



AppCheck

ACCURACY IS EVERYTHING

User Guide

V1.1.9

Table of Contents

TABLE OF CONTENTS.....	2
ABOUT APPCHECK LTD.....	3
ABOUT THE APPCHECK VULNERABILITY SCANNER.....	4
ABOUT THIS GUIDE.....	5
WHAT THIS GUIDE COVERS.....	5
WHAT'S NOT COVERED.....	5
APPCHECK SOFTWARE REQUIREMENTS.....	6
INTERNAL HUB REQUIREMENTS.....	6
LICENSING.....	7
PER-USER LICENSING.....	7
SCAN SCOPES.....	7
LICENSE EXPIRY.....	7
TECHNICAL SUPPORT.....	8
SUPPORTPLUS AND MANAGED SERVICES.....	8
SUPPORT TEAM CONTACT INFORMATION.....	8
THIRD-PARTY INTEGRATIONS.....	9
KEY TERMS.....	10
VULNERABILITY SCORING.....	11
SERVICE ACCESS ENDPOINTS.....	12
APPLICATION PROGRAMMING INTERFACE (API).....	12
CUSTOMER PORTAL (WEB UI).....	12
BASIC ARCHITECTURE SUMMARY.....	13
BEFORE YOU START - WHITELISTING.....	13
PORTAL AUTHENTICATION / LOG IN.....	14
TWO FACTOR AUTHENTICATION WITH GOOGLE AUTHENTICATE.....	14
SESSION TIMEOUT.....	14
PASSWORD RESET.....	15
ACCOUNT LOCKOUT.....	15
APPCHECK WEB PORTAL - USER INTERFACE.....	16
MAIN DASHBOARD.....	18
SIDEBAR.....	18
PORTLETS.....	19
AVAILABLE PORTLETS.....	20
APPCHECK PAGES/VIEWS.....	22
"SCANS" VIEW.....	23
CREATING A NEW SCAN.....	25
NEW SCAN.....	25
COMMON SCAN TEMPLATES.....	26
NEW SCAN ADVANCED / EDIT SCAN.....	28

SCAN CONFIGURATION.....	29
BASIC SETTINGS.....	29
TARGETS.....	30
ADVANCED SETTINGS.....	32
WEB APPLICATION SCANNING.....	33
WEB APPLICATION SCAN OPTIONS.....	33
WEB APPLICATION SCAN PLUGINS.....	34
AUTHENTICATED WEB APPLICATION SCANNING.....	35
GoSCRIPT JOURNEY NAVIGATION.....	37
WEB API SCANNING.....	38
ADVANCED WEBAPP SCAN SETTINGS.....	39
INFRASTRUCTURE SCANNING.....	44
INFRASTRUCTURE SCANNING OPTIONS.....	44
VULNERABILITY SCANNER SETTINGS.....	45
PORT SCANNING.....	45
SCANNING WINDOW SETTINGS.....	48
ADVANCED SCAN CONFIGURATION.....	49
SCAN RESULTS.....	50
SCAN REPORT GROUPS.....	51
SCAN PROFILES.....	53
ORGANISATION SETTINGS.....	54
VULNERABILITIES.....	55
VULNERABILITY ORGANISATION.....	55
ALL VULNERABILITIES.....	56
REPORT GROUPS VULNERABILITIES.....	56
VULNERABILITY MANAGEMENT.....	57
BULK ACTIONS.....	60
VULNERABILITY INFORMATION SCREEN.....	64
USER MANAGEMENT.....	67
USER ROLES & RBAC (ROLE-BASED ACCESS CONTROL).....	67
REGISTERED USERS & USER MANAGEMENT.....	67
USER ACTIVITY LOGS.....	68
ADDING A NEW USER.....	68
USER GROUPS.....	69
ASSET MANAGEMENT.....	70
APPENDICES.....	71
APPENDIX A - GoSCRIPTS.....	71
APPENDIX B - TWO-FACTOR AUTHENTICATION WITH GOOGLE AUTHENTICATOR.....	73

About AppCheck Ltd

AppCheck is a security software vendor based in the UK. We offer a leading vulnerability scanning platform that automates the discovery of security flaws within organisations' websites, applications, APIs, networks, and cloud infrastructure.

Our proprietary scanning technology is built and maintained by leading penetration testing experts, offering unparalleled accuracy and detection rates. Our continuing aim is to bridge the gap between manual and automated testing and to combine the power and performance of an automated scanner with an emulation of the intelligent and context-sensitive progress of a manual penetration tester in stepping through discovery and analysis of a target site or service.

Our area of speciality lies in testing complex websites and applications. In addition to detecting vulnerabilities with known signatures, our ability to detect some of the hardest-to-reach security flaws using a first principles methodology sets us apart from other vendors and is why we're now trusted by some of the worlds most recognised brands.

About the AppCheck Vulnerability Scanner

AppCheck is a cloud-based service that gives you visibility into how, where and why your IT systems and services may be vulnerable to threats across the internet. Attackers can attempt to exploit weaknesses in internet-enabled systems and services to disrupt organisations' services or exploit system weakness to carry out the theft of data or resources. AppCheck helps you to secure your infrastructure by continuously monitoring it for vulnerabilities, reporting where vulnerabilities are found, and providing information on patching and remediation.

AppCheck allows you to keep one step ahead of anyone trying to exploit your IT services, indicating where patching or codebase remediation is needed, as well as generating graphical reports that let you prioritise remediation efforts where they can be best leveraged to provide the maximum benefit for the least effort.

About this guide

This guide is designed to help customers new to scanning with AppCheck get started, as well as enable experienced customers to discover new or more advanced features that are available.

What this guide covers

In this guide, we go over each section of the AppCheck web portal / User Interface (UI) and explain how to use it to get the most out of AppCheck. We also cover the risks from some common high-impact vulnerabilities and provide a broad overview of infrastructure and web application scanning, covering some common troubleshooting and how to diagnose a number of common issues.

What's NOT covered

This guide focuses almost exclusively on the usage of the AppCheck customer web portal (web UI) for interacting with the cloud scan service to configure and execute scans, and view scan results. It is worth noting that there are separate documentation/guides relating to other areas of AppCheck such as:

- **API access and usage** (permitting programmatic access to the AppCheck service)
- Internal hub configuration (to allow scans of internal-infrastructure not exposed on public internet)
- **GoScript usage** (for advanced web crawling and authentication flows)
- **Integration with third-party tools** such as **Atlassian JIRA** and **JetBrains TeamCity (CI)**. Integrations are available with these tools, but not covered in this guide,.

Please contact the central technical support team or your account manager if you require additional information on any of the above areas.

