【知识点——越权基础知识和分类认识】

越权的定义

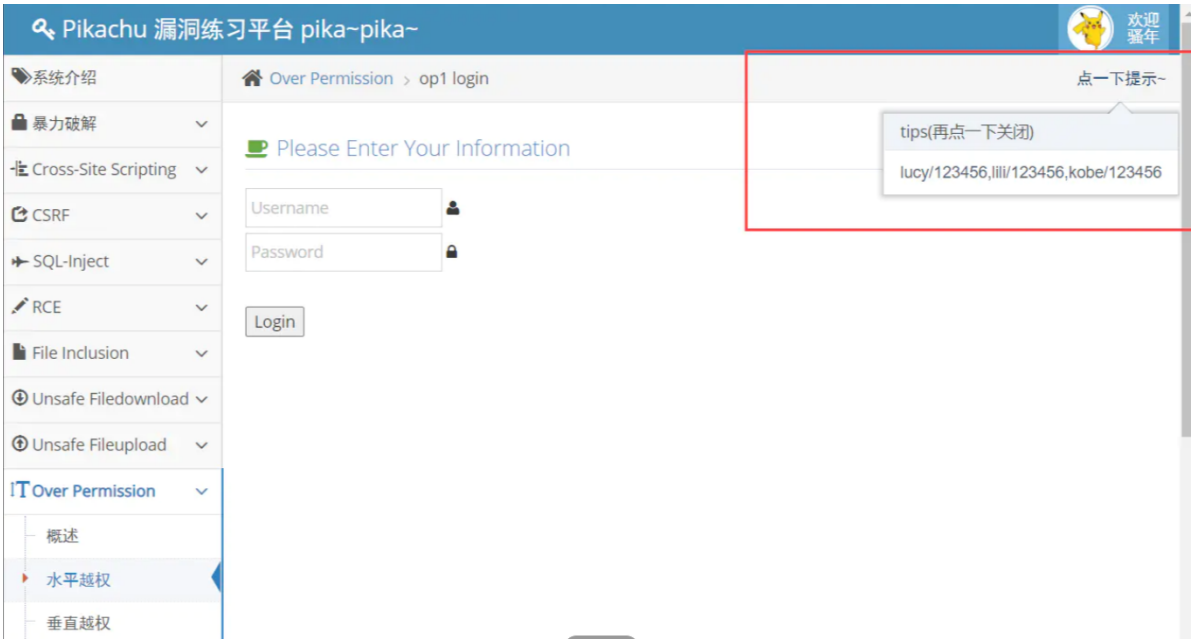
一个用户A一般只能够对自己本身的信息进行增删改查，然而由于后台开发人员的疏忽，没有在信息进行增删改查时候进行用户判断，从而导致用户A可以对其他用户进行增删改查等等操作。

