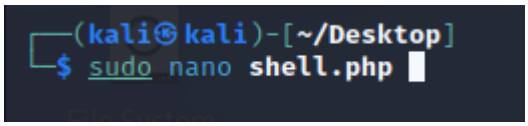
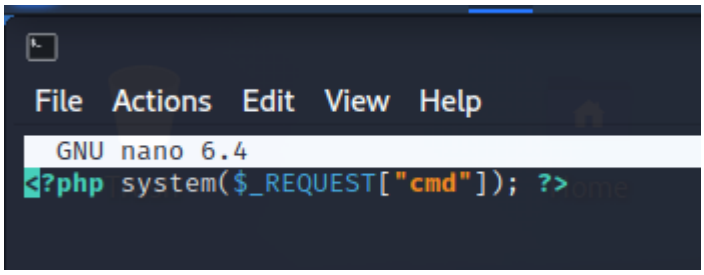
Gabriele Di giampietro **Data 28/11/2022**

Obiettivo: Sfruttare la vulnerabilità su "file upload" della DVWA su metasploitable, attraverso la VM Kali, caricando un shell in PHP per eseguire dei comandi da remoto.

Prima Fase

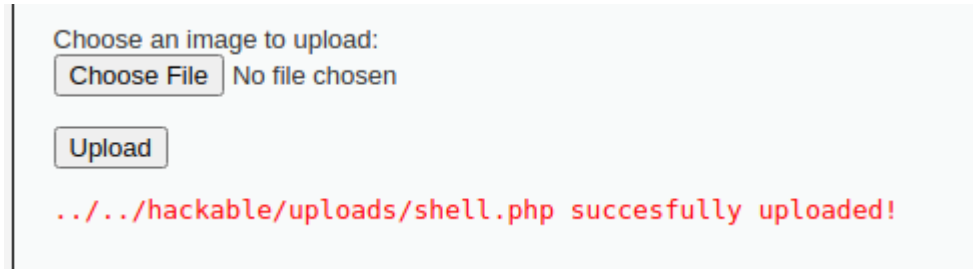
Per prima cosa andiamo a creare la nostra shell in file php che ci faccia inviare una richiesta come **vediamo nelle immagini seguenti.**





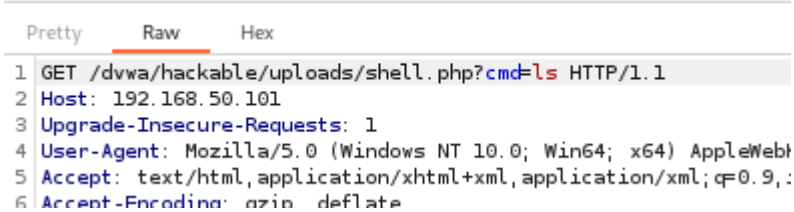
Seconda Fase

Successivamente entriamo tramite browser all'indirizzo url di metasploitable (192.168.50.101), entriamo nella DVWA e cambiamo il livello di sicurezza in low. Dopodiché andiamo a caricare il nostro file php nella sezione upload.



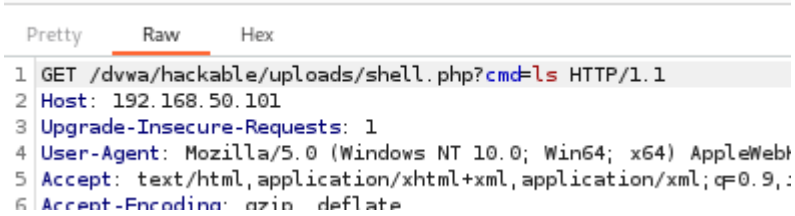
Terza Fase

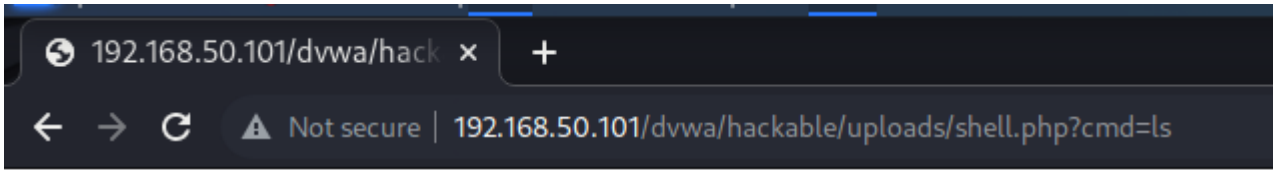
In fine andiamo a verificare che la nostra shell invii i nostri comandi di richiesta, nell'url andiamo ad inserire il nuovo percorso come abbiamo visto sopra in rosso e inseriamo la richiesta di GET con cmd= ls che verifichiamo con il tool Burpsuite in ascolto.



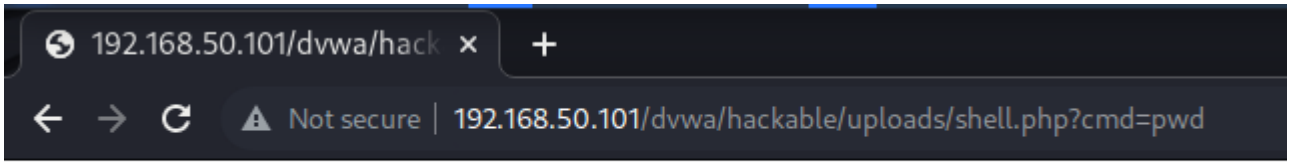
Con il comando ls andiamo a vedere all'interno della directory installata dalla nostra shell, sempre nell'url utilizziamo anche il comando pwd per vedere l'effettivo percorso della nostra shell, utilizzando ls possiamo anche continuare a vedere tutte le sottodirectory aggiungendo /../..

Come possiamo vedere nelle immagini seguenti.

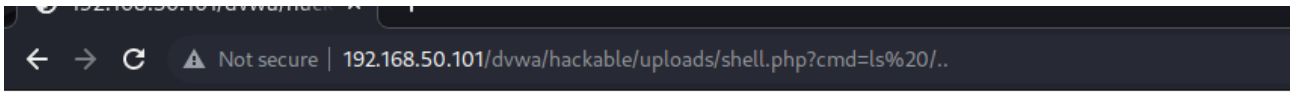




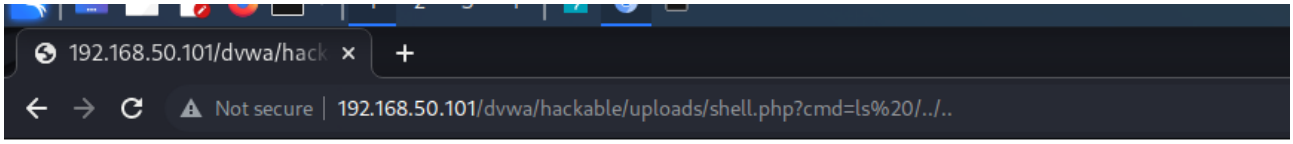
dvwa_email.png shell.php



/var/www/dvwa/hackable/uploads



bin boot cdrom dev etc home initrd initrd.img lib lost+found media mnt nohup.out opt proc root sbin srv sys tmp usr var vmlinuz



bin boot cdrom dev etc home initrd initrd.img lib lost+found media mnt nohup.out opt proc root sbin srv sys tmp usr var vmlinuz