AppCheck Software Requirements

AppCheck is a cloud-based Dynamic Application Scanning Tool (DAST) scanning solution provided in a Software as a Service (SaaS) license agreement. There is no need to download or install any software onto customer laptops/desktops in order to use AppCheck.

Access to the AppCheck customer web portal requires a modern web browser. We test new releases of AppCheck against all modern desktop browsers up to the last three iterations. As of the time of writing the currently supported browsers are as below:

- The current version of Microsoft Edge (Windows)
- Internet Explorer 10 and 11 (Windows)
- The current and previous version of Firefox (Windows, Mac OSX, Linux)
- The current and previous version of Chrome (Windows, Mac OSX, Linux)
- The current and previous version of Safari (Mac OSX)

The AppCheck portal may be accessible via unsupported browsers, however browser-related issues may occur due to the absence of a browser feature or differing standards implementation.

Internal Hub Requirements

Internal hubs that extend the reach of AppCheck to application and infrastructure targets within an organisation's firewall perimeter have a separate set of requirements that are detailed in the separate Hub Setup Guide. Please contact technical support or your account manager for a copy of the guide or for further information on licensing and setup.

Licensing

AppCheck's commercial model is very transparent and is delivered through our trusted Global Partner Program as well as our direct sales team, which is based in the UK. There are multiple licence models available that are all fully scalable meaning that our solution caters for SME's and education, through to public sector and blue-chip organisations.

Licensing typically considers factors such as:

1. The number of target URLS (applications) and IP Addresses (infrastructure)
2. The number of scans that need to be run

Per-User Licensing

Valid licenses permit unlimited number of users per account, as well as unlimited scan executions against a target license scope, with limitations placed on concurrent resource usage dependent on license level.

The unlimited users per account means that multiple departments can run scans against a variety of environments such as Live/Production, Staging/UAT and development instances, and an Application Programming Interface (API) is also available for licensing, permitting custom integrations with services such as Continuous Integration (CI/CD) pipelines.

Scan Scopes

Licenses are restricted to a nominated target scope (list of application and infrastructure endpoints) for scanning. This limits scans so that they can only be run against an agreed set of server and application endpoints. AppCheck will not scan outside of this scope and items for inclusion within an organisation's scope needs to be approved by an AppCheck account manager or through AppCheck's support channel. Within an account scope it is possible to include a mixture of infrastructure targets [IP addresses, FQDNs, hostnames] and web application targets [URLs].

License Expiry

If your organisation's license has expired or your user account has been blocked for misuse, then you will be locked out of your account and will be unable to login. If you believe that this has occurred in error, please contact the AppCheck customer support team (contact details below). If you became an AppCheck partner from 1st May 2019 onwards, then the subscription runs for the initial term shown on the signed subscription agreement and after the end of the initial term, your licence will automatically renew on an annual basis unless and until terminated in accordance with clause 9 of the subscription agreement.

Technical Support

Due to the large range of clients we support, we offer several tailored support services, each depending on our client's requirements and technical understanding which puts our services and support at the heart of what we do.

Basic Support is available to all customers.

SupportPlus and Managed Services

The AppCheck SupportPlus service offers additional technical support that is provided by AppCheck's security consultants. Our consultants are available to provide pre-scan guidance, as well as post-scan consultancy to explain the results in greater depth and provide remediation advice.

SupportPlus Feature Highlights:

- Full access to unlimited AppCheck Scans
- Administrative Support access via our help-desk.
- GoScript writing and training
- Technical Support via the security consultants team
- In depth explanation of results
- Advice on remediation process and remediation of specific vulnerability instances

Support Team Contact Information

Support is available between **09:00am** and **17:30pm**, Monday through Friday.

The AppCheck support team can be emailed at support@appcheck-ng.com or a support ticket system raised via the ZenDesk support ticket system from <https://appcheck.zendesk.com/>.

Third-Party Integrations

Third-party integrations are available for several third-party software tools, including the popular Atlassian JIRA (issue & project tracking software) and JetBrains TeamCity (build management and continuous integration server)

Details of the integrations are available on our online knowledgebase and further information can be obtained via your AppCheck account manager.

Key Terms

The following terms are used widely in this user guide, and it is worth ensuring that you are familiar with the concepts and understand each before reading the User Guide.

Assets & Account Scope	A list of systems or services (targets for scanning), such as IP addresses or URLs, that represent the extent of an organisation's internet-facing services, and which are available for use as scan targets within individual scans.
Scan Scope	The list of systems and services targeted by a particular vulnerability scan.
Vulnerability	A weakness present in the design or configuration of an asset and which can be exploited by a threat actor, such as an attacker, to perform unauthorized actions within that system.
Impact	The effects of a successfully exploited vulnerability on the target system or service that suffers the worst outcome that is most directly and predictably associated with the attack, in terms of a reduction in the Confidentiality, Integrity or Availability of targeted system, service or data.
Vulnerability Scanning	A service such as AppCheck that provides automated crawling and testing of an organisation's web applications via HTTP requests from a cloud scan hub to identify vulnerabilities including Cross-Site Scripting (XSS) and SQL injection as well as open ports, insecure software configurations, and susceptibility to malware infections.
Exploit	An exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended or unanticipated behaviour to occur on a target computer software.
Mitigation & Remediation	Where action is taken, in order of highest priority, against components reported to be vulnerable

Vulnerability Scoring

Most vulnerabilities reported openly are assigned a CVSS (Common Vulnerability Scoring System) score between 0 (no risk) and 10 (critically high risk) based on a number of factors including the likelihood of exploit and their impact if exploited.

Vulnerabilities in AppCheck are tagged with a CVSS score but primarily are reported using a simply High/Medium/Low rating based on their impact. These scores are generally based on their CVSS score. Sometimes however there may be a vulnerability that has a different impact or risk compared to the CVSS score.

This can happen for certain vulnerabilities where the nature of the flaw is not compatible with CVSS. The metrics are based around integrity, availability and confidentiality of the target system as a direct result of the attacker sending the attack.

Vulnerabilities such as Cross Site Scripting (XSS) for example typically don't change data on the system, but rather exploit the system to attack other application users. All scanners and pen tests rank XSS as a high impact issue, but when sticking to the calculations under CVSS, it comes out as a 4.3.

We set our impact ratings based upon industry accepted levels of each vulnerability class, it usually correlates to CVSS but in some cases it doesn't. The most common vulnerabilities to have a mismatch are XSS and related vulnerabilities such as HTML 5 CORS configuration issues.

