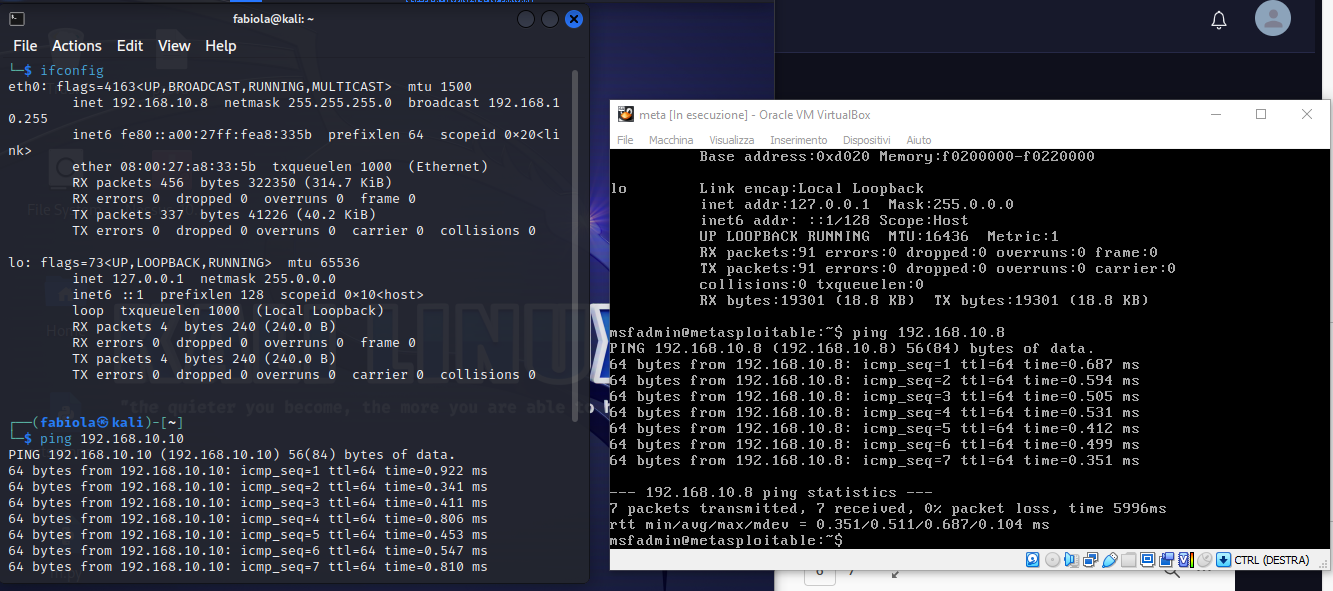
**Traccia:**

Assicuratevi che ci sia comunicazione tra le due macchine.

