xctf攻防世界honey_shop wp

原创

sash1mi 于 2021-01-15 18:15:30 发布 558 收藏

分类专栏： CTF writeup 文章标签： session cookie 安全

本文链接：https://blog.csdn.net/weixin_46676743/article/details/112682143

CTF 同时被 2 个专栏收录

14 篇文章 1 订阅

订阅专栏

writeup

12 篇文章 0 订阅

订阅专栏

访问题目地址

click to download our sweet images

有1336元，但是要购买Flag需要1337元

Herbs honey

$15

This honey is rich in antioxidants, natural enzymes, unique amino acids, which are so necessary for a person.

★★★☆☆

Buy

Flag honey

$1337

Most important honey for you today!

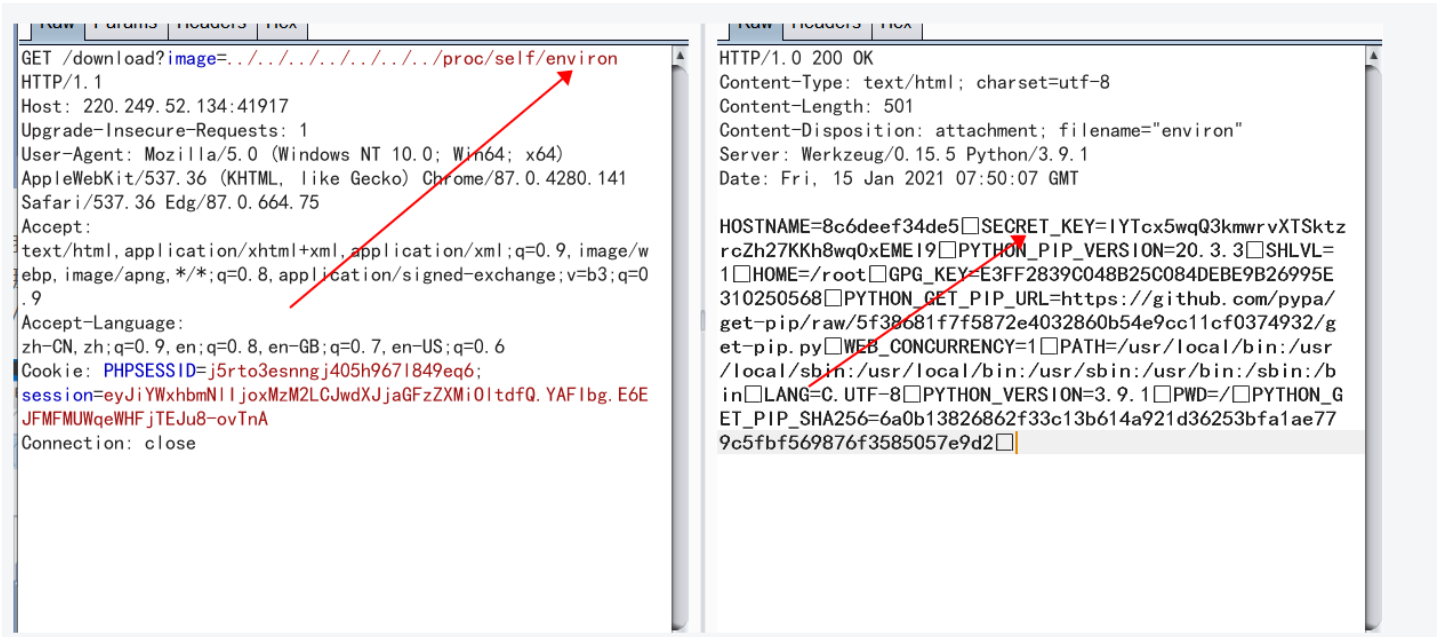
★★★★★

Buy

注意到有一句“click to download our sweet images”，发现访问的是/download?image=1.jpg，这样就可能出现LFI

关于LFI：https://www.cnblogs.com/c1e4r/articles/7806819.html

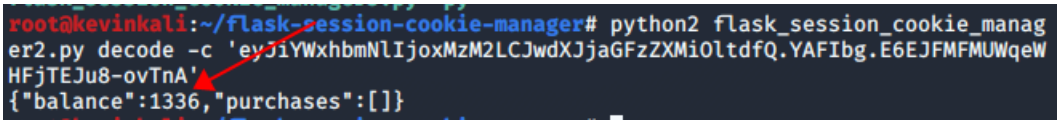
试着读一下/proc的相关信息了，/proc/self/永远指向当前进程，尝试读一下environ文件，这记录着当前进程（本题而言是python）的环境变量信息

