

BUUCTF——web（[极客大挑战 2019]Havefun、[强网杯 2019]随便注、[ACTF2020 新生赛]Includ）

原创

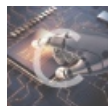
征_程 于 2021-07-13 17:39:20 发布 62 收藏 1

分类专栏：[CTF题目解析](#) 文章标签：[知识图谱](#) [php](#) [安全](#) [web](#)

版权声明：本文为博主原创文章，遵循[CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/LizePing_/article/details/118705186

版权



[CTF题目解析](#) 专栏收录该内容

8 篇文章 0 订阅

订阅专栏

BUUCTF-web

[\[极客大挑战 2019\]Havefun](#)

[做题思路](#)

[\[强网杯 2019\]随便注](#)

[做题思路](#)

[\[ACTF2020 新生赛\]Includ](#)

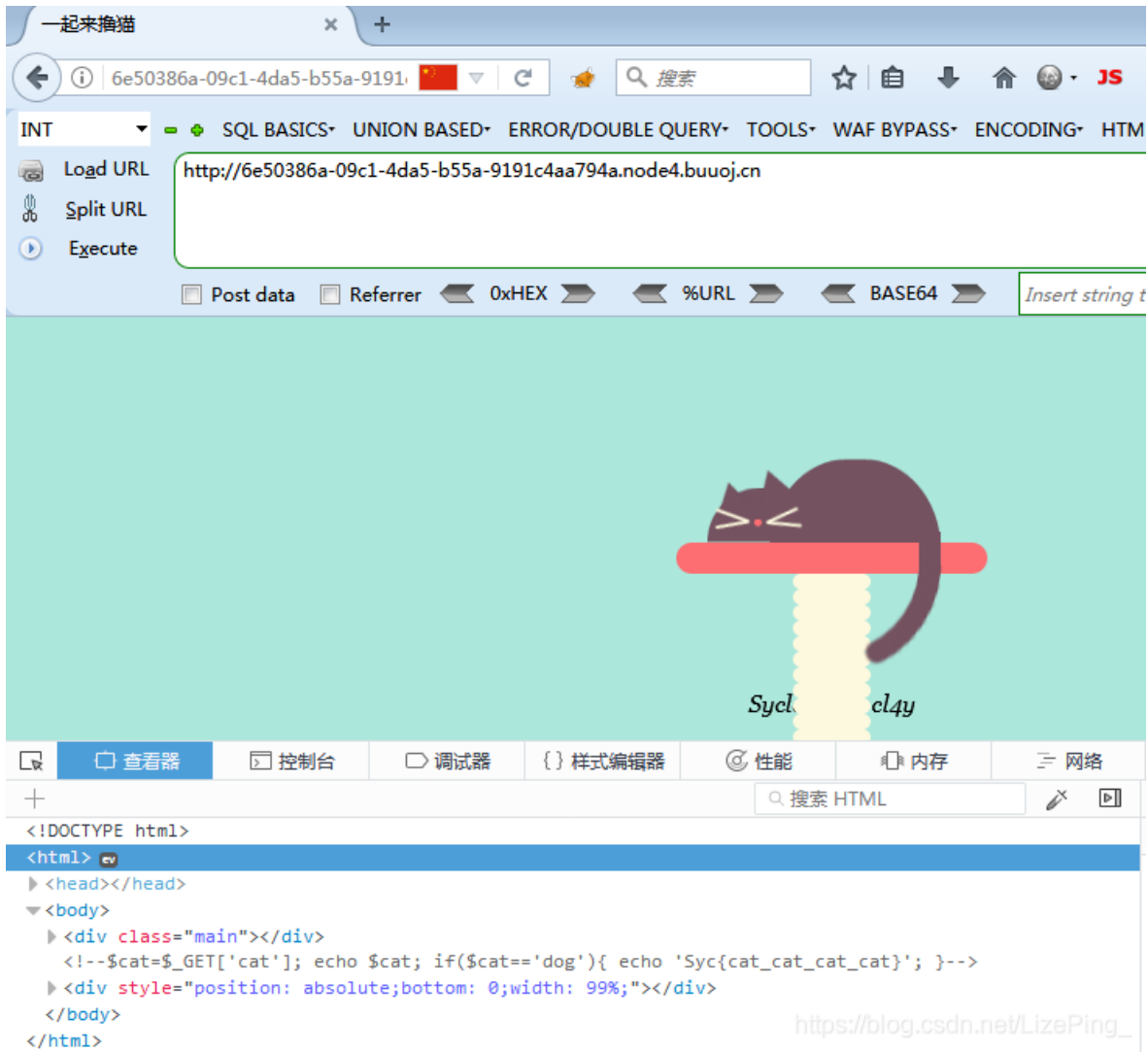
[做题思路](#)

