TECNICHE DI EXPLOIT CON #XSS SHELL PHP:

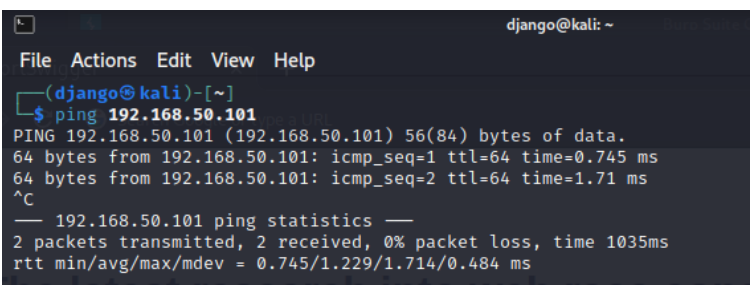
#DVWA + BURPSUITE

NELLA LEZIONE PRATICA DI OGGI VEDREMO COME SFRUTTARE UN **FILE UPLOAD SULLA DVWA PER CARICARE UNA SEMPLICE SHELL IN PHP**. MONITOREREMO TUTTI GLI STEP CON **BURPSUITE**

TRACCIA:
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 DI OGGI 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. INOLTRE, PER FAMILIARIZZARE SEMPRE DI PIÙ CON GLI STRUMENTI UTILIZZATI DAGLI HACKER ETICI, VI CHIEDIAMO DI INTERCETTARE ED ANALIZZARE OGNI RICHIESTA VERSO LA DVWA CON BURPSUITE.

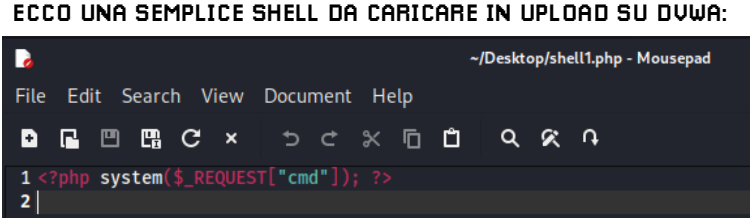
CONSEGNA:
1. CODICE PHP
2. RISULTATO DEL CARICAMENTO (SCREENSHOT DEL BROWSER)
3. INTERCETTAZIONI (SCREENSHOT DI BURPSUITE)
4. RISULTATO DELLE VARIE RICHIESTE
5. EVENTUALI ALTRE SCOPERTE DELLA MACCHINA INTERNA
6. BONUS: USARE UNA SHELL PHP PIÙ SOFISTICATA

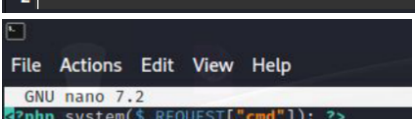
AL FINE DELL'ESERCIZIO È SUFFICIENTE CHE LE DUE MACCHINE (KALI E METASPLOITABLE) SIANO SULLA STESSA RETE, LASCIO QUINDI L'IP DI METASPLOITABLE SIA 192.168.50.101, MENTRE QUELLO DI KALI LINUX RESTERÀ 192.168.50.100. E FACCIO UN PING DI PROVA DA KALI.



#CODICE PHP:

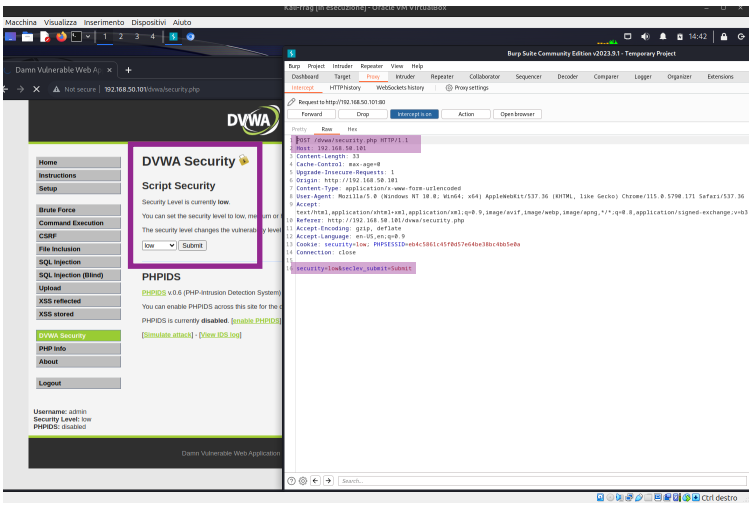
PERSONALMENTE HO APERTO UN FILE TXT DOVE HO INCOLLATO LA STRINGA FORNITACI DALLE SLIDE, SALVANDO A MANO IL FILE COME SHELL1.PHP. MA SI PUÒ FARE ANCHE DA NANO.
ECCO UNA SEMPLICE SHELL DA CARICARE IN UPLOAD SU DVWA:

