AppCheck

ACCURACY IS EVERYTHING

E: info@appcheck-ng.com
W: www.appcheck-ng.com
T: 0113 887 8380

Automate the discovery of security flaws within your network perimeter quicker, easier, and more accurately with the AppCheck scanning tool

AppCheck is a best-in-class Web Application and Infrastructure vulnerability scanner.

Designed and developed by experienced penetration testers, it provides the capability to carry out regular scans to identify vulnerabilities which, if left unchecked, could quickly become a significant business risk.

Deployed as a single SaaS scanning system or as part of a distributed scanning network, AppCheck offers unparalleled detection rates, accuracy and scalability.

Web Applications

Vulnerabilities within web applications pose a significant threat to your organisation's network security.

A recent report revealed that Cross Site Scripting (XSS) and SQL injection attacks increased by more than 30%. In addition, almost half of organisations recently surveyed reported SQL injections as the most serious attacks they've experienced in the past 2-years.

The AppCheck scanner can identify all known web application vulnerabilities and provide exploit capabilities to demonstrate their impact and eradicate false positives.

Infrastructure

Web application vulnerabilities are not the only threat to your network perimeter. Unpatched software, configuration weaknesses and software vulnerabilities also need to be managed effectively. The AppCheck Scanner includes a vulnerability assessment module to perform vulnerability scans across your external network infrastructure.

Key Features

- Access sophisticated scanning and exploit technology designed by experienced penetration testers
- Provides a single platform to identify and manage web application and infrastructure risks
- Offers accurate discovery and analysis of 'Rich' Internet Applications via a combined network and browser-based scanning engine
- Supports complex multi-stage applications and authentication schemes
- Confirms vulnerabilities through safe exploitation to eradicate false positives and provide proof of concept
- Detects critical web application security flaws, including those defined by the OWASP Top Ten, e.g. Injection vulnerabilities such as SQLi and XSS
- Supports security strategy with fast, intelligent web crawling and exceptional detection rates
- Assign and prioritise each vulnerability's remediation to nominated members of your team using AppCheck's workflow management system
- Schedule scans to run at any given date and time. Scan at regular recurring intervals with email notifications
- Generates reports in Microsoft Word and CSV. PCI and UK Government PSN compatible formats

AppCheck

ACCURACY IS EVERYTHING

E: info@appcheck-ng.com
W: www.appcheck-ng.com
T: 0113 887 8380

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 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 can crawl it.

- AppCheck 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 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 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 scanner employs safe custom exploit techniques to actively confirm discovered vulnerabilities.

Microsoft Word and CSV reporting

Download custom filtered results and view via HTML, Docx or CSV. AppCheck includes a simple JSON data API for retrieving, aggregating, processing and reporting raw vulnerability data for use in third party applications.

Workflow Management

Create multiple (unlimited) user accounts to allow team collaboration. AppCheck includes workflow management allowing you to assign and prioritise each vulnerability's remediation to nominated members of your team.

Intelligent Authentication

Complex authentication schemes are supported when AppCheck 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 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.