S6L1

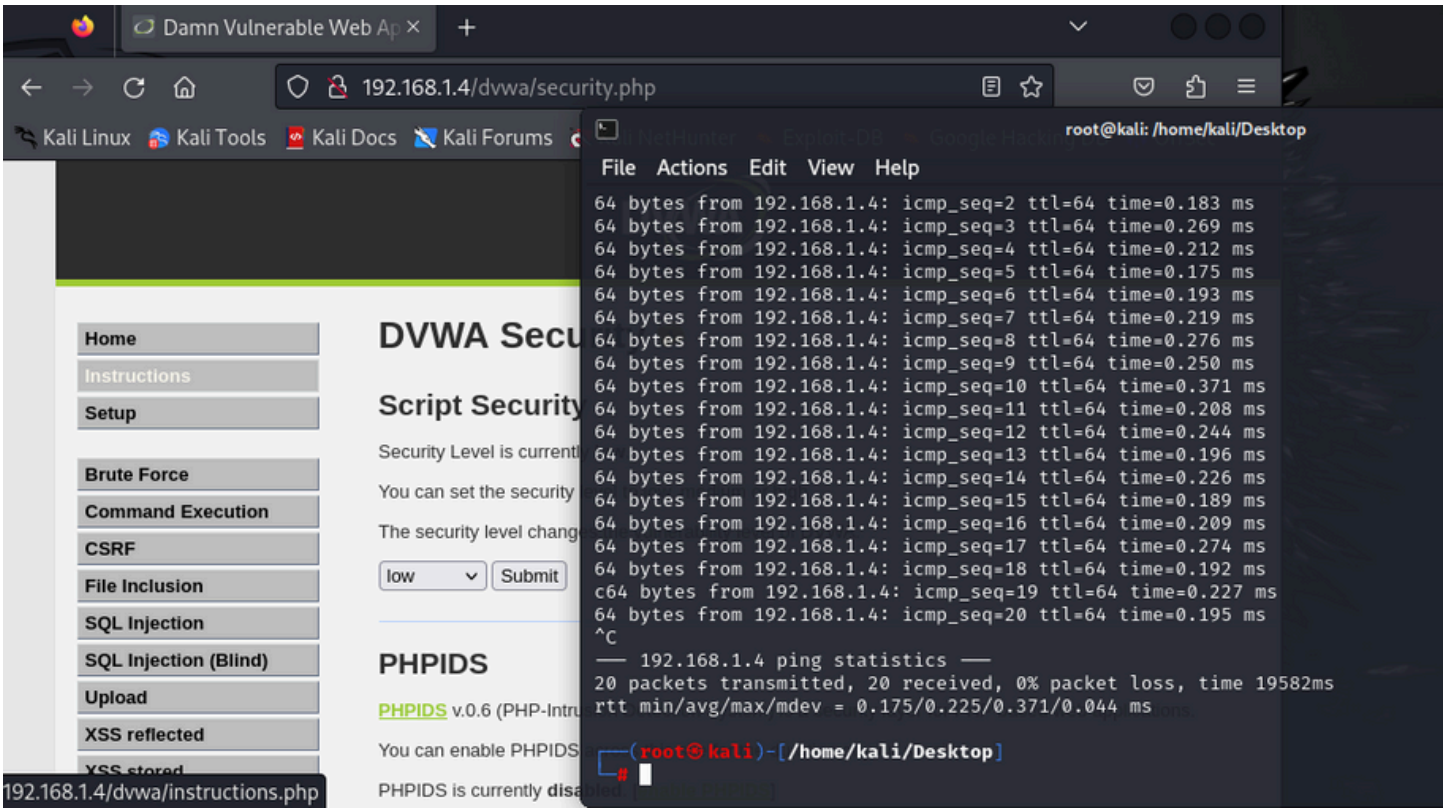
Data: 04/11/24

INFORMAZIONI PRINCIPALI

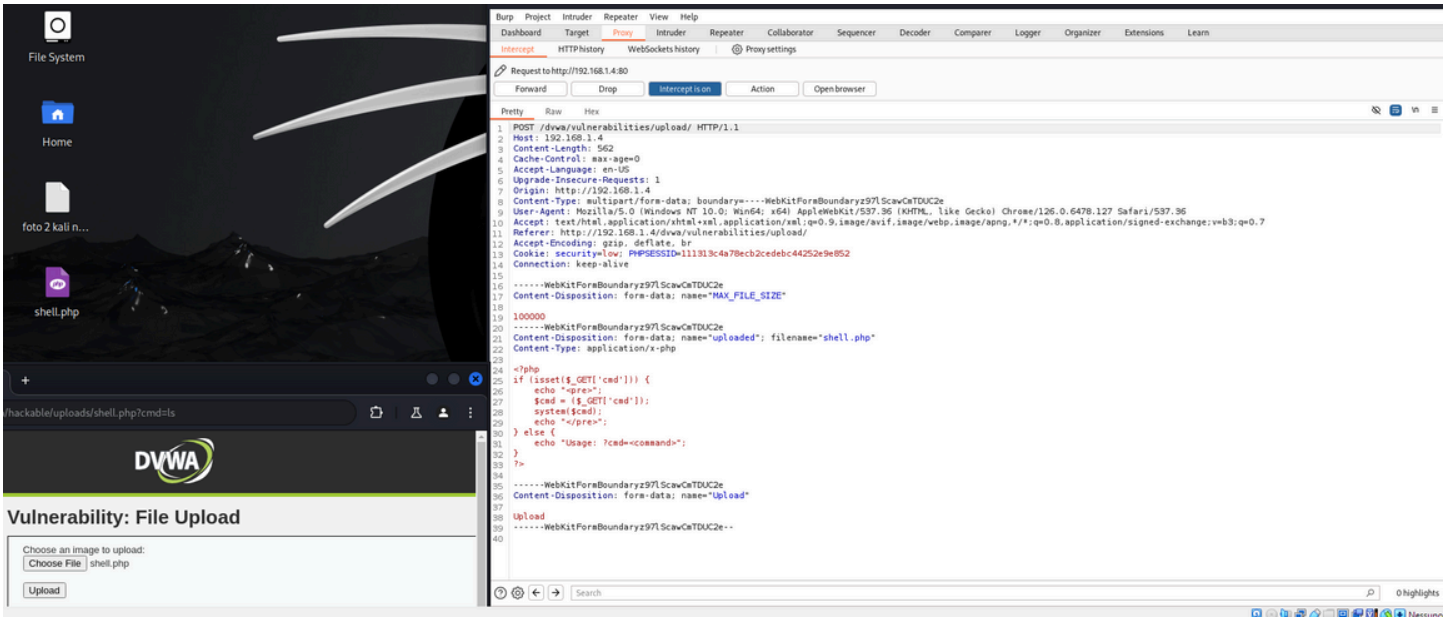
L'esercizio consiste nel configurare Metasploitable e Kali Linux per caricare ed eseguire una shell PHP tramite DVWA, quindi analizzare le richieste HTTP/HTTPS con BurpSuite per identificare vulnerabilità.

