

# App Defense Alliance Mobile Application Profile Assessment

SHEIN-Shopping Online

09/02/2025 - Product Version - 12.9.5

SCOPE VERIFIED:

SHEIN-Shopping Online

DATE OF COMPLETION

September 2, 2025



SHEIN-Shopping Online



<b>Test Results</b>	All the requirements were met.	<b>Pass</b>
---------------------	--------------------------------	-------------

<b>PACKAGE NAME</b>	com.zzkko
<b>TITLE</b>	SHEIN-Shopping Online
<b>DEVELOPER</b>	Roadget Business PTE. LTD.
<b>SHA-256 HASH</b>	cd0f5b969daad514a5b2389bbb1a490f75f1024a9bda539310a064276145bbac
<b>SIZE</b>	85.86MB
<b>VERSION CODE</b>	2159
<b>VERSION NAME</b>	12.9.5
<b>DEVICE</b>	Google Pixel 7
<b>API LEVEL</b>	35
<b>ASSURANCE LEVEL</b>	AL2 - Lab Assessment
<b>SPECIFICATION VERSION</b>	Version 1.0

### Test Background

The Open Web Application Security Project (OWASP) has been around for over 20 years and has helped provide a much more secure experience for both web and mobile users. More recently, it published the Mobile Application Security Verification Standard (MASVS), which aims to define a common standard for secure mobile applications. With the App Defense Alliance, Google has brought together application developers and independent security labs in an effort to improve the security of mobile application security and highlight those apps that meet the standard. The security labs verify the applications against specific MASVS requirements and work with developers to address any issues.

OWASP also publishes the Mobile Security Testing Guide (MSTG), which details how the application should be tested, and provides information to developers on how to write more secure applications. The following section it taken directly from the MSTG to highlight current security best practices, as well as link to additional resources for application developers.

The scope of this work was limited to the specific requirements of the Application Defense Alliance described below and should not be read as a holistic security evaluation or comprehensive penetration test.



## Passed Requirements

CATEGORY	STATUS
<b>Storage</b>	
The application securely stores sensitive data in external storage	Pass
The application prevents leakage of sensitive data	Pass
<b>Crypto</b>	
The application employs current strong cryptography and uses it according to industry best practices	Pass
The application performs key management according to industry best practices	Pass
<b>Auth</b>	
The application uses secure authentication and authorization protocols and follows the relevant best practices	Pass
<b>Network</b>	
The application secures all network traffic according to the current best practices	Pass
<b>Platform</b>	
The application uses IPC mechanisms securely	Pass
The application uses WebViews securely	Pass
The application uses the user interface securely	Pass



---

### Code

---

The application requires an up-to-date platform version

Pass

---

The application only uses software components without known vulnerabilities

Pass

---

The application validates and sanitizes all untrusted inputs

Pass

### Resilience

---

The application implements anti-tampering mechanisms

Pass

---

The application implements anti-static analysis mechanisms

Pass

---

The application implements anti-dynamic analysis mechanisms

Pass

### Privacy

---

The application minimizes access to sensitive data and resources

Pass

---

The application is transparent about data collection and usage

Pass

---

The application offers user control over their data

Pass

---