

# Buuctf Http

原创

Dexret 于 2021-12-07 15:50:22 发布 1298 收藏

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

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/Dexret/article/details/121770979>

版权



[buuctf Web](#) 专栏收录该内容

9 篇文章 0 订阅

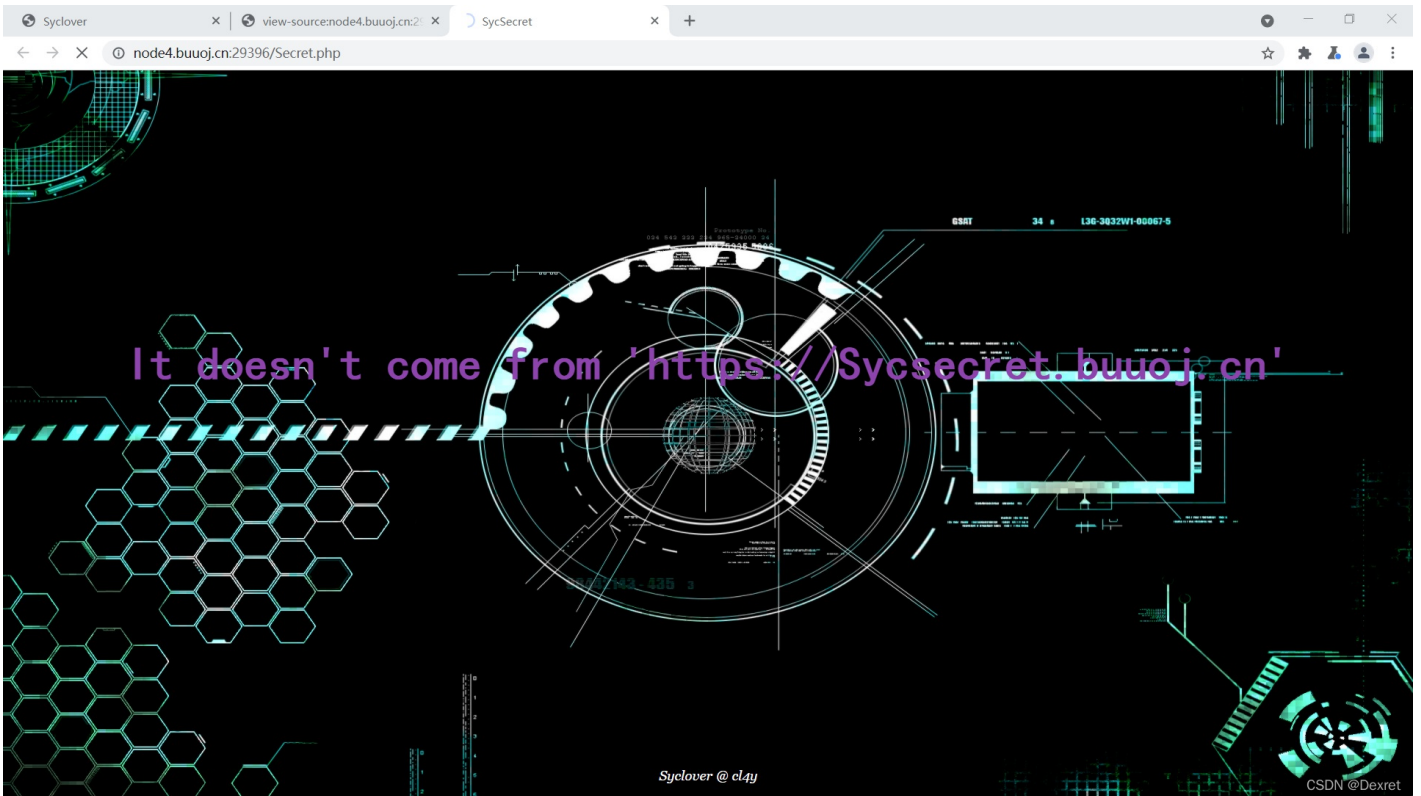
订阅专栏

打开该靶机, 发现该靶机为一个普通的页面

查看一下该网页的源码

```
Syclover x view-source:node4.buuoj.cn:29396 SycSecret x +
不安全 | view-source:node4.buuoj.cn:29396
23 <section id="banner">
24 <div class="inner">
25 <h2>Syclover</h2>
26 <p>Hi Hackers</p>
27 Here is the secret website <br /> of the Syclover <br />
28 </div>
29 <a href="#" class="more scrollly">Learn More</a>
30 </section>
31
32 <!-- One -->
33 <section id="one" class="wrapper style1 special">
34 <div class="inner">
35 <header class="major">
36 <h2>欢迎来到西南某最大卖鞋厂商 !<br />
37 三叶草安全技术小组 (Syclover) </h2>
38 <p>当黑客帝国的梦想成为现实, 你就是下一个奇迹缔造者! <br />
39 三叶草安全技术小组 (Syclover) 等待着同样热爱技术的你 <br />
40 Syclover019招新群: 671301484</p>
41 </header>
42 <ul class="icons major">
43 <li><span class="icon fa-diamond major style1"><span class="label">Lorem</span></span></li>
44 <li><span class="icon fa-heart-o major style2"><span class="label">Ipsum</span></span></li>
45 <li><span class="icon fa-code major style3"><span class="label">Dolor</span></span></li>
46 </ul>
47 </div>
48 </section>
49
50 <!-- Two -->
51 <section id="two" class="wrapper alt style2">
52 <section class="spotlight">
53 <div class="image"></div><div class="content">
54 <h2>小组简介</h2>
55 <p>· 成立时间: 2005年3月<br />
56 · 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 />
57 · 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>!
58 </div>
59 </section>
60 </section>
61 <script src="assets/js/jquery.min.js"></script>
62 <script src="assets/js/jquery.scrollx.min.js"></script>
63 <script src="assets/js/jquery.scrolly.min.js"></script>
64 <script src="assets/js/skel.min.js"></script>
65 <script src="assets/js/util.js"></script>
66 <!--[if lte IE 8]><script src="assets/js/ie/respond.min.js"></script><![endif-->
67 <script src="assets/js/main.js"></script>
68 </script>
69 <footer id="footer">
70 <ul class="copyright">
71 <li>&copy; Syclover</li><li>Design: C14y</li>
72 </ul>
73 </footer>
74 </body>
75 </html>
76
```