Sviluppo Dell'esercizio

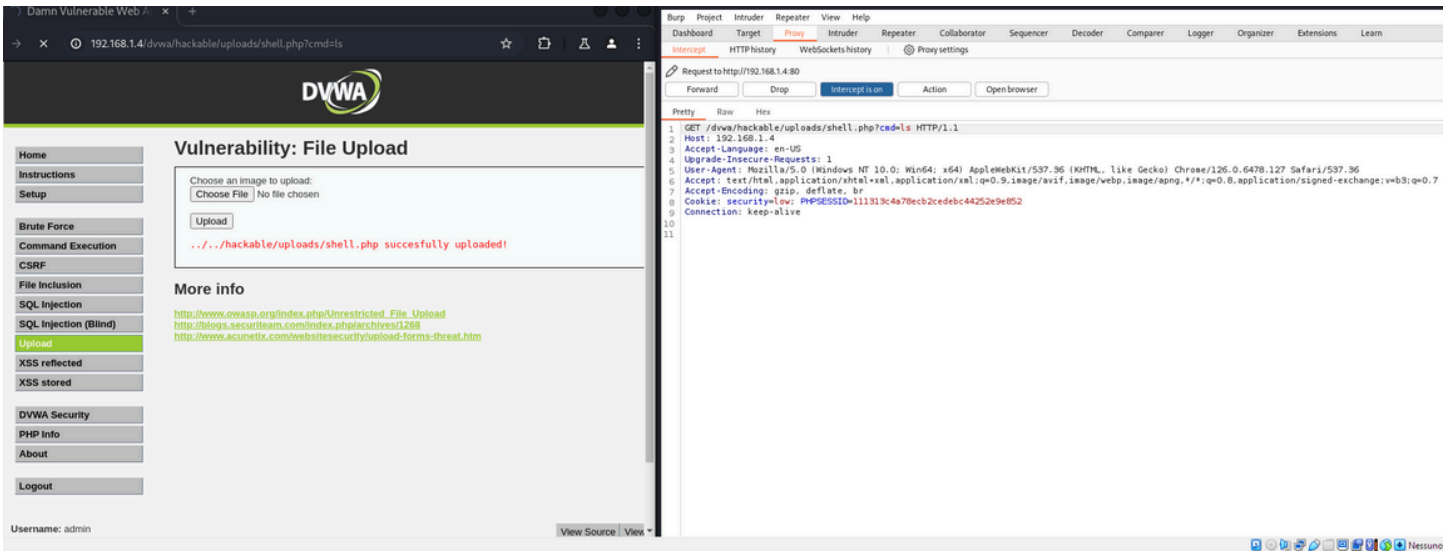
Per prima cosa ho confermato la connessione tra le due macchine tramite accesso al sito (e ping) e ho impostato la DVWA su Low Security.



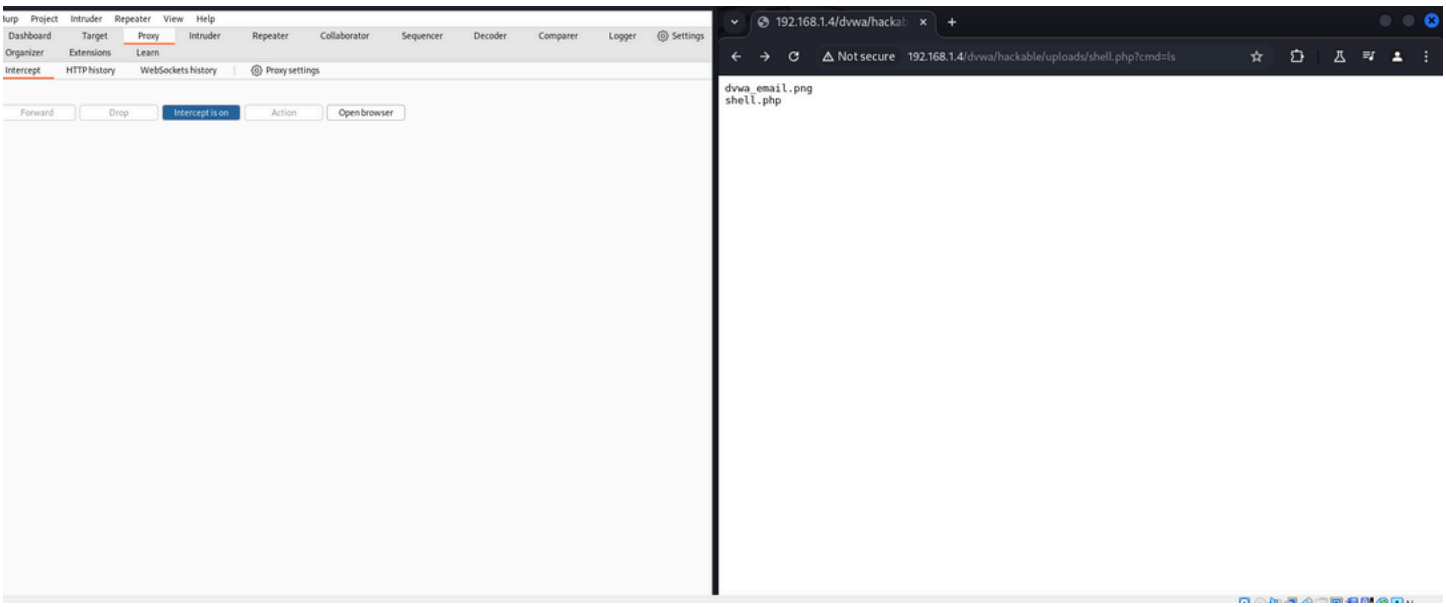
Ho avviato burpsuite e intercettato tutto il traffico da qui in poi. Ho Fatto l'upload dell'exploit e analizzato il "post" di burpsuite.