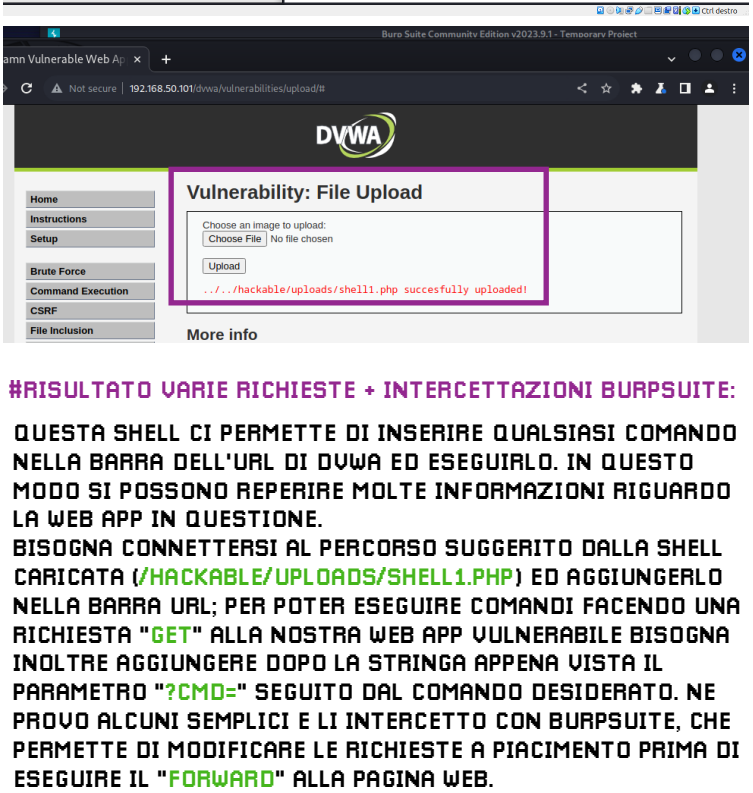




#RISULTATO DEL CARICAMENTO:

PRIMA DI PROCEDERE AL CARICAMENTO DELLA SHELL SU DVWA, BISOGNA RENDERLO PIÙ VULNERABILE POSSIBILE IMPOSTANDO IL LIVELLO DI SICUREZZA SU LOW NELLA PAGINA "DVWA SECURITY" IN MODO DA FACILITARE L'EXPLOIT. SUCESSIVAMENTE POSSO PROCEDERE A CARICARE LA SHELL DALLA PAGINA "UPLOAD". SE LA SHELL VERRÀ CARICATA CORRETTAMENTE APPARIRÀ IL MESSAGGIO NELL'IMMAGINE DI SEGUITO.
TUTTI I PASSAGGI VENGONO ITERCETTATI DA BURPSUITE.





#RISULTATO VARIE RICHIESTE + INTERCETTAZIONI BURPSUITE:

QUESTA SHELL CI PERMETTE DI INSERIRE QUALSIASI COMANDO NELLA BARRA DELL'URL DI DVWA ED ESEGUIRLO. IN QUESTO MODO SI POSSONO REPERIRE MOLTE INFORMAZIONI RIGUARDO LA WEB APP IN QUESTIONE.
BISOGNA CONNETTERSI AL PERCORSO SUGGERITO DALLA SHELL CARICATA (/HACKABLE/UPLOADS/SHELL1.PHP) ED AGGIUNGERLO NELLA BARRA URL; PER POTER ESEGUIRE COMANDI FACENDO UNA RICHIESTA "GET" ALLA NOSTRA WEB APP VULNERABILE BISOGNA INOLTRE AGGIUNGERE DOPO LA STRINGA APPENA VISTA IL PARAMETRO "?CMD=" SEGUITO DAL COMANDO DESIDERATO. NE PROVO ALCUNI SEMPLICI E LI INTERCETTO CON BURPSUITE, CHE PERMETTE DI MODIFICARE LE RICHIESTE A PIACIMENTO PRIMA DI ESEGUIRE IL "FORWARD" ALLA PAGINA WEB.

VEDIAMO LA SHELL PIÙ COMPLESSA NEL SECONDO ESERCIZIO.