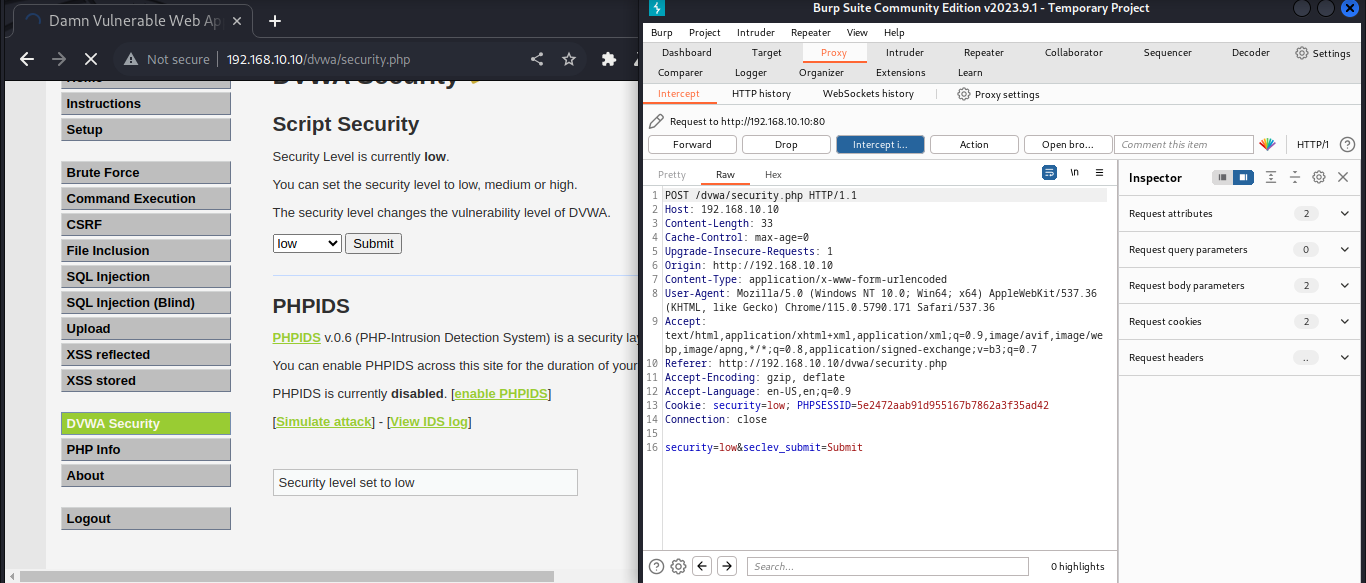
Lo scopo dell’esercizio di oggi è sfruttare la vulnerabilità di «file upload» presente sulla DVWA per prendere controllo della macchina ed eseguire dei comandi da remoto tramite una shell in PHP.

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.

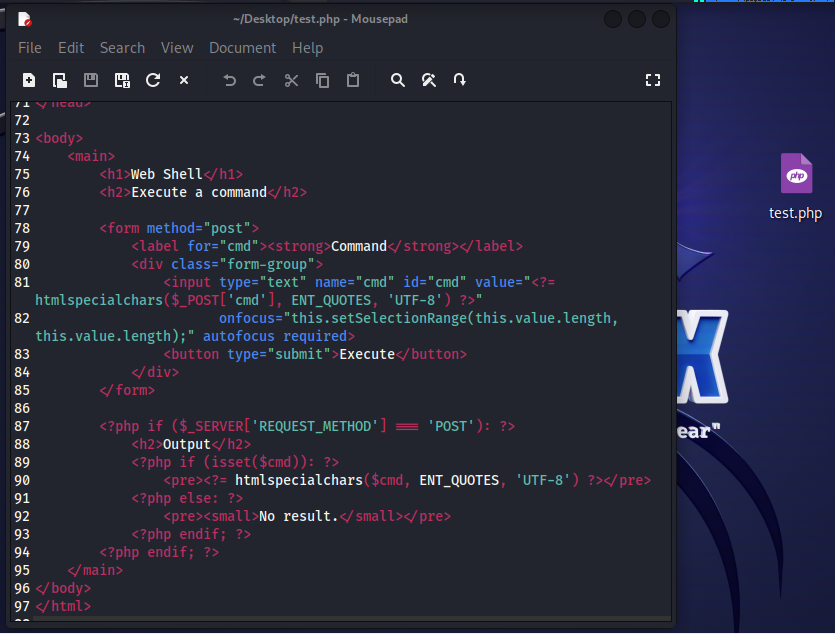
Prima di tutto assicuriamoci che le macchine comunichino tra di loro attraverso il comando Ping:

