MOBSF

ANDROID STATIC ANALYSIS REPORT

PIVAA (1.0)

File Name:	pivaa.apk
Package Name:	com.htbridge.pivaa
Average CVSS Score:	6.4
App Security Score:	0/100 (CRITICAL RISK)
Scan Date:	Oct. 29, 2020, 4:51 p.m.

FILE INFORMATION

File Name: pivaa.apk
Size: 3.02MB
MD5: eaade08f941e47b08cfbce65c37895d6
SHA1: 2bc8ccf3185f5387097c29bfd79453bdb08b4457
SHA256: 57887e1d1e119939eec0e929801b049f8037cf90d2accab479a48f0d4dd2c19a

APP INFORMATION

App Name: PIVAA
Package Name: com.htbridge.pivaa
Main Activity: com.htbridge.pivaa.MainActivity
Target SDK: 26
Min SDK: 19
Max SDK:
Android Version Name: 1.0
Android Version Code: 1

APP COMPONENTS

Activities: 10
Services: 1
Receivers: 1
Providers: 1
Exported Activities: 0
Exported Services: 1
Exported Receivers: 1
Exported Providers: 1

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: CN=Android Debug, O=Android, C=US
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2017-11-21 14:47:12+00:00
Valid To: 2047-11-14 14:47:12+00:00
Issuer: CN=Android Debug, O=Android, C=US
Serial Number: 0x1
Hash Algorithm: sha1
md5: 0197d3002ac9ac35e4f3947e5e5f456a
sha1: 6747332aa82c3ec0e9b74d9cfbeaec56a094c563
sha256: 918b23e3bf7c966db1906bd25d0deaeb42ed8ef76ad609a79c90c7f59ac8dcfd
sha512:
e0930a700698ad149fd5dec650745cb0f7420f6e3c62bc62c134233b8f10caaa6368966e00617eb575e4fbdc5fbe60fe29f3fe40ca5e805412604b40e52c6c30

PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: 701570d3726da7399372db54956f75edadf0e193179f35e94cc80532e14dbc13

STATUS	DESCRIPTION
secure	Application is signed with a code signing certificate
warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android <7.0
bad	Application signed with a debug certificate. Production application must not be shipped with a debug certificate.
warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.READ_PROFILE	dangerous	read the user's personal profile data	Allows an application to read the user's personal profile data.
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.

android.permission.NFC	normal	control Near-Field Communication	Allows an application to communicate with Near-Field Communication (NFC) tags, cards and readers.
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.

APKID ANALYSIS

FILE	DETAILS
assets/com/htbridge/raw/ExternalCode.jar!classes.dex	FINDINGS: Compiler — DETAILS: dexlib 2.x
classes.dex	FINDINGS: Compiler — DETAILS: dx (possible dexmerge); FINDINGS: Manipulator Found — DETAILS: dexmerge

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Debug Enabled For App [android:debuggable=true]	high	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.
2	Application Data can be Backed up	medium	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging

	[android:allowBackup=true]		to copy application data off of the device.
3	Service (com.htbridge.pivaa.handlers.VulnerableService) is not Protected. [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Broadcast Receiver (com.htbridge.pivaa.handlers.VulnerableReceiver) is not Protected. [android:exported=true]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Content Provider (com.htbridge.pivaa.handlers.VulnerableContentProvider) is not Protected. [android:exported=true]	high	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CVSS V2: 7.5 None (high) CWE: CWE-532 Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/htbridge/pivaa/handlers/VulnerableContentProvider.java com/htbridge/pivaa/handlers/Authentication.java com/htbridge/pivaa/LoadCodeActivity.java com/htbridge/pivaa/MainActivity.java com/htbridge/pivaa/AboutActivity.java com/htbridge/pivaa/handlers/database/DatabaseAdapter.java com/htbridge/pivaa/handlers/Encryption.java com/htbridge/pivaa/DatabaseActivity.java com/htbridge/pivaa/ContentProviderActivity.java com/htbridge/pivaa/handlers/VulnerableService.java com/htbridge/pivaa/handlers/database/DatabaseHelper.java com/htbridge/pivaa/handlers/VulnerableReceiver.java com/htbridge/pivaa/handlers/ObjectSerialization.java com/htbridge/pivaa/EncryptionActivity.java com/htbridge/pivaa/handlers/LoadCode.java com/htbridge/pivaa/WebviewActivity.java com/htbridge/pivaa/handlers/about/AboutAdapter.java