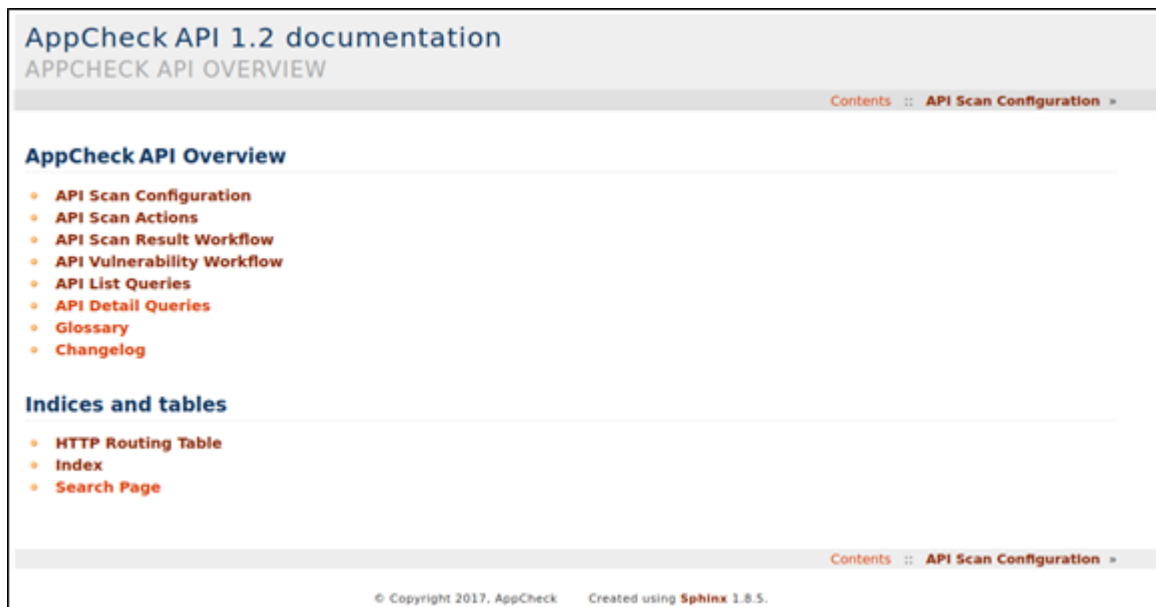
High	Successful exploitation could lead to highly privileged access to the target host or cause a denial of service condition. Vulnerabilities are labelled "High" severity if they have a CVSS base score of 7.0 - 10.0
Medium	Exploitation of the vulnerability will not directly lead to privileged access to the host, service or data. However, vulnerabilities with a Medium impact can often be combined with other flaws to elevate their impact. Vulnerabilities will be labelled "Medium" severity if they have a base CVSS score of 4.0-6.9
Low	This impact rating is assigned to vulnerabilities that, when exploited in isolation, have a negligible impact on security. Typically vulnerabilities that disclose information that may be useful to the attacker are considered to have a low impact. Vulnerabilities are labelled "Low" severity if they have a CVSS base score of 0.0-3.9.

Service Access Endpoints

AppCheck offers both an Application Programming Interface (API) as well as a customer web portal interface (Web UI)

Application Programming Interface (API)

Documentation for the API is available at <https://api.appcheck-ng.com/>. API usage permits computer to computer (automated) interaction with AppCheck services and can be enabled under client licences on request via client account managers.



Customer Portal (Web UI)

The AppCheck portal (web UI) is accessible at the following URL. And is the primary method of permitting human interaction with the AppCheck service. It permits the configuration and setup of scans, as well as the viewing of scan results.

<https://scanner.appcheck-ng.com>



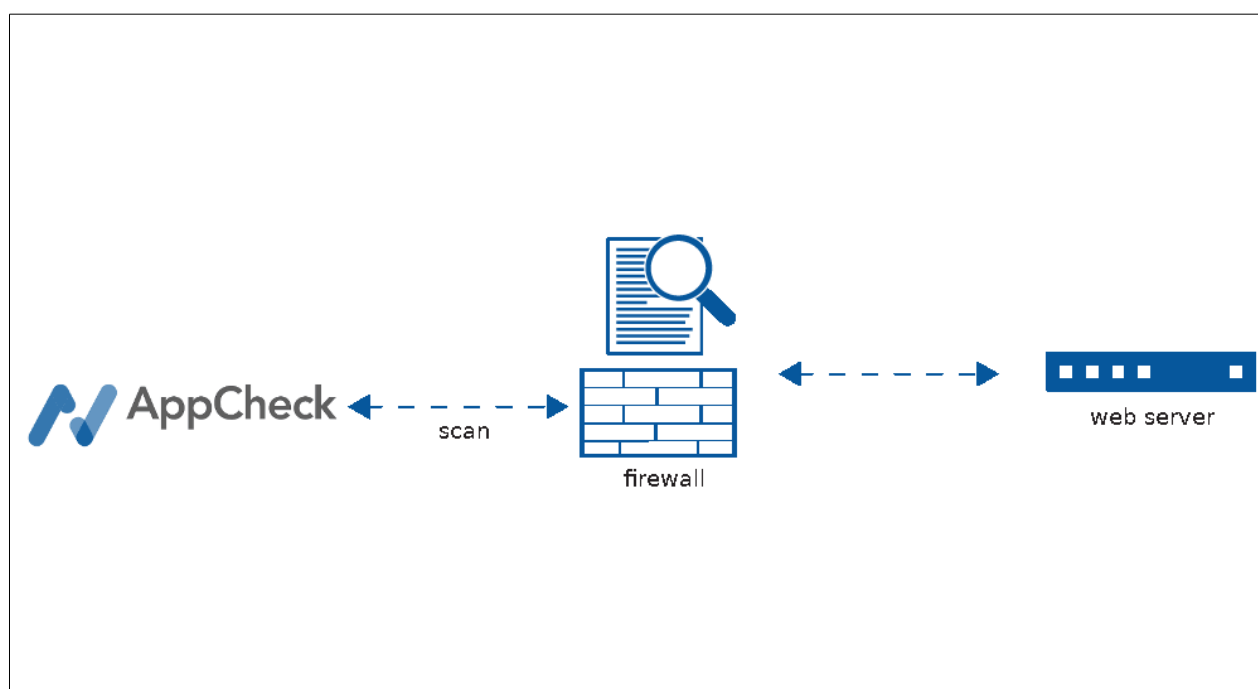
Basic Architecture Summary

AppCheck performs scans across the public internet from cloud-based scan hubs. It therefore scans from outside organisations' firewalls, from the same position as unprivileged internet users:

Before You Start - Whitelisting

To gain the best coverage from your security assessment, the AppCheck Scanner IP address ranges should be added to the "whitelist" of any IPS, WAF, firewall or gateway device that could "black list" AppCheck based on one or more of its security checks. For further information, see:

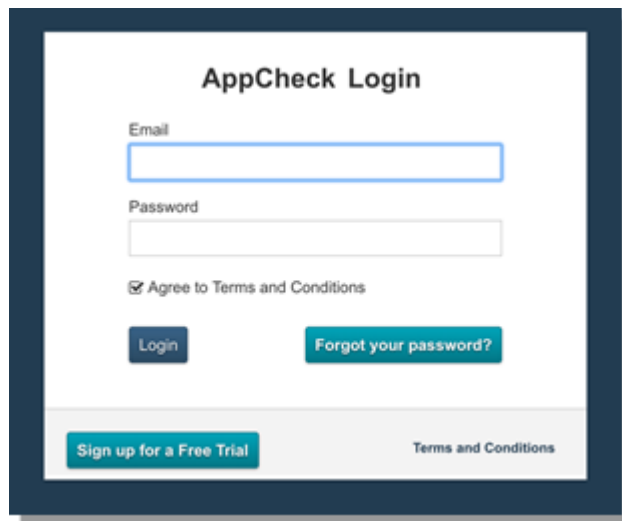
<https://appcheck.zendesk.com/hc/en-us/articles/360001069893-Whitelisting-FAQ>



Portal Authentication / Log In

To get started, it is necessary for customers to log in to the customer portal (web UI) using the login details provided by their AppCheck account manager.

The AppCheck login screen requires that you enter an email address and password in order to authenticate. It also requires that you agree to the terms and conditions to continue.

A screenshot of the AppCheck Login web form. The form is titled "AppCheck Login" and contains fields for "Email" and "Password". Below these fields is a checkbox labeled "Agree to Terms and Conditions". At the bottom of the form are two buttons: "Login" and "Forgot your password?". At the very bottom of the page, there is a "Sign up for a Free Trial" button and a link to "Terms and Conditions".

Two Factor Authentication with Google Authenticate

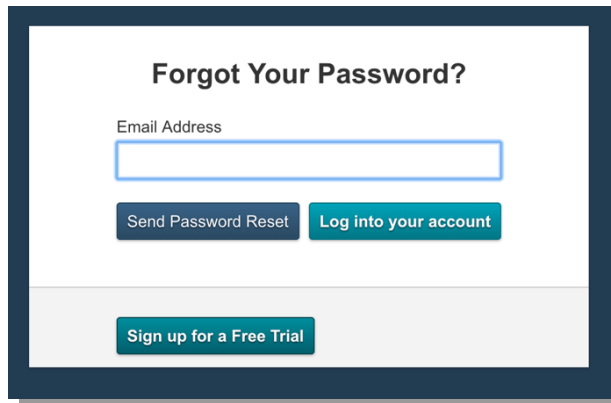
While we don't enforce it as a default, it is strongly recommended that customers enable two-factor authentication (2FA) on their AppCheck account. Two-step authentication is a method of confirming a user's claimed identity by utilizing two pieces of evidence ("factors") - something they know (password) and a second factor such as a six digit number generated by an app that is common to the user and the authentication system. Setting up 2FA on AppCheck is easy to do and is worth it for the additional protections it affords. [Please see Appendix Google Authenticate](#) for further information.

Session Timeout

Due to the sensitivity of the vulnerability data stored within AppCheck, additional security is provided through the enforcement of a browser session timeout. This requires logged-in users to re-authenticate if their session on the AppCheck portal is inactive for more than 1 hour. There is no option to override this security feature.

Password Reset

If you are having difficulty logging into your account then you can use the **“Forgot your password?”** button on the login screen to reset your account password. This will generate a new single-use login token to allow you to get back into the application and change your password. These single-use links are valid for 24 hours: if you do not reset your password within this period then you will need to request another password reset.

A screenshot of a web form titled "Forgot Your Password?". It features a text input field labeled "Email Address". Below the input field are two buttons: "Send Password Reset" and "Log into your account". At the bottom of the form is a button labeled "Sign up for a Free Trial".

Forgot Your Password?

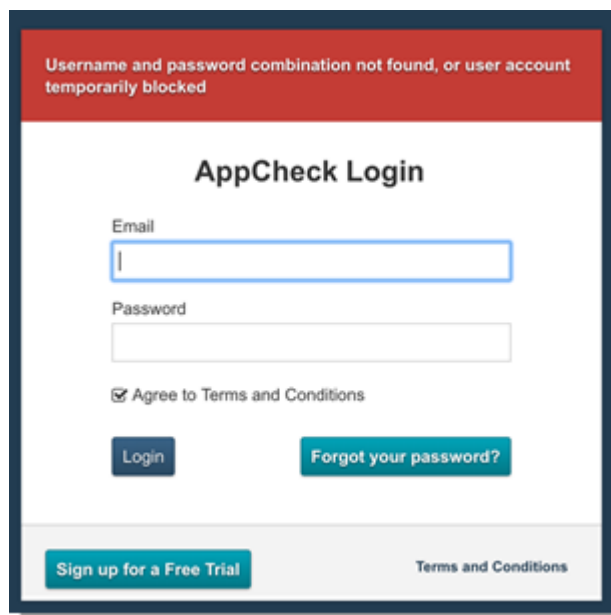
Email Address

[Send Password Reset](#) [Log into your account](#)

[Sign up for a Free Trial](#)

Account Lockout

AppCheck has an account lockout policy in place to help mitigate brute forcing attempts, if three incorrect password attempts are made in a row then the account in question will be locked out for 15 minutes. After this period, the password attempt counter will reset and three more attempts will be permitted. However, any further lockouts will be reported to our administrators.

A screenshot of the AppCheck Login form. At the top, a red banner displays the error message: "Username and password combination not found, or user account temporarily blocked". The form title is "AppCheck Login". It includes input fields for "Email" and "Password". Below these fields is a checkbox labeled "Agree to Terms and Conditions". At the bottom of the form are three buttons: "Login", "Forgot your password?", and "Sign up for a Free Trial". A link for "Terms and Conditions" is located at the bottom right of the form.

