南明离火
移动应用检测平台

ANDROID 静态分析报告

St.John's • v1.0.9

分析日期: 2025-08-27 11:09:07

应用概览

文件名称:	St.John_s v1.0.9.apk
文件大小:	38.99MB
应用名称:	St.John's
软件包名:	com.mcb.stjohnsemschool.activity
主活动:	com.mcb.stjohnsemschool.activity.SplashActivity
版本号:	1.0.9
最小SDK:	21
目标SDK:	34
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	49/100 (中风险)
跟踪器检测:	2/432
杀软检测:	经检测，该文件安全
MD5:	23f3000315b6b20472bce1bf9c9e22e7
SHA1:	eeecc4ba8dffee1774b75f92afe77deb2b3a2ce
SHA256:	624499543329e10ad8263c85833e0e1647035e46d041f7a6f19b1c0c38e4b0e8

分析结果严重性分布

高危	中危	信息	安全	关注
3	17	3	2	0

四大组件导出状态统计

Activity组件：16个，其中export的有： 2个
Service组件：9个，其中export的有： 1个
Receiver组件：4个，其中export的有： 2个
Provider组件：6个，其中export的有： 0个

应用签名证书信息

APK已签名
v1 签名: True
v2 签名: True
v3 签名: True
v4 签名: False
主题: CN=Myclassboard Educational Solutions Pvt ltd
签名算法: rsassa_pkcs1v15
有效期自: 2020-04-28 12:13:30+00:00
有效期至: 2120-04-04 12:13:30+00:00
发行人: CN=Myclassboard Educational Solutions Pvt ltd
序列号: 0x55dc4b0f
哈希算法: sha256
证书MD5: 91aa533820f986d97f38c771dbeab0c4
证书SHA1: aa69be7f142f74adf9a95c1cc64f50feab227bbc
证书SHA256: aaeefa3b304e10d8ec7189a3227c0f7b1efdac53a660b982784e044651278a0b
证书SHA512:
fb778179a5ae1fe0dcaf81091f1eae4223f4a86c4bf4876002085be1abd9dbcf8826bd02f8c1671fd5ed0105c3be65e8ffbfac97ade44891f6aaae253a4aebfa8

公钥算法: rsa
密钥长度: 2048
指纹: 740cef5257812c94526d383470562255d6de4873bd339390cd946c415e0e9b69
共检测到 1 个唯一证书

权限声明与风险分级

权限名称	安全等级	权限内容	权限描述
android.permission.ACCESS_NETWORK_STATE	普通	获取网络状态	允许应用程序查看所有网络的状态。
android.permission.CAMERA	危险	拍照和录制视频	允许应用程序拍摄照片和视频，且允许应用程序收集相机在任何时候拍到的图像。
android.permission.INTERNET	危险	完全互联网访问	允许应用程序创建网络套接字。
android.permission.WAKE_LOCK	危险	防止手机休眠	允许应用程序防止手机休眠，在手机屏幕关闭后后台进程仍然运行。
android.permission.WRITE_EXTERNAL_STORAGE	危险	读取/修改/删除外部存储内容	允许应用程序写入外部存储。
android.permission.READ_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。
android.permission.READ_PHONE_STATE	危险	读取手机状态和标识	允许应用程序访问设备的手机功能。有此权限的应用程序可确定此手机的号码和序列号，是否正在通话，以及对方的号码等。
android.permission.ACCESS_FINE_LOCATION	危险	获取精确位置	通过GPS芯片接收卫星的定位信息，定位精度达10米以内。恶意程序可以用它来确定您所在的位置。
android.permission.ACCESS_COARSE_LOCATION	危险	获取粗略位置	通过WiFi或移动基站的方式获取用户粗略的经纬度信息，定位精度大概误差在30~1500米。恶意程序可以用它来确定您的大概位置。
android.permission.ACCESS_WIFI_STATE	普通	查看Wi-Fi状态	允许应用程序查看有关Wi-Fi状态的信息。