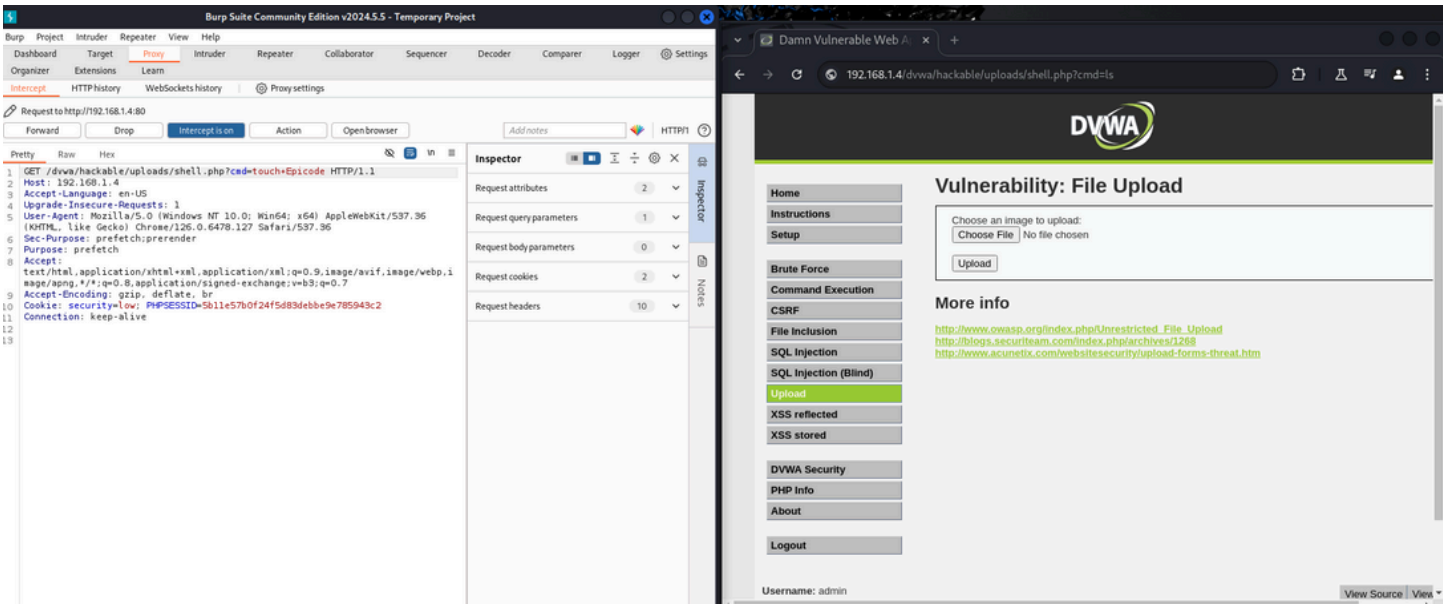
Usando il comando ipmeta/dvwa/hackable/uploads/shell.php?cmd=ls consente di eseguire il comando ls (list) sulla macchina Metasploitable tramite la shell PHP precedentemente caricata.



