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

OBIETTIVI:

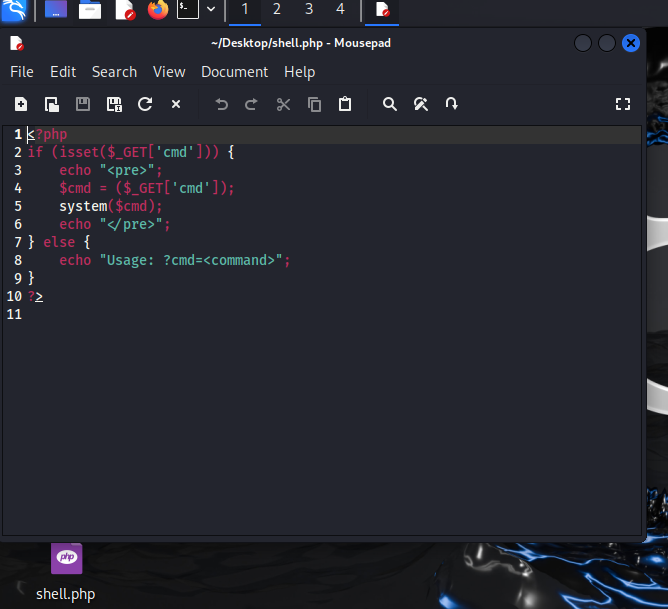
**1. Preparazione dell'Ambiente**

**2. Caricamento della Shell PHP**

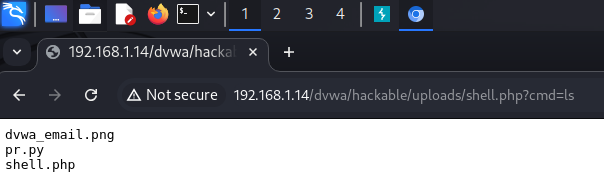
**3. Esecuzione della Shell PHP**

**4. Intercettazione e Analisi con BurpSuite**

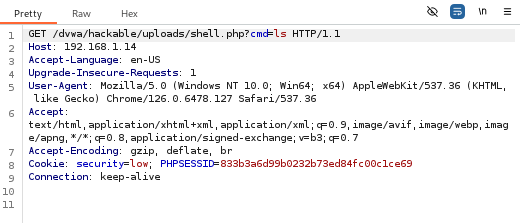
Come prima cosa ho verificato che linux potesse raggiungere metasploitable con un ping e così è stato. Dopodichè ho creato subito la shell PHP che si può vedere qui sotto



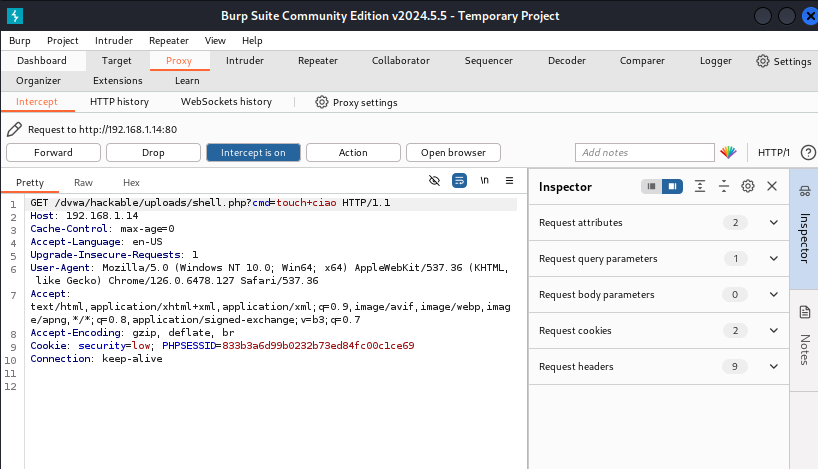
Una volta creata la shell, ho aperto BurpSuite e da lì ho aperto direttamente il browser andando su DVWA inserendo l’indirizzo IP di metasploitable nell’URL. Una volta dentro ho inserito la sicurezza al minimo (low) e ho caricato la shell. Questo è ciò che ho ricevuto in output:

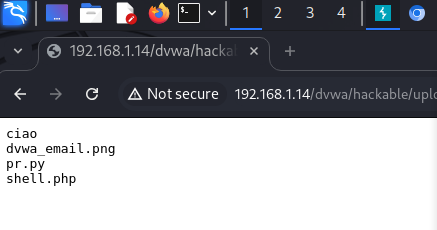


Mentre questo è lo script di BurpSuite:



Ho provato anche a far uscire in output una semplice parola (ciao), modificando lo script di BurpSuite:





Qua riporto i metodi GET e POST:

