

# CVE-2020-7245 (CTFd账户接管漏洞) 复现

WhiteCat安全小组 今天

以下文章来源于字节脉搏实验室，作者Linux



## 字节脉搏实验室

活在字节海洋里面的一群渔民：我们的方向是那云计算、系统集成、网工、运维、大数据还有那黑暗...

章源自【字节脉搏社区】-字节脉搏实验室

作者-Linux

扫描下方二维码进入社区：



## 0x01 漏洞描述

在CTFd v2.0.0-v2.2.2的注册过程中，错误的用户名验证方式会允许攻击者接管任意帐户，前提是用户名已知并且在CTFd平台上启用了电子邮件功能。



## 0x02 漏洞分析


CTFd v2.0.0版本注册部分的代码

CTFd/CTFd/auth.py#159


CTFd/CTFd/auth.py#207



```
159 def register():
160     errors = get_errors()
161     if request.method == "POST":
162         name = request.form["name"]
163         email_address = request.form["email"]
164         password = request.form["password"]
165
166         name_len = len(name) == 0
167         names = Users.query.add_columns("name", "id").filter_by(name=name).first()
168         emails = (
169             Users.query.add_columns("email", "id")
170             .filter_by(email=email_address)
171             .first()
172         )
173         pass_short = len(password) == 0
174         pass_long = len(password) > 128
175         valid_email = validators.validate_email(request.form["email"])
176         team_name_email_check = validators.validate_email(name)
# 省略部分代码
```

 字节脉搏实验室

```
207     else:
208         with app.app_context():
209             user = Users(
210                 name=name.strip(),
211                 email=email_address.lower(),
212                 password=password.strip(),
213             )
```

 字节脉搏实验室

可以看到用户注册时name参数并未经过任何处理，判断用户名是否重复时使用的就是没有经过任何处理的name值，然而存入数据库时却将这个name值做了 strip处理，去掉name值首尾的空字符。

这就意味着只要注册一个首尾添加空格的用户名即可绕过用户名不能重复的限制。



## CTFd v2.0.0版本找回密码部分的代码

CTFd/CTFd/auth.py#95



```

95 @auth.route("/reset_password", methods=["POST", "GET"])
96 @auth.route("/reset_password/<data>", methods=["POST", "GET"])
97 @ratelimit(method="POST", limit=10, interval=60)
98 def reset_password(data=None):
99     if data is not None:
100         try:
101             name = unserialize(data, max_age=1800)
102         except (BadTimeSignature, SignatureExpired):
103             return render_template(
104                 "reset_password.html", errors=["Your link has expired"]
105             )
106         except (BadSignature, TypeError, base64.binascii.Error):
107             return render_template(
108                 "reset_password.html", errors=["Your reset token is invalid"]
109             )
110
111     return render_template("reset_password.html", mode="set")
112 if request.method == "POST":
113     user = Users.query.filter_by(name=name).first_or_404()
114     user.password = request.form["password"].strip()
115     db.session.commit()
116     log(
117         "logins",
118         format="[{date}] {ip} - successful password reset for {name}",
119         name=name,
120     )
121     db.session.close()
122     return redirect(url_for("auth.login"))

```

字节脉搏实验室

大致可以理解为找回密码时从链接参数中取data值，将其反序列化后获得用户名，即可重置任意用户的密码。



### 利用该漏洞需要以下几步：

- 利用首尾添加空格绕过限制，注册一个与受害者用户名相同的账号
- 找回密码链接发送到自己的邮箱
- 修改自己账号的用户名（与受害者不同）
- 点击重置密码链接，设置新密码



## 0x03 漏洞复现

V&N 2020公开赛HappyCTFd原题， buuoj有对应的环境。



MiaoCTF Users Scoreboard Challenges

Register Login



A cool CTF platform from [ctfd.io](https://ctfd.io)

Follow us on social media:



