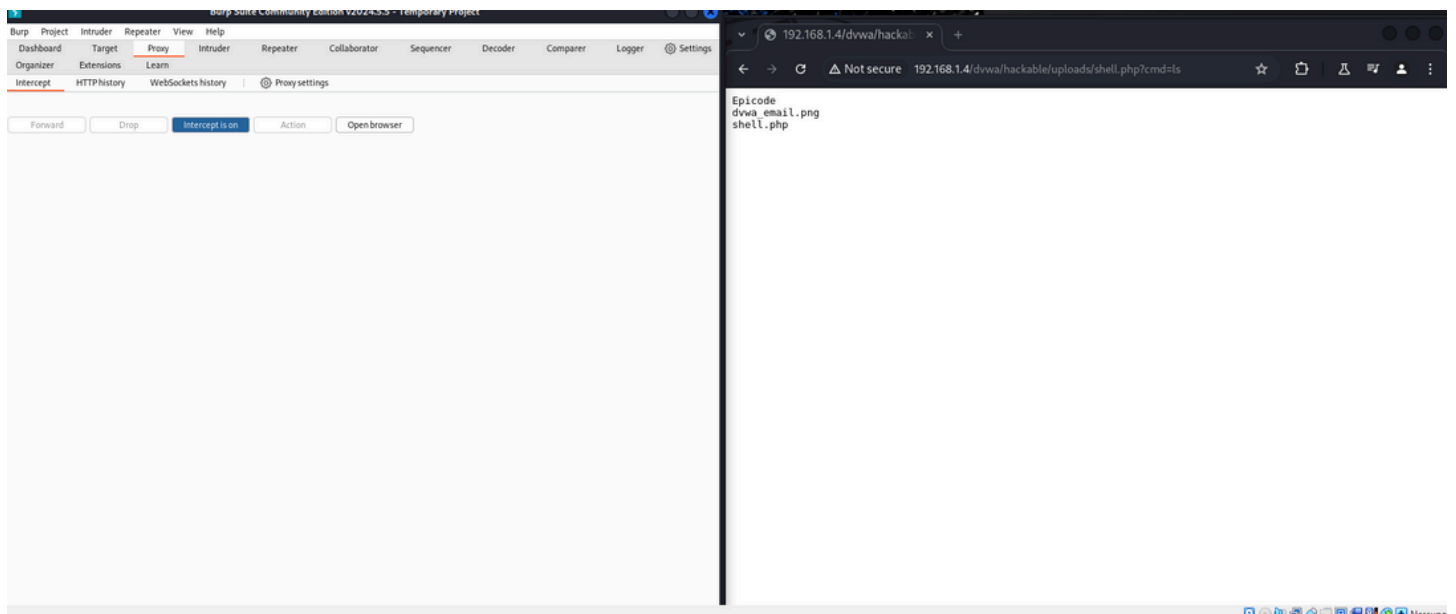
Questa è la lista dei file e andremo ad aggiungerne uno.



Questa Shell PHP è stata progettata per accettare comandi tramite il parametro cmd. L'utente invia un comando tramite ?cmd=<comando>, che PHP esegue sulla macchina attaccata. in questo caso dopo cmd= rimuoviamo il comando ls e aggiungiamo touch+Epicode, per creare un nuovo file (Epicode) nella directory della macchina attaccata.



**Il risultato finale è un file creato con nome Epicode sulla DVWA di Meta.**



## **Conclusioni e riassunto.**

Utilizzando la piattaforma vulnerabile DVWA (Damn Vulnerable Web Application) presente su Metasploitable, è possibile caricare un file PHP (molto basico), che agisce come una "shell". Questa shell, una volta caricata, consente l'esecuzione di comandi di sistema direttamente da un browser web.

