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

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

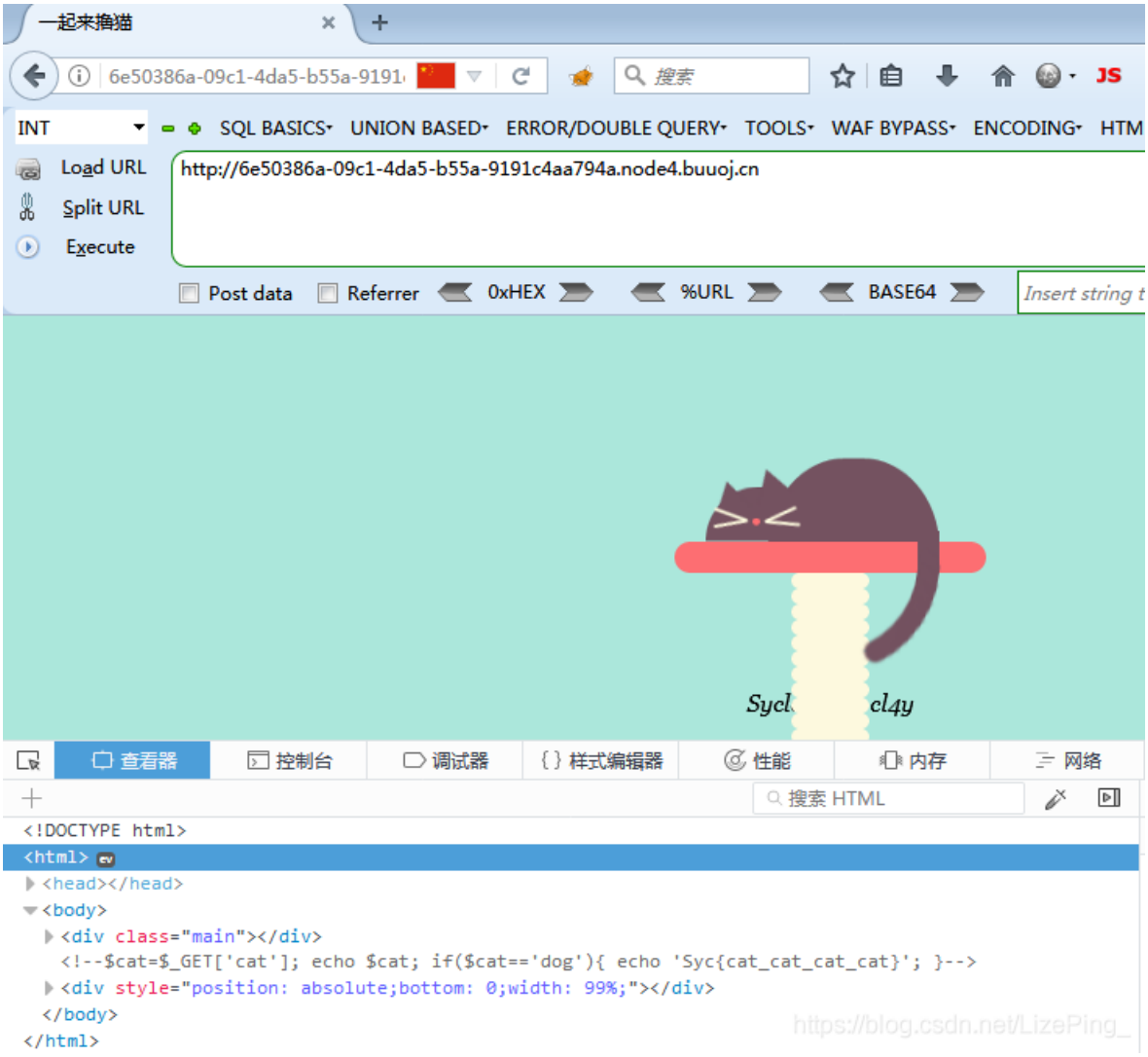
BUUCTF-web

可食用，有助消化，促进身心健康，早睡早起

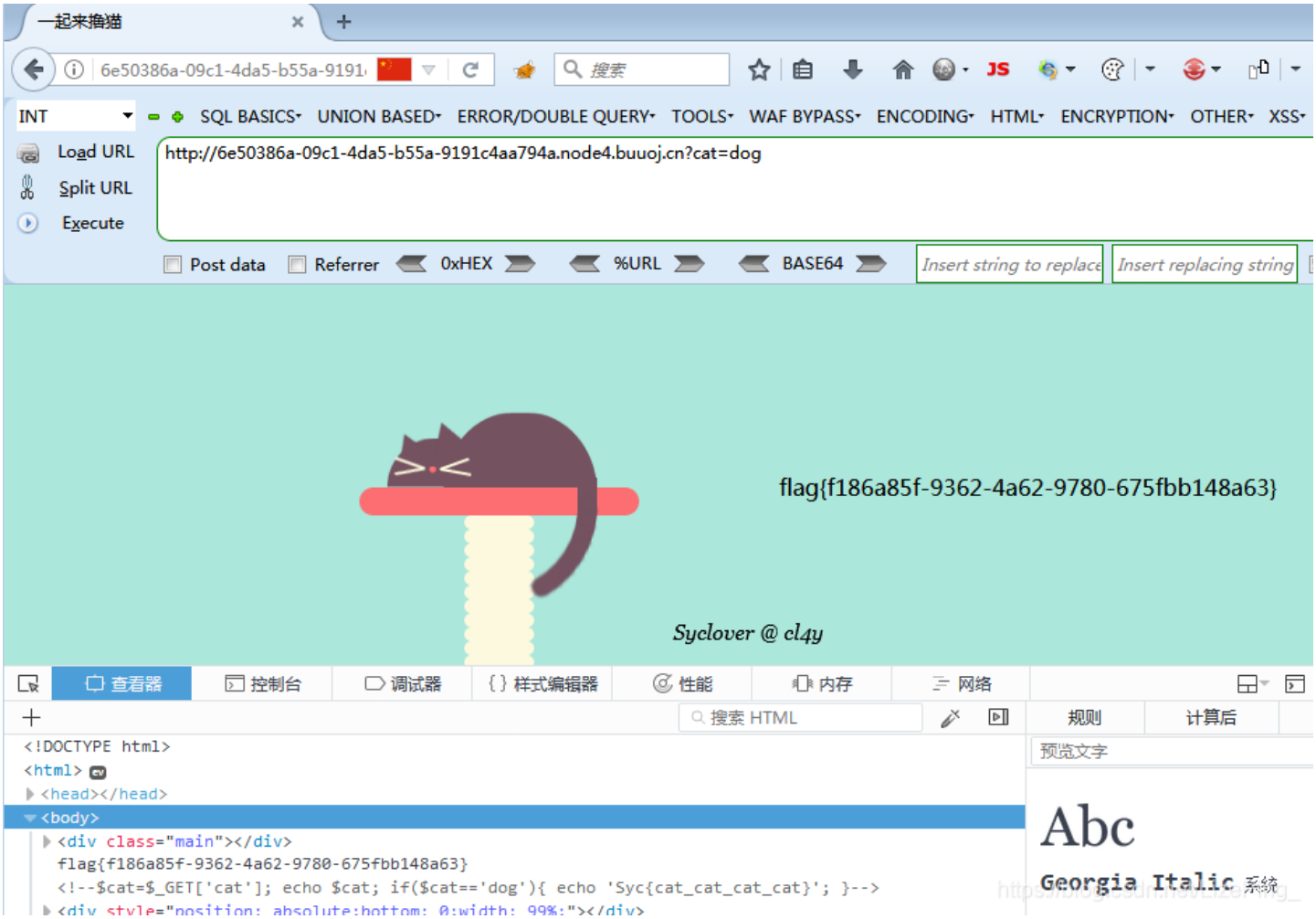
[极客大挑战 2019]Havefun

做题思路

一起来撸猫啊！



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



为啥猫要等于狗呢？不理解。。

[强网杯 2019]随便注