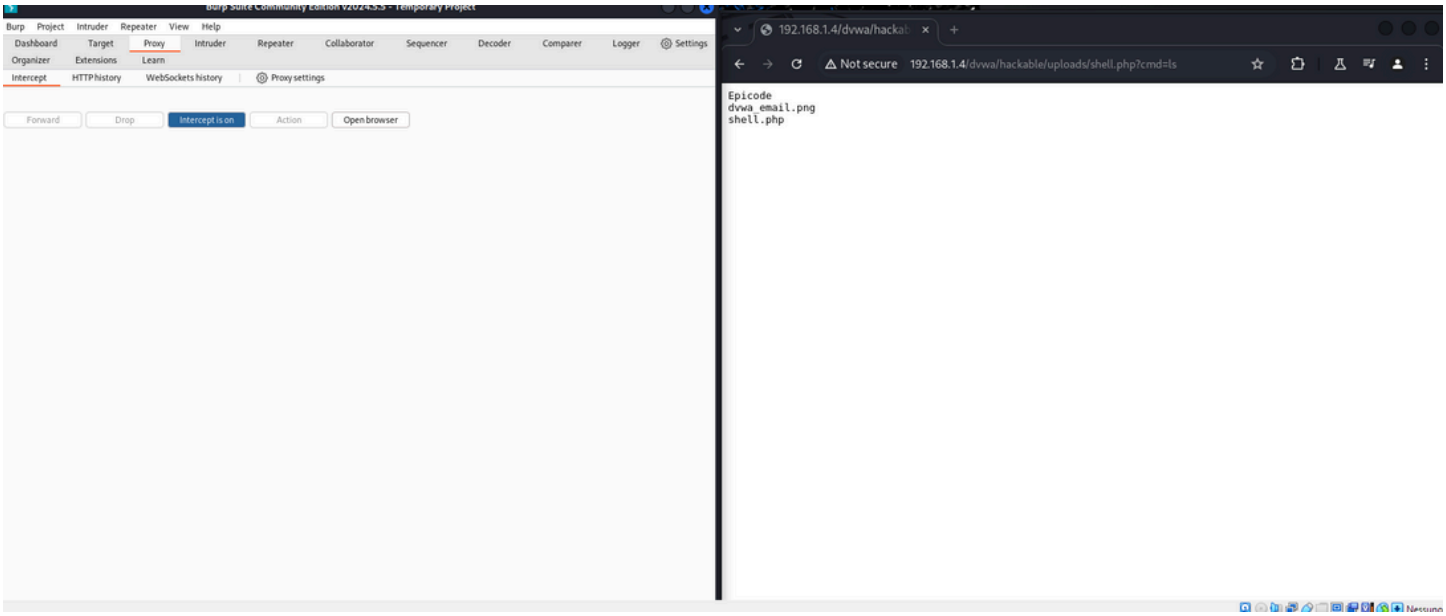
Questa è la lista dei file e andremo ad aggiungerne uno.



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 quesot 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.

