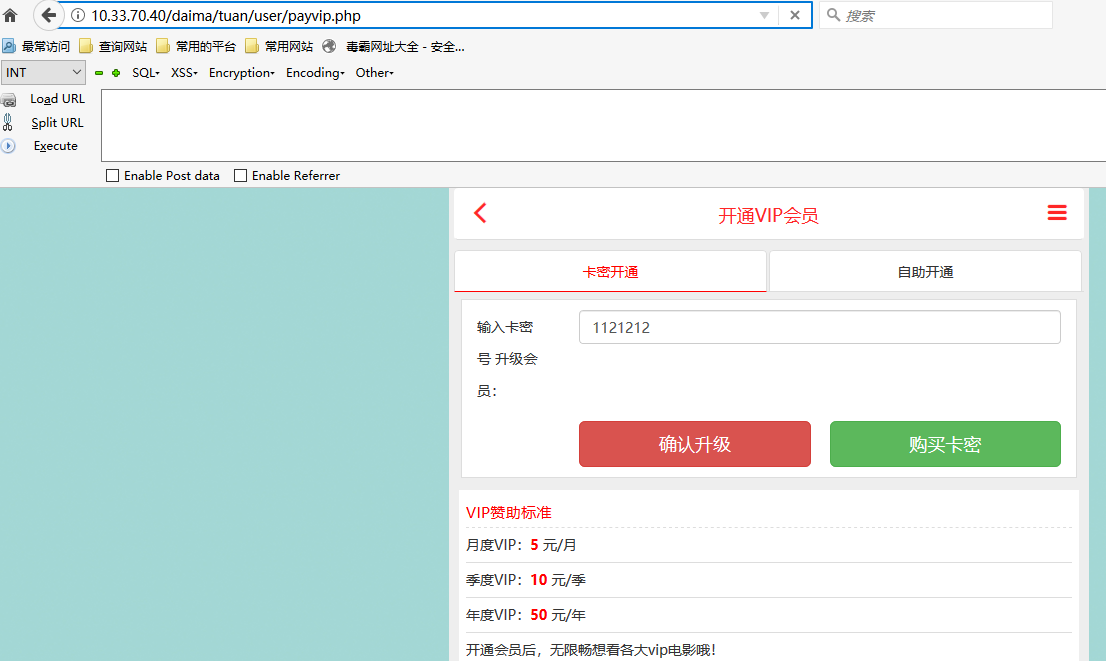
1. 漏洞复现

本地搭建环境：

<http://10.33.70.40/daima/tuan/user/payvip.php>

输入卡密，升级模块



数据包：

POST /daima/tuan/user/payvip.php?act=number 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: 23

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

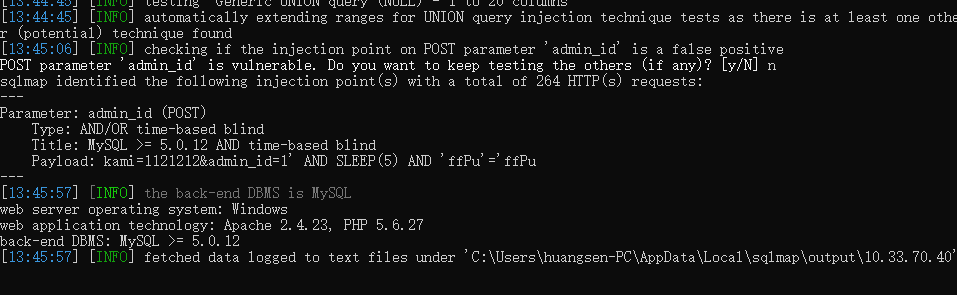
Cookie: PHPSESSID=2et4sgvdacmi44hdqghigo46h7

Connection: close

Upgrade-Insecure-Requests: 1

kami=1121212&admin\_id=1

抓包测试



存在SQL注入

1. 代码



没有对敏感参数过滤。