越权漏洞——分为水平越权和垂直越权。

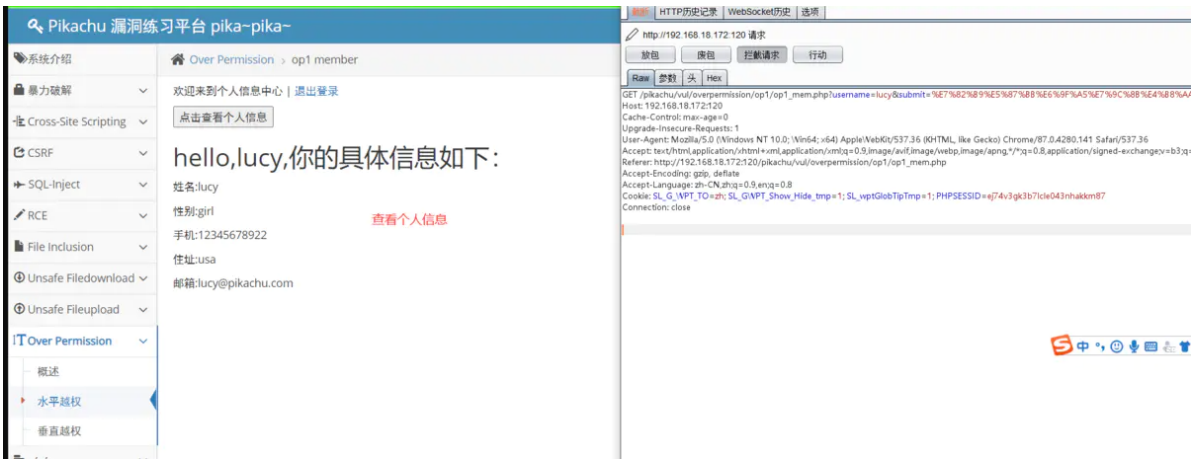
越权原理

如果使用A用户的权限去操作B用户的数据，A的权限小于B的权限，如果能够成功操作，则称之为越权操作。 越权漏洞形成的原因是后台使用了不合理的权限校验规则导致的。

【知识点——水平越权】



抓包查看信息

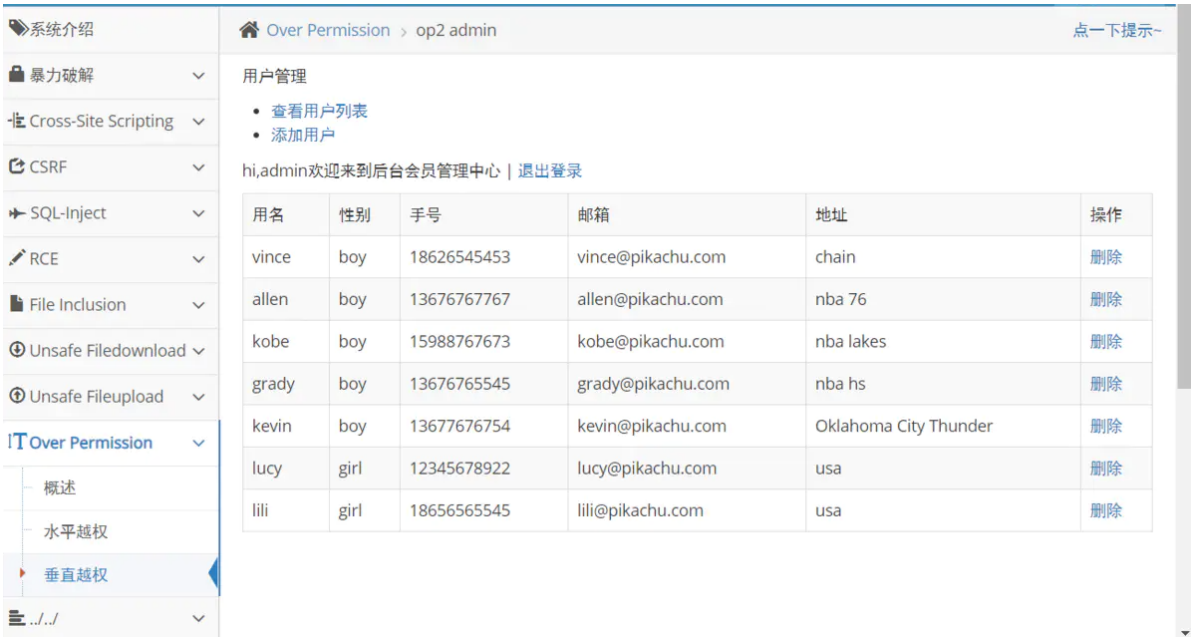


修改用户名

