Apache Fineract SQL Inject—【CVE-2017-5663】

orich1 / 2018-01-23 12:25:00 / 浏览数 3043 安全技术 漏洞分析 顶(1) 踩(0)

漏洞简介

In Apache Fineract 0.4.0-incubating, 0.5.0-incubating, and 0.6.0-incubating, an authenticated user with client/loan/center/staff/group read permissions is able to inject malicious SQL into SELECT queries. The 'sqlSearch' parameter on a number of endpoints is not sanitized and appended directly to the query

Apache Fineract

Fineract
为创业者、金融机构和服务提供商提供了一个可靠、健壮的、可负担得起的金融服务解决方案。可在任何环境中部署，无论是云端还是内部，也可在移动设备或 PC 上进行在线或离线操作。Fineract
可扩展到足以支持任何组织类型或交付渠道，并且足够灵活以支持任何产品，服务或方法。对于大型或小型企业而言，提供客户数据管理、贷款和储蓄组合管理，集成实时会

漏洞分析

从漏洞简介中可以得到很多信息了，比如注入参数是 'sqlSearch' ，含有注入的模块有 client、loan、center、staff、group ，只需要用户拥有各个模块的读权限，就可以造成 sql 注入

从github拿到的 fineract-0.4.0-incubating 版本，不知道怎么回事，数据库相关的一直出错，导致没法让组件跑起来，就只能静态分析了

先不管各种模块，我们去全局搜一下 'sqlSearch'

信息很杂乱，那么首先去看一下这个参数和啥有关系

随便找一个作为函数参数传入的地方

跟进 forAccountTransfer 函数发现，只是将 sqlSearch 作为参数新建了一个 SearchParameters 对象

那么仔细看一下这个 SearchParameters 类的结构

（ emmm，太长截不完 ）

可以从上图看出，这个类将很多 sql 关键字都存储起来，并且也能通过相应的接口访问到已经存储的信息

回到刚才 sqlSearch 作为参数传入的函数里（ 随便一个都行 ），会发现这个 sql 关键词存储类会被带入类似如下图的函数里

如上图， retrieveAll 函数就带入了 searchParameters
跟进去

（ 函数体过长，只截关键部分 ）

如上图，可见从 searchParameters 中，并没有将之前的 sqlSearch 的值提取出来，但是我们注意到 searchParameters 被带入了 buildSqlStringFromClientCriteria 函数里，返回的 extraCriteria 又被拼接进了 sql 语句中，那我们跟进去看看这个函数

这里已经提取出 sqlSearch ，并且将其拼接进 extraCriteria 中

那么至此，由于没有任何过滤，导致了 sql 注入

既然碰到了 web 形式的组件，而且还是最常见的 sql 注入，那么我们继续跟进一下它的补救方式

下好 fineract-1.1.0 的源码包，跟入相同的参数传入点

这里是没变的，继续跟到 buildSqlStringFromClientCriteria 函数

如上图，似乎多了两个参数
跟进去

一般在挖洞的时候，碰见类似上图中红框中的函数名，心里都会咯噔一下，无奈只能去看看能不能绕过之类的了

跟进去

很明显的 sql 注入处理，跟进去

不用细看函数体，只用看看下图，这个 SQLInjectinValidator 类中的变量就行了

虽说可能被绕过，但是危害降低了很多
我这儿也没有去琢磨到底怎么绕过了：）

点击收藏 | 0 关注 | 1

上一篇：Web Hacking 101 中文版 下一篇：某电商前台代码注入

1. 0 条回复
   - 动动手指，沙发就是你的了！