Penetration Testing
Service Definition Document

Service overview

AppCheck NG is a leading cloud based web application penetration scanning system.

Isotoma will configure and operate the service on your behalf, using our expertise in web application testing and delivery to ensure the scanner is correctly configured and that reports are relevant and useful.

Isotoma can provide expert help you manage your ongoing vulnerability detection and management process, to ensure you scan the right environments, with the right configuration at the appropriate frequency

Integrated with your development processes this can provide a high degree of confidence that you are compliant with best practice in managing your application security.

Service definition

AppCheck NG

Intelligent discovery

Accurate and efficient component discovery (crawling) is commonly cited as one of the key challenges when performing an automated web application assessment.

Many existing web application scanners rely on parsing web pages in order to discover application components (e.g. links and forms). This approach is no longer effective when testing modern web 2.0 based applications. Components generated at runtime using JavaScript, Flash or Silverlight components will remain invisible to traditional discovery techniques.

The AppCheck NG scanning engine employs two integrated crawling technologies to overcome this challenge. Our HTTP/HTML based crawler is used to discover components quickly and to identify hidden components through forced browsing. A second integrated crawling engine then executes web pages in the same way a normal browser would. Any embedded scripts or components are then able to run as intended whilst allowing full visibility to the discovery engine. If a modern web browser such as Google Chrome can access the application, AppCheck NG can crawl it.

- AppCheck NG uses multiple crawling technologies to accurately identify application components even in JavaScript and Flash rich applications.
- Hooks within our customised browser engine allow the interception and analysis of Ajax calls whilst maintaining accurate client side state.

Sophisticated Assessment Techniques

AppCheck NG has been designed from the ground up to offer the most sophisticated scanning engine available. By working closely with some of the UK's leading penetration testers, each scanning module has been designed to maximise detection accuracy whilst minimising false positives.

- Thorough assessment of all known web application vulnerability classes such as those defined within the OWASP top ten.
- Advanced detection of DOM based Cross Site Scripting (XSS) vulnerabilities through JavaScript taint analysis.
- Decompilation and static analysis of Adobe Flash files.
- HTML5 postMessage analysis.
- Confirmation of discovered flaws through safe vulnerability exploitation.

Advanced, platform agnostic fuzzing technology

The AppCheck NG scanner incorporates dynamic fuzzing technology whereby arbitrary protocol structures treated blindly by other scanners as opaque single inputs are broken down accurately into their true and deeper attack surface.

For example, cookie values often encode multiple sub parameters using bespoke serialisation encodings (e.g. "the_cookie=1234|65[a=b;c=[1,2,3]]"), and so vulnerable server-side code paths are frequently missed using traditional fuzzing technology.

Eliminate False Positives through Vulnerability Exploitation

A false positive is where a vulnerability scanner indicates there is a vulnerability when in fact there isn't one. Sorting through scanner results to determine which reported issues are real and which are false positive is a time consuming process.

To eliminate false positives, and to provide proof of concept evidence, the AppCheck NG scanner employs safe custom exploit techniques to actively confirm discovered vulnerabilities.

Intelligent Authentication

Complex authentication schemes are supported when AppCheck NG is supplied with the minimal information, such as a username and password pair. Optionally, a login URL may be provided to direct the scanner where to use the credentials and for scenarios such as single sign-on.

The scanner may easily be adapted to support bespoke authentication schemes that require non-standard credentials or processes.

Hosting Environment

AppCheck NG can provide comprehensive vulnerability assessment and analysis against remote hosts to determine if a misconfiguration exists that could allow an attack to get behind the application and into sensitive data.

Reporting

Reports are securely delivered in PDF format, or for the license purchase model you can have complete access to the scanning portal, with real-time visibility of scanning progress and identified vulnerabilities.

Configuration and setup

Assessment of your application to ensure the scanner can access all areas of your application - even those behind a password or deep in a set of forms

Remediation

Vulnerability tracker and progress

Manage and easily track discovered vulnerabilities and your organisations remediation progress through the vulnerability tracker and analysis tool.

Integration with Jira

Identified vulnerabilities can be automatically added to your development teams Jira boards to aid tracking and remediation.

Consultancy and advice

We can provide expert advice to help you with prioritisation, reporting, process management and technical advice on best practice and approaches. We can also provide access to Appcheck NG's team of penetration testing experts who can provide in-depth technical advice on impact and remediation of specific flaws.

Regular automated scanning

Automatically rescan your application regularly to ensure it remains secure. Many customers opt to rescan their applications monthly, or even more frequently, to ensure they are compliant with security requirements.

Completely integrated with the vulnerability tracking and remediation process this can provide clear reassurance for your stakeholders that web vulnerabilities are completely under control.

Developer integration

We can work with your development team to integrate vulnerability scanning into your existing Continuous Integration process, using tools you have already selected such as Jenkins, Travis or CircleCI.

When added to unit testing and integration testing, vulnerability testing can ensure your new features are secure before they are deployed. Existing CI tools will ensure a release is not marked as green before all scans pass with a defined level of success.