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

**优贝（ 1.0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 | 优贝 |
| 版本 | 1.0 |
| 包名 | com.hammer.ubet.wap |
| 域名线索 | 28条 |
| URL线索 | 6条 |
| APP图标 |  |
| 分析日期 | 2025年6月30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 | apk.APK |
| 文件大小 | 5.49MB |
| MD5值 | 9e5252169469585780c64c96b124ef1b |
| SHA1值 | 517cdf5df3902138b0ca9df23dbf86b208b6a319 |
| SHA256值 | 461fbdd644d9e2c3edab2e06f515ab932dbd372ea8cf6fefad945697e288b0b2 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 优贝 |
| 包名 | com.hammer.ubet.wap |
| 主活动Activity | com.hammer.ubet.wap.MainActivity |
| 安卓版本名称 | 1.0 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| www.recent | 没有服务器地理信息.  |
| mozilla.github.io | IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| apis.oss.img.ub999.vip | IP: 103.212.99.42 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| www.usdt888m.com | IP: 43.240.12.9 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| www.c | 没有服务器地理信息.  |
| .jpg | 没有服务器地理信息.  |
| capacitorjs.com | IP: 172.67.203.214 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.a | 没有服务器地理信息.  |
| www.interpretation | 没有服务器地理信息.  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.style | IP: 99.83.155.228 所属国家: United States of America 地区: Washington 城市: Seattle  |
| www.text-decoration | 没有服务器地理信息.  |
| www.language | 没有服务器地理信息.  |
| socket.io | IP: 76.76.21.93 所属国家: United States of America 地区: California 城市: Walnut  |
| www.hortcut | 没有服务器地理信息.  |
| www.icon | 没有服务器地理信息.  |
| stackoverflow.com | IP: 172.64.155.249 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.css | 没有服务器地理信息.  |
| api.capgo.app | IP: 108.160.169.37 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.world | IP: 99.83.155.228 所属国家: United States of America 地区: Washington 城市: Seattle  |
| www.lia | 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  |
| .css | 没有服务器地理信息.  |
| www.wencodeuricomponent | 没有服务器地理信息.  |
| www.years | 没有服务器地理信息.  |
| localforage.github.io | IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| vuejs.org | IP: 3.33.186.135 所属国家: United States of America 地区: Washington 城市: Seattle  |
| ricostacruz.com | IP: 172.67.221.161 所属国家: United States of America 地区: California 城市: San Francisco  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://dictionaryperceptionrevolutionfoundationpx;height:successfulsupportersmillenniumhis  | org/brotli/dec/Dictionary.java  |
| http://mathematicsmargin-top:eventually  | org/brotli/dec/Dictionary.java  |
| http://Descriptionrelatively  | org/brotli/dec/Dictionary.java  |
| http://applicationslink\  | org/brotli/dec/Dictionary.java  |
| http://navigation\  | org/brotli/dec/Dictionary.java  |
| http://px;  | org/brotli/dec/Dictionary.java  |
| https://www.World  | org/brotli/dec/Dictionary.java  |
| http://www.years  | org/brotli/dec/Dictionary.java  |
| http://interested  | org/brotli/dec/Dictionary.java  |
| http://familiar  | org/brotli/dec/Dictionary.java  |
| https://was  | org/brotli/dec/Dictionary.java  |
| https://aIn  | org/brotli/dec/Dictionary.java  |
| http://whether  | org/brotli/dec/Dictionary.java  |
| http://interpreted  | org/brotli/dec/Dictionary.java  |
| http://\  | org/brotli/dec/Dictionary.java  |
| http://);  | org/brotli/dec/Dictionary.java  |
| http://addEventListenerresponsible  | org/brotli/dec/Dictionary.java  |
| http://.jpg  | org/brotli/dec/Dictionary.java  |
| http://<a  | org/brotli/dec/Dictionary.java  |
| https://<div  | org/brotli/dec/Dictionary.java  |
| http://according  | org/brotli/dec/Dictionary.java  |
| http://www.interpretation  | org/brotli/dec/Dictionary.java  |
| http://s;text-align:centerfont-weight:  | org/brotli/dec/Dictionary.java  |
| http://html4/loose.dtd\  | org/brotli/dec/Dictionary.java  |
| http://style=\  | org/brotli/dec/Dictionary.java  |
| http://staticsuggested  | org/brotli/dec/Dictionary.java  |
