BUUCTF web admin (flask_session问题)

转载

H4ppyD0g 于 2020-02-23 13:54:14 发布 863 收藏 2
分类专栏： CTF
原文链接：https://www.jianshu.com/p/42011eb79f8b

检查源码，发现有注释`<!-- you are not admin -->`，应该是提示用admin账号登录。

两个功能，注册和登录，想到之前做过一个注册admin加空格的题，试了一下不成功。

然后老老实实注册一个普通用户

Hello admin123

Welcome to hctf

显示了自己的用户名，我们的目的因该是让自己的用户名变成admin才行。

change password只能修改自己账号的密码，没有漏洞。

post可能有xss漏洞，交了一个弹框，什么反应都没有，可能只是一个摆设吧。

在change password一栏的源码里有提示`<!-- https://github.com/woadsl1234/hctf_flask/ -->`
说明这个网站是用python的flask搭建的，git下载下来看看。

接下来代码审计就不会了，以下是wp思路

看到了index函数，没有做任何操作，直接返回给了index.html,去找这个文件看看

```
@app.route('/')
@app.route('/index')
def index():
    return render_template('index.html', title = 'hctf')
```

```
{% include('header.html') %}
{% if current_user.is_authenticated %}
<h1 class="nav">Hello {{ session['name'] }}</h1>
{% endif %}
{% if current_user.is_authenticated and session['name'] == 'admin' %}
<h1 class="nav">hctf{xxxxxxxxx}</h1>
{% endif %}
<!-- you are not admin -->
<h1 class="nav">Welcome to hctf</h1>

{% include('footer.html') %}
```


看到flag相关信息，验证session，如果session是admin的session，就会爆出flag。
所以目的就是在index页面把自己的session改成admin的。

知识盲区

flask的session是存储在客户端cookie中的，而且flask仅仅对数据进行了签名。签名的作用是防篡改，而无法防止被读取。而flask并没有提供加密操作，所以其session的全部内容都是可以在客户端读取的。
flask中session的计算是统一的，这里附上找到的脚本
https://pan.baidu.com/s/13H5kJlxhAjTeUoZyj-dC3A 提取码: kxck
密码的计算需要明文加秘钥，而session的计算也一样，明文自己造(这里就需要把明文设成admin)，但是我们需要找到秘钥。

这里说一下这个脚本的用法
解密：`python 1.py decode -s "密钥" -c "session值"`
加密：`python 1.py encode -s "密钥" -t "明文"`

好了，到现在我们已经明确了只要利用自己的session解密，然后把明文部分改成admin在加密一下，伪造session就可以以admin的身份登录而获取flag了。

现在还需要找一个密钥，他就在confg.py文件里`ckj123`

然后根据上面的使用说明就可以获取admin的session，改包后就可以获取flag。