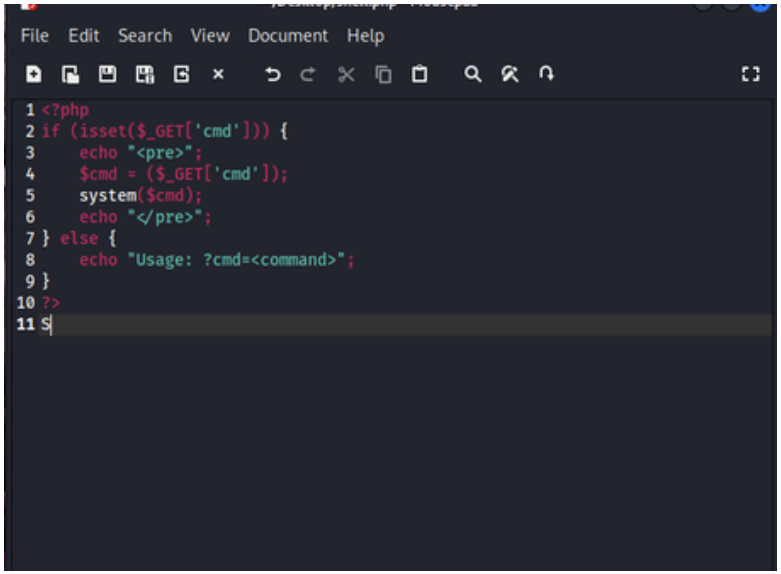
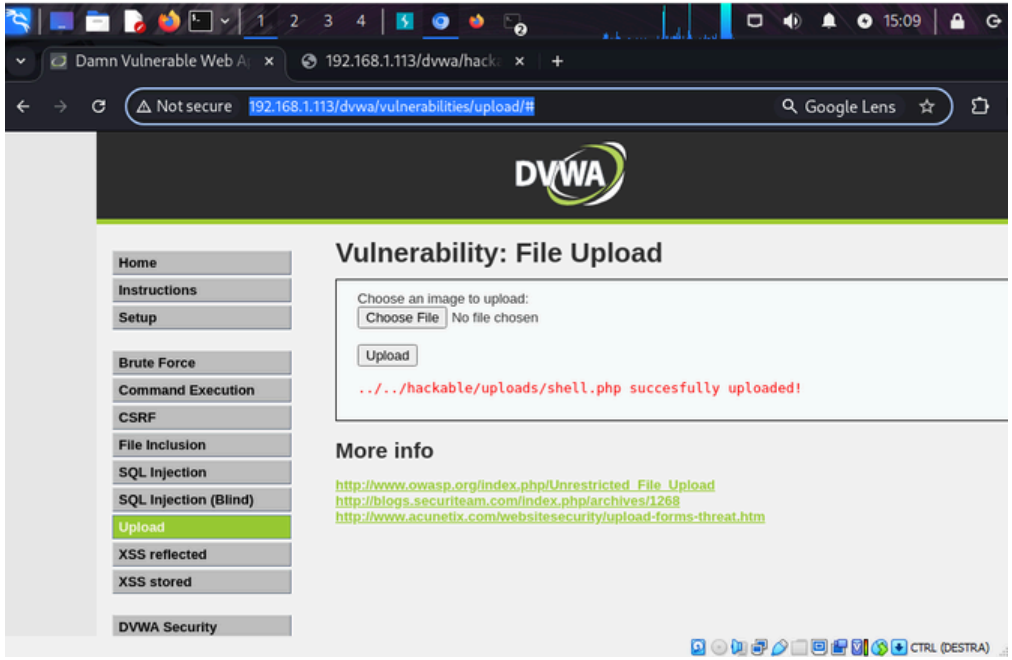
Pratica S6/L1

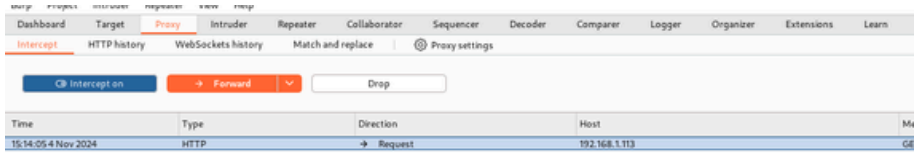
Sfruttamento di una vulnerabilità di File Upload sulla DVWA per l'inserimento di una shell in PHP



Prepariamo il nostro laboratorio virtuale, collegando le due macchine, Kali e Meta, mettendole in comunicazione tra loro.
Scriviamo una semplice shell e salviamola sulla nostra VM

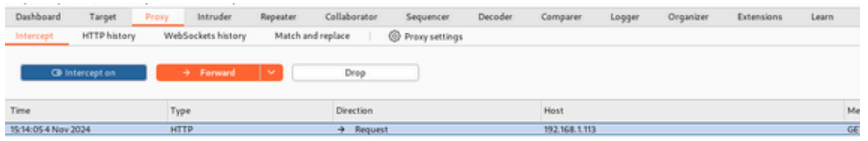
Colleghiamoci sulla nostra DVWA e inseriamo il file appena creato su upload

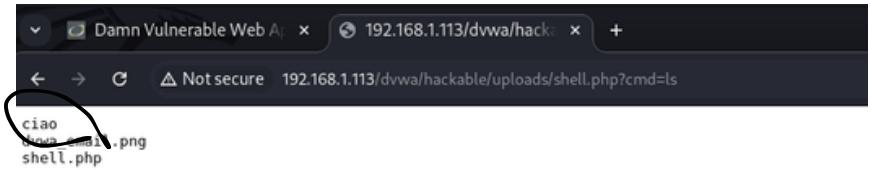




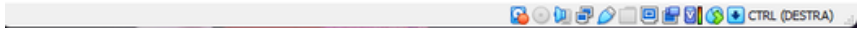
Apriamo Burpsuite e intercettiamo le richieste HTTP.
Sul campo Ls modifichiamo il nostro testo inserendo “Ciao”

Con Forward attiviamo le nostre modifiche





Ora andiamo nel sito http://192.168.1.113/dvwa/hackable/uploads/shell.php?cmd=ls aggiorniamo la pagina e la nostra modica apparirà come in figura.



Lo sfruttamento di una vulnerabilità di File Upload nella Damn Vulnerable Web Application (DVWA) è un'operazione comune per esercitarsi nell'inserimento di una web shell in PHP. Una web shell è uno script caricato sul server di destinazione che consente un controllo remoto attraverso comandi eseguiti nel contesto dell'utente del server web.