Attraverso l'URL ipmeta/dvwa/hackable/uploads/shell.php?cmd=ls, Kali Linux comunica con Metasploitable utilizzando il parametro cmd. In questo caso, il valore ls permette di elencare i file e le directory presenti nella posizione in cui la shell è stata caricata. Di fatto, l'utente può inserire altri comandi dopo cmd=, ottenendo un controllo a distanza sulla macchina Metasploitable. Questo processo evidenzia l'esistenza di vulnerabilità nel sistema di upload di DVWA e consente di esplorare l'ambiente della macchina bersaglio senza accesso diretto alla riga di comando, solo tramite un'interfaccia web.

**Extra&Http History: trovata un email nel server dvwa forzando l'accesso con l'url, e indagando oltre ho trovato questi, Molto carino. (modificando l'url si può esplorare altre directory.)**

192.168.1.4/dvwa\_email.png  
shell.php

Burp Suite Community Edition v2024.5.5 - 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
1	http://192.168.1.4	GET	/dvwa/hackable/uploads/shell.php?cmd=ls			200	268	XML	php	Metasploitable2 - Linux			192.168.1.4	
2	http://192.168.1.4	GET	/			200	1134	HTML		404 Not Found			192.168.1.4	
3	http://192.168.1.4	GET	/favicon.ico			404	513	HTML	ico				192.168.1.4	
4	http://192.168.1.4	GET	/dvwa/			302	482	HTML					192.168.1.4	PHPSESSID=ea12bc8f567
5	http://192.168.1.4	GET	/dvwa/login.php			200	1636	HTML	php	Damn Vulnerable Web App (DVWA) ...			192.168.1.4	
6	http://192.168.1.4	POST	/dvwa/login.php			302	391	HTML	php				192.168.1.4	
7	http://192.168.1.4	GET	/dvwa/index.php			200	4932	HTML	php	Damn Vulnerable Web App (DVWA) ...			192.168.1.4	
8	http://192.168.1.4	GET	/dvwa/security.php			200	4453	HTML	php	Damn Vulnerable Web App (DVWA) ...			192.168.1.4	
9	http://192.168.1.4	POST	/dvwa/security.php			302	426	HTML	php				192.168.1.4	security=low
10	http://192.168.1.4	GET	/dvwa/security.php			200	4534	HTML	php	Damn Vulnerable Web App (DVWA) ...			192.168.1.4	
11	http://192.168.1.4	GET	/dvwa/vulnerabilities/upload/			200	4863	HTML		Damn Vulnerable Web App (DVWA) ...			192.168.1.4	
12	http://192.168.1.4	POST	/dvwa/vulnerabilities/upload/			200	4928	HTML		Damn Vulnerable Web App (DVWA) ...			192.168.1.4	
13	http://192.168.1.4	GET	/dvwa/hackable/uploads/shell.php?cmd=ls			200	268	XML	php				192.168.1.4	
14	http://192.168.1.4	GET	/dvwa/hackable/uploads/shell.php?cmd=ls			200	243	XML	php				192.168.1.4	
15	http://192.168.1.4	GET	/dvwa/hackable/uploads/shell.php?cmd=ls			200	275	XML	php				192.168.1.4	



dvwa@ethicalhack3r.co.uk

Home

foto 2 kali n

shell.php

Dashboard

Target

Proxy

Intruder

Repeater

Collaborator

Sequencer

Decoder

Comparer

Logger

Settings

Intercept

HTTP history

WebSockets history

Proxy settings

Forward

Drop

Intercept is on

Action

Open browser

Index of /dvwa/hackable

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>	-	-	
<a href="#">uploads/</a>	04-Nov-2024 09:36	-	
<a href="#">users/</a>	20-May-2012 15:22	-	

Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.1.4 Port 80

# Index of /dvwa/hackable/users

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
<hr/>			
 <a href="#">Parent Directory</a>		-	
 <a href="#">1337.jpg</a>	16-Mar-2010 01:56	3.6K	
 <a href="#">admin.jpg</a>	16-Mar-2010 01:56	3.5K	
 <a href="#">gordonb.jpg</a>	16-Mar-2010 01:56	3.0K	
 <a href="#">pablo.jpg</a>	16-Mar-2010 01:56	2.9K	
 <a href="#">smithy.jpg</a>	16-Mar-2010 01:56	4.3K	

Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.1.4 Port 80