| http://www.a  | org/brotli/dec/Dictionary.java  |
| http://An  | org/brotli/dec/Dictionary.java  |
| https://www.recent  | org/brotli/dec/Dictionary.java  |
| http://In  | org/brotli/dec/Dictionary.java  |
| http://www./div></div><div  | org/brotli/dec/Dictionary.java  |
| http://cript\  | org/brotli/dec/Dictionary.java  |
| http://\n<script  | org/brotli/dec/Dictionary.java  |
| http://www.wencodeURIComponent(\  | org/brotli/dec/Dictionary.java  |
| http://encoding=\  | org/brotli/dec/Dictionary.java  |
| http://www.icon\  | org/brotli/dec/Dictionary.java  |
| http://imEnglish  | org/brotli/dec/Dictionary.java  |
| http://i  | org/brotli/dec/Dictionary.java  |
| http://www.<li><a  | org/brotli/dec/Dictionary.java  |
| http://site\_name\  | org/brotli/dec/Dictionary.java  |
| http://www.hortcut  | org/brotli/dec/Dictionary.java  |
| http://</a></li><li  | org/brotli/dec/Dictionary.java  |
| http://<div  | org/brotli/dec/Dictionary.java  |
| http://iparticipation  | org/brotli/dec/Dictionary.java  |
| http://www.\  | org/brotli/dec/Dictionary.java  |
| http://xt/css\  | org/brotli/dec/Dictionary.java  |
| http://link  | org/brotli/dec/Dictionary.java  |
| http://www.text-decoration:underthe  | org/brotli/dec/Dictionary.java  |
| http://option><option  | org/brotli/dec/Dictionary.java  |
| http://www</a><a  | org/brotli/dec/Dictionary.java  |
| http://w  | org/brotli/dec/Dictionary.java  |
| http://.css\  | org/brotli/dec/Dictionary.java  |
| http://www.style=\  | org/brotli/dec/Dictionary.java  |
| http://www.css\  | org/brotli/dec/Dictionary.java  |
| http://ator\  | org/brotli/dec/Dictionary.java  |
| http://www.language=\  | org/brotli/dec/Dictionary.java  |
| http://www-//W3C//DTD  | org/brotli/dec/Dictionary.java  |
| http://UA-Compatible\  | org/brotli/dec/Dictionary.java  |
| http://www.C//DTD  | org/brotli/dec/Dictionary.java  |
| http://www.  | org/brotli/dec/Dictionary.java  |
| https://api.capgo.app/channel\_self  | ee/forgr/capacitor\_updater/CapacitorUpdaterPlugin.java  |
| https://api.capgo.app/stats  | ee/forgr/capacitor\_updater/CapacitorUpdaterPlugin.java  |
| https://api.capgo.app/updates  | ee/forgr/capacitor\_updater/CapacitorUpdaterPlugin.java  |
| https://capacitorjs.com/  | 摸瓜V2引擎  |
| https://stackoverflow.com/questions/29249132/wkwebview-complex-communication-between-javascript-native-code/49474323  | 摸瓜V2引擎  |
| https://stackoverflow.com/a/57382543  | 摸瓜V2引擎  |
| https://vuejs.org/error-reference/  | 摸瓜V2引擎  |
| https://capacitorjs.com/  | 摸瓜V2引擎  |
| https://apis.oss.img.ub999.vip:443  | 摸瓜V2引擎  |
| https://localforage.github.io/localForage  | 摸瓜V2引擎  |
| https://mozilla.github.io/localForage/  | 摸瓜V2引擎  |
| https://github.com/emn178/js-md5  | 摸瓜V2引擎  |
| http://ricostacruz.com/nprogress  | 摸瓜V2引擎  |
| https://github.com/nodeca/pako  | 摸瓜V2引擎  |
| https://socket.io/docs/v3/migrating-from-2-x-to-3-0/)  | 摸瓜V2引擎  |
| https://www.usdt888m.com/  | 摸瓜V2引擎  |
| https://www.usdt888m.com/  | 摸瓜V2引擎  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| jhruby.web@gmail.com emn178@gmail.com  | 摸瓜V2引擎  |

### **4.4 手机号线索**

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: True 找到 1 个唯一证书 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值: e89b158e4bcf988ebd09eb83f5378e87 sha1值: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81 sha256值: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc sha512值: 5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea303977272d17958704d89b7711292a4569 公钥算法: rsa 密钥长度: 2048 指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75**

## **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.READ\_CLIPBOARD\_IN\_BACKGROUND | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.WRITE\_CLIPBOARD | 未知 | Unknown permission | Unknown permission from android reference |
| com.hammer.ubet.wap.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |

## **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。**