Advanced VAPT Syllabus   AppSec Scorecard × dineshshetty/Android-InsecureB   Git commit and push fix   cyart-vapt-team/Week-1/Week1   diva-apk-file/DivaApplication.ap   +

localhost:8000/appsec_dashboard/82ab8b2193b3cfb1c737e3a786be363a/

RECENT SCANS   STATIC ANALYZER   DYNAMIC ANALYZER   API   DONATE ♥   DOCS   ABOUT   Search

MobSF Application Security Scorecard - Diva 1.0

⭐ Security Score

36

Security Score 36/100

🎖 Risk Rating

High Risk

Grade

A   B   **C**   F

🌐 Severity Distribution (%)

■ High   ■ Medium   ■ Info
■ Secure

🔒 Privacy Risk

0

User/Device Trackers

📋 Findings

🐞 High	⚠ Medium	ℹ Info	✔ Secure	🔍 Hotspot
5	7	1	1	1

high Application vulnerable to Janus Vulnerability	CERTIFICATE
	CERTIFICATE

high Application vulnerable to Janus Vulnerability | CERTIFICATE

high Application signed with debug certificate | CERTIFICATE

high App can be installed on a vulnerable unpatched Android version | MANIFEST

high Debug Enabled For App | MANIFEST

```
[android:debuggable-true]
Debugging was enabled on the app which makes it easier for reverse engineers to hook a debugger to it. This allows dumping a stack trace and accessing debugging helper classes.
```

high Debug configuration enabled. Production builds must not be debuggable. | CODE

medium Application Data can be Backed up | MANIFEST

medium Activity (jakhar.aseem.diva.APICredsActivity) is not Protected. | MANIFEST

medium Activity (jakhar.aseem.diva.APICreds2Activity) is not Protected. | MANIFEST

medium Content Provider (jakhar.aseem.diva.NotesProvider) is not Protected. | MANIFEST

📄 Findings

🐛 High 5	⚠️ Medium 7	ℹ️ Info 1	✅ Secure 1	🔍 Hotspot 1

---

high Application vulnerable to Janus Vulnerability   **CERTIFICATE**

```
Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with
v1, and v2/v3 scheme is also vulnerable.
```

---

high Application signed with debug certificate   **CERTIFICATE**

---

high App can be installed on a vulnerable unpatched Android version   **MANIFEST**

---

high Debug Enabled For App   **MANIFEST**

---

high Debug configuration enabled. Production builds must not be debuggable.   **CODE**

---

medium Application Data can be Backed up   **MANIFEST**