Evaluation Warning: The document was created with Spire.Doc for Python.

**PH（ 1.1.1版本）   
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。  
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | PH |
| 版本 | 1.1.1 |
| 包名 | com.zq.ph |
| 域名线索 | 42条 |
| URL线索 | 19条 |
| APP图标 |  |
| 分析日期 | 2025年6月21日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | phxyw001\_2024.11.9.1000.apk |
| 文件大小 | 12.76MB |
| MD5值 | 76f966122117caec3ec2584a8b87b9bc |
| SHA1值 | 00a7706fc827284477426458efdc2745180c1759 |
| SHA256值 | b945b31987a9add7c39da681d74f2f3ca6d8fd888038a77e00b9055e277e4500 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | PH |
| 包名 | com.zq.ph |
| 主活动Activity | com.zq.douyin.MainActivity |
| 安卓版本名称 | 1.1.1 |
| 安卓版本 | 3 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| developer.mozilla.org | IP: 34.111.97.67  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| douyin-api.ybunx.com | IP: 172.67.139.69  所属国家: United States of America  地区: California  城市: San Francisco |
| ldy.nroom10.com | 没有服务器地理信息. |
| cdn.plyr.io | IP: 104.26.13.19  所属国家: United States of America  地区: California  城市: San Francisco |
| html2canvas.hertzen.com | IP: 104.21.65.51  所属国家: United States of America  地区: California  城市: San Francisco |
| 34.150.33.40 | IP: 34.150.33.40  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| bk.dlkxi.cc | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| www.youtube-nocookie.com | IP: 31.13.73.9  所属国家: Ireland  地区: Dublin  城市: Dublin |
| noembed.com | IP: 151.101.65.91  所属国家: United States of America  地区: California  城市: San Francisco |
| www.w3.org | IP: 104.18.22.19  所属国家: United States of America  地区: California  城市: San Francisco |
| api.h-gpro.com | 没有服务器地理信息. |
| cres.rqi564.com | IP: 149.104.35.195  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| chen.ybunx.com | IP: 172.67.139.69  所属国家: United States of America  地区: California  城市: San Francisco |
| schemas.android.com | 没有服务器地理信息. |
| aomedia.org | IP: 199.16.156.71  所属国家: United States of America  地区: Georgia  城市: Atlanta |
| d3n2vdp1h9ohbb.cloudfront.net | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| vimeo.com | IP: 157.240.17.35  所属国家: Switzerland  地区: Zurich  城市: Zurich |
| cdn.jsdelivr.net | IP: 46.82.174.69  所属国家: Germany  地区: Niedersachsen  城市: Braunschweig |
| kk.xcdwt.com | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| 43.231.0.225 | IP: 43.231.0.225  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| pan.baidu.com | IP: 110.242.69.174  所属国家: China  地区: Hebei  城市: Baoding |
| axios-http.com | IP: 52.76.120.174  所属国家: Singapore  地区: Singapore  城市: Singapore |
| jsperf.com | IP: 104.16.228.18  所属国家: United States of America  地区: California  城市: San Francisco |
| i.ytimg.com | IP: 23.234.30.58  所属国家: United States of America  地区: Delaware  城市: Newark |
| img01.yzcdn.cn | IP: 60.25.92.83  所属国家: China  地区: Tianjin  城市: Tianjin |
| t.me | IP: 149.154.167.99  所属国家: United Kingdom of Great Britain and Northern Ireland  地区: England  城市: Warrington |
| baq.fbafb.cn | 没有服务器地理信息. |
| hfive.qsxon.com | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| dfe.hapha.cn | 没有服务器地理信息. |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| swiperjs.comn | 没有服务器地理信息. |
| 101.132.69.237 | IP: 101.132.69.237  所属国家: China  地区: Shanghai  城市: Shanghai |
| brianleroux.github.com | 没有服务器地理信息. |
| go.aniview.com | IP: 104.83.102.21  所属国家: Italy  地区: Lombardia  城市: Milan |
| player.vimeo.com | IP: 199.59.148.229  所属国家: United States of America  地区: California  城市: San Francisco |
| issues.apache.org | IP: 168.119.33.54  所属国家: Germany  地区: Bayern  城市: Gunzenhausen |
| www.apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| faw.douying8.com | 没有服务器地理信息. |
| raw.githubusercontent.com | IP: 185.199.108.133  所属国家: United States of America  地区: Pennsylvania  城市: California |
