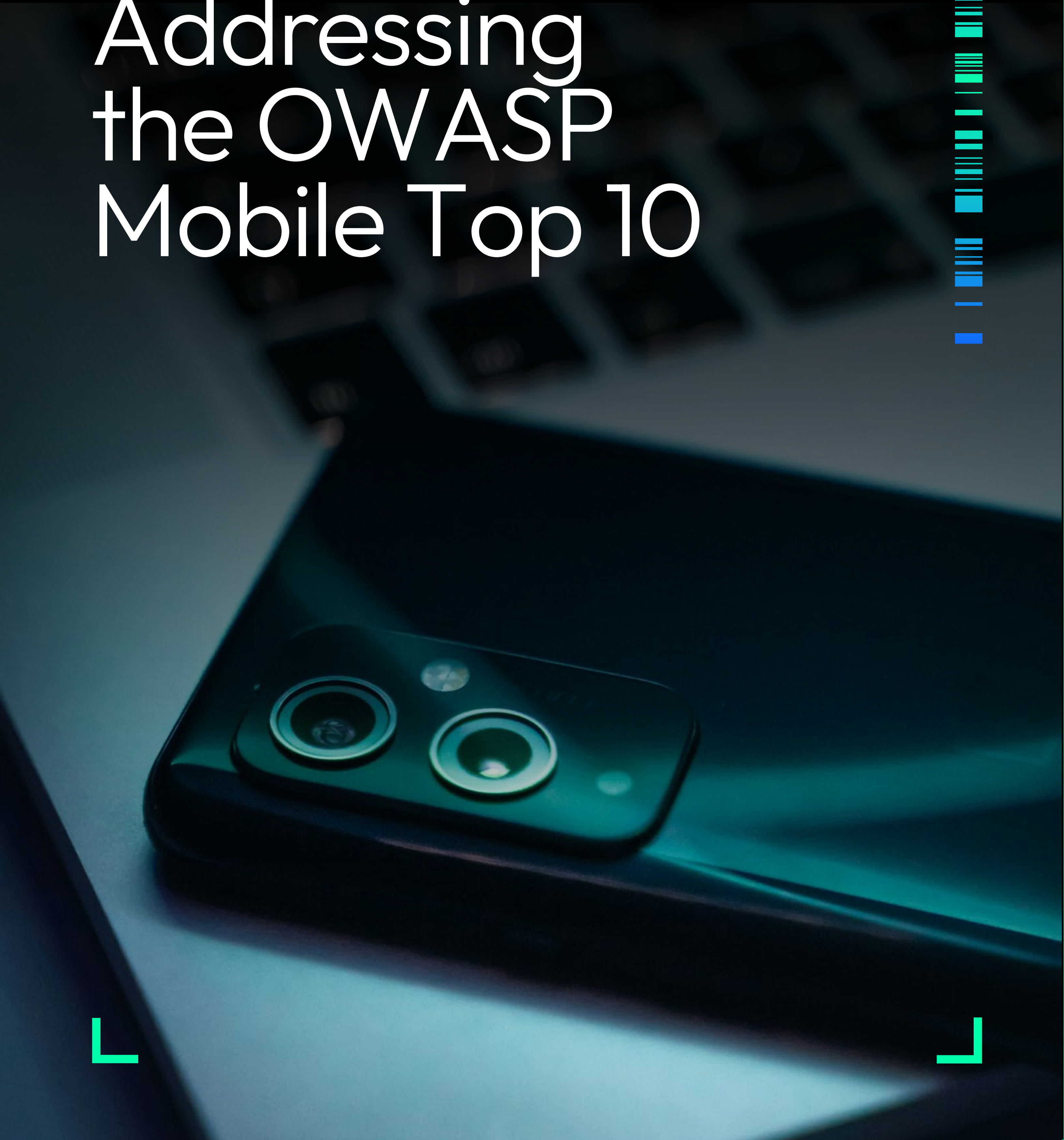
Quokka

GUIDE

Addressing the OWASP Mobile Top 10



Addressing the OWASP Mobile Top 10

Today, there are a range of risks that expose mobile applications—and the personal and corporate data these apps access. As mobile apps become more sophisticated, the avenues for cyberattacks increases.

How do you identify the most critical risks and take steps to address them?