Username and password combination not found, or user account temporarily blocked

AppCheck Login

Email

Password

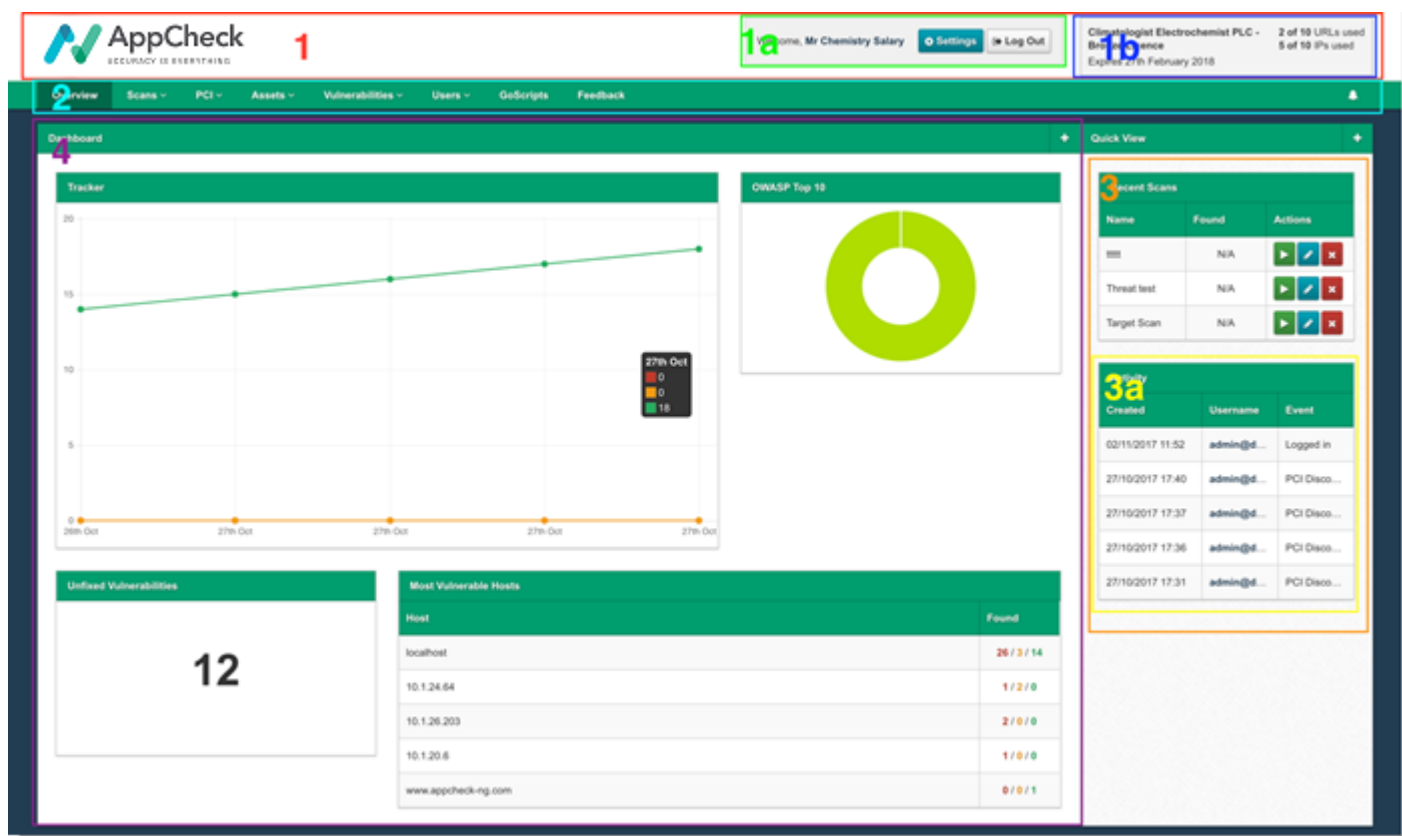
☒ Agree to Terms and Conditions

[Login](#) [Forgot your password?](#)

[Sign up for a Free Trial](#) [Terms and Conditions](#)

AppCheck Web Portal - User Interface

The user interface is broadly broken down into the following sections seen below and indicated by the numbers **1** through **4**:



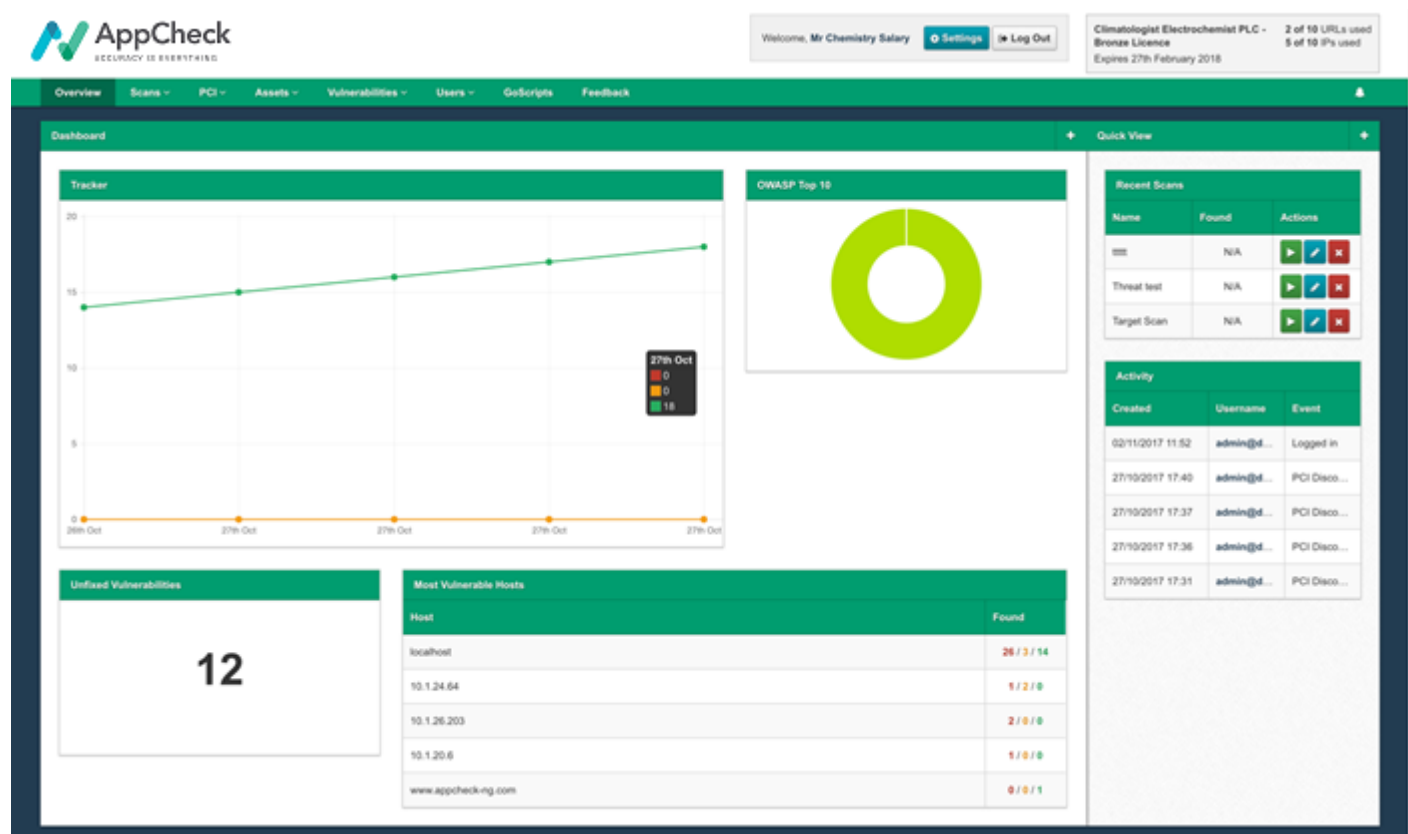
These areas are explained in more detail in the table below:

1	Header	<p>The main header of the application contains the following useful items of information</p> <p>(1a) Account Control Provides quick access to change your user settings and logout of the application</p> <p>(1b) License Information Shows what your current license is as well as scope usage.</p>
2	Navigation	The main means of navigating round the application, notifications appear here as well.
3	Sidebar	<p>Displays useful information throughout the application and in most places, has configurable portlets that remain in place throughout the application.</p> <ul style="list-style-type: none"> (3a) Portlets

		These are small customisable informational panels that allow you to configure AppCheck to show the information you need on your scans. From what's presently running to how vulnerability resolution is progressing
4	Main View Port	This is the main viewing area within the application and is where most core interaction takes place.

Main Dashboard

Once you have logged into AppCheck you will then be presented with the main **Dashboard** view. This is a large portlet area, which you can customise by adding or removing individual data summaries known as “portlets” which present information important to you and the management of your vulnerabilities. If this is your first time logging in then a selection of default portlets will be populated in your dashboard and down the sidebar:



Info:

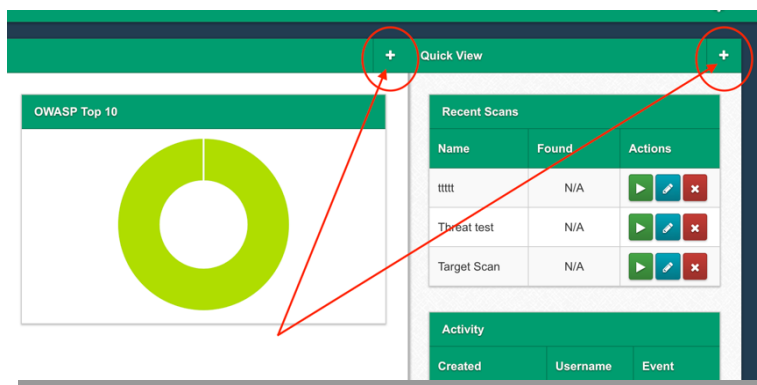
The dashboard has space for three small portlets per row or one large portlet and one small portlet, the sidebar ignores size and arranges portlets vertically.

Sidebar

The **Sidebar** is a portlet area and behaves in the same way as the **dashboard** and accepts the same portlets. Portlets are draggable between the two views, by pressing the left mouse button in the header of each portlet and dragging it into an available portlet slot. The main difference is that the **sidebar** is available throughout the application (not just on the dashboard screen). This allows you to keep your most important informational portlets within easy reach.

Portlets

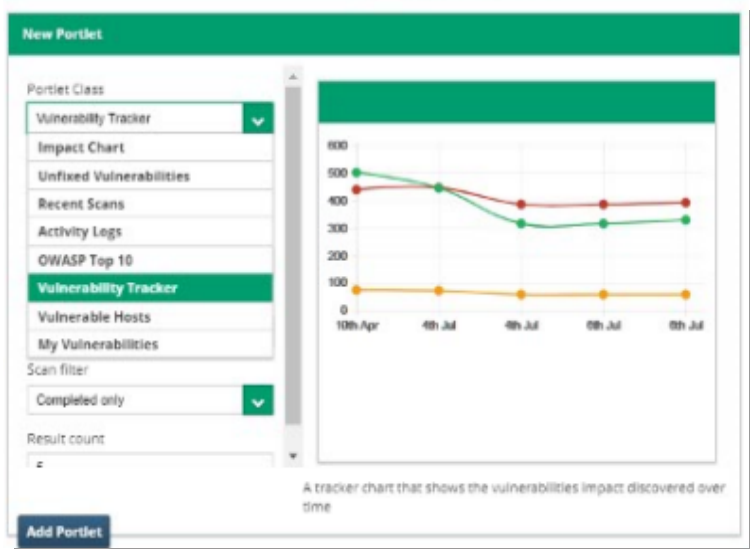
The AppCheck **portlet** tool provides a set of graphs showing a quick overview of information about various parts of the scanner. These range from vulnerability Impact Charts to an overview of vulnerabilities assigned to you. The **dashboard** and **sidebar** can be customised to each individual by adding additional portlets to by selecting the add portlet option (+) in the upper right corner of the interface.



Portlet Customisation

All portlets available within AppCheck have some degree of customisation. A preview of the presently selected portlet and a preview of what will be added to the portal are available in this screen.

All Portlets have the option to change their title and size and provide a basic description of their function and purpose underneath the preview window.



Available Portlets

There are 12 portlet types available within AppCheck at the time of writing, the options and configurations for which are listed below.

Impact Chart	This portlet shows a chart of your vulnerabilities broken down by impact and probability, high impact high probability vulnerabilities being of critical importance to resolve with low impact low probability vulnerabilities being more informational or only relevant when combined with other attacks. This portlet also interacts with the vulnerability results list on individual scans and the all vulnerabilities view, to filter these views by the impact selected in the chart.
Unfixed Vulnerabilities	This portlet shows a count of presently outstanding unfixed vulnerabilities, it is purely informational and provides no further interactivity.
Recent Scans	Shows lists of recent scans, options exist to sort these by running scans or by the scan created date to suit an individual users style of working. This portlet provides shortcut access to start, pause, resume and abort scans. Clicking on the row will take you to the results view for that scan.
Running Scans	Displays a list of scans that are currently in the Scanning phase and are actively executing
Activity Logs	Displays recent activity logs for this account, actions performed by users within AppCheck are logged here, clicking on a row will take the user to the logs view which has further details and a searchable history of actions.
OWASP Top 10	Breaks the discovered vulnerabilities down to those that are included as part of the OWASP Top 10, OWASP is an open source advisory group, more information on the OWASP top 10 can be found on our knowledge base https://appcheck.zendesk.com/hc/en-us/articles/115002662489-OWASP-Top-10-2017-RC-
Vulnerability Trend	Shows a chart of the 5 most common vulnerabilities within a defined time window (e.g. 30 days) in terms of number of instances of the vulnerability seen across all assets.
Vulnerability Tracker	This portlet shows how the rate of vulnerabilities discovered or resolved changes overtime, it can be viewed against the group as a whole, or just an individual scan. A downward trend here indicates vulnerabilities are being resolved, an upward trend indicates that more vulnerabilities are being discovered than are

	being resolved.
Total Scans	Displays a simple numerical count showing the number of running scans
Vulnerabilities Status	Displays a bar chart showing the total numbers of unfixed vulnerabilities, by impact (High, Medium, Low) and whether they are fixed or unfixed.
My Vulnerabilities	Displays all vulnerabilities assigned to the current user who is logged in and viewing the panel.
Vulnerable Hosts	Displays a table showing the the top 5 most vulnerable hosts (by unfixed issues count per host)

AppCheck Pages/Views

Once logged in, it is possible to click on different tabs along the top of the main dashboard to access different portions of the AppCheck application.

