

AppCheck vs OWASP Top Ten 2021

Based on a broad consensus, the OWASP Top Ten defines the current most critical web application security flaws.



The following table outlines how AppCheck identifies these vulnerabilities and helps to mitigate risk.

Category	Description	AppCheck Coverage
----------	-------------	-------------------

A01:2021-Broken Access Control



Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the user's limits.

AppCheck attempts all routes it discovers during a crawl, both as an authorised user and an unauthorised user, and reports back on this. Access control mechanisms are validated by attempting to access components that should be restricted or should require prior authentication but fail to protect the resource.

Insecure or superficial access control systems that simply hide components but do not properly secure them are also identified.

Unfortunately, due to the custom nature of applications, AppCheck is unable to rule on whether a given instance of forced browsing discovery is expected behaviour or an unintentional vulnerability, as it lacks context – however it does present this list in its report for review.

A02:2021-Cryptographic Failures



Previously known as Sensitive Data Exposure.

More of a broad symptom rather than a root cause, the focus is on failures related to cryptography (or lack thereof) which often lead to exposure of sensitive data.

AppCheck can check for and report on many cryptographic issues, including checks for weak passwords, the use of cleartext (unencrypted) protocols for data transport (e.g., HTTP being offered rather than HTTPS), the use of weak or outdated encryption algorithms on HTTPS services, and many other issues.

All reported issues typically need manual review to determine whether there is a need for the data on the system or service in question to be encrypted in transport or at rest – if the data is intended to be publicly readable, then it is arguable that the use of weak (or no) encryption is acceptable and not a vulnerability.

AppCheck vs OWASP Top Ten 2021

Category

Description

AppCheck Coverage

A03:2021-Injection



Injection attacks are the most common type of fault found in web applications, they are usually the result of unfiltered user input being directly included into command executions or database queries.

AppCheck performs comprehensive checks for a wide range of injection vulnerabilities including:

- SQL Injection
- NoSQL Injection
- XSS / Cross-Site Scripting
- XPath Injection
- Code Injection
- Command Injection
- LDAP Injection
- Expression Language Injection

The AppCheck Vulnerability Analysis Engine provides detailed rationale behind each finding including a custom narrative to explain the detection methodology, verbose technical detail and proof of concept evidence through safe exploitation.

A04:2021-Insecure Design



A new category for 2021 focuses on risks related to design and architectural flaws, with a call for more use of threat modelling, secure design patterns, and reference architectures.

There is a difference between insecure design and insecure implementation.

The “Insecure Design” category is incredibly broad. Many of the CWEs mapped to this category rely on human-aware context of intended business logic vs actual implemented behaviour for example. However, AppCheck can check for many other types of vulnerability within this category, such as sensitive information displayed in error messages, missing encryption, and the ability to control file name or path traversal.

A05:2021-Security Misconfiguration






Applications often have some form of misconfiguration, which is unsurprising given the shifts into highly configurable software. This category includes missing security hardening of the application stack or cloud services, default credentials, verbose error messages, and disabled security features.

AppCheck maintains a database of common configuration faults and out of date and un-patched frameworks and will flag these if detected. It will also check for many other issue types due to underlying misconfigurations, including default passwords that have been left unchanged, the use of verbose error messages, sensitive cookies without the “http only” flag, overly permissive cross-domain whitelists, or weak configured ciphers. AppCheck also checks for XML External Entity issues which now fall into this category.

If configured to do so, AppCheck will perform a comprehensive infrastructure assessment against all IP addresses and web applications defined within the scope.