As a security or application development leader, it's critical to have a clear understanding of what you're trying to defend against. That's why the OWASP Mobile Top 10 is an essential AppSec resource. First released in 2014 and then updated in 2016 and 2024, The OWASP Mobile Top 10 offers a detailed look at the top ten most critical vulnerabilities that mobile apps are exposed to and it details security best practices that can be employed to address these threats.

How Quokka Q-mast Helps You Address OWASP Mobile Top 10 Threats

As mobile devices continue to become increasingly integral in our professional lives, the demand for a privacy-first mobile security approach keeps getting more urgent. With its innovative Q-mast (Mobile Application Security Testing) solution, Quokka is uniquely equipped to help secure coding.

Q-mast delivers defense-grade mobile app security testing, leveraging extensive threat research for unparalleled insights and preemptive capabilities. In the following, we examine how Q-mast can help you address each of the OWASP Mobile Top 10 requirements.

How Q-mast Addresses OWASP Mobile Top 10 Risks

THE STANDARD, WHY IT MATTERS

HOW QUOKKA CAN HELP

M1: Improper Credential Usage

When credentials are exposed to improper usage, it can lead to unauthorized access and data breaches. Using publicly available or custom-built tools, threat actors can wage automated attacks to find and collect vulnerable credentials. Hardcoded, improperly validated, or insecurely stored credentials can all be vulnerable, enabling attackers to gain unauthorized access to sensitive assets and potentially access functionality of the mobile device.

Q-mast discovers potential credential risks. The solution can simulate attack scenarios to identify weaknesses in credential management and suggest enhancements to strengthen security. For example, the solution can identify credentials that are stored in clear text within an application or hard-coded credentials that are typically remnants of testing by developers. With these capabilities, the solution can help ensure mobile security is not compromised by credential exploitation.

M2: Inadequate Supply Chain Security

The use of third-party libraries and components can offer invaluable assistance in streamlining mobile application development. However, without proper security checks, the use of these third-party components can introduce critical vulnerabilities. Of the top 10 mobile risks, this is rated the most difficult to detect.

Q-mast solution employs a comprehensive process to vet all mobile app components, including third-party libraries and code.

Q-mast offers a mix of static, dynamic, behavioral, and interactive testing. The solution can conduct a broad and in-depth range of tests covering every stage of the software development lifecycle (SDLC), from design to deployment.

M3: Insecure Authentication/Authorization

Authentication and authorization represent the gatekeepers of mobile app security. When weaknesses exist in these mechanisms, sensitive data can ultimately be exposed.

Once vulnerabilities are identified, attackers can bypass authentication and gain direct access to backend systems. In addition, they can log into an app as a legitimate user, bypass the authentication control, and gain access to a vulnerable endpoint.

Q-mast features advanced testing protocols that rigorously assess authentication and authorization mechanisms. It detects if there are any dynamically-loaded libraries, class loaders, or code that can introduce vulnerable or malicious code into the app if the app does not verify the security and integrity of the third-party library/class loader/code.

Checking for trusted environments helps ensure that authentication routes cannot be bypassed. Proper platform keychain usage, encryption, and credential usage, which Q-mast checks, are also related to this risk. Through these protocols, you can spot potential vulnerabilities and strengthen your mobile app cybersecurity foundation.

M4: Insufficient Input/Output Validation

To establish effective mobile app security, it is vital to validate and sanitize data from external sources, including user inputs and network data. Failing to employ these mechanisms can introduce exposure to serious security threats, including SQL injection, command injection, and cross-scripting attacks.

Input/output validation is critical to securing an app from injection attacks. With Q-mast, you can detect potential code weakness for proactive remediation to ensure that the data entering and exiting the app does not become a vector for security breaches.

M5: Insecure Communication

Today's mobile apps typically share data with multiple remote servers. When these communications aren't secure, transmissions can be vulnerable to eavesdropping and interception.

When data is transmitted over unencrypted channels or encrypted via weak algorithms, it may be exposed to a number of threats. Q-mast evaluates encryption and data transmission protocols to ensure sensitive information is safeguarded against eavesdropping, man-in-the-middle attacks, or interception.

M6: Inadequate Privacy Controls

Failing to implement strong privacy protections around personally identifiable information (PII) can lead to a range of potential issues. When a users' private data is exposed, they can be susceptible to identity theft, financial fraud, and many other dangers. Privacy breaches can also present a significant risk to businesses, leaving them exposed to fines, lawsuits, and reputational damage.