android.permission.CHANGE_NETWORK_STATE	危险	改变网络连通性	允许应用程序改变网络连通性。
android.permission.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi状态。
android.permission.POST_NOTIFICATIONS	危险	发送通知的运行时权限	允许应用发布通知，Android 13 引入的新权限。
android.permission.READ_MEDIA_IMAGES	危险	允许从外部存储读取图像文件	允许应用程序从外部存储读取图像文件。
android.permission.READ_MEDIA_AUDIO	危险	允许从外部存储读取音频文件	允许应用程序从外部存储读取音频文件。
android.permission.READ_MEDIA_VIDEO	危险	允许从外部存储读取视频文件	允许应用程序从外部存储读取视频文件。
com.google.android.providers.gsf.permission.READ_GSERVICES	未知	未知权限	来自 android 引用的未知权限。
android.permission.USE_BIOMETRIC	普通	使用生物识别	允许应用使用设备支持的生物识别方式。
android.permission.USE_FINGERPRINT	普通	允许使用指纹	此常量在 API 级别 28 中已弃用。应用程序应改为请求USE_BIOMETRIC
android.permission.VIBRATE	普通	控制振动器	允许应用程序控制振动器，用于消息通知振动功能。
com.google.android.c2dm.permission.RECEIVE	普通	接收推送通知	允许应用程序接收来自云的推送通知。
com.google.android.gms.permission.AD_ID	普通	应用程序显示广告	此应用程序使用 Google 广告 ID，并且可能会投放广告。
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	普通	Google 定义的权限	由 Google 定义的自定义权限。
android.permission.NFC	危险	控制nfc功能	允许应用程序与支持nfc的物体交互。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.microsoft.identity.client.BrowserTabActivity	Schemes: msauth://, Hosts: com.mcb.stjohnsemschool.activity, Paths: /qmm+fxQvdK35qVwcxk9Q/qsie7w=,

网络通信安全风险分析

序号	范围	严重级别	描述

证书安全合规分析

高危: 0 | 警告: 1 | 信息: 1

标题	严重程度	描述信息
已签名应用	信息	应用已使用代码签名证书进行签名。

Manifest 配置安全分析

高危: **0** | 警告: **5** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用已配置网络安全策略 [android:networkSecurityConfig=@7F150000]	信息	网络安全配置允许应用通过声明式配置文件自定义网络安全策略，无需修改代码。可针对特定域名或应用范围进行灵活配置。
2	Activity (com.microsoft.identity.client.BrowserTabActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
3	Activity (com.microsoft.identity.client.CurrentTaskBrowserTabActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
4	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) 受权限保护，但应检查权限保护级别。 Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
5	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
6	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。

代码安全漏洞检测

高危: **3** | 警告: **10** | 信息: **2** | 安全: **1** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	文件可能包含硬编码的敏感信息，如用户名、密码、密钥等	警告	CWE: CWE-312: 明文存储敏感信息 OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	升级会员：解锁高级权限
2	应用程序记录日志信息,不得记录敏感信息	信息	CWE: CWE-532: 通过日志文件的信息暴露 OWASP MASVS: MSTG-STORAGE-3	升级会员：解锁高级权限
3	此应用程序使用SSL Pinning 来检测或防止安全通信通道中的MITM攻击	安全	OWASP MASVS: MSTG-NETWORK-4	升级会员：解锁高级权限
4	不安全的Web视图实现。可能存在WebView任意代码执行漏洞	警告	CWE: CWE-749: 暴露危险方法或函数 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
5	可能存在跨域漏洞。在 WebView 中启用从 URL 访问文件可能会泄漏文件系统中的敏感信息	警告	CWE: CWE-200: 信息泄露 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
6	应用程序可以读取/写入外部存储器，任何应用程序都可以读取写入外部存储器的数据	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员：解锁高级权限
7	应用程序使用SQLite数据库并执行原始SQL查询。原始SQL查询中不受信任的用户输入可能会导致SQL注入。敏感信息也应加密并写入数据库	警告	CWE: CWE-89: SQL命令中使用的特殊元素转义处理不恰当（'SQL 注入'） OWASP Top 10: M7: Client Code Quality	升级会员：解锁高级权限
8	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-2	升级会员：解锁高级权限

9	应用程序使用带PKCS5/PKCS7填充的加密模式CBC。此配置容易受到填充oracle攻击。	高危	CWE: CWE-649: 依赖于混淆或加密安全相关输入而不进行完整性检查 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	升级会员：解锁高级权限
10	应用程序使用不安全的随机数生成器	警告	CWE: CWE-330: 使用不充分的随机数 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	升级会员：解锁高级权限
11	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
12	不安全的Web视图实现。Web视图忽略SSL证书错误并接受任何SSL证书。此应用程序易受MITM攻击	高危	CWE: CWE-295: 证书验证不恰当 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	升级会员：解锁高级权限
13	应用程序创建临时文件。敏感信息永远不应该被写进临时文件	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员：解锁高级权限
14	此应用程序将数据复制到剪贴板。敏感数据不应复制到剪贴板，因为其他应用程序可以访问它	信息	OWASP MASVS: MSTG-STORAGE-10	升级会员：解锁高级权限
15	如果一个应用程序使用WebView.loadDataWithBaseURL方法来加载一个网页到WebView，那么这个应用程序可能会遭受跨站脚本攻击	高危	CWE: CWE-79: 在Web页面生成时对输入的转义处理不恰当（'跨站脚本'） OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-6	升级会员：解锁高级权限