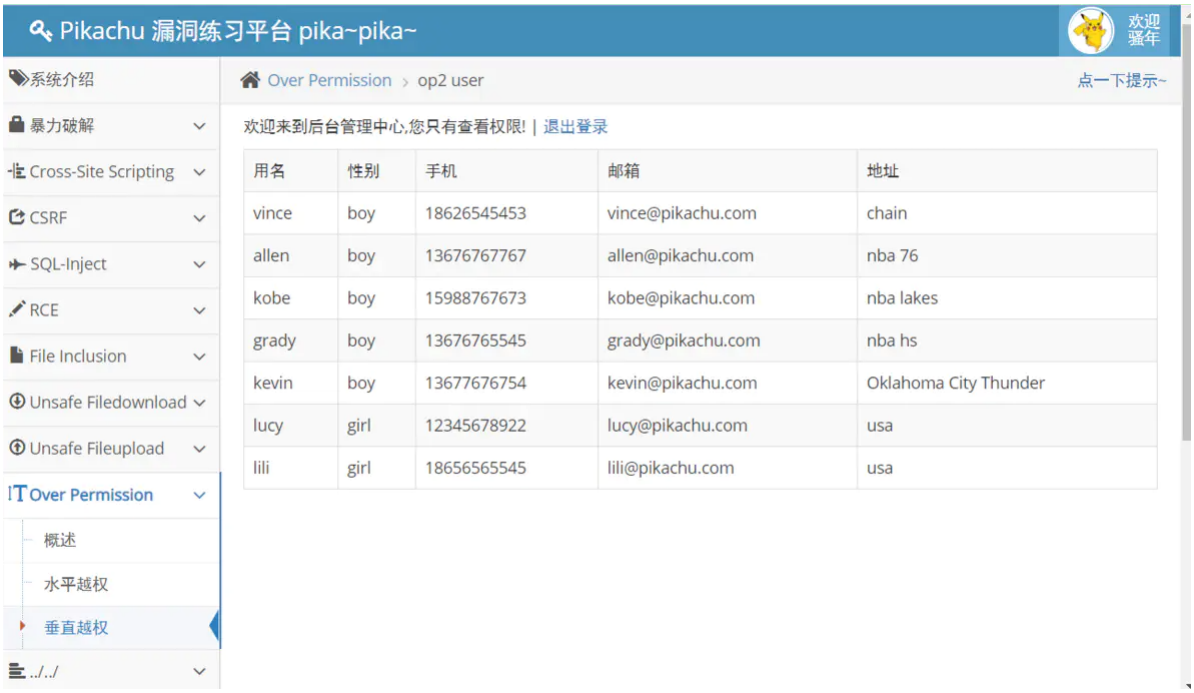
【知识点——垂直越权】

A用户的权限高于B用户，B用户越权操作A用户的权限的情况称为垂直越权

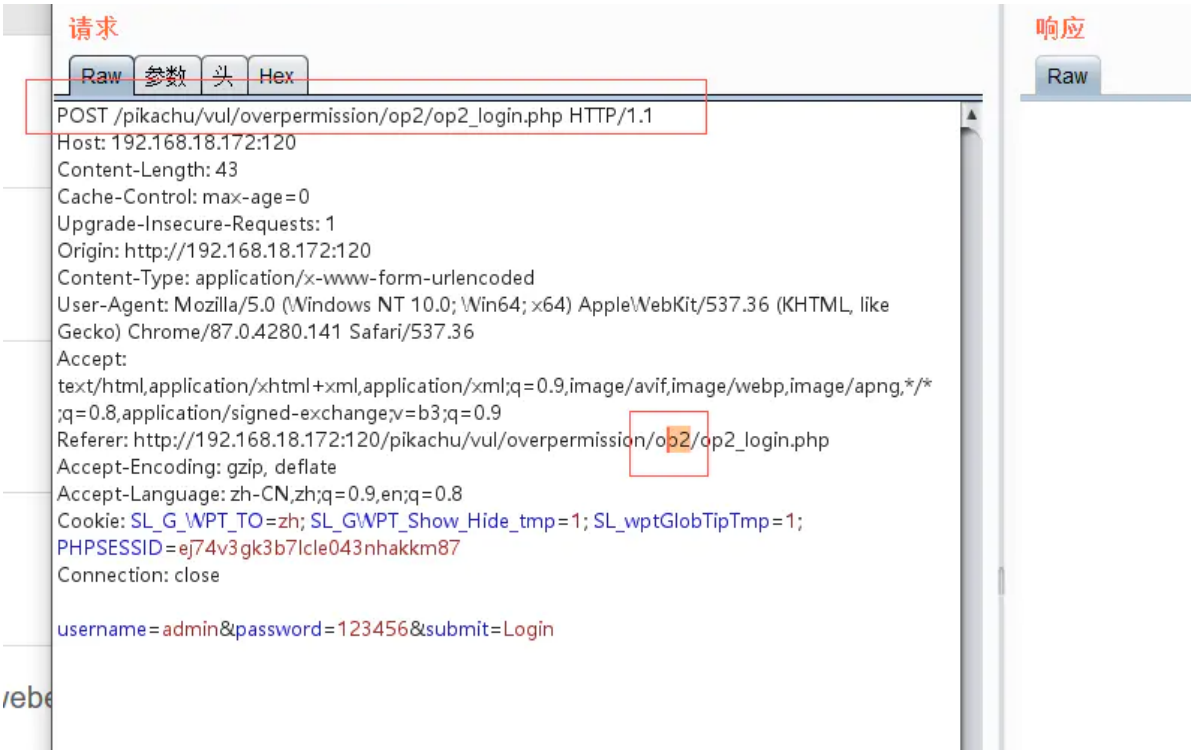
可以添加无权限的用户，此处是admin



用低权限用户登录，提示只有查看权限



抓包注意修改来源和refer



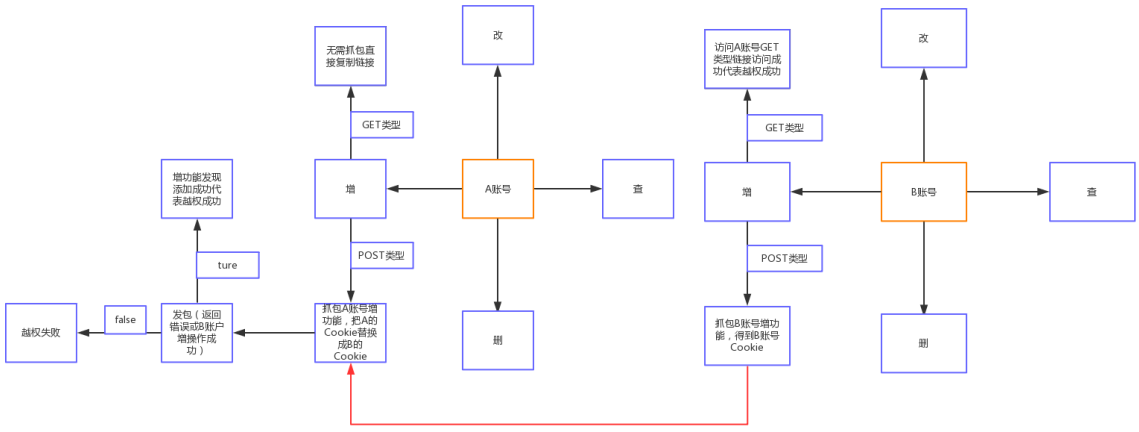
