SAPPHIRE™

Application Security Service Definition

Classification: Public

Contents

Proprietary Notice

Overview

Application security is the process of developing, adding, and testing security features within applications to prevent security vulnerabilities against threats such as unauthorised access and modification. We embed ourselves into your secure software development lifecycle and support your development teams with web, mobile and API assessments.

Services features:

- Component based testing and black box-based testing
- Testing based on a release candidate or interim test phase
- Iterative risk-based assessments aligned with change and release cycles
- Annual full system testing of the application layer
- Anonymous and authenticated application testing
- Application hosting and infrastructure testing
- Web, API and mobile OWASP based testing
- Identify API endpoint URL security vulnerabilities
- iOS (IPA) and android (APK) testing of prototype/live apps
- Artificial Intelligence (AI) and Large Language Model (LLM) testing

Service benefits:

- Testing based on a release candidate or interim test phase.
- Iterative 'time-box' testing aligned with change and release cycle.
- Annual full system testing of the application layer.
- Anonymous and authenticated based application testing.
- Application hosting and infrastructure testing.
- Web, API and mobile OWASP based testing.
- Identify API endpoint URL security vulnerabilities.

Functional and Non-Functional Detail

Organisations today face the challenge of securing complex and diverse environments encompassing mobile workers, cloud infrastructures, networks, applications, devices and back-end systems. Only by achieving full visibility can you gain a true understanding of how effective your IT security programme is and where the real risks lie. Without this, it is challenging to adequately plan on how best to protect against the threats to your business.

To stay on top of impending attacks, it is crucial that businesses are aware of the vulnerabilities within their environment so that they can mitigate the risk and should a breach occur, they have

the tools and resources to respond and remediate quickly. Once the vulnerability has been rectified it is essential to carry out the necessary analysis and assess the impact on your business.

To be effective when identifying and remediating found vulnerabilities, Sapphire recommends that you implement a testing programme that embeds with your development lifecycle which is in line with the risk appetite of your business and incorporates your testing, risk management and threat analysis regime.

The strength and effectiveness of our testing services lie with the expert conducting the engagement and the quality of the report generated as a result. We pride ourselves on the high quality of our reports which provide a thorough vulnerability analysis, detailed evidence of the associated risks and remediation advice. In addition to this, our consultants are on-hand throughout to offer their expertise, helping you to secure your infrastructure and re-testing if and when required.

As security becomes more important and part of the everyday business function, our G-Cloud customers need more data assurance services to safeguard their applications, business and their client base.

Web Application Testing

As organisations conduct more business online and deliver services for convenience these systems are actively targeted by threat actors for exploitation. Sapphire will assess these systems, advise on the security configuration and vulnerabilities within a selected website application.

Typically, in two stages, the assessment will be completed initially with no authentication to the portal or application and then with a valid user account for testing privilege escalation vulnerabilities and assess any weaknesses with the authentication and authorisation mechanisms. Sapphire follow the OWASP 2025 guidelines and testing will focus on the top 10 application threats, namely:

- A1:2025 - Broken Access Control
- A2:2025 - Security Misconfiguration
- A3:2025 - Software Supply Chain Failures
- A4:2025 - Cryptographic Failures
- A5:2025 - Injection
- A6:2025 - Insecure Design
- A7:2025 - Authentication Failures
- A8:2025 - Software or Data Integrity Failures
- A9:2025 - Security Logging and Alerting Failures
- A10:2025 - Mishandling of Exceptional Conditions

Using the guide, we will check all website functionality, authentication and validation.

Sapphire will typically conduct a web application assessment of the system based on two user roles (basic level and admin level).

As part of our structured report, Sapphire will respond to your key security questions, namely:

- Are the web applications suitably protected from unauthenticated users gaining access to user or admin data services?
- Are the web applications suitably protected from malicious authenticated users?
- Are the correct user management practices in place to prevent horizontal and vertical privilege escalation to obtain personal details?
- Is there correct segregation between standard user and admin accounts?

During testing, it may be possible for Sapphire to see Personally Identifiable Information (PII) in the G-Cloud customer application. It is not our intention to do anything with this data. We will acknowledge it by describing the data in general by our methods of discovery and then anonymise it within our test report. At this stage the data will then be deleted. However, for the short term that Sapphire is holding the data, we do become a processor.

Mobile Application Testing

Similarly to the web application assessment, Sapphire will test the mobile based systems, advise on the security configuration and vulnerabilities within the iOS and Android mobile application. Sapphire follow the OWASP 2025 guidelines and testing will focus on the top 10 mobile application threats, namely:

- M1:2025 - Improper credential usage
- M2:2025 - Inadequate Supply Chain Security
- M3:2025 - Insecure Authentication/Authorization
- M4:2025 - Insufficient Input/Output Validation
- M5:2025 - Insecure Communication
- M6:2025 - Lack of Privacy Controls
- M7:2025 - Insufficient Binary Protections
- M8:2025 - Security Misconfiguration
- M9:2025 - Insecure Data Storage
- M10:2025 - Insufficient Cryptography

Sapphire can test a prototype of the application or live apps that can be downloaded from the relevant stores. Typically, the test will focus on the users' data entered on the mobile app, the user

experience and check if the data is securely stored on the iOS and Android for a time limited purpose. Testing can also include versions that are pushed to a device via an MDM solution.

The application behaviour will be different for iOS and Android so we will test both independently. For mobile testing, the use of emulator/simulator builds does not reflect a normal user environment due to this we would prefer G-Cloud customer can provide test provide a device builds for each version.

API Endpoint Testing

As part of the portals, Sapphire can test API endpoints that are integrated into the web application functionality or individual API services. Sapphire follow the OWASP 2025 top 10 for API security vulnerabilities, and the methodologies used to mitigate them, including:

- A01:2025 – Broken Access Control
- A02:2025 – Security Misconfiguration
- A03:2025 – Software Supply Chain Failures
- A04:2025 – Cryptographic Failures
- A05:2025 – Injection Attack
- A06:2025 – Insecure Design Flaws
- A07:2025 – Authentication Failures
- A08:2025 – Software or Data Integrity Failures
- A09:2025 – Logging and Alerting Failures
- A10:2025 – Mishandling of Exceptional Conditions

Sapphire will require a list of the API endpoint URLs from our G-Cloud customer, along with the methods (POST, GET, PUSH etc). Preferably we will require a set of Postman files or access to your Swagger document which will save testing time having to capture and document API calls from the front-end application. We also need to know how they authenticate. For example, if the application relies on Auth0 as their identity provider, we will check the instance has been implemented incorrectly and confirm that a logged-out user's authentication token cannot be reused where the log out action has not been communicated back to the API/back end to invalidate it.

Sapphire's Certifications and Associations