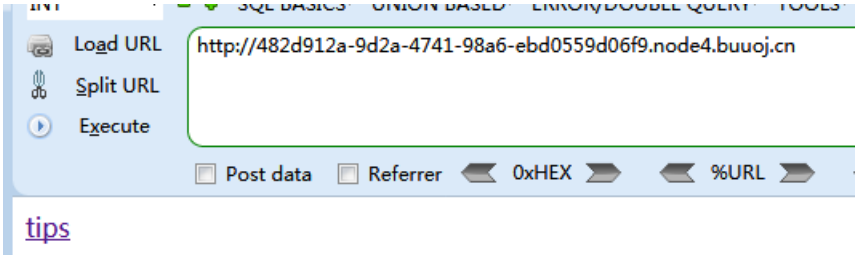
做题思路

这个来我的博客看，和bmzctf题一样，，我没偷懒！

传送门：题解地址

[ACTF2020 新生赛]Includ

做题思路



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

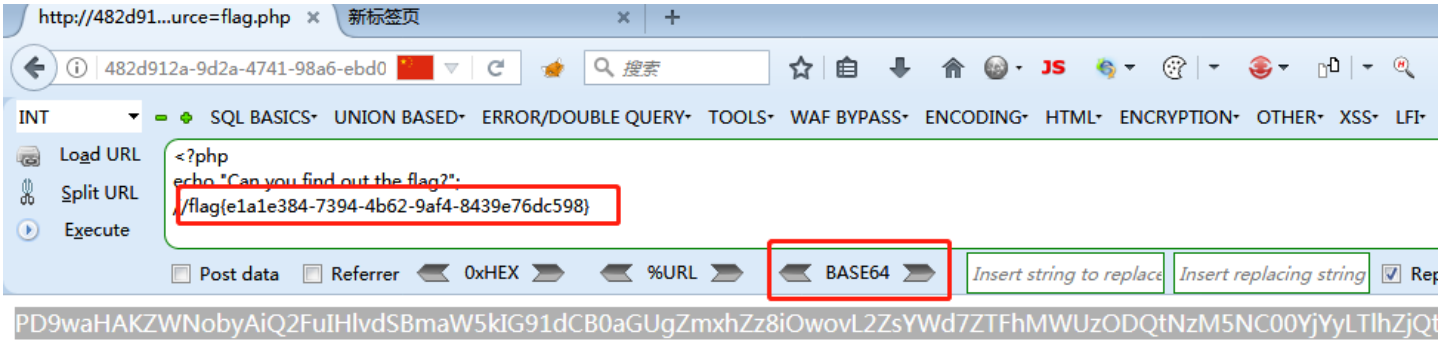
```
找了找文件包含漏洞利用的资料

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



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。