The majority of this guide covers the functionality under the **Scans** view, and this is where the bulk of the configuration of scans as well as access of vulnerability data is typically performed, however the following views are accessible

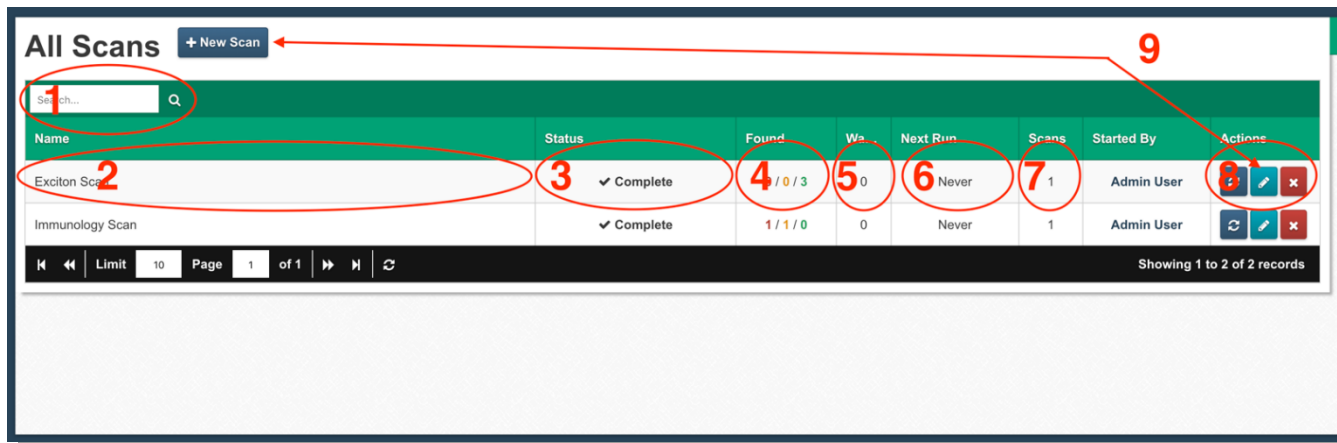
Scans	An area to create, manage, view, edit and show reports on vulnerabilities found in scans of your target infrastructure and applications
PCI	A list of scans specific to Payment Card Industry Digital Security Standard (PCI-DSS) standards, useful for organisations that operate web services that process credit/debit card payments and need to evidence PCI-DSS compliance
GoScripts	An area for storing and configuring “GoScripts”. These are covered later in this guide, but can be used to model complex “flows” or customer journeys through your website (such as multi-page registrations) for the vulnerability scanner to follow
Assets	A list of assets (targets for scanning), along with the ability to group assets into groups for easier management and tracking
Vulnerabilities	A list of vulnerabilities across the entire customer account
Users	An area permitting the management and creation of user accounts as well as user groups governing permissions.
<i>Scan Hubs [optional]</i>	For customers with an internal hub deployment, a page allowing listing and configuration of deployed hubs.
Feedback	A form for creating a support request
Organisation settings	Additional functionality such as scan notification URL paths

“Scans” View

The scans view is where all of your scan definitions are created, edited and controlled from. As well as adding a number of useful features to help with scan and management, such as grouping multiple scans into a single result set to scan profiles to manage a standardised configuration of scan settings.

All Scans / My Scans

Both these views are identical apart from the latter filters the view to scan definitions created by only you and not others in your organisation. From here you can manage your various scan settings, control your scans and view and manage scan results.



Name	Status	Found	Wa	Next Run	Scans	Started By	Actions
Exciton Scan	✓ Complete	4 / 0 / 3	0	Never	1	Admin User	[Edit] [Delete]
Immunology Scan	✓ Complete	1 / 1 / 0	0	Never	1	Admin User	[Refresh] [Edit] [Delete]

Showing 1 to 2 of 2 records

- (1) Search
A search field to look for existing scans, here you can search on scan names.
- (2) Scan Name
The name that has been given to this scan.
- (3) Scan Status
What the current status of this scan is, if a scan is in progress a progress bar displays here with an approximation of how far through the scan process is.
Application scans can take upward of 48 hours to complete depending on how exhaustively it's configured due to the number of iterations it has to go through to identify and confirm a flaw, it's often a good idea to have a look at the number of requests the application scanner has made over a five minute period to get an idea of how it is progressing.
Infrastructure scanning on the other hand due to it looking for known flaws tends to be faster typically only requiring a few hours per target.
There are presently 7 possible scan statuses:
 - o Unscheduled
 - o Scheduled
 - o In Progress
 - o Detached
 - o Aborted
 - o Failed
 - o Complete
- (4) Results Count
Displays a count of the high, medium and low vulnerabilities discovered during a scan.

- (5) Warnings Count
Displays a count if there are any warnings on the current scan, these warnings can be viewed in the scan results warnings tab, typically these will include the following items.
 - o Unresolved Hosts
 - o Unreachable Hosts
 - o Unresponsive Hosts
 - o Scan failures
- (6) Next Schedule
When this scan is next scheduled to run and if there is a scan window active.
- (7) Run Count
Shows a count of how many times this scan definition has been run and the number of results sets stored against it.
- (8) Scan Actions
 - o Start Scan / Restart Scan
Starts a scan process running, if no previous scan has been run for this scan configuration then the **start scan** button will be displayed if there have been no previous scans run against this configuration then the **rescan** button will be displayed.
 - o Pause Scan
Pauses a currently running scan, manually paused scans will not resume if the scan has been set to run within a scheduled window. Manually pausing overrides this.
 - o Resume Scan
Resumes a paused scan, if the scan's pause-resume cycle is being controlled by a scheduled scan window resuming a scan will result in it automatically being paused again.
 - o Abort Scan
Aborts a currently running or paused scan, these scans can then be restarted again afterwards. Aborting can sometimes take a couple of seconds for the abort state to be reached as the action is asynchronous and requires the **scanning hub** to return a confirmation message.
 - o Remove Scan
Deletes this **scan definition** and all associated **results sets** and **vulnerabilities** not associated with other **scan definitions**.
 - o Scan Settings
Edit the settings of this scan definition, this view is identical to the **new scan** view.
- (9) Scan Actions
New scan and scan edit button, the new scan button is a shortcut to the navigation item in the scans menu and the edit scan button it a shortcut to the settings tab in a scan results view

Info:

All scanning actions that require communication with the scanning hubs are asynchronous and do not necessarily provide immediate feedback on the requested action it can sometimes take a few seconds for the scan status to be updated.