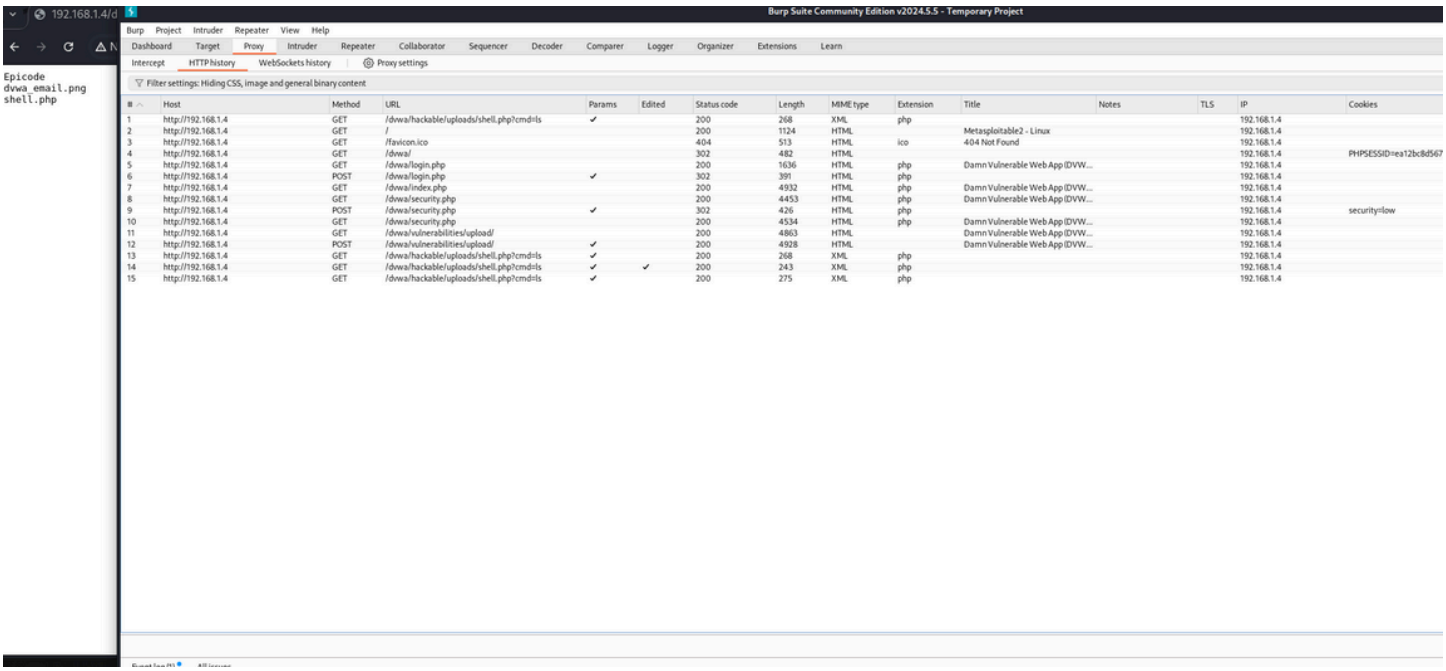


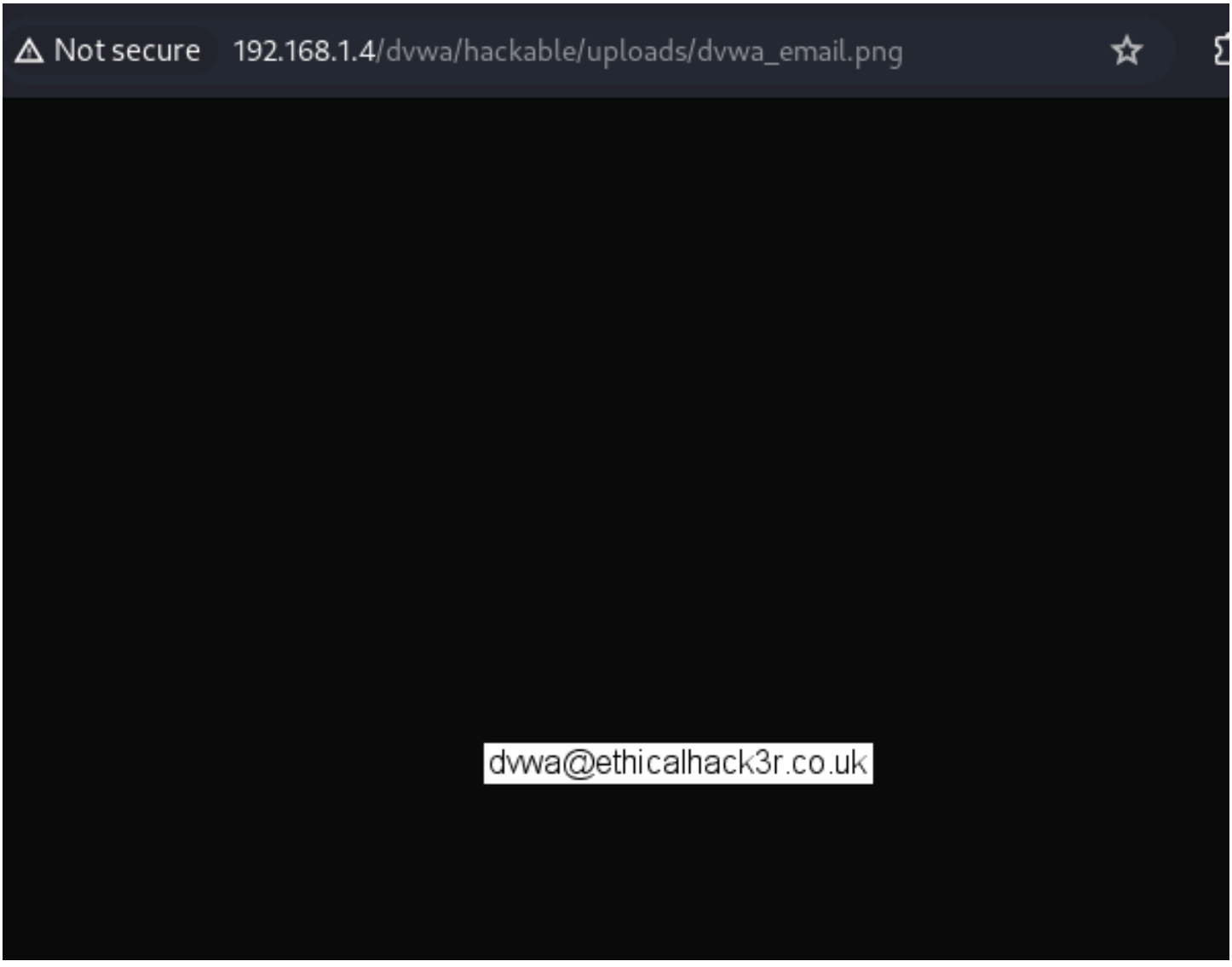
Conclusioni e riassunto.