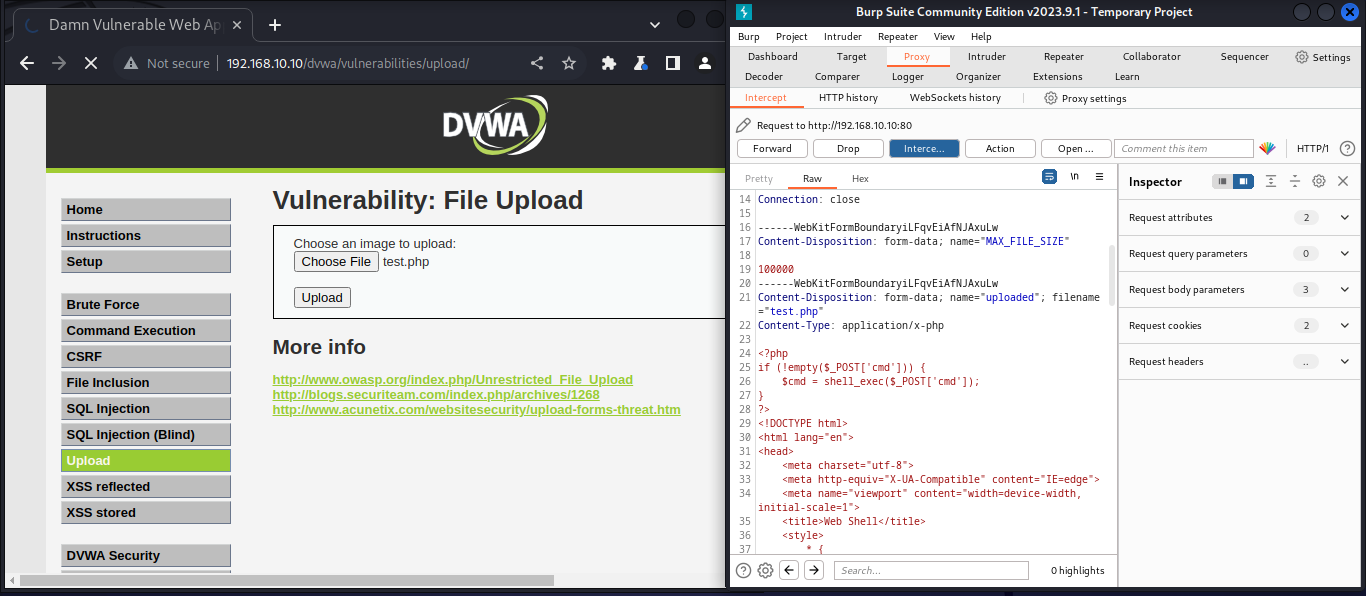


Apriamo **Burpsuite**, strumento per la sicurezza che, tra le altre cose, funge da proxy web e consente agli utenti di intercettare, modificare e ispezionare le richieste e le risposte HTTP tra il browser e il server web. Questo è utile per analizzare il traffico web durante i test, apriamo **DVWA** di Metasploitable2 e per prima cosa impostiamo il livello di sicurezza, in questo caso su low:

