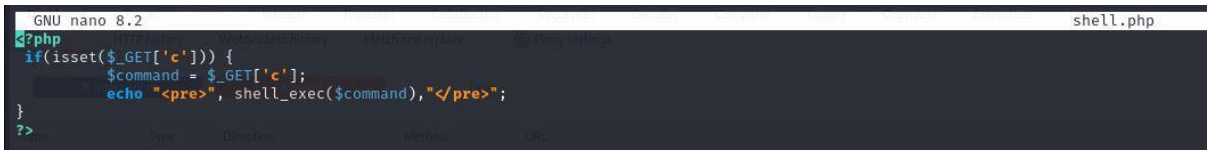
Passaggi per sfruttare la vulnerabilità di file upload su DVWA

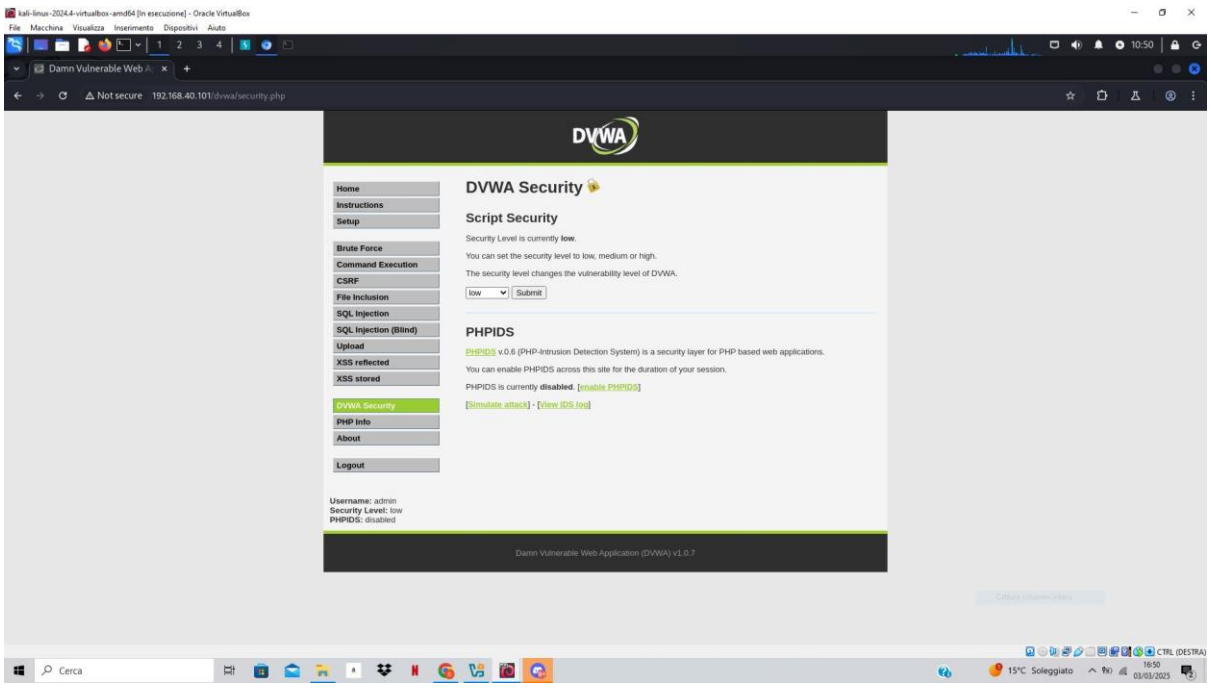
1. Terminale

Nel terminale creo una shell da caricare in DVWA con livello di sicurezza low:

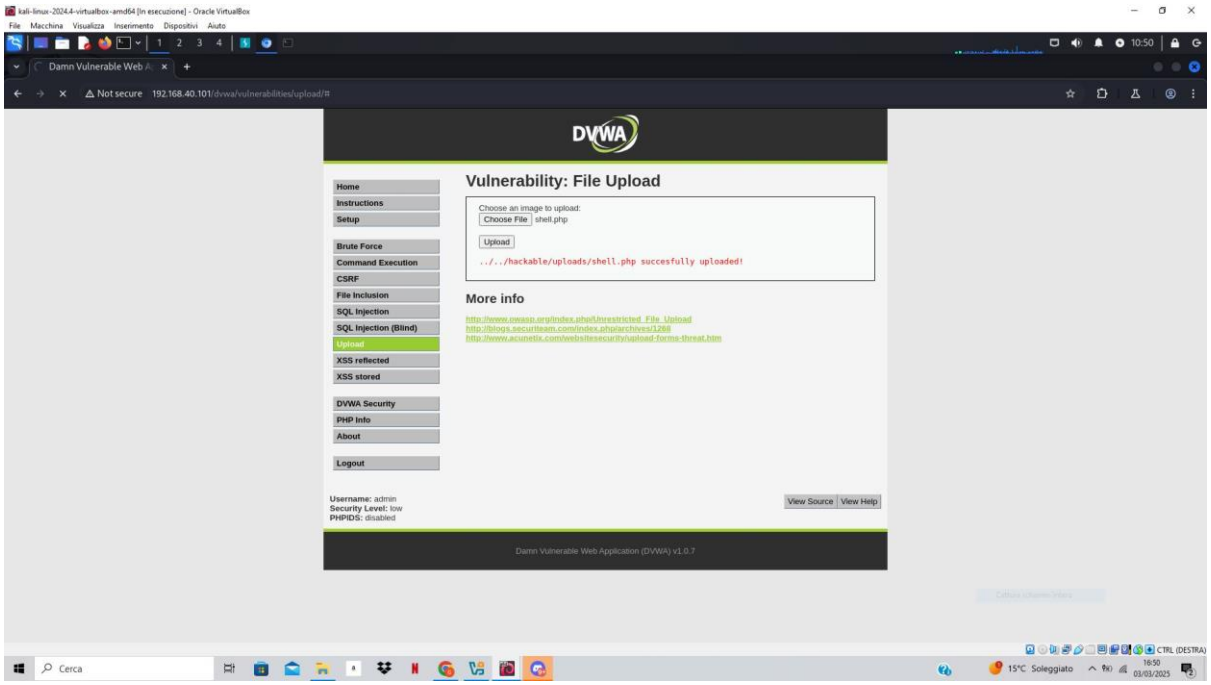


2. Configurare DVWA e Intercetto su BurpSuite

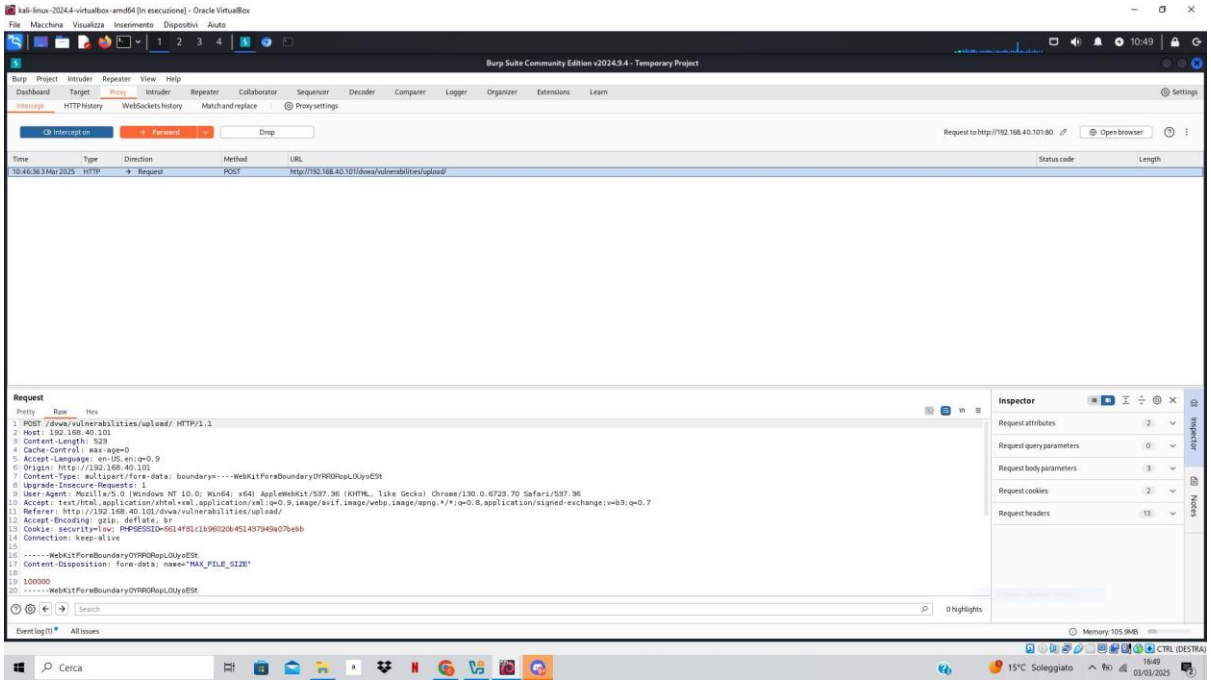
Direttamente in BurpSuite apro il broswer e accedo a DVWA, abbasso il livello di sicurezza;



