# Android Static Analysis Report

## Detected Vulnerabilities:

### Type: Insecure Debuggable Flag

Severity: High

Description: The 'android:debuggable' flag is set to 'true' in AndroidManifest.xml.

File: AndroidManifest.xml

> This allows attackers to debug your application, potentially gaining access to sensitive data or bypassing security controls. Ensure this is 'false' in production builds.

### Type: Insecure Backup Allowed

Severity: Medium

Description: The 'android:allowBackup' flag is not explicitly set to 'false' (or is set to 'true').

File: AndroidManifest.xml

> This allows users (or attackers with adb access) to backup and restore application data, including sensitive information. Set 'android:allowBackup="false"' to prevent this, or implement a custom backup agent to secure sensitive data.

### Type: Unprotected Exported Component

Severity: High

Description: An exported activity ('com.android.insecurebankv2.LoginActivity') does not require a permission.

File: AndroidManifest.xml

> Exported components without proper permission protection can be invoked by any other application, potentially leading to unauthorized access, data leakage, or denial of service. Apply appropriate 'android:permission' to restrict access.

### Type: Unprotected Exported Component

Severity: High

Description: An exported activity ('com.android.insecurebankv2.PostLogin') does not require a permission.

File: AndroidManifest.xml

> Exported components without proper permission protection can be invoked by any other application, potentially leading to unauthorized access, data leakage, or denial of service. Apply appropriate 'android:permission' to restrict access.

### Type: Unprotected Exported Component

Severity: High

Description: An exported activity ('com.android.insecurebankv2.DoTransfer') does not require a permission.

File: AndroidManifest.xml

> Exported components without proper permission protection can be invoked by any other application, potentially leading to unauthorized access, data leakage, or denial of service. Apply appropriate 'android:permission' to restrict access.

## Detected Vulnerabilities (continued):

### Type: Unprotected Exported Component

Severity: High

Description: An exported activity ('com.android.insecurebankv2.ViewStatement') does not require a permission.

File: AndroidManifest.xml

> Exported components without proper permission protection can be invoked by any other application, potentially leading to unauthorized access, data leakage, or denial of service. Apply appropriate 'android:permission' to restrict access.

### Type: Unprotected Exported Component

Severity: High

Description: An exported activity ('com.android.insecurebankv2.ChangePassword') does not require a permission.

File: AndroidManifest.xml

> Exported components without proper permission protection can be invoked by any other application, potentially leading to unauthorized access, data leakage, or denial of service. Apply appropriate 'android:permission' to restrict access.

### Type: Unprotected Exported Component

Severity: High

Description: An exported receiver ('com.android.insecurebankv2.MyBroadCastReceiver') does not require a permission.

File: AndroidManifest.xml

> Exported components without proper permission protection can be invoked by any other application, potentially leading to unauthorized access, data leakage, or denial of service. Apply appropriate 'android:permission' to restrict access.

### Type: Unprotected Exported Component

Severity: High

Description: An exported receiver ('com.google.android.gms.wallet.EnableWalletOptimizationReceiver') does not require a p

File: AndroidManifest.xml

> Exported components without proper permission protection can be invoked by any other application, potentially leading to unauthorized access, data leakage, or denial of service. Apply appropriate 'android:permission' to restrict access.

### Type: Unprotected Exported Component

Severity: High

Description: An exported provider ('com.android.insecurebankv2.TrackUserContentProvider') does not require a permission

File: AndroidManifest.xml

> Exported components without proper permission protection can be invoked by any other application, potentially leading to unauthorized access, data leakage, or denial of service. Apply appropriate 'android:permission' to restrict access.

### Type: Hardcoded Sensitive Information

Severity: High

Description: Potential hardcoded sensitive data found in source code.

File: /home/venom/android_analyzer_java/android-analyzer/sources/android/support/v7/internal/view/menu/MenuBuilder.jav

Found: 'KEY = "android:menu:actionviewstates"' in line 31. Avoid hardcoding sensitive values directly in code. Use Android Keystore, environment variables, or secure configuration files.