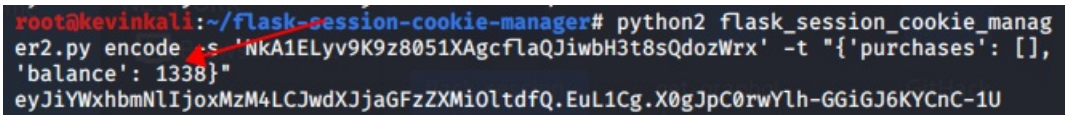


注意这个SECRET_KEY，一会儿要用到

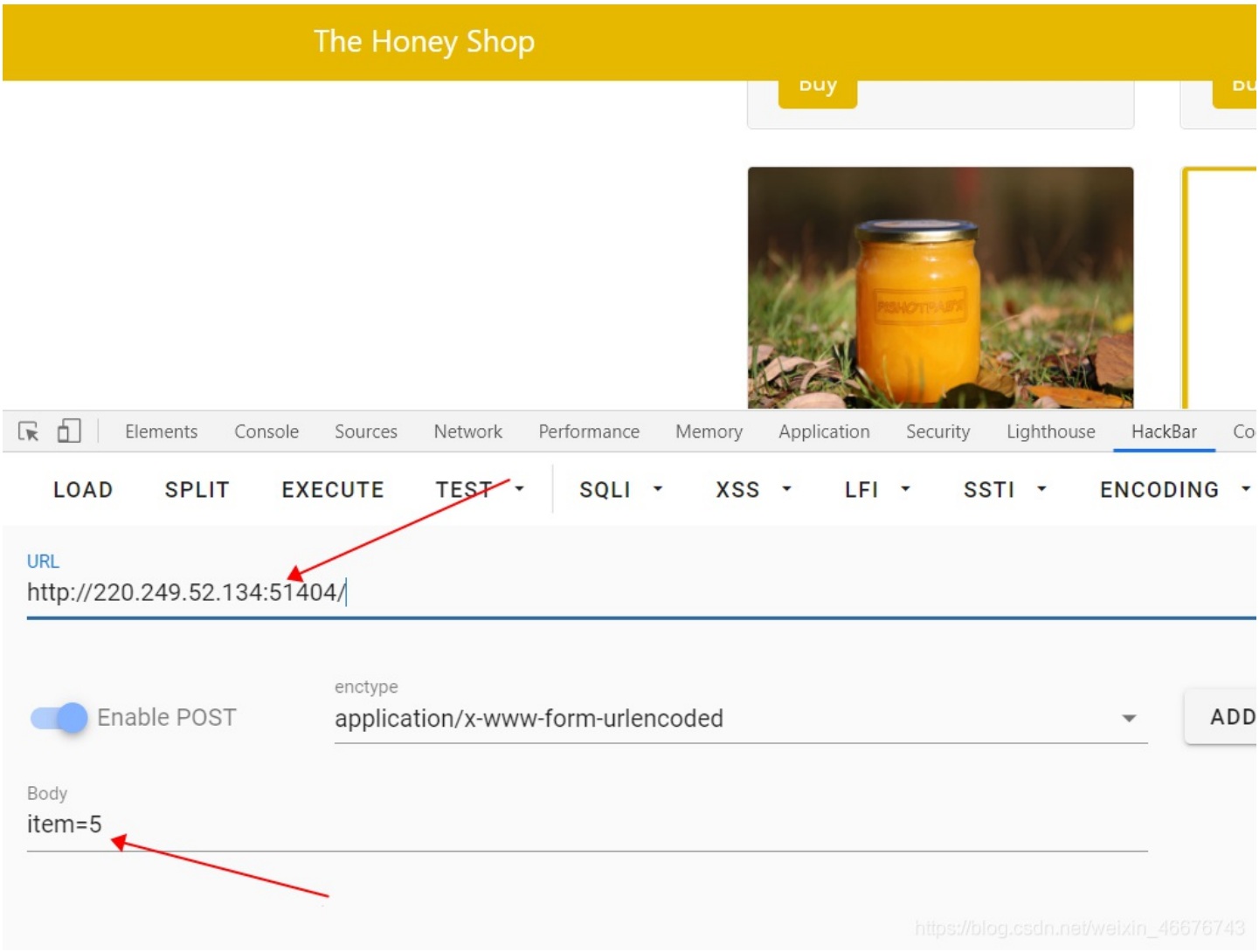
猜测key是用来加密Flask的Cookie的，那么，Cookie就可以解密了，github上有现成的脚本可以用：`https://github.com/noraj/flask-session-cookie-manager`

可以解出Cookie的内容{“balance”:1336,“purchases”:[]}，那么把balance改成1338就可以购买flag了





把当前页面的session改为新的session



攻防世界的题目环境可能有问题，我这儿改了session但钱还是不变，此处已向xctf提出建议，buuctf上的环境可以复现

```
https://buuoj.cn/
```