16	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限

应用行为分析

编号	行为	标签	文件
00063	隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00091	从广播中检索数据	信息收集	升级会员：解锁高级权限
00001	初始化位图对象并将数据（例如JPEG）压缩为位图对象	相机	升级会员：解锁高级权限
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00022	从给定的文件绝对路径打开文件	文件	升级会员：解锁高级权限
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00012	读取数据并放入缓冲流	文件	升级会员：解锁高级权限
00192	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00191	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00051	通过setData隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00125	检查给定的文件路径是否存在	文件	升级会员：解锁高级权限
00104	检查给定路径是否是目录	文件	升级会员：解锁高级权限
00029	动态初始化类对象	反射	升级会员：解锁高级权限
00157	使用反射实例化新对象，可能用于 dexClassLoader	反射 dexClassLoader	升级会员：解锁高级权限
00046	方法反射	反射	升级会员：解锁高级权限
00026	方法反射	反射	升级会员：解锁高级权限
00054	从文件安装其他APK	反射	升级会员：解锁高级权限
00024	Base64解码后写入文件	反射 文件	升级会员：解锁高级权限
00096	连接到 URL 并设置请求方法	命令 网络	升级会员：解锁高级权限

00109	连接到 URL 并获取响应代码	网络 命令	升级会员：解锁高级权限
00089	连接到 URL 并接收来自服务器的输入流	命令 网络	升级会员：解锁高级权限
00030	通过给定的 URL 连接到远程服务器	网络	升级会员：解锁高级权限
00112	获取日历事件的日期	信息收集 日历	升级会员：解锁高级权限
00121	创建目录	文件 命令	升级会员：解锁高级权限
00079	隐藏当前应用程序的图标	规避	升级会员：解锁高级权限
00092	发送广播	命令	升级会员：解锁高级权限
00163	创建新的 Socket 并连接到它	socket	升级会员：解锁高级权限
00025	监视要执行的一般操作	反射	升级会员：解锁高级权限
00202	打电话	控制	升级会员：解锁高级权限
00203	将电话号码放入意图中	控制	升级会员：解锁高级权限
00003	将压缩后的位图数据放入JSON对象中	相机	升级会员：解锁高级权限
00009	将游标中的数据放入JSON对象	文件	升级会员：解锁高级权限
00004	获取文件名并将其放入 JSON 对象	文件 信息收集	升级会员：解锁高级权限

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	6/30	android.permission.CAMERA android.permission.WAKE_LOCK android.permission.READ_PHONE_STATE android.permission.ACCESS_FINE_LOCATION android.permission.ACCESS_COARSE_LOCATION android.permission.VIBRATE

其它常用权限	13/46	android.permission.ACCESS_NETWORK_STATE android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_NETWORK_STATE android.permission.CHANGE_WIFI_STATE android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_AUDIO android.permission.READ_MEDIA_VIDEO com.google.android.c2dm.permission.RECEIVE com.google.android.gms.permission.AD_ID com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

常用: 已知恶意软件广泛滥用的权限。

其它常用权限: 已知恶意软件经常滥用的权限。

恶意域名威胁检测

域名	状态	中国境内	位置信息
login.partner.microsoftonline.cn	安全	是	**IP地址:** 40.72.70.132 **国家:** 中国 **地区:** 中国江苏 **城市:** 南通 **纬度:** 31.980172 **经度:** 120.894291 **查看:** 高德地图
graph.microsoft.com	安全	否	**IP地址:** 20.190.144.171 **国家:** 大不列颠及北爱尔兰联合王国 **地区:** 威尔士 **城市:** 卡迪夫 **纬度:** 51.480000 **经度:** -3.180000 **查看:** Google 地图
internet-up.ap[illegible]time.com	安全	否	**IP地址:** 104.18.11.70 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图
login.microsoftonline.com	安全	否	**IP地址:** 20.190.151.133 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 华盛顿 **纬度:** 38.713848 **经度:** -78.159439 **查看:** Google 地图