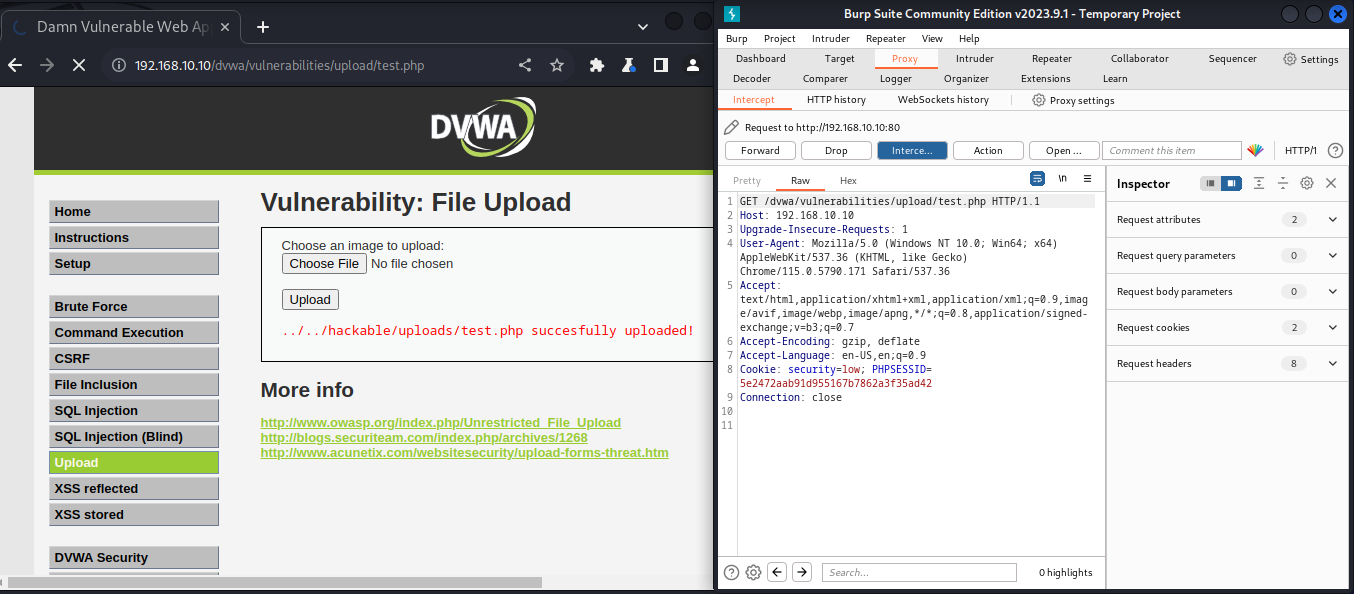


Scriviamo il nostro codice shell in un file di testo, salviamolo (test.php) e apriamo la sezione upload di DVWA. Carichiamo il file e lanciamo l’upload:

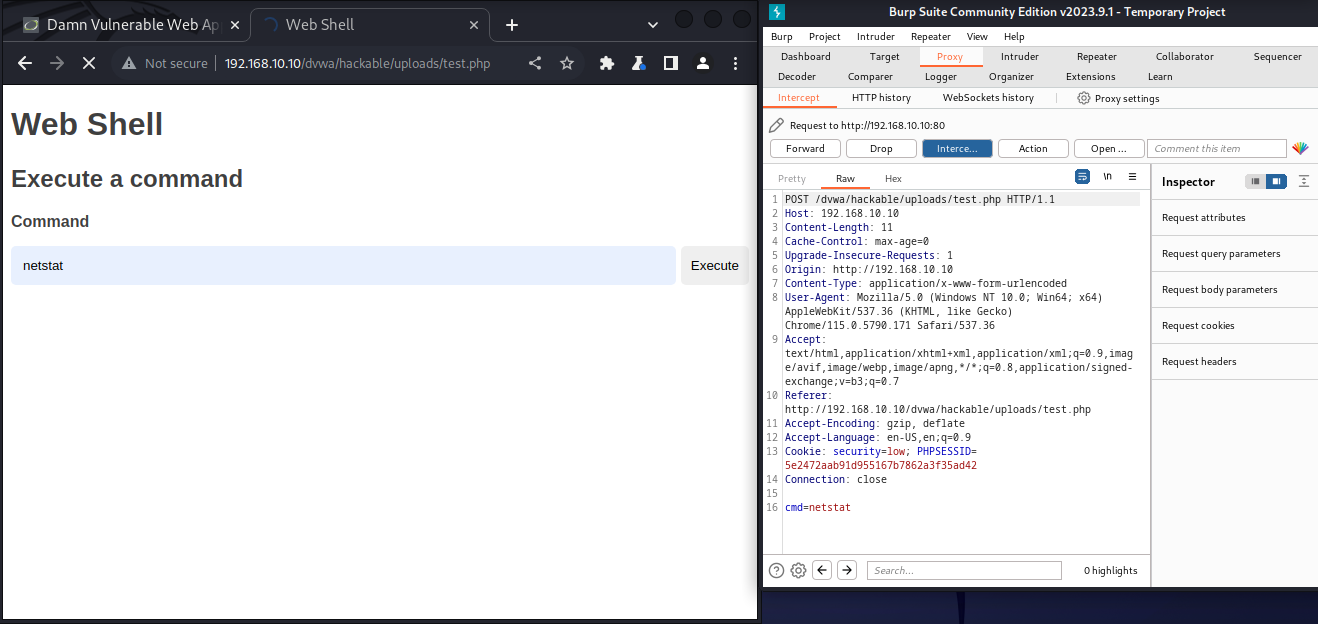


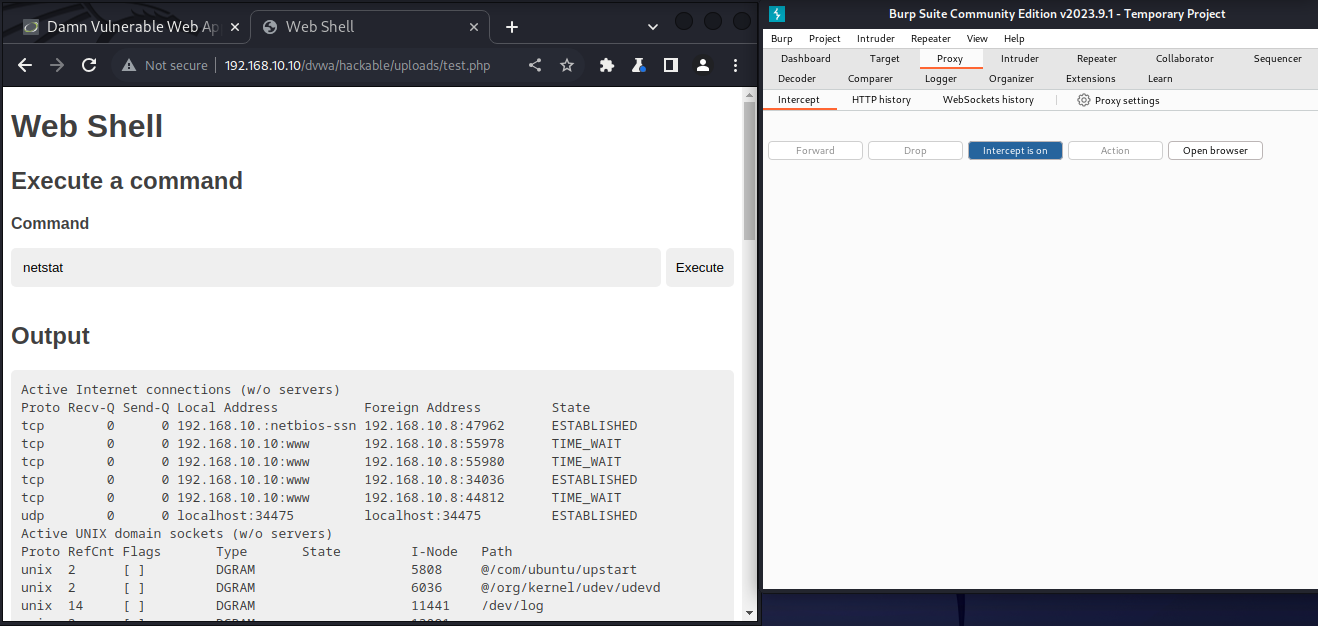


A file caricato uscirà la conferma e la stringa di testo da inserire nel browser per verificare che la shell sia stata caricata:



Cambiamo l’url 192.168.10.10/dvwa/vulnerabilities/upload/test.php 🡪 192.168.10.10/dvwa/hackable/uploads/test.php e vediamo il risultato:





Facciamo una prova con la barra di comandi risultante, ad es. Netstat, utilizzato per visualizzare le informazioni sulle connessioni di rete, le tabelle di routing, le statistiche delle interfacce di rete e altri dettagli.