把普通用户的cookie信息粘贴到管理员cookie下

可以创建用户 存在垂直越权

在普通用户权限下添加账号，可以添加上

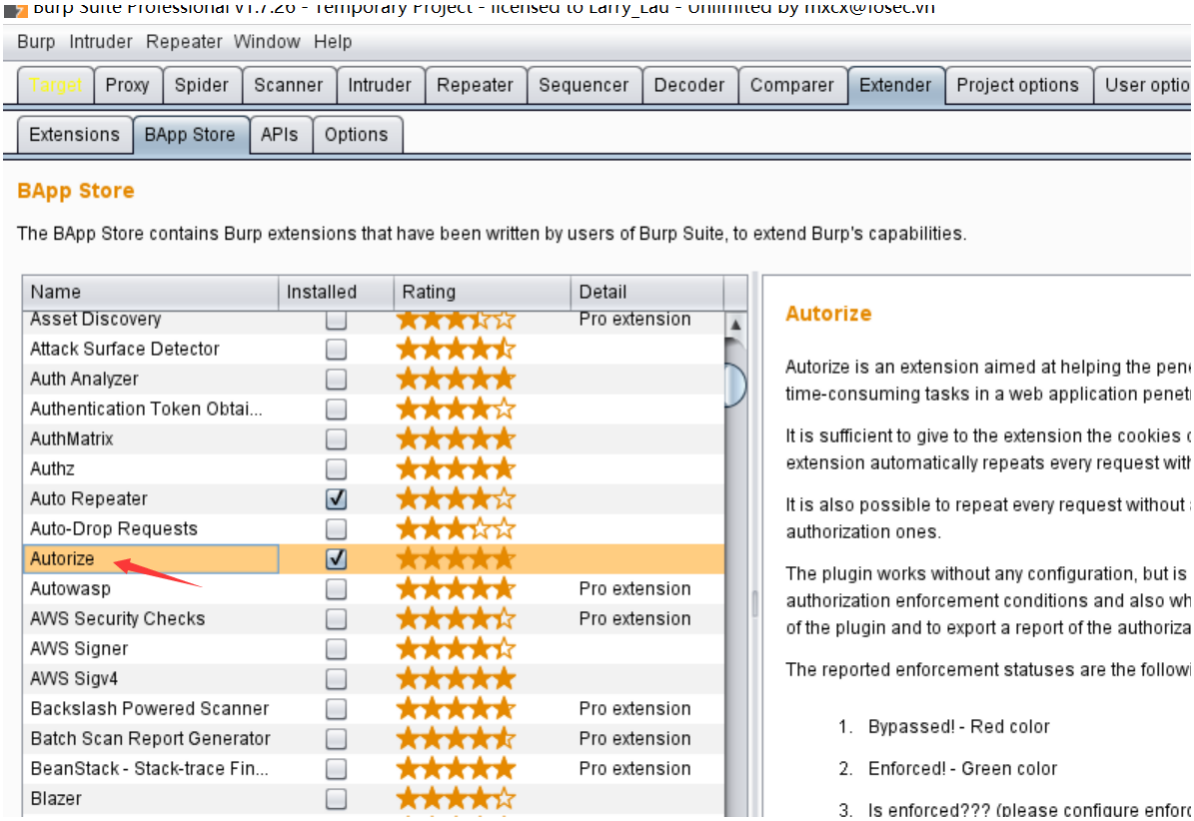
越权产生原理：没有做会话session判断（leve级别l=1）level级别一定要判断，可能在登录页面进行判断，但是登录之后的页面没有判断

【知识点——流程逻辑原理】