AppCheck vs OWASP Top Ten 2021

Category	Description	AppCheck Coverage
<p>A06:2021-Vulnerable and Outdated Components</p> 	<p>Previously titled Using Components with Known Vulnerabilities.</p> <p>With the rise of the huge number of 3rd party components freely available on the internet for inclusion in applications, it's not uncommon for a developer to find a component or library and include it in an application to solve a problem or provide a widget. However vulnerabilities are often discovered in these components and either newer versions are released or they have been abandoned.</p>	<p>AppCheck includes a regularly updated database containing thousands of known vulnerabilities within content management systems, application frameworks, server and client-side components.</p> <p>The following dedicated assessment components are also provided by AppCheck:</p> <ul style="list-style-type: none"> • CMS Build review for; Umbraco, WordPress, Drupal, Magento, Joomla and DNN. • Web Server & Proxy vulnerability checks for nginx, Apache, IIS, Tomcat, Struts, F5 Load balancers plus many more. • Scanning for known server-side script vulnerabilities. • Client-Side JavaScript library checks to identify vulnerable and unsupported components.
<p>A07:2021-Identification and Authentication Failures</p> 	<p>Previously known as Broken Authentication.</p> <p>Sometimes authentication can be implemented incorrectly, or an application can contain routes to sensitive data that haven't been correctly protected by an authentication barrier. In other cases, it can be the session token that is vulnerable either to enumeration or not expiring, this can allow an attacker to guess the session token of another user (e.g., an administrator) and take control of their session to steal data.</p>	<p>While crawling an application AppCheck analyses the session for the possibility of enumeration by activating many sessions and examining the tokens. It will also look out for weakly implemented authentication, for example long response 302 redirects, which usually happens when the application serves up the content of a restricted view in the response of the page but then sends a redirect in the header.</p> <p>AppCheck also includes configurable password guessing modules to identify weak account credentials with many systems, as well as specific checks for known default or hard-coded vendor passwords on equipment and services, the use of session IDs in the URL, plaintext passwords emailed to users during registration, vulnerabilities in forgot-password processes, and authentication bypass.</p>
<p>A08:2021-Software and Data Integrity Failures</p> 	<p>Another new category for 2021, Software and Data Integrity Failures focuses on the category of vulnerabilities that relate to making assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity.</p>	<p>As part of its injection checks, AppCheck will attempt to exploit both generic and specific deserialization vulnerabilities across a wide variety of frameworks and libraries.</p> <p>AppCheck also has plug-ins to identify dependency confusion vulnerabilities which may affect the application's build process based on the libraries detected to be in use by the application.</p>

AppCheck vs OWASP Top Ten 2021

Category

Description

AppCheck Coverage

A09:2021-Security Logging and Monitoring Failures



Previously Insufficient Logging & Monitoring.

This category is expanded to include more types of failures, is challenging to test for, and isn't well represented in the CVE/CVSS data. However, failures in this category can directly impact visibility, incident alerting, and forensics.

This category is extremely challenging to test for. Since logs are not typically exposed externally, it is not possible for a scanner to confirm if security events are audited (recorded) correctly – and certainly not whether logs are then subject to triggering alerts and being manually reviewed by security staff. To fully review this area would involve interviews with security operations staff or asking if attacks were detected during a scan.

Through creating a realistic attack scenario, AppCheck helps to flex monitoring and logging solutions and so can highlight weaknesses and omissions in current processes, but this must be performed in hand with manual review by customer security or incident response teams – for which our security team are always on hand to offer advice on best practice.

A10:2021-Server-Side Request Forgery



SSRF is a particular variant of injection attack – SSRF vulnerabilities are those specific attacks in which an untrusted remote party (an attacker) is able (via the malicious payload submitted) to force a server to perform requests on their behalf.

SSRF flaws occur whenever a web application is fetching a remote resource without validating the user-supplied URL. It allows an attacker to coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall, VPN, or another type of network ACL.

AppCheck performs comprehensive checks for a massive range of web application vulnerabilities from first principle to detect vulnerability – including SSRF. AppCheck uses a variety of techniques to detect SSRF, including an out of band monitoring system to detect DNS and HTTP requests from the application in response to injected payloads, and proof of concept exploitation in cloud environments which interacts with services which are not exposed to the internet. AppCheck also draws on checks for known SSRF vulnerabilities in vendor software from a large database of known and published CVEs.