[Click here](#) to login and setup your CTF

字节脉搏实验室

Powered by CTFd

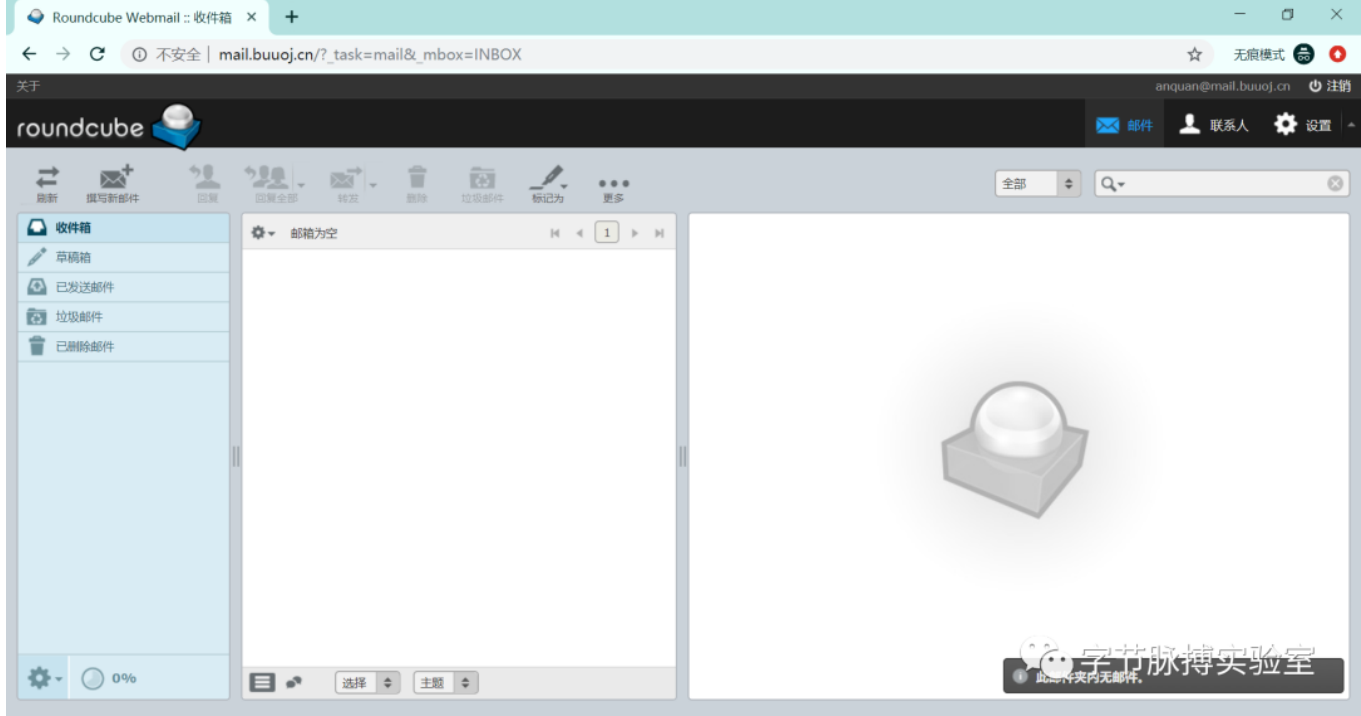
具体操作主要分为以下几步：

- 先在buuoj注册个邮箱
- 利用首尾添加空格绕过限制来注册一个与受害者用户名相同的账号
- 找回密码链接发送到自己的邮箱
- 修改自己账号的用户名（与受害者不同）
- 点击重置密码链接，设置新密码