Successivamente carico la shell.php creata su upload;

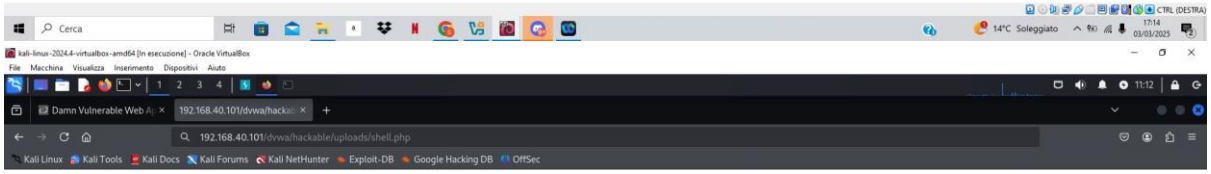


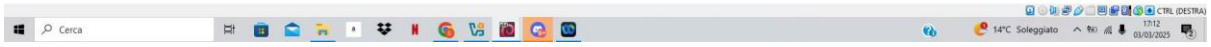
E attivo l'intercettazione su Burp Suite per notarne tutti i traffici;

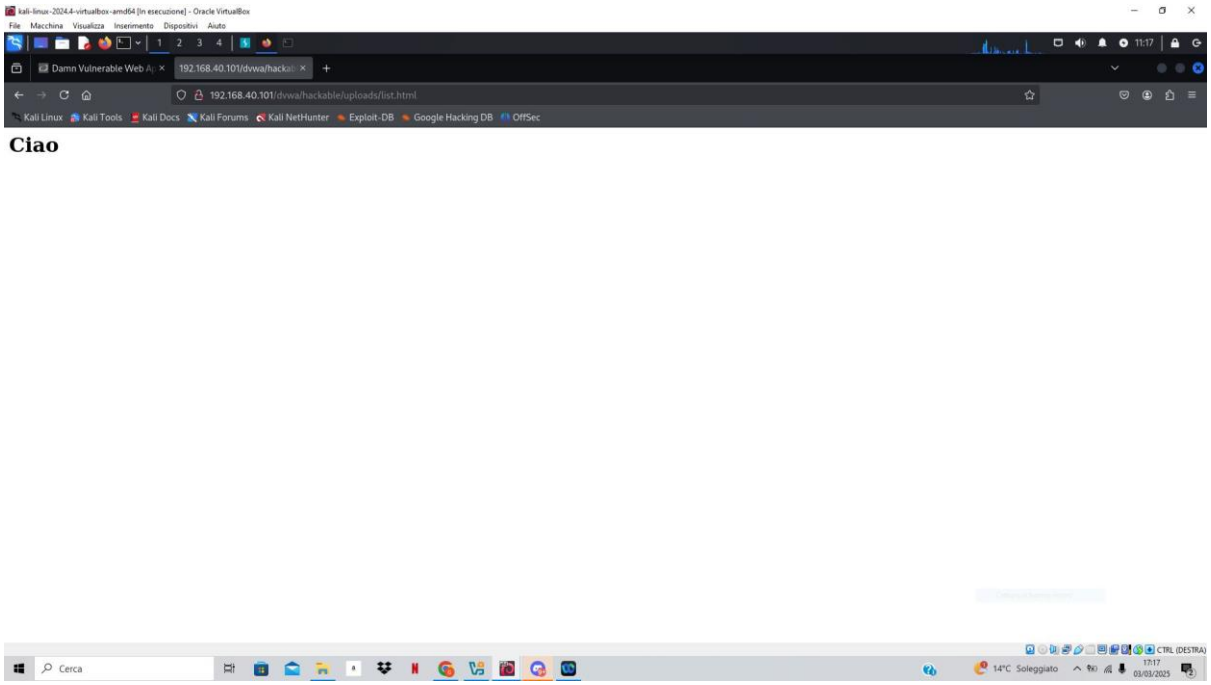


Ora posso interagire con la shell direttamente dal browser http://192.168.40.101/dvwa/hackable/uploads/shell.php ;


kali-linux-2024.4-virtualbox-amd64 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Damn Vulnerable Web A
192.168.40.101/dvwa/hackable/uploads/shell.php?c=ls
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
dvwa_email.png
list.html
shell.php


Cerca
14°C Soleggiato
CTRL (DESTRA)
kali-linux-2024.4-virtualbox-amd64 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Damn Vulnerable Web A
192.168.40.101/dvwa/hackable/uploads/shell.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec


Cerca
14°C Soleggiato
CTRL (DESTRA)



Semplicemente posso scrivere in riga di comando nel curl http://192.168.40.101/dvwa/hackable/uploads/shell.php?c=.....