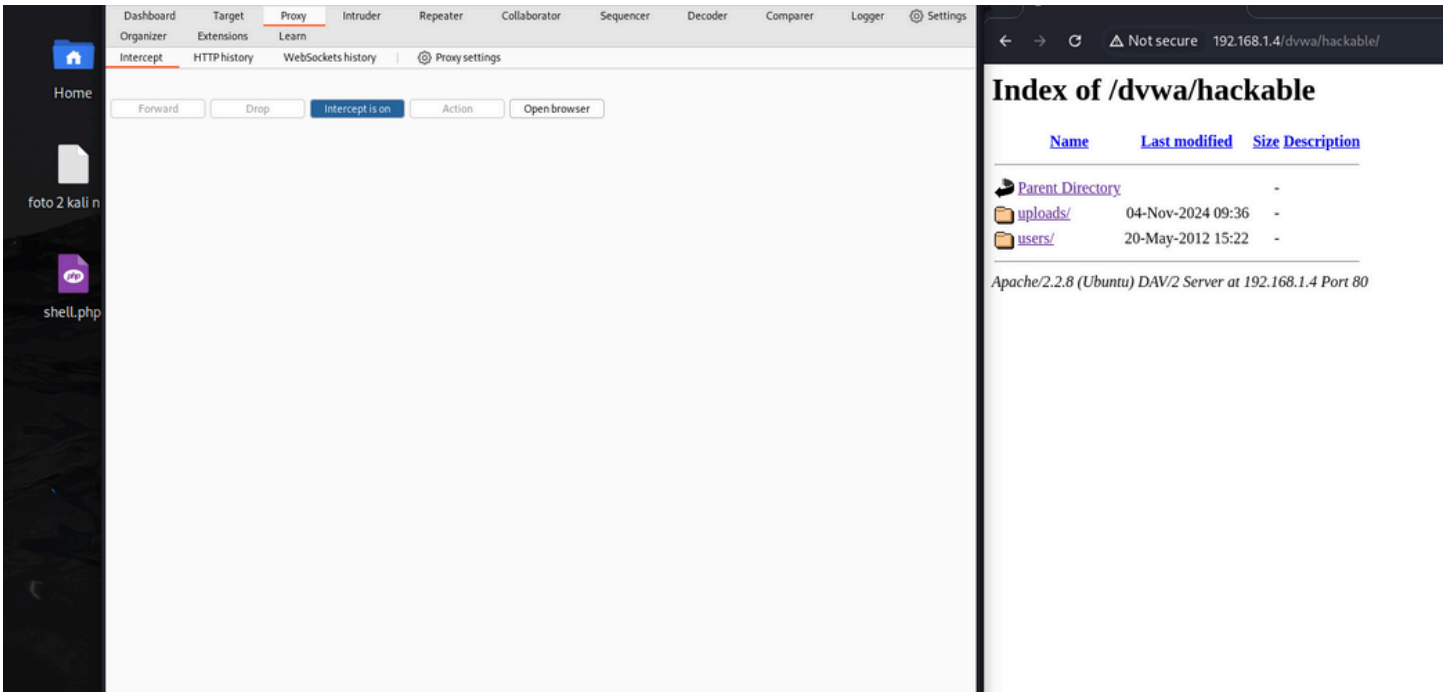
Utilizzando la piattaforma vulnerabile DVWA (Damn Vulnerable Web Application) presente su Metasploitable, è possibile caricare un file PHP (molto basico), che agisce come una "shell". Questa shell, una volta caricata, consente l'esecuzione di comandi di sistema direttamente da un browser web.

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.)






Home
foto 2 kali n
shell.php
Dashboard
Target
Proxy
Intruder
Repeater
Collaborator
Sequencer
Decoder
Comparer
Logger
Settings
Organizer
Extensions
Learn
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