



ANDROID 静态分析报告



digitalacademyinvest • v1.0

分析日期: 2025-06-20 20:59:26

i应用概览

文件名称:	digitalacademyinvest_1_1.0.apk
文件大小:	1.04MB
应用名称:	digitalacademyinvest
软件包名:	digital.academy.invest
主活动:	digital.academy.invest.MainActivity
版本号:	1.0
最小SDK:	17
目标SDK:	30
加固信息:	未加壳
应用程序安全分数:	47/100 (中风险)
杀软检测:	3 个杀毒软件报毒
MD5:	fee2effc1ee86cf11aefc197952aea87
SHA1:	4afed02c39bb18d3524d1e154c7225bc6f9f6050
SHA256:	b089d6e4c1db465bf0ac085ee0470a18eb95f9c3258ab019f1521ed904cc7be2

📊 分析结果严重性分布

🚨 高危	⚠️ 中危	ℹ️ 信息	✅ 安全	🔍 关注
2	7	1	1	0

📦 四大组件导出状态统计

Activity组件: 1个, 其中export的有: 0个
Service组件: 0个, 其中export的有: 0个
Receiver组件: 0个, 其中export的有: 0个
Provider组件: 0个, 其中export的有: 0个

🌸 应用签名证书信息

二进制文件已签名

v1 签名: True

v2 签名: True

v3 签名: False

v4 签名: False

主题: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com

签名算法: rsassa_pkcs1v15

有效期自: 2008-02-29 01:33:46+00:00

有效期至: 2035-07-17 01:33:46+00:00

发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com

序列号: 0x936eacbe07f201df

哈希算法: sha1

md5: e89b158e4bcf988ebd09eb83f5378e87

sha1: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81

sha256: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc

sha512: 5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccb6b34ec4233f5f640703581053abfea303977272d17958704d89b7711292a4569

公钥算法: rsa

密钥长度: 2048

指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75

找到 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	查看网络状态	允许应用程序查看所有网络的状态。
android.permission.ACCESS_FINE_LOCATION	危险	访问精准的位置源，例如手机上的全球定位系统（如有）当前设备的位置	访问精准的位置源，例如手机上的全球定位系统（如有）。恶意程序可以用它来确定您所在的位置，并可能消耗额外的电池电量。
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.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.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.VIBRATE	普通	控制振动器	允许应用程序控制振动器。
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。

可浏览 Activity 组件分析

ACTIVITY	INTENT
digital.academy.invest.MainActivity	Schemes: https://, Hosts: null, Path Prefixes: /,

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	应用程序已使用代码签名证书进行签名
应用程序存在Janus漏洞	警告	应用程序使用了v1签名方案进行签名，如果只使用v1签名方案，那么它就容易受到安卓5.0-8.0上的Janus漏洞的攻击。在安卓5.0-7.0上运行的使用了v1签名方案的应用程序，以及同时使用了v2/v3签名方案的应用程序也同样存在漏洞。

Manifest 配置安全分析

高危: 0 | 警告: 2 | 信息: 0 | 屏蔽: 0

序号	问题	严重程度	描述信息
1	应用程序可以安装在一个有漏洞的安卓版本上 [minSdk=17]	警告	这个应用程序可以安装在一个有漏洞的旧版本的安卓上。建议使用安卓系统8.0以上版本，API级别大于26 以获得合理的安全更新。
2	应用程序数据可以被备份 [android:allowBackup=true]	警告	这个标志允许任何人通过adb备份你的应用程序数据。它允许已经启用了USB调试的用户从设备上复制应用程序数据。

代码安全漏洞检测

高危: 2 | 警告: 4 | 信息: 1 | 安全: 0 | 屏蔽: 0

序号	问题	等级	参考标准	文件位置
1	应用程序记录日志信息,不得记录敏感信息	信息	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	升级会员: 解锁高级权限
2	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: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员: 解锁高级权限
3	应用程序创建临时文件. 敏感信息永远不应该被写入临时文件	警告	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	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: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
5	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: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	升级会员：解锁高级权限
6	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
7	WebView域控制不严格漏洞	高危		升级会员：解锁高级权限

🔍 恶意域名威胁检测

域名	状态	中国境内	位置信息
digitalacademy-invest.win	安全	否	IP地址: 194.233.70.31 国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289670 经度: 103.850067 查看: Google 地图
www.digitalacademy-invest.win	安全	否	IP地址: 194.233.70.31 国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289670 经度: 103.850067 查看: Google 地图
websitetopk.com	安全	否	IP地址: 172.67.132.1 国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203 查看: Google 地图

URL 链接安全分析

URL信息	源码文件
- file:///android_asset/404r.html - https://websitetoapk.com/ - https://digitalacademy-invest.win/loginapp.php	digital/academy/invest/MainActivity.java
- https://websitetoapk.com/ - https://digitalacademy-invest.win/loginapp.php - file:///android_asset/404r.html - www.digitalacademy-invest.win	自研引擎分析结果

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，深入扫描软件中潜在的漏洞和安全隐患。

© 2025 南明离火 - 移动安全分析平台自动生成