www.wireless-village.org	安全	否	**IP地址:** 172.67.131.214 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图
login.windows-ppe.net	安全	否	**IP地址:** 52.126.194.164 **国家:** 美国 **地区:** 亚利桑那州 **城市:** 凤凰 **纬度:** 33.448231 **经度:** -112.074051 **查看:** Google 地图
mcbapi.myclassboard.com	安全	否	**IP地址:** 104.18.3.223 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图
st-johns-em-high-school.firebaseio.com	安全	否	**IP地址:** 34.120.160.131 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
api.pearson.com	安全	否	**IP地址:** 23.49.107.153 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
login.microsoftonline.us	安全	否	**IP地址:** 52.126.194.164 **国家:** 美国 **地区:** 爱荷华州 **城市:** 得梅因 **纬度:** 41.600449 **经度:** -93.609116 **查看:** Google 地图
stjohnsschool.myclassboard.com	安全	否	**IP地址:** 104.18.3.223 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图

login.live.com	安全	否	**IP地址:** 20.190.151.8 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 华盛顿 **纬度:** 38.713848 **经度:** -78.159439 **查看:** Google 地图
www.idpf.org	安全	否	**IP地址:** 20.190.190.196 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图
native-ux-mock-api.azurewebsites.net	安全	否	No Geolocation information available.
ssolive.myclassboard.com	安全	否	**IP地址:** 104.18.2.223 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图
www.openmobilealliance.org	安全	否	**IP地址:** 104.26.8.105 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图
devicemgmt.teams.microsoft.com	安全	否	**IP地址:** 52.113.194.132 **国家:** 美国 **地区:** 华盛顿 **城市:** 雷德蒙 **纬度:** 47.682220 **经度:** -122.123009 **查看:** Google 地图
www.myclassboard.com	安全	否	**IP地址:** 104.18.2.223 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图
www.xx.com	安全	否	**IP地址:** 86.105.245.69 **国家:** 荷兰（王国） **地区:** 北布拉邦省 **城市:** 埃因霍温 **纬度:** 51.441029 **经度:** 5.478038 **查看:** Google 地图

login.windows.net	安全	否	**IP地址:** 20.190.190.196 国家: 美国 地区: 亚利桑那州 城市: 凤凰 纬度: 33.448231 经度: -112.074051 查看: Google 地图
tempuri.org	安全	否	**IP地址:** 20.231.239.246 国家: 美国 地区: 弗吉尼亚州 城市: 华盛顿 纬度: 38.713848 经度: -78.159439 查看: Google 地图
youtu.be	安全	否	**IP地址:** 142.250.72.174 国家: 美国 地区: 加利福尼亚 城市: 洛杉矶 纬度: 34.052570 经度: -118.243904 查看: Google 地图
login.microsoftonline.de	安全	否	**IP地址:** 51.5.145.123 国家: 德国 地区: 拜仁 城市: Unterschleissheim 纬度: 48.280380 经度: 11.576840 查看: Google 地图
go.microsoft.com	安全	否	**IP地址:** 23.218.109.152 国家: 新加坡 地区: 新加坡 城市: 新加坡 纬度: 1.289987 经度: 103.850281 查看: Google 地图
cdndatastatic.myclassboard.com	安全	否	**IP地址:** 104.18.3.223 国家: 美国 地区: 加利福尼亚 城市: 旧金山 纬度: 37.774929 经度: -122.419418 查看: Google 地图
readium.org	安全	否	**IP地址:** 185.199.109.153 国家: 美国 地区: 宾夕法尼亚 城市: 加利福尼亚 纬度: 40.065647 经度: -79.891724 查看: Google 地图

help.ably.io	安全	否	**IP地址:** 104.21.14.228 国家: 美国 地区: 加利福尼亚 城市: 旧金山 纬度: 37.774929 经度: -122.419418 查看: Google 地图
kb.myclassboard.com	安全	否	**IP地址:** 104.18.3.223 国家: 美国 地区: 加利福尼亚 城市: 旧金山 纬度: 37.774929 经度: -122.419418 查看: Google 地图
parentapi.myclassboard.com	安全	否	**IP地址:** 104.18.2.223 国家: 美国 地区: 加利福尼亚 城市: 旧金山 纬度: 37.774929 经度: -122.419418 查看: Google 地图
corp14api.myclassboard.com	安全	否	**IP地址:** 104.18.3.223 国家: 美国 地区: 加利福尼亚 城市: 旧金山 纬度: 37.774929 经度: -122.419418 查看: Google 地图
www.ccil.org	安全	否	**IP地址:** 142.251.40.51 国家: 美国 地区: 纽约 城市: 纽约市 纬度: 40.713192 经度: -74.006065 查看: Google 地图
corp14.myclassboard.com	安全	否	**IP地址:** 104.18.2.223 国家: 美国 地区: 加利福尼亚 城市: 旧金山 纬度: 37.774929 经度: -122.419418 查看: Google 地图

URL 链接安全分析

URL信息	源码文件

• https://github.com/eslint/eslint/issues/3229 • https://github.com/aFarkas/html5shiv/issues/64 • https://html.spec.whatwg.org/multipage/forms.html • https://web.archive.org/web/20141116233347/http • http://www.idpf.org/epub/linking/cfi/epub-cfi.html • http://github.com/timcameronryan/IERange • http://www.ecma-international.org/ecma-262/7.0 • https://jsperf.com/getall-vs-sizzle/2 • http://aryeh.name/spec/innertext/innertext.html • https://infra.spec.whatwg.org • http://peter.michaux.ca/articles/feature-detection-state-of-the-art-browser-scripting • https://github.com/jrburke/requirejs/wiki/Updating-existing-libraries • https://html.spec.whatwg.org/multipage/scripting.html • https://promisesaplus.com • https://web.archive.org/web/20100324014747/http • http://html5.org/specs/dom-parsing.html • https://jsperf.com/thor-indexof-vs-for/5 • https://github.com/edg2s/rangefix • http://ecma-international.org/ecma-262/7.0 • https://github.com/eslint/eslint/issues/6125 • https://html.spec.whatwg.org/multipage/syntax.html • https://html.spec.whatwg.org • https://github.com/timdown/rangy • http://pegjs.org • https://connect.microsoft.com/IE/feedback/details/1736512 • https://bugzilla.mozilla.org/show_bug.cgi?id=687787 • https://sizzlejs.com	自研引擎
• https://mcbapi.myclassboard.com/school/getAllSchools	com/mcb/stjohnsemschool/activity/SchoolSelectionActivity.java
• https://ssolive.myclassboard.com/connect/token • https://ssolive.myclassboard.com/connect/userinfo • https://play.google.com/store/apps/details?id=	com/mcb/stjohnsemschool/activity/LoginActivity.java
• javascript:inithorizontaldirection • javascript:rewindcurrentindex • javascript:checkcompatmode	com/folioreader/ui/fragment/FolioPageFragment.java
• javascript:isreadyforpullup • javascript:isreadyforpulldown	com/handmark/pulltorefresh/library/extras/PullToRefreshWebView2.java
• https://parentapi.myclassboard.com/appgraph/	com/mcb/stjohnsemschool/fragment/TodayUpdatesFragment.java
• https://login.microsoftonline.com/common/oauth2/v2.0/authorize	com/microsoft/identity/common/java/providers/microsoft/azureactivedirectory/AzureActiveDirectory.java
• https://youtu.be/	com/mcb/stjohnsemschool/utils/Utility.java

• javascript:getlocatorsusingrangyfind	org/readium/r2/streamer/server/handler/SearchQueryHandler$runWebviewForRangyFind$1.java
• javascript:getlocatorsusingwindowfind	org/readium/r2/streamer/server/handler/SearchQueryHandler$runWebviewForWindowFind$1.java
• http://www.xx.com/x.mp4	com/chinalwb/are/styles/toolitems/styles/ARE_Style_Video.java
• http://www.wireless-village.org/pa • http://www.openmobilealliance.org/dtd/wv-pa • http://www.openmobilealliance.org/dtd/wv-trc • www.wireless-village.org • http://www.wireless-village.org/csp • http://www.openmobilealliance.org/dtd/wv-csp • http://www.wireless-village.org/trc	org/kxml2/wap/wv/WV.java
• http://www.ccil.org/~cowan/tagsoup/properties/schema	com/chinalwb/are/android/inner/Html.java
• https://go.microsoft.com/fwlink/?linkid=2138180	com/microsoft/identity/common/internal/ui/webview/OAuth2WebViewClient.java
• https://devicemgmt.teams.microsoft.com/.default	com/microsoft/identity/common/java/foci/FociQueryUtilities.java
• http://www.idpf.org/2008/embedding	org/readium/r2/streamer/fetcher/FontDecoder.java
• https://login.microsoftonline.com • https://login.windows-ppe.net	com/microsoft/identity/common/java/providers/microsoft/azureactivedirectory/AzureActiveDirectoryEnvironment.java
• https://login.microsoftonline.com/{microsoft.com/oauth2/token	com/microsoft/identity/common/java/providers/microsoft/azureactivedirectory/AzureActiveDirectoryOAuth2Strategy.java
• https://github.com/TooTallNate/Java-WebSocket/wiki/lost-connection-detection	org/java_websocket/AbstractWebSocket.java
• http://readium.org/2014/01/lcp	org/readium/r2/shared/drm/Drm.java
• https://help.ably.io/error/	io/ably/lib/types/ErrorInfo.java
• https://drive.google.com • https://drive.google.com/file/d/	com/mcb/stjohnsemschool/utils/CustomLinkMovementMethod.java
• https://docs.google.com/gview?embedded=true&url=	com/mcb/stjohnsemschool/activity/ViewFileFromUrlActivity.java
• https://play.google.com/store/apps/details?id=	com/mcb/stjohnsemschool/activity/SplashActivity.java

