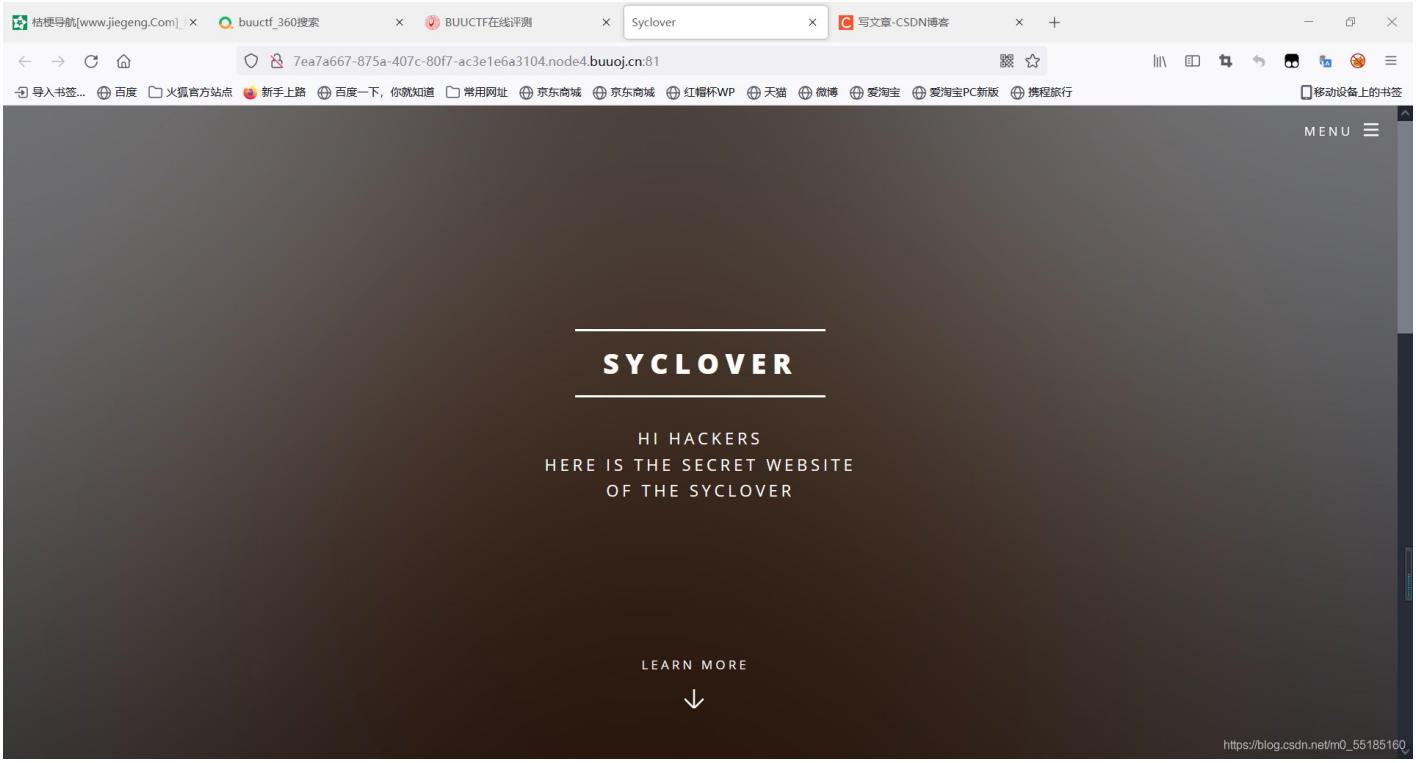
buuctf buyflag wp

原创

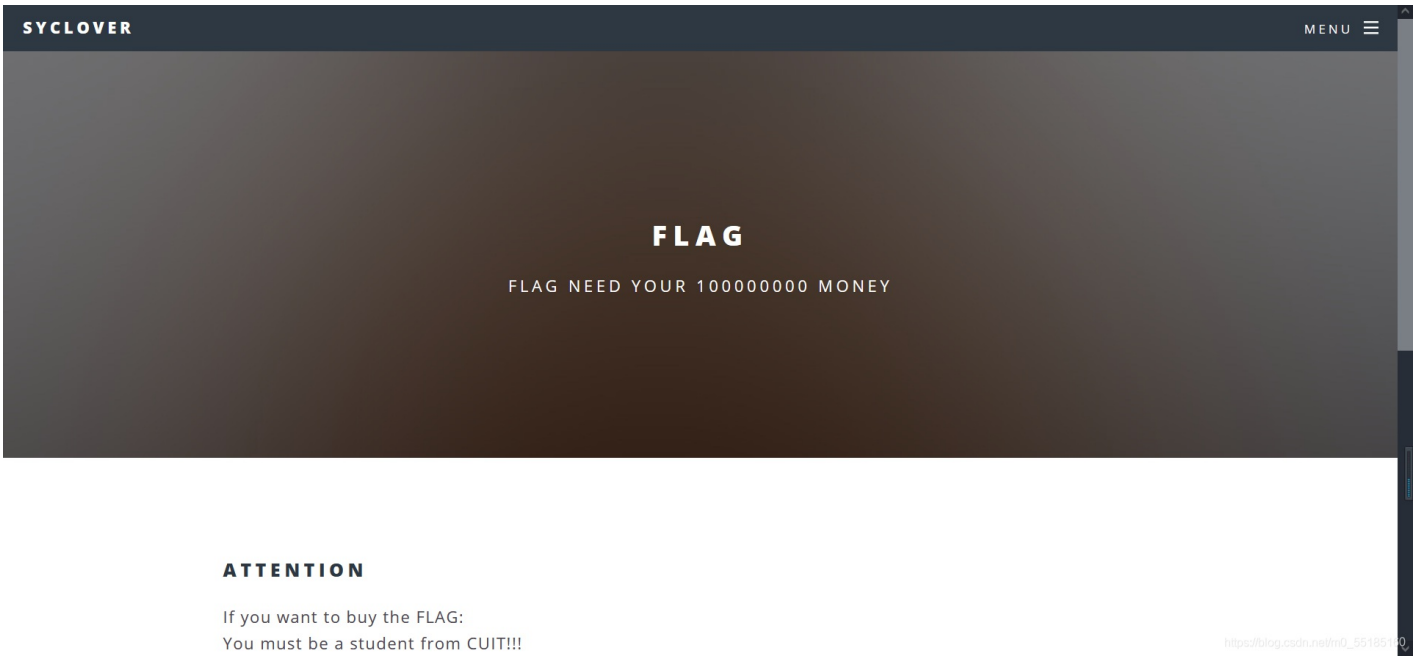
冷血小白 于 2021-08-08 11:26:11 发布 74 收藏
分类专栏： 笔记

