

逻辑漏洞简单的小汇总


逻辑漏洞涵盖的范围很广，对于那种修改放回包进行跳过验证步骤的其实是最常见的，还有一种的话就是类似**手机号的唯一性**并没有进行严格的验证，又又又有一种是对**短信唯一性**进行验证，但是没有对手机号有验证。

详细就以遇到过的真实案例进行分析：

首先在账户名可以进行**拦截验证码**，进行对用户名的 **FUZZ**

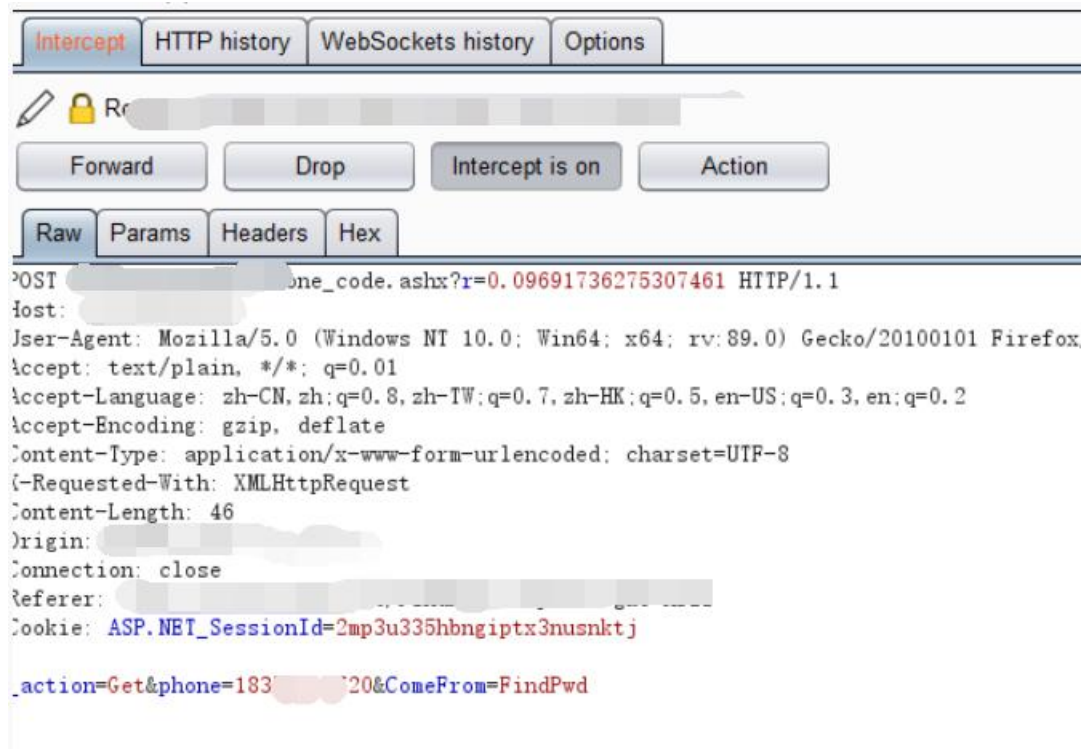


除非万不得已就别用 **admin** 的哈哈，毕竟有些管理员的手机号都是测试手机号 你改了 到时候操作者改不回来就麻烦了，这边利用 **fuzz** 到的系统内普通用户



当点击获取验证码的时候，进行**拦截数据包** 会发现用户的**手机号完整**显示出来了。看到这个完整的手机号就可以进行直接**猜测**：**1.此手机号在后端进行发送的有无唯一性的验证** **2.验证码能否重复利用**（前提是自己手机号能够收到短信）。

这边发送验证码的功能点就是**缺失了对获取验证码的手机号唯一性的认定**，导致这边可以直接**修改成自己手机号**来获取验证码



填入自己获取到的手机号码，会发现在提交会有修改用户的手机号当第一步是尝试有无**验证码重复使用**，发现不行。可以结合经验 应该是有对**短信验证码唯一性的认定**，所以导致验证不成功。

