1. 漏洞复现

本地搭建环境：

http://10.33.70.40/daima/tuan/user/register.php

会员注册模块



数据包：

POST /daima/tuan/user/register.php HTTP/1.1

Host: 10.33.70.40

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3

Accept-Encoding: gzip, deflate

Content-Type: application/x-www-form-urlencoded

Content-Length: 126

Referer: http://10.33.70.40/daima/tuan/user/register.php

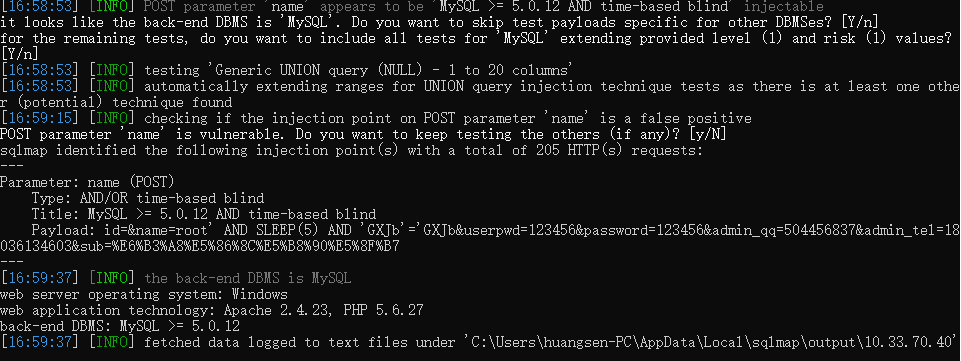
Cookie: PHPSESSID=t1keklhakiptniij22s2u6pni4; xinhu\_mo\_adminid=gg0yd0df0jjr0gg0yy0gz0jzg0dg0dj0yg0ty03; xinhu\_ca\_adminuser=admin; xinhu\_ca\_rempass=0; deviceid=1585121772176; UM\_distinctid=17110d604f3306-090c84779b397c8-4c322f7c-1fa400-17110d604f42d0; CNZZDATA1258845289=520756444-1585124022-%7C1585124022

Connection: close

Upgrade-Insecure-Requests: 1

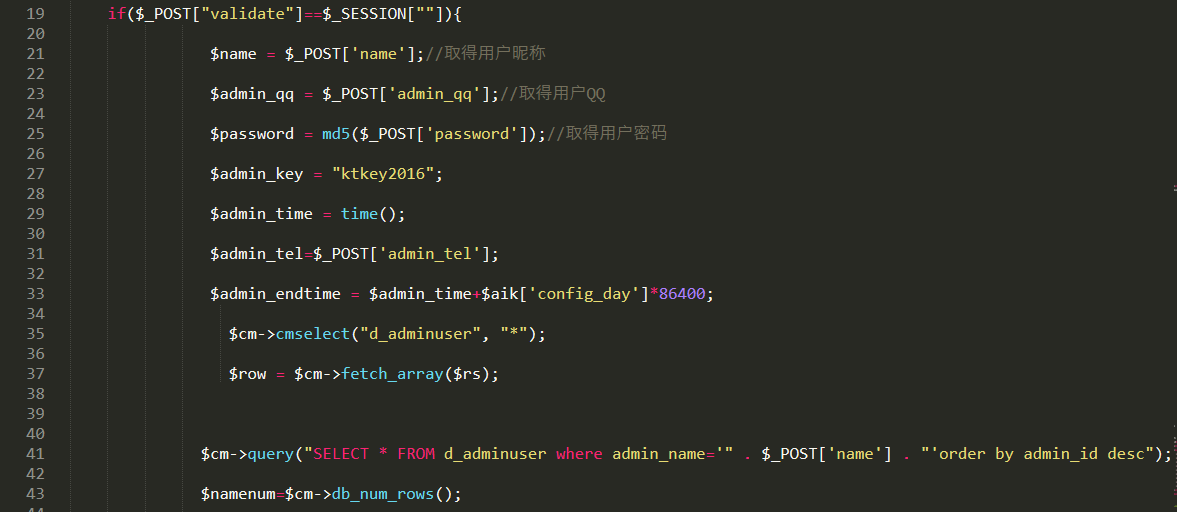
id=&name=root&userpwd=123456&password=123456&admin\_qq=504456837&admin\_tel=18036134603&sub=%E6%B3%A8%E5%86%8C%E5%B8%90%E5%8F%B7

抓包测试



存在SQL注入

1. 代码



没有对敏感参数过滤。