# 【F2C】hacker101 writeup（更新中）

原创

KANITAN___ 于 2019-07-23 09:16:17 发布 1777 收藏 1

分类专栏： writeup 文章标签： ctf writeup



本文链接：https://blog.csdn.net/KANITAN___/article/details/96964973



Hacker101练习地址

## 目录



一些参考：

https://www.anquanke.com/post/id/180186#h2-1

https://github.com/testerting/hacker101-ctf

https://zhuanlan.zhihu.com/p/61338756

Hacker101](https://ctf.hacker101.com/ctf)练习地址

一些参考：

https://www.anquanke.com/post/id/180186#h2-1

https://github.com/testerting/hacker101-ctf

https://zhuanlan.zhihu.com/p/61338756

## Petshop Pro

**flag0

- Something looks out of place with checkout
- It's always nice to get free stuff

选了个小动物加入购物车之后去结账

checkout界面

```
POST /43a063d40c/checkout HTTP/1.1
Host: 34.74.105.127
Content-Length: 188
Cache-Control: max-age=0
Origin: http://34.74.105.127
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3
770.100 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed
-exchange;v=b3
Referer: http://34.74.105.127/43a063d40c/cart
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: session=eyJjYXJ0IjpbMF0sIm1vZGlmaWVkIjp0cnVlfQ.XTKvXQ.sWSc3unmCOQG1axQ55vqwvP9P3o
Connection: close

cart=%5B%5B0%2C+%7B%22logo%22%3A+%22kitten.jpg%22%2C+%22price%22%3A+8.95%2C+%22name%22%3A+%22Kitten%22%2C+%22des
c%22%3A+%228%5C%22x10%5C%22+color+glossy+photograph+of+a+kitten.%22%7D%5D%5D
```

解码后变成

```
[[0, {"logo": "kitten.jpg", "price": 8.95, "name": "Kitten", "desc": "8\"x10\" color glossy photograph of a kitt
en."}]]
```

提示说要免费，价格改为0再提交一次，flag get#

## flag1

- There must be a way to administer the app
- Tools may help you find the entrypoint

在没看到第二条提示的情况下试了试在url后面加了个login，还真的有[手动狗头]

先试了下注入，不是很行。暴力破解吧那就……

# PostBook

## flag0

- The person with username "user" has a very easy password…

user/password

## flag get#

## flag1

- Try viewing your own post and then see if you can change the ID

第一个helloword是

```
http://35.227.24.107/684e8372d4/index.php?page=view.php&id=1
```

第二个hello everyone是

```
http://35.227.24.107/684e8372d4/index.php?page=view.php&id=3
```

看一下id为2的，flag get#

## flag2

在创建新post的时候发现参数里带了个user_id，改了改

（一开始没找到，原来藏在返回头里），flag get#

## flag3

- 189 * 5

这个题有点重复了，访问id为189*5的页面。

## flag4

- You can edit your own posts, what about someone else's?

第一篇helloworld是admin用户写的，没有编辑按钮，直接从编辑url进入

```
http://35.227.24.107/684e8372d4/index.php?page=edit.php&id=1
```

保存一下，flag get#

## flag5

cookie就是id的md5，改一下访问home页面。