本文链接：https://blog.csdn.net/m0_55185160/article/details/119508102

打开网页



点击menu旁的三条线，



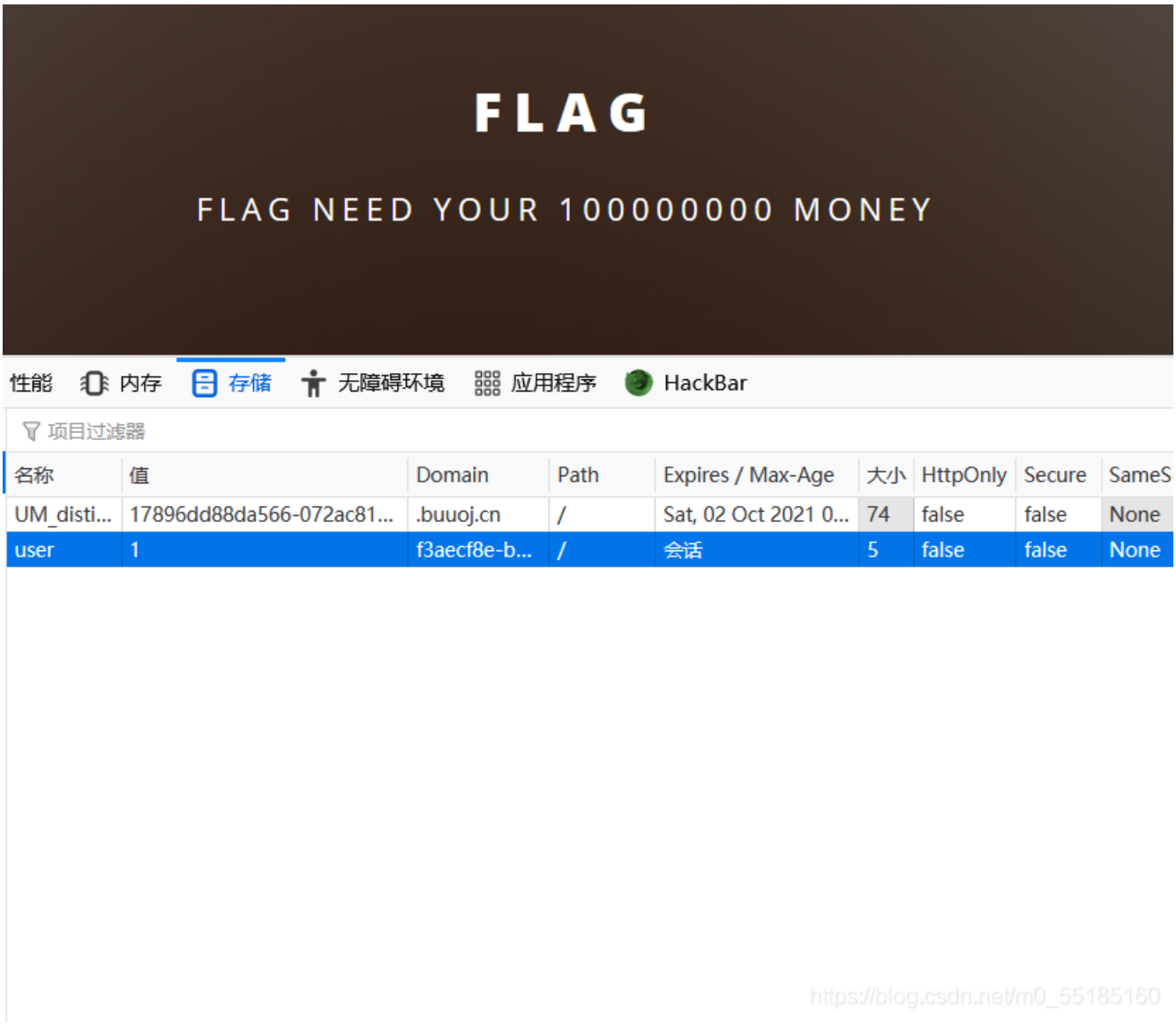
可以看到flag需要100000000来buy，我们查看源代码

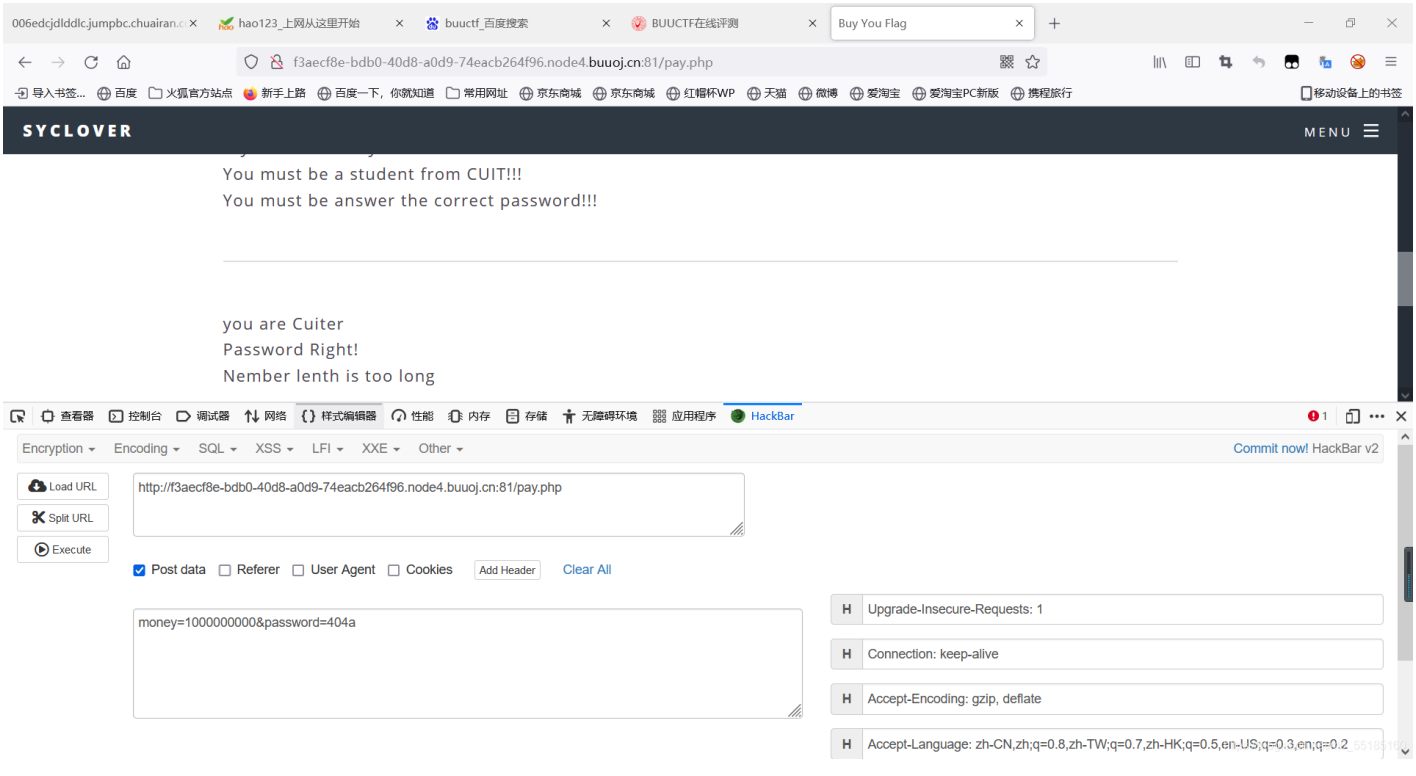
```
<!--
    ```post money and password```
if (isset($_POST['password'])) {
    $password = $_POST['password'];
    if (is_numeric($password)) {
        echo "password can't be number</br>";
    }elseif ($password == 404) {
        echo "Password Right!</br>";
    }
}
-->
</html>

