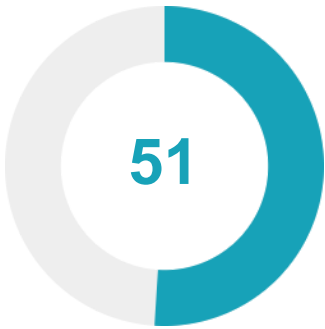


★ Security Score



Security Score 51/100

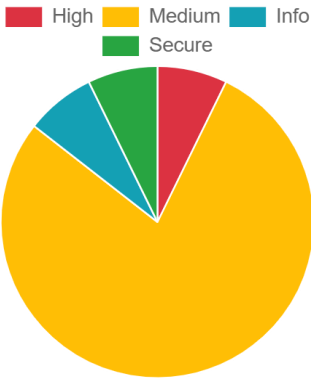
🚧 Risk Rating



Grade



📊 Severity Distribution (%)



🛡️ Privacy Risk



User/Device Trackers

📄 Findings



High
2



Info
2



Hotspot
1




Medium
20



Secure
2

<div>high</div>	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	CODE
<div>high</div>	Insecure WebView Implementation. WebView ignores SSL Certificate errors and accept any SSL Certificate. This application is vulnerable to MITM attacks	CODE
<div>medium</div>	App can be installed on a vulnerable Android version	MANIFEST
<div>medium</div>	Activity (proton.android.pass.ui.shortcuts.ShortcutActivity) is not Protected.	MANIFEST
<div>medium</div>	Service (proton.android.pass.autofill.ProtonPassAutofillService) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
<div>medium</div>	Service (proton.android.pass.features.passkeys.service.PasskeyProviderService) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
<div>medium</div>	Activity (me.proton.core.auth.presentation.ui.LoginTwoStepActivity) is not Protected.	MANIFEST
<div>medium</div>	Activity (me.proton.core.auth.presentation.ui.LoginSsoActivity) is not Protected.	MANIFEST
<div>medium</div>	Activity (me.proton.core.plan.presentation.ui.DynamicUpgradePlanActivity) is not Protected.	MANIFEST
<div>medium</div>	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
<div>medium</div>	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
<div>medium</div>	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
<div>medium</div>	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	CODE
<div>medium</div>	App creates temp file. Sensitive information should never be written into a temp file.	CODE
<div>medium</div>	The App uses an insecure Random Number Generator.	CODE
<div>medium</div>	SHA-1 is a weak hash known to have hash collisions.	CODE
<div>medium</div>	This App may request root (Super User) privileges.	CODE
<div>medium</div>	IP Address disclosure	CODE
<div>medium</div>	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	CODE
<div>medium</div>	App can read/write to External Storage. Any App can read data written to External Storage.	CODE
<div>medium</div>	Application contains Privacy Trackers	TRACKERS
<div>medium</div>	This app may contain hardcoded secrets	SECRETS
<div>info</div>	The App logs information. Sensitive information should never be logged.	CODE
<div>info</div>	This app listens to Clipboard changes. Some malware also listen to Clipboard changes.	CODE
<div>secure</div>	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	CODE
<div>secure</div>	This App may have root detection capabilities.	CODE

MobSF Application Security Scorecard generated for  (Proton Pass 1.30.1) 