

## 任意用户密码重置（一）：重置凭证泄漏

人

共60976人围观，发现9个不明物体

WEB安全

数据安全

\*本

本文属 FreeBuf 原创奖励计划，未经许可禁止转载。

在  
者

析，这次，关注我们，分享每日精选文章

重置最为常见，可能出现在新用户注册页面，也可能是用户登录后重置密码的页面，其中，密码找回功能是重灾区。我把日常渗透过程中遇到的案例作了漏洞成因分析，这次，关注男重置凭证泄漏导致的任意用户密码重置问题。

### 案例一

用邮件找回密码时，作为重置凭证的验证码在 HTTP 应答中下发客户端，抓包后可轻易获取。先用攻击者账号走一密码找回流程，测试账号 yangyangwithgnu@yeah.net 选用邮箱找回密码：



点击获取验证码后抓取如下应答：



关注我们 分享每日精选文章

其中，VFCode 从字面理解很可能是校验码。登录邮箱查看网站发过来的密码找回邮件：



关注我们 分享每日精选文章

发现两者一致，那么，几乎可以确认服务端将密码找回的校验码泄漏至客户端，可导致任意账号密码重置问题。

尝试找回普通账号的密码。密码找回首页输入邮箱后，系统将立即校验该邮箱是否注册：



关注我们 分享每日精选文章

将 UName 参数定义为枚举变量，以常见 qq 邮箱作为字典，可枚举出多个有效邮箱：



关注我们 分享每日精选文章

以 chenwei@qq.com 为例，在应答包中找到校验码，成功将其密码重置为 PenTest1024，验证可登录：



关注我们 分享每日精选文章

尝试找回管理员账号的密码。从该网站的域名注册信息中找到联系人的邮箱为 fishliu@xxxx.cn，可推测后台用户的箱后缀为 @xxxx.cn，所以，用常见后台用户名简单调整可构造出后台用户邮箱字典，枚举出大量后台用户：





关注我们 分享每日精选文章

同理可重置这些后台用户的账号密码，为避免影响业务，不再实际操作。

## 案例二

用邮件找回密码时，带凭证的重置链接泄漏至客户端，抓捕可获取。用攻击者账号走一次密码找回流程。在找回密码页面输入攻击者账号及其邮箱（yangyangwithgnu、yangyangwithgnu@yeah.net）后提交：





关注我们 分享每日精选文章

拦截如下应答：





关注我们 分享每日精选文章

显然是个重定向，isVerify、PassPhrase 这两个参数很可疑，后续交互中应留意，先放包，进入发送重置邮件的页面输入验证码后提交。登录攻击者邮箱查看重置邮件：



关注我们 分享每日精选文章

这个带 token 的重置链接似曾相识，对，就是前面抓包获取的 token 信息，比对看下：

```
forgotPwdEa.php?isVerify=eWfuZ3lhbm d3aXR oZ251fHlhbmd5YW5nd2l0aGdudUB5ZW FoLm51dHw2M
```

```
forgotPwdEc.php?isVerify=eWfuZ3lhbm d3aXR oZ251fHlhbmd5YW5nd2l0aGdudUB5ZW FoLm51dHw2M
```

唯一区别 forgotPwdEa 和 forgotPwdEc 两个文件名。

接下来验证通过服务端泄漏的 token 能否重置普通用户的账号密码。从重置流程可知，要重置密码必须提供用户名其邮箱（或手机号）。





关注我们 分享每日精选文章

对应请求、应答如下：



关注我们 分享每日精选文章

用户名已存在返回 failed，不存在返回 ok。以此特征，用常见国人姓名字典，可枚举出大量有效用户名（如 chenchuan、chenanqi、chenanxiu、zhangfeng 等等），存为 username.txt。

获取有效用户名对应邮箱。密码找回首页提交的请求中，user\_name 与 email 参数匹配情况下，HTTP 应答代码为 302，交互包如下：



关注我们 分享每日精选文章

可以此特征枚举有效用户名及其邮箱。现在考虑如何制作邮箱字典？很多用户喜欢用用户名注册 qq 邮箱，换言之，用户名 yangyangwithgnu 可能对应邮箱 yangyangwithgnu@qq.com。所以，用前面已经获取有效用户名字典 username.txt 快速制作了邮箱字典 qq-email.txt，其中，username.txt 与 qq-email.txt 逐行对应。