2	App can read/write to External Storage. Any App can read data written to External Storage.	high	CVSS V2: 5.5 None (medium) CWE: CWE-276 Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/htbridge/pivaa/handlers/Authentication.java com/htbridge/pivaa/handlers/VulnerableService.java
3	App creates temp file. Sensitive information should never be written into a temp file.	high	CVSS V2: 5.5 None (medium) CWE: CWE-276 Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/htbridge/pivaa/handlers/Authentication.java
4	The file is World Writable. Any App can write to the file	high	CVSS V2: 6 None (medium) CWE: CWE-276 Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/htbridge/pivaa/handlers/Authentication.java
5	Files may contain hardcoded sensitive informations like usernames, passwords, keys etc.	high	CVSS V2: 7.4 None (high) CWE: CWE-312 Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/htbridge/pivaa/handlers/Authentication.java com/htbridge/pivaa/Configuration.java
6	This App uses an SSL Pinning Library (org.thoughtcrime.ssl.pinning) to prevent MITM attacks in secure communication channel.	secure	CVSS V2: 0 None (info) OWASP MASVS: MSTG-NETWORK-4	com/htbridge/pivaa/handlers/API.java
7	The App uses an insecure Random Number Generator.	high	CVSS V2: 7.5 None (high) CWE: CWE-330 Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/htbridge/pivaa/handlers/Encryption.java
8	The App uses ECB mode in Cryptographic encryption algorithm. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.	high	CVSS V2: 5.9 None (medium) CWE: CWE-327 Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	com/htbridge/pivaa/handlers/Encryption.java
9	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	high	CVSS V2: 5.9 None (medium) CWE: CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/htbridge/pivaa/handlers/database/DatabaseHelper.java

NIAP ANALYSIS

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application invoke platform-provided DRBG functionality for its cryptographic operations.

2	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
3	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['camera', 'location', 'microphone', 'NFC', 'network connectivity'].
4	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to ['address book'].
5	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
6	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application implement functionality to encrypt sensitive data in non-volatile memory.
7	FMT_MEC_EXT.1.1	Security Functional Requirements	Supported Configuration Mechanism	The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.
8	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.
9	FCS_RBG_EXT.2.1,FCS_RBG_EXT.2.2	Selection-Based Security Functional Requirements	Random Bit Generation from Application	The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using Hash_DRBG. The deterministic RBG is seeded by an entropy source that accumulates entropy from a platform-based DRBG and a software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.
10	FCS_CKM_EXT.1.1	Selection-Based Security Functional Requirements	Cryptographic Key Generation Services	The application generate no asymmetric cryptographic keys.
11	FCS_COP.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Operation - Encryption/Decryption	The application perform encryption/decryption not in accordance with FCS_COP.1.1(1), AES-ECB mode is being used.
12	FCS_TLSC_EXT.1.2	Selection-Based Security Functional Requirements	TLS Client Protocol	The application verify that the presented identifier matches the reference identifier according to RFC 6125.
13	FCS_HTTPS_EXT.1.1	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement the HTTPS protocol that complies with RFC 2818.
14	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.

15	FCS_HTTPS_EXT.1.3	Selection-Based Security Functional Requirements	HTTPS Protocol	The application notify the user and not establish the connection or request application authorization to establish the connection if the peer certificate is deemed invalid.
16	FIA_X509_EXT.1.1	Selection-Based Security Functional Requirements	X.509 Certificate Validation	The application invoked platform-provided functionality to validate certificates in accordance with the following rules: ['The certificate path must terminate with a trusted CA certificate'].
17	FIA_X509_EXT.2.1	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS , TLS.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
xss.rocks	good	**IP:** 172.67.194.87 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.7757 **Longitude:** -122.395203 **View:** Google Map
www.htbridge.com	good	**IP:** 192.175.111.230 **Country:** Canada **Region:** Quebec **City:** Montreal **Latitude:** 45.508839 **Longitude:** -73.587807 **View:** Google Map
google.com	good	**IP:** 172.217.172.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

URLS

URL	FILE
http://google.com javascript:alert('Hello	com/htbridge/pivaa/WebviewActivity.java
https://www.htbridge.com/ssl/api/v1/load_all/1510314123771.html?_=1510314123152 https://www.htbridge.com/ssl/	

file:///etc/hosts https://xss.rocks/scriptlet.html	com/htbridge/pivaa/Configuration.java

App Security Score Calculation

Every app is given an ideal score of 100 to begin with.
For every findings with severity high we reduce 15 from the score.
For every findings with severity warning we reduce 10 from the score.
For every findings with severity good we add 5 to the score.
If the calculated score is greater than 100, then the app security score is considered as 100.
And if the calculated score is less than 0, then the app security score is considered as 10.

Risk Calculation

APP SECURITY SCORE	RISK
0 - 15	CRITICAL
16 - 40	HIGH
41 - 70	MEDIUM
71 - 100	LOW

Report Generated by - MobSF v3.1.7 Beta

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.