```

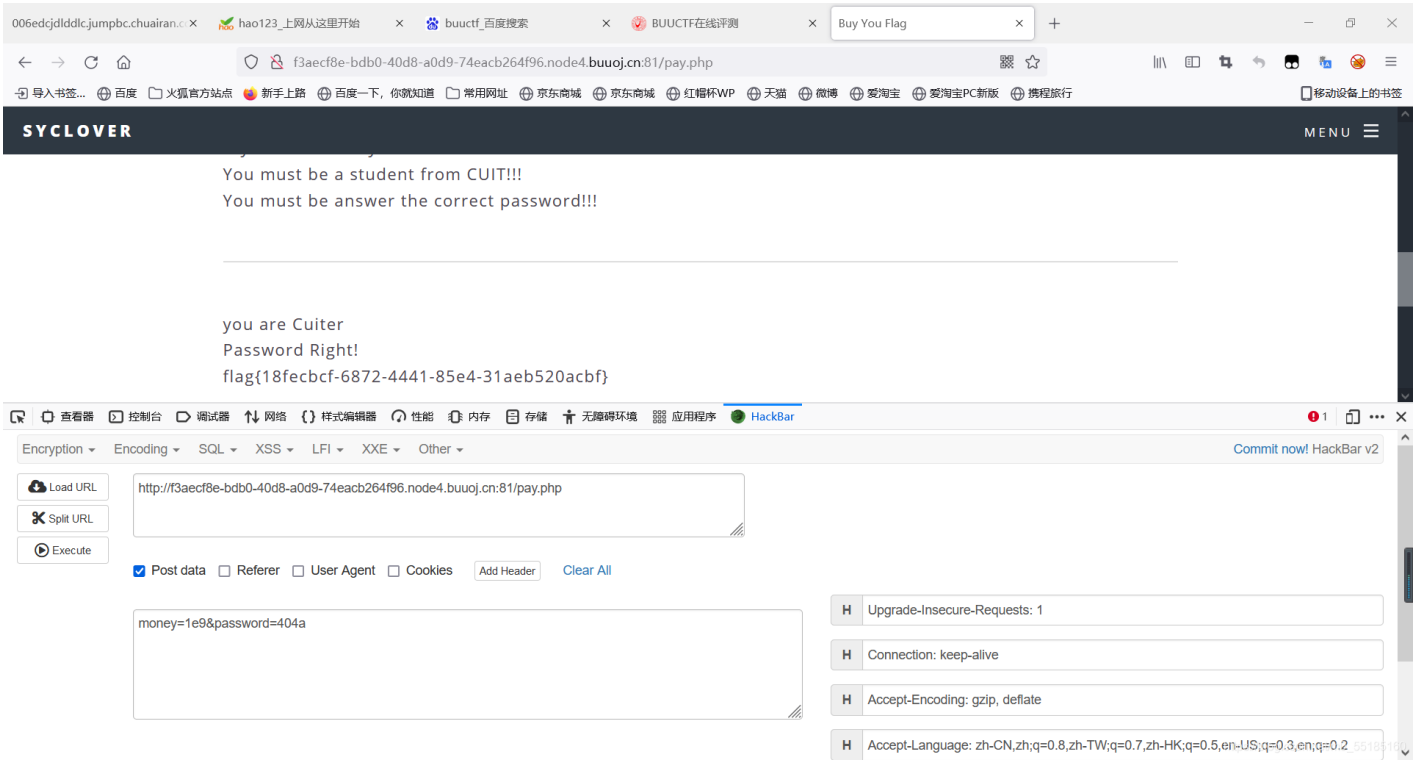
发现这段，通过代码审计后我们知道 通过post方式传参需要传money和password 如果password为404就可以通过。
```

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





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



于是得到flag。