例如，前者第一行为 yangyangwithgnu、后者第一行为 yangyangwithgnu@qq.com。将上面的数据包放入 burp 的 intruder 中，攻击类型选 pitchfork、user\_name 的参数值定义为枚举变量 1 并加载字典 username.txt、email 的参数值定义为枚举变量 2 并加载字典 qq-email.txt，可枚举出大量有效用户名/邮箱信息，如，zhangfeng/zhangfeng@qq.com、chenchuan/chenchuan@qq.com 等等。

用普通账号 chenchuan/chenchuan@qq.com 演示密码重置漏洞。输入用户名、密码提交，正常完成密码找回逻辑，从响应包中获取服务端下发的重置 token：

拼装为重置链接 [http://www.xxxx.com/user/forgotPwdEc.php?](http://www.xxxx.com/user/forgotPwdEc.php?isVerify=Y2hlbmNodWFufGN0ZW5jaHVhbkbXcS5jb218MTE2MDIzNw==&PassPhrase=cbf0160662358808f3586868f04aa)

[isVerify=Y2hlbmNodWFufGN0ZW5jaHVhbkbXcS5jb218MTE2MDIzNw==&PassPhrase=cbf0160662358808f3586868f04aa](http://www.xxxx.com/user/forgotPwdEc.php?isVerify=Y2hlbmNodWFufGN0ZW5jaHVhbkbXcS5jb218MTE2MDIzNw==&PassPhrase=cbf0160662358808f3586868f04aa)，访问之，即可进入密码重置页面：



关注我们 分享每日精选文章

输入新密码 PenTest1024 后系统提示修改成功。用 chenchuan/PenTest1024 成功登录：



关注我们 分享每日精选文章

防御措施上，密码找回的凭证切勿下发客户端，另外，校验邮箱是否有效应添加图片验证码，以防止关键参数被枚举。

**\*本文作者：yangyangwithgnu，本文属 FreeBuf 原创奖励计划，未经许可禁止转载。**

上一篇：[大数据安全保护思考](#)

下一篇：[本篇已是最新文章](#)

已有 **9** 条评论

比尔.绿帽 2018-01-22

1楼 回

不错，继续

亮了

tombstonc 2018-01-22

2楼 回

见到



支持作者继续分享

亮了

想个

3楼 回

给改:

亮了

yangyangwithgnu (3级) 任何事情都有无穷乐趣! yangyangwithgnu.gi... 2018-01-22

关注我们 分享每日精选文章

@ 想个名字好难

知道是哪个站?

亮了

想个名字好难 (1级) 2018-01-22

@ yangyangwithgnu \*\*维? 不知道对不对? 搜了一下, 收到的, 感觉界面、地址啥的和你文中的图是一样的。。。

亮了

yangyangwithgnu (3级) 任何事情都有无穷乐趣! yangyangwithgnu.gi... 2018-01-22

@ 想个名字好难

来人, 发现一个社工高手。

亮了

想个名字好难 (1级) 2018-01-22

@ yangyangwithgnu 大神, 别闹。。。

亮了



苏苏苏苏苏 (1级) 2018-01-22

4楼 回

谢谢大神分享，

亮了

nolove 2018-01-22

5楼 回

有一  
请继



亮了

选择

昵称 关注我们 分享每日精选文章

请输入昵称

必须 您当前尚未登录。[登陆?](#) [注册](#)

邮箱

请输入邮箱地址

必须（保密）

表情 插图

提交评论(Ctrl+Enter) [取消](#) ☒ 有人回复时邮件通知我



[yangyangwithgnu](#)

任何事情都有无穷乐趣！ [yangyangwithgnu.github.io](#)

2  
文章数

2  
评论数

最近文章

- 任意用户密码重置（一）：重置凭证泄漏

- 不请自来 | Redis 未授权访问漏洞深度利用

2017.09.25

浏览更多

相



C

rite-up

安全公告：CVE-2017-1540 (Redis 3.0.0-3.2.0)

关注我们 分享每日精选文章  
大数据安全分析之三（可视化篇）

Python黑客学习笔记：从HelloWorld到...

如何渗透Pocket内网

特别推荐



不容错过

OpenVAS开源风险评估系统部署方案

双刃剑与灰色地带：“泄露数据收藏家”的素描

[2015最酷的Hack方式有哪些？](#)

[简单](#)

2016-01-05

[【限时优惠】FreeBuf精品公开课！  
36W漏洞奖金先生CplusHua：](#)

[FB客服](#)


2017-09-16



关注我们 分享每日精选文章



Copyright © 2018 WWW.FREEBUF.COM All Rights Reserved [沪ICP备13033796号](#)

 阿里云 提供计算与安全服务