| hertzen.com | IP: 172.67.140.170  所属国家: United States of America  地区: California  城市: San Francisco |
| imasdk.googleapis.com | IP: 114.250.70.33  所属国家: China  地区: Beijing  城市: Beijing |
| www.youtube.com | IP: 157.240.17.35  所属国家: Switzerland  地区: Zurich  城市: Zurich |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://chen.ybunx.com/apk/app-1.1.0-3.apk | defpackage/j00.java |
| https://dfe.hapha.cn | defpackage/l00.java |
| https://api.h-gpro.com | defpackage/l00.java |
| https://baq.fbafb.cn | defpackage/l00.java |
| https://faw.douying8.com | defpackage/l00.java |
| https://douyin-api.ybunx.com | defpackage/l00.java |
| http://schemas.android.com/apk/res/android | defpackage/b0.java |
| http://www.apache.org/licenses/LICENSE-2.0 | 摸瓜V2引擎 |
| http://jsperf.com/b64tests | 摸瓜V2引擎 |
| http://server/myapp/index.html | 摸瓜V2引擎 |
| https://issues.apache.org/jira/browse/CB-11522) | 摸瓜V2引擎 |
| https://html2canvas.hertzen.com> | 摸瓜V2引擎 |
| https://hertzen.com> | 摸瓜V2引擎 |
| https://cdn.jsdelivr.net/npm/workbox-cdn@5.1.4/workbox | 摸瓜V2引擎 |
| https://cdn.plyr.io/3.7.2/plyr.svg | 摸瓜V2引擎 |
| https://cdn.plyr.io/static/blank.mp4 | 摸瓜V2引擎 |
| https://player.vimeo.com/api/player.js | 摸瓜V2引擎 |
| https://player.vimeo.com/video/ | 摸瓜V2引擎 |
| https://vimeo.com/api/oembed.json?url= | 摸瓜V2引擎 |
| https://www.youtube.com/iframe\_api | 摸瓜V2引擎 |
| https://noembed.com/embed?url=https://www.youtube.com/watch?v= | 摸瓜V2引擎 |
| https://imasdk.googleapis.com/js/sdkloader/ima3.js | 摸瓜V2引擎 |
| https://www.youtube-nocookie.com | 摸瓜V2引擎 |
| http://www.youtube.com | 摸瓜V2引擎 |
| https://i.ytimg.com/vi/ | 摸瓜V2引擎 |
| https://go.aniview.com/api/adserver6/vast/ | 摸瓜V2引擎 |
| https://hfive.qsxon.com | 摸瓜V2引擎 |
| https://t.me/ | 摸瓜V2引擎 |
| https://pan.baidu.com/s/1wPlQE5srd\_cGuPVqBWNUxw?pwd=1234 | 摸瓜V2引擎 |
| https://ldy.nroom10.com:19999/nhfth001 | 摸瓜V2引擎 |
| https://cres.rqi564.com | 摸瓜V2引擎 |
| https://kk.xcdwt.com/api/v1/ | 摸瓜V2引擎 |
| https://43.231.0.225:19888/api/v1/ | 摸瓜V2引擎 |
| https://34.150.33.40:19888/api/v1/ | 摸瓜V2引擎 |
| https://bk.dlkxi.cc/api/v1/ | 摸瓜V2引擎 |
| https://d3n2vdp1h9ohbb.cloudfront.net/api/v1/ | 摸瓜V2引擎 |
| https://101.132.69.237:16888/api/v1/ | 摸瓜V2引擎 |
| https://aomedia.org/emsg/ID3 | 摸瓜V2引擎 |
| https://github.com/mathiasbynens/CSS.escape). | 摸瓜V2引擎 |
| https://github.com/zloirock/core-js/blob/v3.37.1/LICENSE | 摸瓜V2引擎 |
| https://github.com/zloirock/core-js | 摸瓜V2引擎 |
| http://a | 摸瓜V2引擎 |
| http://a/c%20d?a=1&c=3 | 摸瓜V2引擎 |
| https://a@b | 摸瓜V2引擎 |
| http://x | 摸瓜V2引擎 |
| https://github.com/crypto-browserify/crypto-browserify | 摸瓜V2引擎 |
| https://img01.yzcdn.cn/vant/share-sheet- | 摸瓜V2引擎 |
| https://img01.yzcdn.cn/vant/empty-image- | 摸瓜V2引擎 |
| http://swiperjs.com\n | 摸瓜V2引擎 |
| https://github.com/indutny/elliptic/issues | 摸瓜V2引擎 |
| https://github.com/indutny/elliptic | 摸瓜V2引擎 |
| https://github.com/axios/axios.git | 摸瓜V2引擎 |
| https://github.com/axios/axios/issues | 摸瓜V2引擎 |
| https://axios-http.com | 摸瓜V2引擎 |
| https://developer.mozilla.org/fr/docs/Web/API/CustomEvent | 摸瓜V2引擎 |
| http://www.apache.org/licenses/LICENSE-2.0 | 摸瓜V2引擎 |
| http://brianleroux.github.com/lawnchair/), | 摸瓜V2引擎 |
| http://www.apache.org/licenses/LICENSE-2.0 | 摸瓜V2引擎 |
| http://www.apache.org/licenses/LICENSE-2.0 | 摸瓜V2引擎 |
| http://www.apache.org/licenses/LICENSE-2.0 | 摸瓜V2引擎 |
| http://www.apache.org/licenses/LICENSE-2.0 | 摸瓜V2引擎 |
| http://www.apache.org/licenses/LICENSE-2.0 | 摸瓜V2引擎 |
| http://www.apache.org/licenses/LICENSE-2.0 | 摸瓜V2引擎 |
| http://www.apache.org/licenses/LICENSE-2.0 | 摸瓜V2引擎 |
| http://www.apache.org/licenses/LICENSE-2.0 | 摸瓜V2引擎 |
| https://raw.githubusercontent.com/stefanpenner/es6-promise/master/LICENSE | 摸瓜V2引擎 |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| sy12god@gmail.com | 摸瓜V2引擎 |
| git@github.com  fedor@indutny.com | 摸瓜V2引擎 |
| solderzzc@gmail.com  stefano.magrassi@gmail.com | 摸瓜V2引擎 |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 19919152923 | 摸瓜V2引擎 |