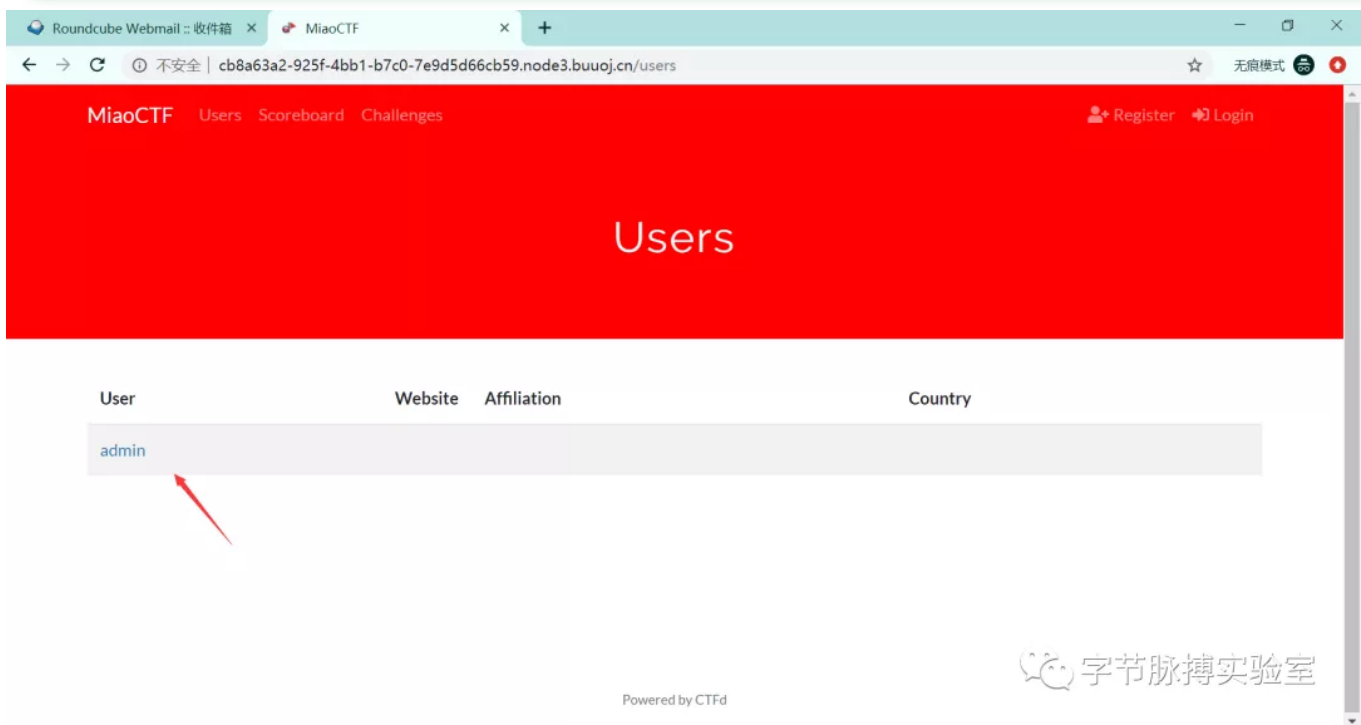
由于buuoj靶机无法访问外网，所以需要在buuoj的邮件系统注册邮箱。

<http://mail.buoj.cn/admin/ui/user/signup/mail.buoj.cn>





然后我们访问靶机地址，发现该ctfd平台有一个admin账号，所以我们尝试重置admin账号的密码。



首先注册一个首或者尾带空格的admin账号，邮箱需要设置正确。



Roundcube Webmail :: 收件箱 x MiaoCTF x +

← → ↻ 不安全 | cb8a63a2-925f-4bb1-b7c0-7e9d5d66cb59.node3.buuoj.cn/register ☆ 无痕模式

MiaoCTF Users Scoreboard Challenges Register Login

## Register

User Name

Email

Password

Submit

字节脉搏实验室

注册成功可以发现自己后台的用户名首尾并没有空格。



Roundcube Webmail :: 收件箱 x MiaoCTF x +