但是这个点出现了一个**极大的弊端**，这边的 **手机号** 依旧是可以被 **自定义**！

那么这边就出现了**两个可控参数**，之前发短信的时候 没有手机号唯一性验证

所以这边**修改成自己的手机号和自己手机接收到的验证码**！！



成功抵达密码填写，哈哈哈 这边依旧是司空见惯的问题：在进行新密码填写的时候 并没有再一次对上一步的验证码 手机号进行校验。直接填写新密码就可以了！



再举例一个案例，是因为一个弱密保的用户导致的沦陷
这个页面的忘记密码功能点已经被修复 被撤销 但是我有后台地址呀哈哈 只是删除了转跳接口 有后台地址 直接访问 还是存在的（修复真牛马）



这边**验证码不会刷新**！又让我们有机可乘，这边常见的用户名没有，直接上 **bp**，跑出 **gaof** 对应的 **uid 223**

lt 对应的 **uid 194**

lw 对应的 **uid 209**

请输入您要找回密码的账号

01 输入用户名 > 02 进行安全验证 > 03 设置新密码

用户名:

请输入用户名

验证码:

验证码

下一步

发现一些问题是**数字**，或者一些**特意字符串** 那么极大概率是**弱密保**，填入 **123456** 之后居然**成功抵达设置新密码页面**

您正在找回用户名 gaof 的密码

01 输入用户名 > 02 进行安全验证 > 03 设置新密码

问题:

123456

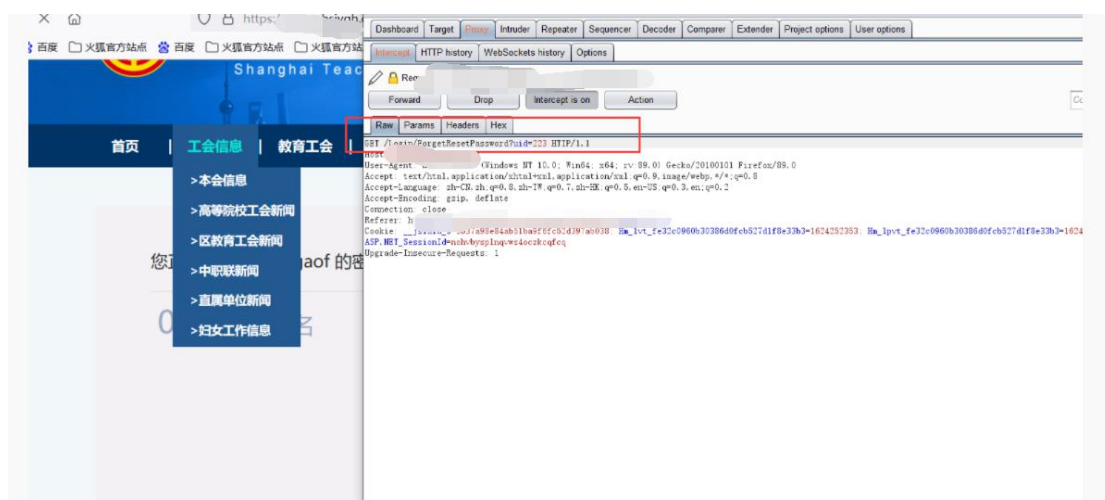
答案:

123456

下一步

渗透测试的尽量在重要步骤都开启 bp 一个包一个包的看。

看到这个数据包的时候会发现一个极具敏感存在越权的 uid



改成 1 之后发包，成功切换到了另一个用户！而且这个系统极具友好 还会提示用户名是什么啊哈哈哈哈哈啊哈！！ 遍历 uid 就可以对任意用户进行密码修改！！

您正在找回用户名 shsjyghsys 的密码

01 输入用户名 > 02 进行安全验证 > 03 设置新密码

新密码:

请输入密码

确认密码:

请输入密码

提交

改了一个普通用户的密码，进入之后会发现密码重置的时候会存在一个 未授权且任意用户

密码重置的功能点，这个的话 主要还是对 重要功能点进行越权和未授权的测试

未授权任意修改密码：

漏洞 URL: <https://www.xxx.org.cn/Login/ForgetResetPassword>

POST 数据: NewPwd=360src&ReNewPwd=360src&uid=194