• https://login.live.com/	com/microsoft/identity/common/internal/ui/webview/AzureActiveDirectoryWebViewClient.java
• http://www.ccil.org/~cowan/tagsoup/features/root-bogons • http://www.ccil.org/~cowan/tagsoup/features/bogons-empty • http://www.ccil.org/~cowan/tagsoup/properties/schema • http://www.ccil.org/~cowan/tagsoup/features/default-attributes • http://www.ccil.org/~cowan/tagsoup/properties/scanner • http://www.ccil.org/~cowan/tagsoup/features/ignorable-whitespace • http://www.ccil.org/~cowan/tagsoup/features/cdata-elements • http://www.ccil.org/~cowan/tagsoup/features/translate-colons • http://www.ccil.org/~cowan/tagsoup/features/restart-elements • http://www.ccil.org/~cowan/tagsoup/properties/auto-detector • http://www.ccil.org/~cowan/tagsoup/features/ignore-bogons	org/ccil/cowan/tagsoup/Parser.java
• http://tempuri.org/	com/mcb/stjohnsemschool/activity/SoapObjectProvider.java
• https://go.microsoft.com/fwlink/?linkid=2138180 • https://login.microsoftonline.com/common/oauth2/v2.0/logout	com/microsoft/identity/common/adal/internal/AuthenticationConstants.java
• https://api.pearson.com/v2/dictionaries/entries?headword= • http://127.0.0.1 • http://127.0.0.1:8080/	com/foobnix/Constants.java
• https://kb.myclassboard.com/notifications/notifications/	com/mcb/stjohnsemschool/settings/SettingsActivity.java
• https://cdndatastatic.myclassboard.com/img/video_placeholder.jpg	com/mcb/stjohnsemschool/adapter/LearningTopicContentsAdapter.java
• http://3deureka.in&port=8602&userid=	com/mcb/stjohnsemschool/activity/DesignMateTopicsActivity.java
• https://cdndatastatic.myclassboard.com/img/video_placeholder.jpg	com/mcb/stjohnsemschool/adapter/LearningSubjectVideosAdapter.java
• https://native-ux-mock-api.azurewebsites.net/lumonconvergedps.onmicrosoft.com	com/microsoft/identity/common/java/nativeauth/providers/NativeAuthOAuth2Configuration.java
• http://mcbapi.myclassboard.com/onlinepayment_web.aspx?postdata=	com/mcb/stjohnsemschool/fragment/DesignMateCoursePacksFragment.java
• 127.0.0.1	org/nanohttpd/protocols/http/HTTPSession.java
• https://login.microsoftonline.us • https://login.partner.microsoftonline.cn • https://login.microsoftonline.de	com/microsoft/identity/client/AzureCloudInstance.java
• https://login.partner.microsoftonline.cn/common • https://login.microsoftonline.com/consumers • https://login.microsoftonline.us/common • https://login.microsoftonline.de/common • https://login.windows.net/common	com/microsoft/identity/common/adal/internal/tokensharing/TokenShareUtility.java

• https://mcbapi.myclassboard.com/	com/mcb/stjohnsemschool/services/ApiClient.java
• http://www.idpf.org/2007/ops	org/readium/r2/streamer/parser/epub/NameSpaceResolver.java
• javascript:ontextselectionitemclicked • javascript:clearselection • javascript:deletethishighlight • javascript:getselectionrect	com/folioreader/ui/view/FolioWebView.java
• https://graph.microsoft.com/v1.0/me	com/mcb/stjohnsemschool/utils/MSGraphRequestWrapper.java
• http://mcbapi.myclassboard.com/onlinepayment_web.aspx?postdata=	com/mcb/stjohnsemschool/fragment/DesignMateSubscribedCoursePacksFragment.java
• https://internet-up.ably-realtime.com/is-the-internet-up.txt	io/ably/lib/transport/ConnectionManager.java
• https://corp14.myclassboard.com/ • https://corp14.myclassboard.com/mcbmobileappservice.asmx • https://github.com/scottyab/showhidepasswordedittext • https://stjohnsschool.myclassboard.com • https://play.google.com/store/apps/details?id= • https://www.myclassboard.com/privacy • javascript:clearselection • javascript:computelastreadcfi • https://st-johns-em-high-school.firebaseio.com • https://corp14api.myclassboard.com/mcbmobileappservice.asmx • javascript:highlightsearchlocator	自研引擎-S