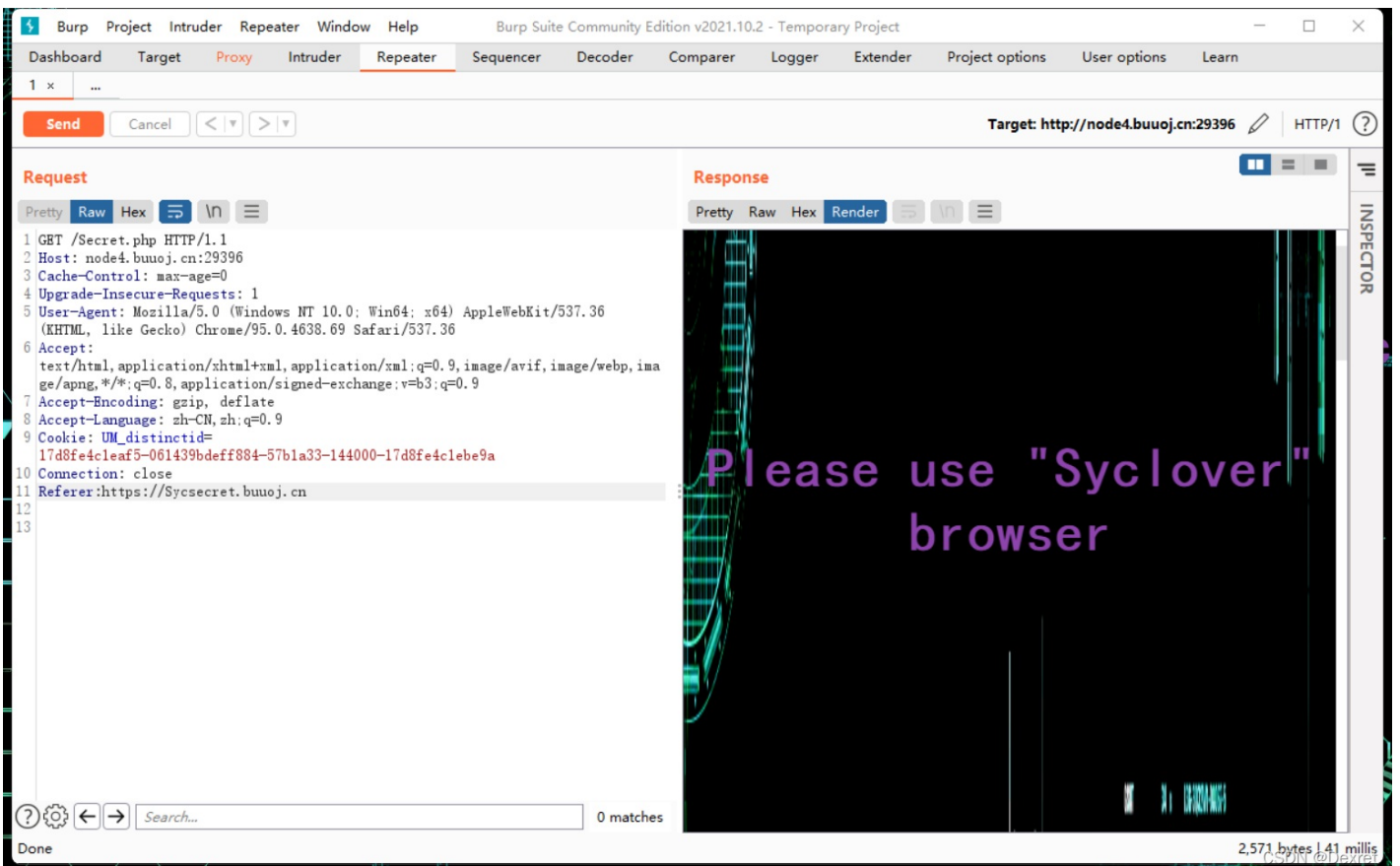
发现有一个Secret.php的网页, 打开该网页



这里提示我们需要从<https://Sycsecret.buuoj.cn>去访问该网页

利用Burpsuite对该网页进行抓包，添加referer值

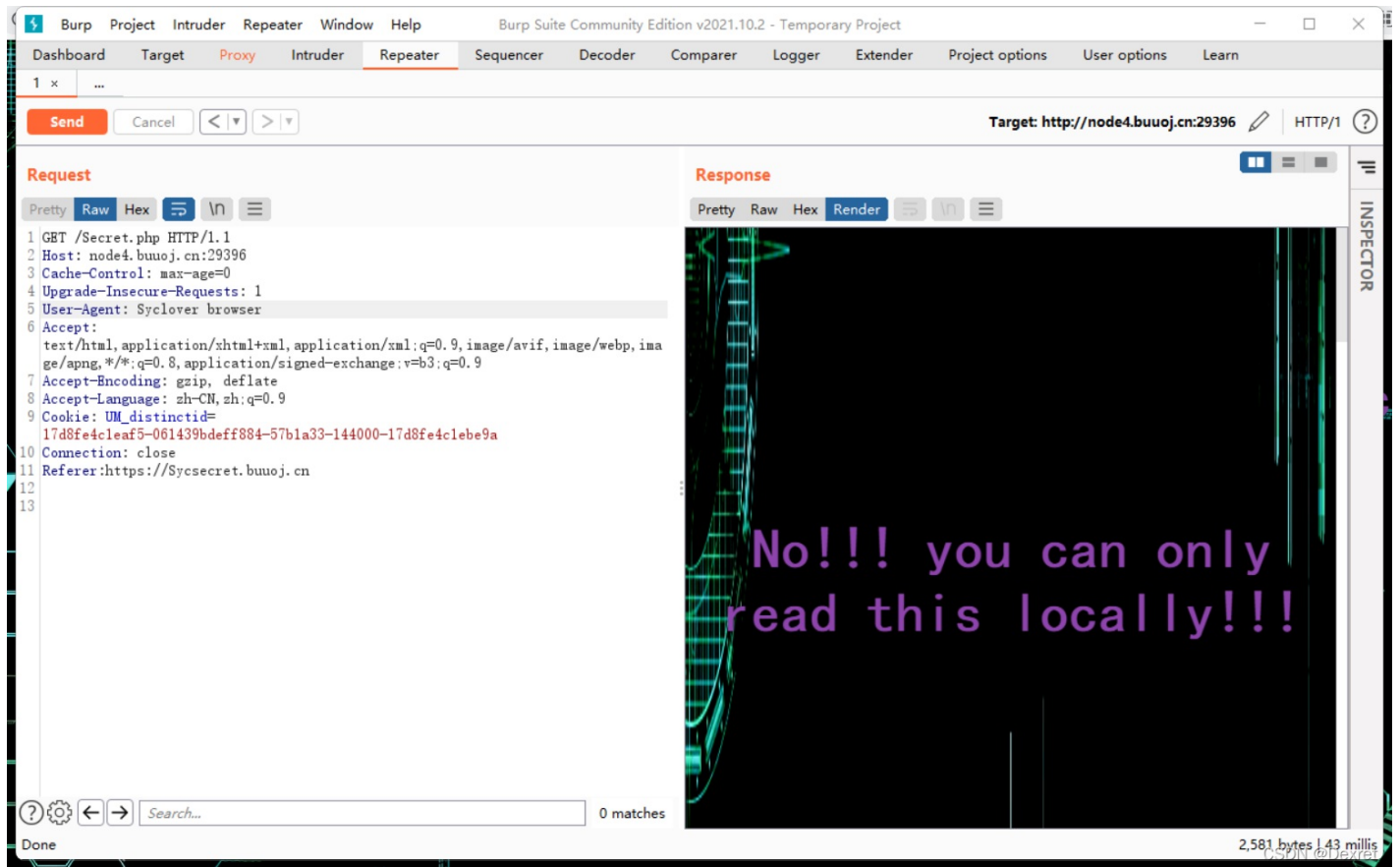
```
Referer: https://Sycsecret.buuoj.cn
```



添加完referer值后发现，又需要我们通过Syclover浏览器去访问该网页

## 修改User-Agent值

User-Agent: Syclover browser



The screenshot shows the Burp Suite interface with the Repeater tab active. The target is `http://node4.buwoj.cn:29396`. The request is as follows:

```
1 GET /Secret.php HTTP/1.1
2 Host: node4.buwoj.cn:29396
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Syclover browser
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=
  17d8fe4c1eaf5-061439bdeff884-57b1a33-144000-17d8fe4c1e9a
10 Connection: close
11 Referer: https://Sycsecret.buwoj.cn
12
13
```

The response is a black image with purple text: `No!!! you can only read this locally!!!`. The status bar at the bottom right indicates `2,581 bytes | 1.43 millis`.

修改完User-Agent值后，这里需要通过本机ip去访问该网页

X-Forwarded-For: 127.0.0.1

The screenshot shows the Burp Suite interface with the Repeater tab active. The target is `http://node4.buuoj.cn:29396`. The request is a GET to `/Secret.php`. The response is a black image with a green grid and a purple flag string: `flag{3f3d1917-c1a4-4ab1-86b9-1e83a68fb400}`. The response size is 2,585 bytes and it took 136 milliseconds to receive.

修改完成后最终获取到该题的flag

```
flag{3f3d1917-c1a4-4ab1-86b9-1e83a68fb400}
```