

Please support the OWASP mission to improve software security through open source initiatives and community education. [Donate Now!](#)

[Store](#)[PROJECTS](#) [CHAPTERS](#)[Donate](#)[ABOUT](#) [Q](#)[Store](#)[Join](#)[Donate](#)[Join](#)[Watch](#)

44

[Star](#)

108

OWASP Mobile Top 10

[Main](#)[Acknowledgements](#)

Mobile Top 10 2024: Final Release Updates

The new Mobile Top 10 list for 2024 is out now. We would love to see you participate and contribute to the research we are doing.

[Join the SLACK Channel](#)

If you face any issues joining us on Slack, please feel free to reach out to Project Leads.

Let's get started!

Join us on the Slack channel for contributions!!

More updates to follow soon...

Below is the OWASP Mobile Top-10 2024 Release

The OWASP® Foundation works to improve the security of software through its community-led open source software projects, hundreds of chapters worldwide, tens of thousands of members, and by hosting local and global conferences.

Other OWASP Mobile Projects

[OWASP Mobile Security Testing Guide](#)

Code Repository

[Github Repository](#)

Leaders

[Milan Singh Thakur](#)
[Alaeddine MESBAHI](#)
[Kunwar Atul](#)

Top 10 Mobile Risks - Final release 2024



- **M1: Improper Credential Usage**
- **M2: Inadequate Supply Chain Security**
- **M3: Insecure Authentication/Authorization**
- **M4: Insufficient Input/Output Validation**
- **M5: Insecure Communication**
- **M6: Inadequate Privacy Controls**
- **M7: Insufficient Binary Protections**
- **M8: Security Misconfiguration**
- **M9: Insecure Data Storage**
- **M10: Insufficient Cryptography**

Comparison between 2016 and 2024

Comparison Between 2016-2024		
OWASP-2016	OWASP-2024-Release	Comparison Between 2016-2024
M1: Improper Platform Usage	M1: Improper Credential Usage	New
M2: Insecure Data Storage	M2: Inadequate Supply Chain Security	New
M3: Insecure Communication	M3: Insecure Authentication / Authorization	Merged M4&M6 to M3
M4: Insecure Authentication	M4: Insufficient Input/Output Validation	New
M5: Insufficient Cryptography	M5: Insecure Communication	Moved from M3 to M5
M6: Insecure Authorization	M6: Inadequate Privacy Controls	New
M7: Client Code Quality	M7: Insufficient Binary Protections	Merged M8&M9 to M7
M8: Code Tampering	M8: Security Misconfiguration	Rewording [M10]
M9: Reverse Engineering	M9: Insecure Data Storage	Moved from M2 to M9
M10: Extraneous Functionality	M10: Insufficient Cryptography	Moved from M5 to M10

Vulnerabilities that didn't make the place on the initial release list, but

Mohamed Benchikh

Top Contributors

Mohammed Junaid Tariq
Steffen Lortz

Upcoming OWASP Global Events

OWASP Global AppSec
EU 2026 - Vienna, Austria

- June 22-26, 2026

OWASP Global AppSec
USA 2026 - San Francisco, CA

- November 2-6, 2026

OWASP Global AppSec
EU 2027 - Vienna, Austria

- June 21-25, 2027

OWASP Global AppSec
USA 2027 - Atlanta, GA

- September 20-24, 2027

OWASP Global AppSec
EU 2028 - Vienna, Austria

- June 19-23, 2028

in the future, we may consider them.

- Data Leakage
- Hardcoded Secrets
- Insecure Access Control
- Path Overwrite and Path Traversal
- Unprotected Endpoints (Deeplink, Activity, Service ...)
- Unsafe Sharing

Top 10 Mobile Risks - Final List 2016

- [M1: Improper Platform Usage](#)
- [M2: Insecure Data Storage](#)
- [M3: Insecure Communication](#)
- [M4: Insecure Authentication](#)
- [M5: Insufficient Cryptography](#)
- [M6: Insecure Authorization](#)
- [M7: Client Code Quality](#)
- [M8: Code Tampering](#)
- [M9: Reverse Engineering](#)
- [M10: Extraneous Functionality](#)

Top 10 Mobile Risks - Final List 2014

- [M1: Weak Server Side Controls](#)
- [M2: Insecure Data Storage](#)
- [M3: Insufficient Transport Layer Protection](#)
- [M4: Unintended Data Leakage](#)
- [M5: Poor Authorization and Authentication](#)
- [M6: Broken Cryptography](#)

- [M7: Client Side Injection](#)
- [M8: Security Decisions Via Untrusted Inputs](#)
- [M9: Improper Session Handling](#)
- [M10: Lack of Binary Protections](#)

 [Edit on GitHub](#)

Spotlight: SQ1 Security Infotech, Inc.



SQ1, formerly SecureOne, is a global cybersecurity leader offering end-to-end cybersecurity and compliance solution. Our AI-powered security platforms are designed to protect endpoints & cloud assets from advanced cyber-attacks and threats, including APTs, malware, and ransomware. SQ1 offers a comprehensive range of managed cybersecurity services that identify & assess, protect and prevent, detect, analyse & respond to cyber threats and risks. SQ1 has been a trusted security partner for several thousands of businesses globally of various sizes across verticals from Healthcare, Pharma, Financial Services, Govt, Manufacturing, Technology, Oil and Energy.

Corporate Supporters



[Become a corporate supporter](#)

[HOME](#) [PROJECTS](#) [CHAPTERS](#) [EVENTS](#) [ABOUT](#)



[PRIVACY](#) [SITEMAP](#) [CONTACT](#)

OWASP, the OWASP logo, and Global AppSec are registered trademarks and AppSec Days, AppSec California, AppSec Cali, SnowFROC, OWASP Boston Application Security Conference, and LASCON are trademarks of the OWASP Foundation, Inc. Unless otherwise specified, all content on the site is Creative Commons Attribution-ShareAlike v4.0 and provided without warranty of service or accuracy. For more information, please refer to our [General Disclaimer](#). OWASP does not endorse or recommend commercial products or services, allowing our community to remain vendor neutral with the collective wisdom of the best minds in software security worldwide. Copyright 2025, OWASP Foundation, Inc.