Dolibarr文件上传漏洞(CVE-2020-14209)

概述

该漏洞允许低权权用户上传危险文件，从而导致任意代码执行。

影响版本

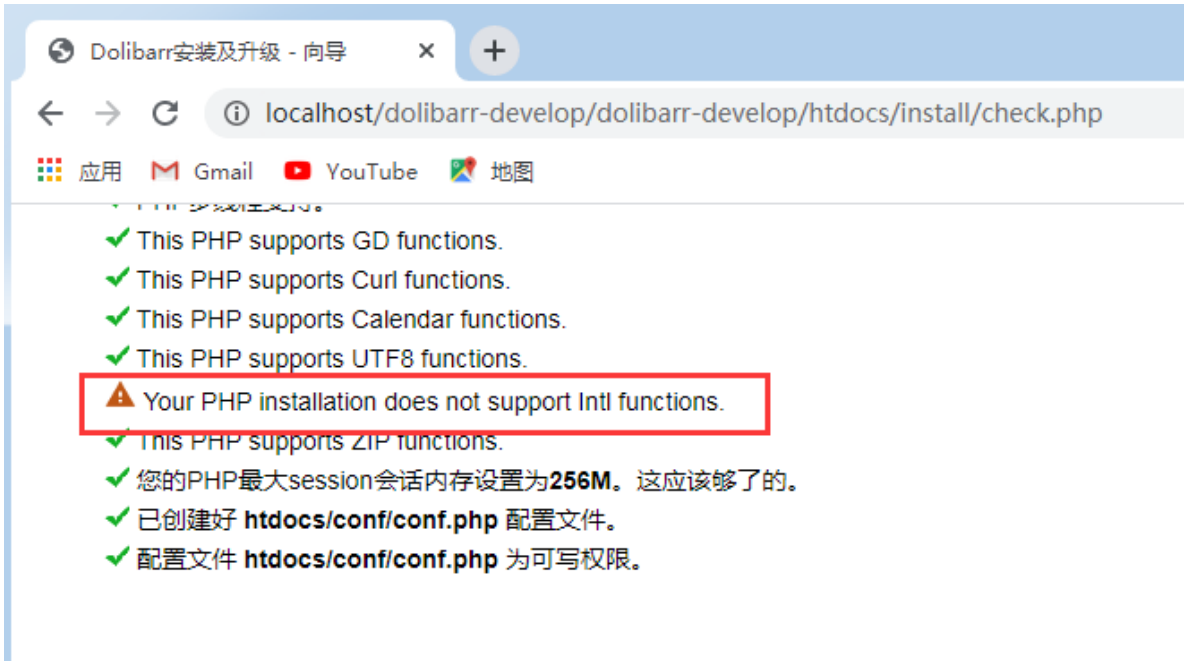
Dolibarr 11.0.5之前版本存在安全漏洞

环境搭建

到GitHub上下载源码

https://github.com/Dolibarr/dolibarr/archive/develop.zip

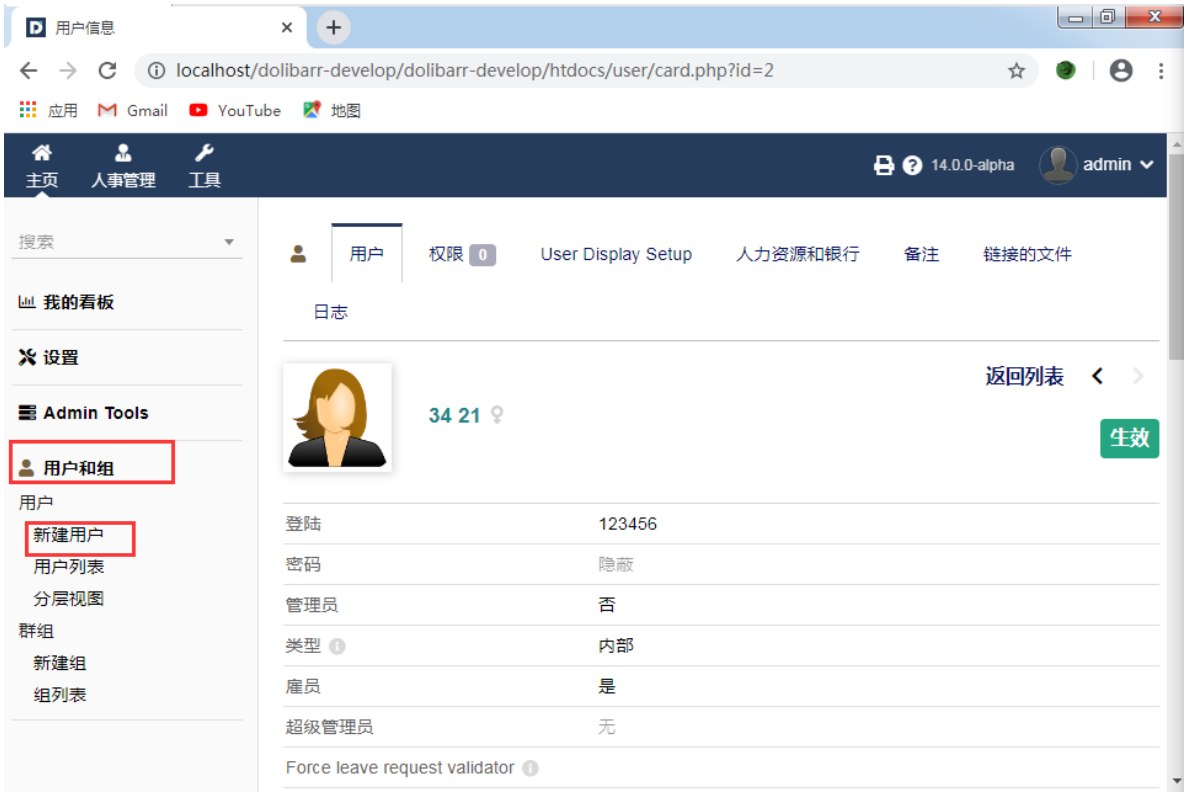
注：安装过程中出现 您的PHP安装不支持Intl函数 报错时



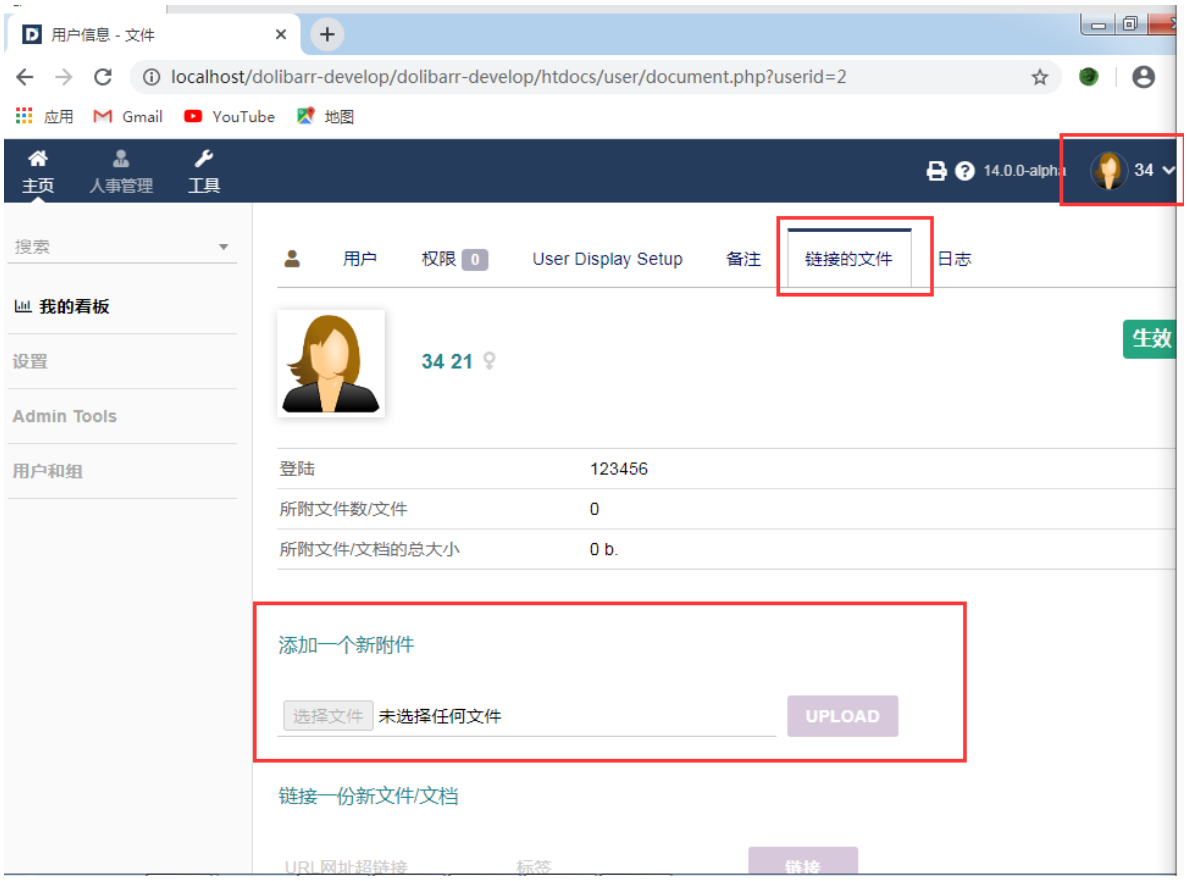
解决办法：在phpstudy中开启PHP扩展intl

漏洞复现

1.创建一个拥有管理员权限的用户



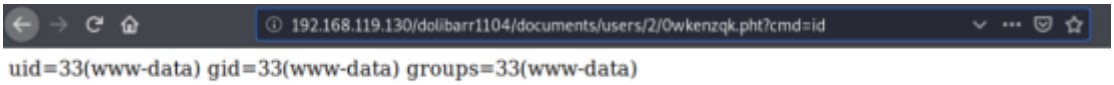
2.使用管理员用户登录到后台。用户的链接的文件模块，有一个添加一个新附件



3.burp抓包，构造语句绕过，上传一句话木马

正则表达式显示允许使用".pht",".phar"和".shtml"之类的扩展名，Apache 2.4.25的默认配置将“.pht”文件作为PHP脚本执行。

4.上传文件默认存放在/documents/users/<user_id>/webshell,访问文件



uid=33(www-data) gid=33(www-data) groups=33(www-data)

5.蚁剑连接