可食用，有助消化，促进身心健康，早睡早起

[\[极客大挑战 2019\]Havefun](#)

[做题思路](#)

一起来撸猫啊！



The screenshot shows a web browser window with the URL `http://6e50386a-09c1-4da5-b55a-9191c4aa794a.node4.buuoj.cn`. The page displays a stylized illustration of a dark purple cat sitting on a red mushroom cap, with a yellow stem. Below the illustration, the text `Sycl cl4y` is visible. The browser's developer tools are open, showing the HTML structure of the page. The code in the developer tools is as follows:

```
<!DOCTYPE html>
<html>
  <head></head>
  <body>
    <div class="main"></div>
    <!--$cat=$_GET['cat']; echo $cat; if($cat=='dog'){ echo 'Syc{cat_cat_cat_cat}'; }-->
    <div style="position: absolute;bottom: 0;width: 99%;"></div>
  </body>
</html>
```

The URL `https://blog.csdn.net/LizePing_` is also visible in the bottom right corner of the developer tools.

根据元素里面的提示，需要用get请求，cat=dog。那就可以构建payload：?cat=dog成功吃鸡

一起来撸猫

6e50386a-09c1-4da5-b55a-9191c4aa794a.node4.buuoj.cn?cat=dog

SQL BASICS UNION BASED ERROR/DOUBLE QUERY TOOLS WAF BYPASS ENCODING HTML ENCRYPTION OTHER XSS

Load URL Split URL Execute

Post data Referrer 0xHEX %URL BASE64

Insert string to replace Insert replacing string

flag{f186a85f-9362-4a62-9780-675fbb148a63}

Syclover @ cl4y

查看器 控制台 调试器 样式编辑器 性能 内存 网络

```
<!DOCTYPE html>
<html>
  <head></head>
  <body>
    <div class="main"></div>
    flag{f186a85f-9362-4a62-9780-675fbb148a63}
    <!--$cat=$_GET['cat']; echo $cat; if($cat=='dog'){ echo 'Syc[cat_cat_cat_cat]'; }-->
    <div style="position: absolute;bottom: 0;width: 99%;"></div>
```

规则 计算后

预览文字

Abc
Georgia Italic 系统

为啥猫要等于狗呢？不理解。。

[强网杯 2019]随便注

做题思路

这个来我的博客看，和bmc2ctf题一样，，我没偷懒！

传送门：[题解地址](#)

[ACTF2020 新生赛]Includ

做题思路

SQL BASICS UNION BASED ERROR/DOUBLE QUERY TOOLS

Load URL Split URL Execute

Post data Referrer 0xHEX %URL

tips

跟随链接点进去

Can you find out the flag?

yes i can!

好，下一题

当然没有这么草率

找了找文件包含漏洞利用的资料

php伪协议，有两种类型 input 和 filter

input需要allow_url_include:On,在input中POST提交的数据都会被当作php代码处理

filter 不需要开启allow_url_fopen 或者 allow_url_include

filter://resource=文件路径（可以绝对或者相对）

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



https://blog.csdn.net/LizePing_

php://filter 伪协议，涨姿势了。

resource=<要过滤的数据流>	指定了你要筛选过滤的数据流。
read=<读链的筛选列表>	可以设定一个或多个过滤器名称，以管道符()分隔。
write=<写链的筛选列表>	可以设定一个或多个过滤器名称，以管道符()分隔。