### Type: Hardcoded Sensitive Information

Severity: High

Description: Potential hardcoded sensitive data found in source code.

File: /home/venom/android_analyzer_java/android-analyzer/sources/android/support/v7/internal/view/menu/MenuBuilder.jav

Found: 'KEY = "android:menu:presenters"' in line 33. Avoid hardcoding sensitive values directly in code. Use Android Keystore, environment variables, or secure configuration files.

### Type: Hardcoded Sensitive Information

Severity: High

Description: Potential hardcoded sensitive data found in source code.

File: /home/venom/android_analyzer_java/android-analyzer/sources/android/support/v4/app/NotificationCompatJellybean.ja

Found: 'KEY = "android.support.groupKey"' in line 21. Avoid hardcoding sensitive values directly in code. Use Android Keystore, environment variables, or secure configuration files.

### Type: Hardcoded Sensitive Information

Severity: High

Description: Potential hardcoded sensitive data found in source code.

File: /home/venom/android_analyzer_java/android-analyzer/sources/android/support/v4/app/NotificationCompatJellybean.ja

Found: 'KEY = "android.support.sortKey"' in line 25. Avoid hardcoding sensitive values directly in code. Use Android Keystore, environment variables, or secure configuration files.

### Type: Hardcoded Sensitive Information

Severity: High

Description: Potential hardcoded sensitive data found in source code.

File: /home/venom/android_analyzer_java/android-analyzer/sources/android/support/v4/app/NotificationCompatExtras.java

Found: 'KEY = "android.support.groupKey"' in line 5. Avoid hardcoding sensitive values directly in code. Use Android Keystore, environment variables, or secure configuration files.

### Type: Hardcoded Sensitive Information

Severity: High

Description: Potential hardcoded sensitive data found in source code.

File: /home/venom/android_analyzer_java/android-analyzer/sources/android/support/v4/app/NotificationCompatExtras.java

Found: 'KEY = "android.support.sortKey"' in line 9. Avoid hardcoding sensitive values directly in code. Use Android Keystore, environment variables, or secure configuration files.

## Detected Vulnerabilities (continued):

### Type: Hardcoded Sensitive Information

Severity: High

Description: Potential hardcoded sensitive data found in source code.

File: /home/venom/android_analyzer_java/android-analyzer/sources/android/support/v4/app/RemoteInputCompatJellybean.

Found: 'KEY = "resultKey"' in line 15. Avoid hardcoding sensitive values directly in code. Use Android Keystore, environment variables, or secure configuration files.

### Type: Hardcoded Sensitive Information

Severity: High

Description: Potential hardcoded sensitive data found in source code.

File: /home/venom/android_analyzer_java/android-analyzer/sources/android/support/v4/view/accessibility/AccessibilityNode

Found: 'password: ").append(isPassword());' in line 1759. Avoid hardcoding sensitive values directly in code. Use Android Keystore, environment variables, or secure configuration files.

### Type: Hardcoded Sensitive Information

Severity: High

Description: Potential hardcoded sensitive data found in source code.

File: /home/venom/android_analyzer_java/android-analyzer/sources/com/google/android/gms/auth/api/credentials/Credentia

Found: 'KEY = "com.google.android.gms.credentials.Credential"' in line 14. Avoid hardcoding sensitive values directly in code. Use Android Keystore, environment variables, or secure configuration files.

### Type: Hardcoded Sensitive Information

Severity: High

Description: Potential hardcoded sensitive data found in source code.

File: /home/venom/android_analyzer_java/android-analyzer/sources/com/google/android/gms/auth/api/credentials/IdentityPr

Found: 'https://login.live.com' in line 11. Avoid hardcoding sensitive values directly in code. Use Android Keystore, environment variables, or secure configuration files.

### Type: Hardcoded Sensitive Information

Severity: High

Description: Potential hardcoded sensitive data found in source code.

File: /home/venom/android_analyzer_java/android-analyzer/sources/com/google/android/gms/auth/api/credentials/IdentityPr

Found: 'https://login.yahoo.com' in line 14. Avoid hardcoding sensitive values directly in code. Use Android Keystore, environment variables, or secure configuration files.