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: C=a, ST=a, L=a, O=a, OU=a, CN=a 签名算法: rsassa\_pkcs1v15 有效期自: 2022-06-21 05:32:57+00:00 有效期至: 2049-11-06 05:32:57+00:00 发行人: C=a, ST=a, L=a, O=a, OU=a, CN=a 序列号: 0x41772888 哈希算法: sha256 md5值: d49d20229d9dab896e21574bc3232c24 sha1值: 97b79fd8c8827cda42e464328c46dfb462f81b1e sha256值: ba05c89d57a24934d976a647b91f733d38eb6f32d0c254b52aaba0ac1cc13b4b sha512值: 4cf78e142e057f170c4bab11acec9f775015ff9539379b930d33d62c7587815ea44a53570eaa9b1ac1d1c4688d43d0d0a45c6a70ed86ddffcfff7caaac0389fb 公钥算法: rsa 密钥长度: 2048 指纹: a8622d5e2214871f8de1d32546543dce06b23472ccf6ef958be849992a5043d9**

## **6. 硬编码敏感信息**

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看 |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看 |  |  |

## **9. 此APP的危险动作**

| 向手机申请的权限 | 是否危险 | 类型 | 详细情况 |
| --- | --- | --- | --- |
| android.permission.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| android.permission.ACCESS\_NETWORK\_STATE | 正常 | 查看网络状态 | 允许应用程序查看所有网络的状态 |
| android.permission.ACCESS\_WIFI\_STATE | 正常 | 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.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.REQUEST\_INSTALL\_PACKAGES | 危险 | 允许应用程序请求安装包。 | 恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。 |
| android.permission.READ\_EXTERNAL\_STORAGE | 危险 | 读取外部存储器内容 | 允许应用程序从外部存储读取 |

## **10. 应用内通信**

**报告由**  [**摸瓜APK反编译平台**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**