← → ↻ 不安全 | cb8a63a2-925f-4bb1-b7c0-7e9d5d66cb59.node3.buoj.cn/settings ☆ 无痕模式

MiaoCTF Users Scoreboard Challenges Notifications Profile Settings

## Settings

Profile Access Tokens

User Name

Email

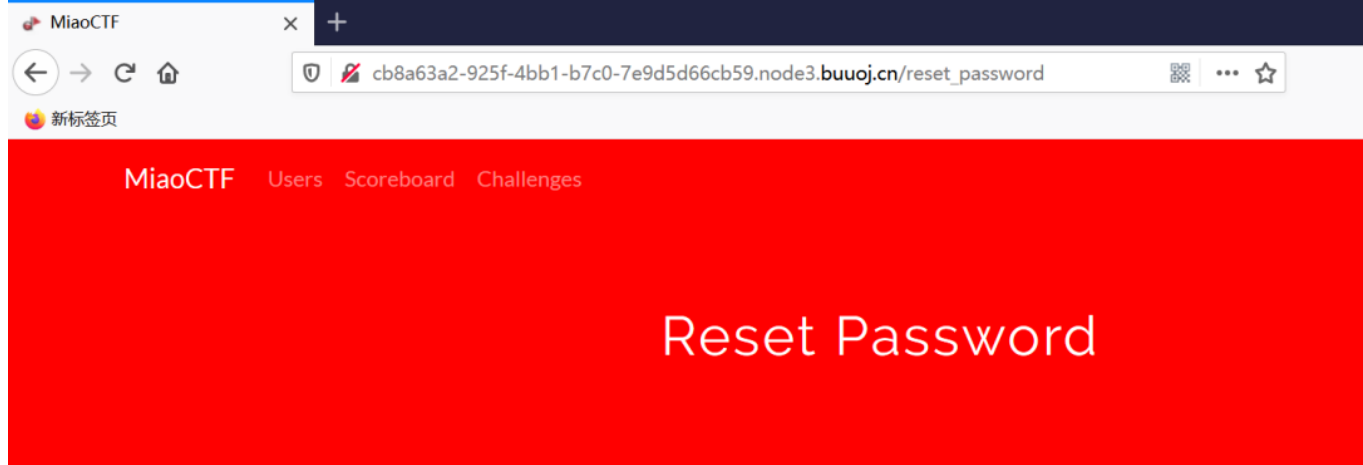
Current Password

New Password

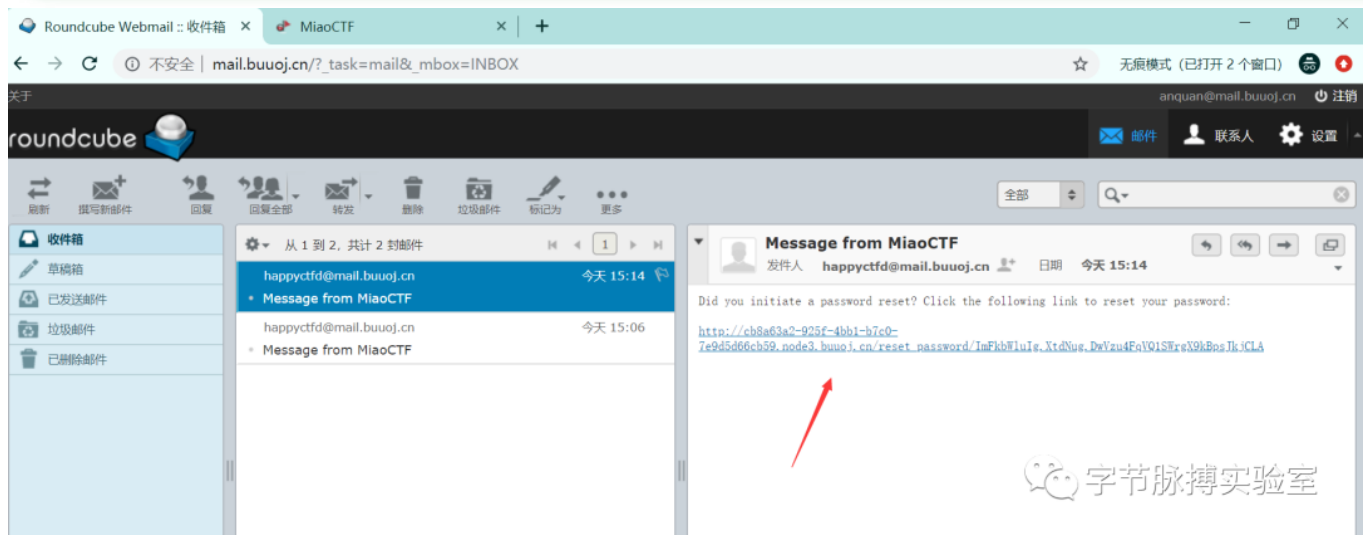
字节脉搏实验室

然后尝试重置admin密码，浏览器另外开一个页面，输入自己注册账号的邮箱，获取重置密码链接。



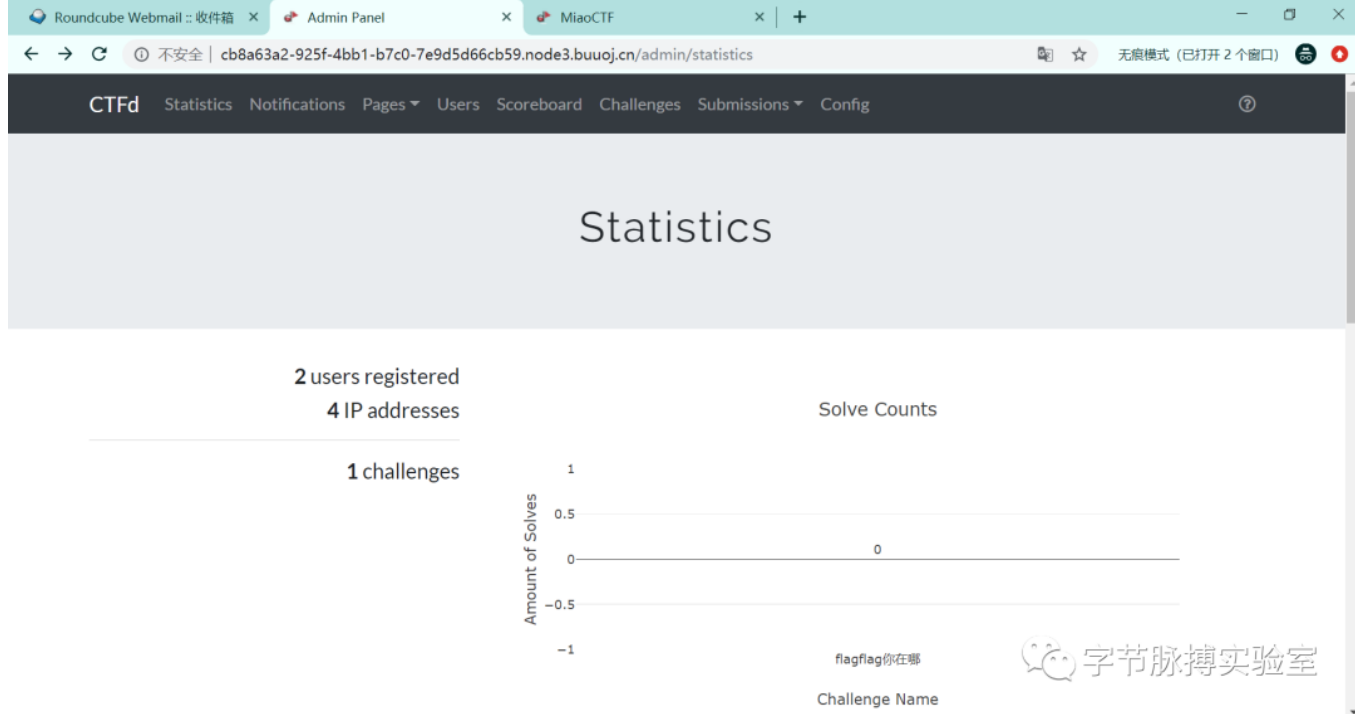


在收件箱中收到重置密码链接后，先不要操作，需要去用户后台页面修改用户名（任意）。



修改完自己的用户名直接点击邮箱里的重置密码链接，对admin账号进行密码重置，设置一个你想要的密码。

再次用admin和你设置的密码登录，就成功拿到了超级管理员权限。



flag 在 challenges 里面找一下，发现有个 "flagflag 你在哪" 的挑战，打开后找到一个 "miaoflag.txt" 的附件，即 flag。

Solves Flags Files Tags Hints Requirements

Files

File Settings

miaoflag.txt

选择文件 未选择任何文件

Attach multiple files using Control+Click or

Name

Challenge Name

flagflag你在哪

Category

Challenge Category

Misc

Message

miaoflag.txt - 记事本

文件(E) 编辑(E) 格式(O) 查看(V) 帮助(H)

flag{2d148dfa-c473-4633-887d-801924b2be60}

## 0x04 漏洞修补

更新CTFd为最新版即可。

参考链接：

<https://www.colabug.com/2020/0204/6940556/amp/>

### 通知！

公众号招募文章投稿小伙伴啦！只要你有技术有想法要分享给更多的朋友，就可以参与到我们的投稿计划当中哦~感兴趣的朋友公众号首页菜单栏点击【商务合作-我要投稿】即可。期待大家的参与~