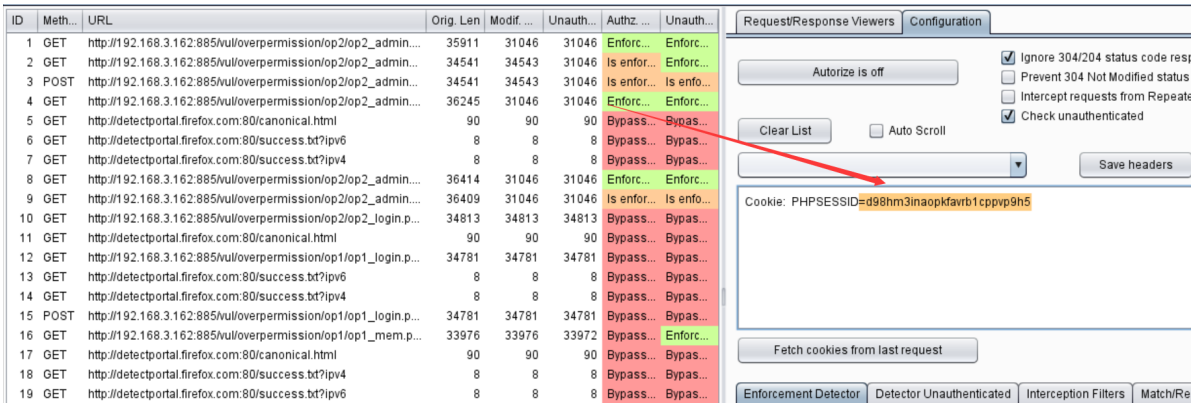


【知识点——burp插件】

BP测试越权插件，Autorize



对话框内设置不同权限用户的认证信息



正常访问数据，数据包信息会显示在左侧，红色为可能存在越权，可在此模块对比修改前后的数据包。

越权漏洞修复

1、前端和后端同时对用户输入信息进行校验，双重验证机制

2、调用功能前验证用户是否有权限调用相关功能

3、执行关键操作前必须验证用户身份，验证用户是否具备操作数据的权限