Privacy is a driving force of Q-mast. With the solution, you can ensure mobile apps secure private data and adhere to privacy regulations. With the solution's static and dynamic testing, you can thoroughly test how mobile apps access or store sensitive PII and identify any potential privacy and security issues.

For example, Q-mast ensures that data is not being written to a log or debug file and Q-mast detects risky nations where the app is communicating that could cause PII to be exfiltrated.

M7: Insufficient Binary Protections

App binaries can contain a range of sensitive assets, including API keys, cryptographic assets, and critical business logic. App binaries are susceptible to reverse engineering and code tampering. For example, if attackers can gain access to binaries, they can manipulate the code to include malware and even repackage the code and distribute it via app stores.

Q-mast analyzes the compiled app binary, including all embedded third-party libraries. This ensures comprehensive coverage of the entire code base. Additionally, Q-mast detects whether additional binary protections, such as RASP, have been implemented.

M8: Security Misconfiguration

Today's mobile apps can be exposed through a broad range of misconfigurations. When security settings, permissions, or controls aren't optimally configured, apps can be vulnerable to a significant number of threats.

Q-mast identifies misconfigurations, enabling developers to rectify them before they can be exploited. The solution can identify weak default settings, unprotected storage of sensitive elements, poor access controls, and more. Q-mast offers granular scanning and identifies misconfigurations in both iOS and Android environments. The solution can be integrated with CI/CD pipelines, helping teams detect and remediate misconfigurations early in the software development lifecycle.

In fact, in an academic paper Quokka researchers found that 33% of apps on Google Play contain manifest configurations.

M9: Insecure Data Storage

Mobile devices and apps now store a range of sensitive assets—assets that may be targeted by cyber criminals, nation-states, malicious insiders, data brokers, and other nefarious actors. At any given time, weak encryption, exposed credentials, and more can leave these sensitive repositories exposed.

With Q-mast, you can ensure mobile apps consistently employ robust safeguards around data storage. Q-mast can identify a wide range of storage vulnerabilities, including weak or missing encryption, credentials stored in clear text, and more.

M10: Insufficient Cryptography

In many ways, encryption represents the last, most vital line of defense for sensitive assets. While encryption can offer essential safeguards, weak or improperly configured implementations can be vulnerable to cryptographic, brute-force, or side-channel attacks. Through these approaches, adversaries can decrypt, access, and manipulate sensitive assets.

Q-mast evaluates cryptographic implementations to ensure they provide robust protections. The solution can help you preserve the integrity and confidentiality of sensitive data, both at rest and in transit.

Through its advanced capabilities, the solution can spot weaknesses in encryption algorithms, key management, or implementation. For example, the solution can identify if an app does not use secure key or random number generation or if data at rest encryption is not used.

Key Takeaways

The OWASP Mobile Top 10 outlines the most significant security risks for mobile apps and it provides best practices for addressing these threats. This resource serves as a critical guide for developers and security experts, offering key insights for where to focus security initiatives and investments.

Quokka's Q-mast solution is engineered to tackle these OWASP standards directly. It employs automated testing to detect and address security, privacy, and compliance vulnerabilities. Q-mast's comprehensive testing protocols simulate attack scenarios, scrutinize third-party components, and evaluate encryption and data handling practices, ensuring mobile apps conform to high security, privacy, and compliance benchmarks.

In addition to covering the OWASP Mobile Top 10, Q-mast enhances mobile app security with compatibility, performance, and compliance testing. These tests ensure apps function flawlessly across various devices and systems, maintain performance under different conditions, and meet standards like OWASP, NIAP, and GDPR.

Find out more

To learn more about how Q-mast enables organizations to meet the OWASP Mobile Top 10 standard, contact us for a demo.

Quokka

About Quokka

Quokka protects mobile apps and devices used by millions globally. Formerly known as Kryptowire, the company was founded in 2011 with grants from DARPA and NIST, making Quokka the first and now longest-standing mobile app security solution for the US Federal Government. In over a decade since, defense-grade technology has enabled organizations from all sectors to deliver secure mobile apps to their customers and employees, while respecting privacy. With investment from USVP and Crosslink Capital, Quokka is bringing trusted mobile privacy and security to millions more.

www.quokka.io

Quokka