Firebase 配置安全检测

标题	严重程度	描述信息
应用与Firebase数据库通信	信息	该应用与位于 https://st-johns-em-high-school.firebaseio.com 的 Firebase 数据库进行通信

Firebase远程配置已禁用	安全	Firebase远程配置URL（ https://firebaseremoteconfig.googleapis.com/v1/projects/718163066574/namespaces/firebase:fetch?key=AIzaSyBeHcP7FXpiEpxb4lb7iaHgOT-Hhk55KiA ）已禁用。响应内容如下所示：
		{
		"state": "NO_TEMPLATE"
		}

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Google Sign-In	Google	提供使用 Google 登录的 API。

Google Play Service	Google	借助 Google Play 服务，您的应用可以利用由 Google 提供的最新功能，例如地图，Google+ 等，并通过 Google Play 商店以 APK 的形式分发自动平台更新。 这样一来，您的用户可以更快地接收更新，并且可以更轻松地集成 Google 必须提供的最新信息。
File Provider	Android	FileProvider 是 ContentProvider 的特殊子类，它通过创建 content://Uri 代替 file:///Uri 以促进安全分享与应用程序关联的文件。
Jetpack App Startup	Google	App Startup 库提供了一种直接，高效的方法来在应用程序启动时初始化组件。库开发人员和应用程序开发人员都可以使用 App Startup 来简化启动顺序并显式设置初始化顺序。App Startup 允许您定义共享单个内容提供程序的组件初始化程序，而不必为需要初始化的每个组件定义单独的内容提供程序。这可以大大缩短应用启动时间。
Firebase	Google	Firebase 提供了分析、数据库、消息传递和崩溃报告等功能，可助您快速采取行动并专注于您的用户。
Picasso	Square	一个强大的 Android 图片下载缓存库。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
Firebase Analytics	Google	Google Analytics（分析）是一款免费的应用衡量解决方案，可提供关于应用使用情况和用户互动度的分析数据。

邮箱地址敏感信息提取

EMAIL	源码文件
mcbmobile@myclassboard.com	com/mcb/stjohnsemschool/settings/SettingsActivity.java

第三方追踪器检测

名称	类别	网址
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
OpenTelemetry (OpenCensus, OpenTracing)	Analytics	https://reports.exodus-privacy.eu.org/trackers/412

敏感凭证泄露检测

可能的密钥
凭证信息=> "com.google.android.geo.API_KEY" : "@7F12002A"
"api_key_map" : "AIzaSyDvRRbEuf9FM_PPb7bz4i9ePto6sRkFIR0"
"firebase_database_url" : "https://st-johns-em-high-school.firebaseio.com"
"google_api_key" : "AIzaSyBeHcP7FXpiEpxb4lb7iaHgOT-Hhk55KiA"
"google_app_id" : "1:718163066574:android:ac8846d0cd50f5b9b5da9f"

"google_crash_reporting_api_key" : "AIzaSyBeHcP7FXpiEpxb4lb7iaHgOT-Hhk55KiA"
"http_auth_dialog_cancel" : "Cancel"
"http_auth_dialog_login" : "Login"
"http_auth_dialog_password" : "Password"
"http_auth_dialog_username" : "Username"
"password" : "Password"
"service_url_api" : "https://corp14api.myclassboard.com/MCBMobileAppService.asmx"
xxAk8S05zu0Nkce+X2J6IKJ2e7YE4F9ZorZj0YnYUQ2vw8vLc8VGGOqJdTnVySbbcy9VY8UDbOfeOETSErYllw==
32670510020758816978083085130507043184471273380659243275938904335757337482424
jPpMoaNvcxSLMX4yG4C3Gf86rtTqh33SqpuRKg4WOP+MnnpA52zZgvKLW76U4Cqqf68iaBk9W7k/ihmiSAtgQ==
VCpKgbYCXucoq1mZ4BZPsh5taNE=
2LHYpyDYp9mG2KrYrtin2Kgg2qnZhtuM2K8g24zaqSDZgdin24zZhA==
7fmduHKTdHHrlMvldlEqAIlSfii1tl35bxj1OXN5Ve8c4lU6URVu4xtSHc3BVZxS6WWlnxMDnIfQN0N0K2NDJg==
26247035095799689268623156744566981891852923491109213387815615900925518854738050089022538053975719786650872476732087
27580193559959705877849011840389048093056905856361568521427073019886892413098108651362607648837451077654397612305 75
55066263022277343669578718895168534326250603453777594175500187360389116729240
39402006196394479212279040100143613805079732726544666794690527962765399113263569398956308152294913554433653942643
375718002577002046354550722449118360355445134769762486694567779615544477440556316691234405012945539562144444537289428522585666729196580810124344277578376784
41058363725152142129326129780047264091144410159937255543532631403946740129 1
36134250956749795798585127919587881956611106672985015071877198253568414405109
MAppParentAPI/GetStudentObjectiveExamMarksDetailsByExamType
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
eyJhdWQiOiJkQ0JDdXN0b21QYXJlbnRBUFAiLCJqdGkiOiJmYWU2M2M0NS1mYTBlLTQ4YmQtOGY1OS02ZWNjMzU0N2ZlNDIiLCJpYXQiOjE2MjczMjY4MDh9
2KfbjNqpINmB2KfYptmE2YNmF24zauiDYs9uSINin2YbYqtiu2KfYqCDaqdix24zaug==
109384903807373424745111239076680556993620759895168374899458639449595311615073501601370873757375962324859213229670631330943845253159101297214231748847898598 4
AIzaSyA49tz6flcjjZXVenZ12eTXfoJ1ujDofG0
11579208921035624876269744694940757352999695522413576034242225906106851204436 9

1157920892373161954235709850086879078528375642790749043826051631415181614943337
1157920892103562487626974469494075735300861434152903141955336313088670978539 51
87749df4-7ccf-48f8-aa87-704bad0e0e16
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
pdAtoxfsEwbpQsIaua5Uobl5AQEjqt40aPXI7UY1lIW0NTmg0G4jHQ5T5mujSjjU06q4mEHs5hb6z/Mr0PNlmQ==
1157920892103562487626974469494075735300861434152903141955336313088670978539 48
2661740802050217063228768716723360960729859168756973147706671368418802944996427808491545080627771902352094211225065558662157113545570916814161637315895999846
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186160697311231 6
29d9ed98-a469-4536-ade2-f981bc1d605e
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825895800186160697311231 9
9188040d-6c67-4c5b-b112-36a304b66dad
7ZWY64KY7J2YIO2MjOydvOydhCDshKDtg50=
MAppParentAPI/GetStudentObjectiveExamMarksDetailsBySubjectWise
Gu8CuaYmSV5CHWd6dz3tGPXIE+YTalCVIXi5lEBXpvUgsMKoHbU9Rqou3WNRNU1tdz8pVEADTCCJ5f02fbw9qw==
fcg80qvoM1YMKJZibjBwQcDfOno=
x28mHDILP8IZRH6EfjD4zC1bcpgk8euKS51KiyoddU8+e34xEgy3Q9XTazyS/C7EXX4o/EJpDV8MqmEfIf7LA==
832571096148902998554675128952018879287853048861315594139205902480503199884419224438643760392947333078086511627871
EZ2RCcsmf869Ec41PgHHnF0I0MqmVsADFFy8AtcfEKsjDYAPtKxCMZVdT+y+K1IWRnPk4Lf2PUAcL5N49OqAA==
484395612939064517990525852527979142027629435260417479958440807170824046352 86
cec596b4528bb016aeeb46a678a68e28
1157920892373161954235709850086879078532699846656405640394575840079088346716 63
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057148

Google Play 应用市场信息

标题: St.John's E.M High School

评分: 4.23741 安装: 10,000+ 价格: 0 **Android**版本支持: 分类: 教育 **Play Store URL:** com.mcb.stjohnsemschool.activity

开发者信息: Myclassboard Educational Solutions Pvt Ltd, Myclassboard+Educational+Solutions+Pvt+Ltd, None, https://www.myclassboard.com,

admin@myclassboard.com,

发布日期: 2020年4月30日 **隐私政策:** Privacy link

关于此应用:

MyClassboard为父母提供了交流应用程序，他们可以使用该应用程序下载学校公告，班级作业，事件。

免责声明及风险提示:

本报告由南明离火移动安全分析平台自动生成，内容仅供参考，不构成任何法律意见或建议。本平台对使用本产品及其内容所引发的任何直接或间接损失概不负责。本报告内容仅供网络安全研究，不得违反中华人民共和国相关法律法规。如有任何疑问，请及时与我们联系。

南明离火移动安全分析平台是一款专业的移动端恶意软件分析和安全评估框架。它能够执行静态分析和动态分析，深入扫描软件中中潜在的漏洞和安全隐隐患。