Danger:

Great care should be taken when removing a **scan definition** as the action **cannot be undone** and any associated data **will be lost** once done!

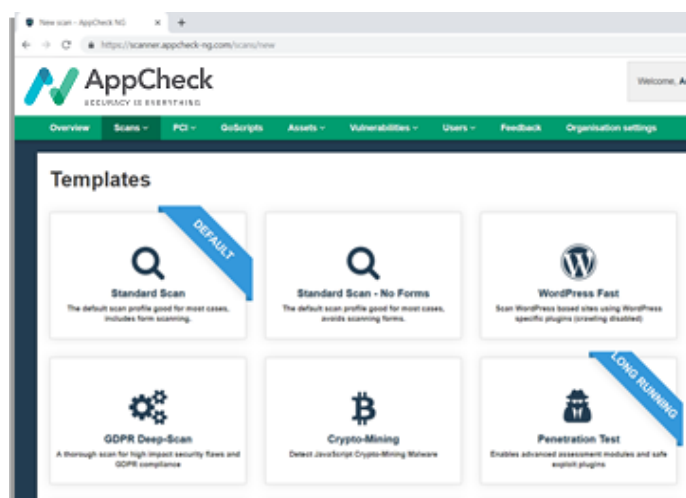
Creating a New Scan

There are two options for creating a new scan; *New Scan* and *New Scan Advanced*. In most cases, selecting *New Scan* from the *Scan* menu is the recommended option since this provides access to pre-configured templates built by our research team. The *New Scan Advanced* option skips the template selection phase and is typically used by advanced users who wish to configure their own scan profile (by default Standard Scan options are selected by clicking this option).

Regardless of which option you chose, all scan options are configurable in the same way.

New Scan

Selecting the New Scan option will take you to the Template selection screen.



Scan Template Selection

Scan Templates are used to apply common configuration options for a number of different scenarios. The configuration options applied by each template can be fine-tuned before the scan is scheduled.

Note: AppCheck is platform agnostic, templates that name a specific technology stack are provided as a convenience to streamline configuration. Typically, selecting a platform specific template will disable scan options that are not applicable for a particular platform to reduce scan duration. If your stack is not listed, select “Standard Scan” or “Penetration Test”.

Common Scan Templates

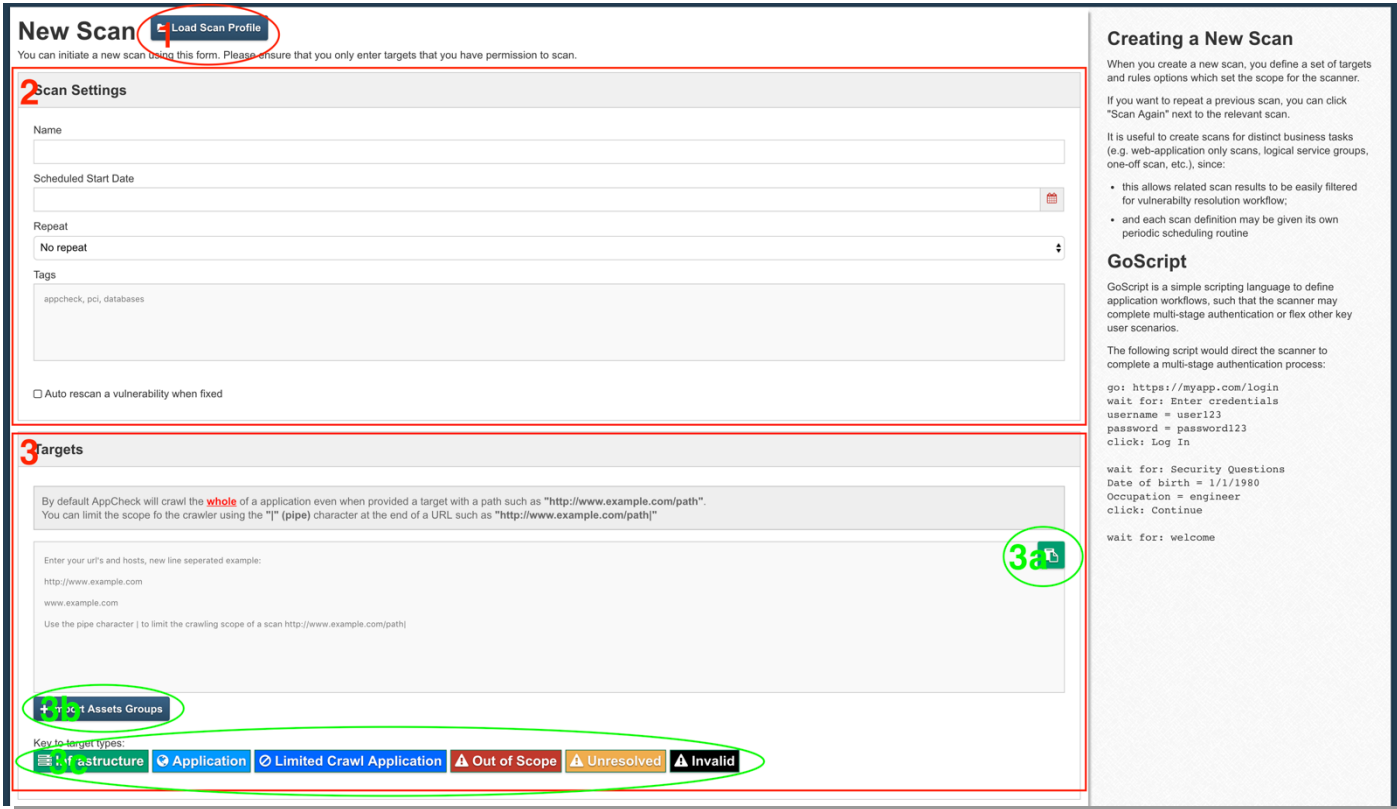
Templates are continually added based on customer feedback and events such as the disclosure of a high priority security flaw or new attack technique. The table below details some of the most popular profiles which are suitable for any environment.

Profile	Description
Standard <i>(Recommended for most users)</i>	<p>The Standard profile is configured to strike a balance between coverage and scan duration. Selecting this template configures each plugin with optimal settings for general scanning. Some information gathering plugins and checks for exceptionally rare vulnerabilities are disabled or limited to basic checks to improve efficiency.</p>
Penetration test	<p>The Penetration Test profile was designed with professional security consultants in mind. Selecting this profile automatically enables all security checks including checks for rare edge case vulnerabilities. Additionally, each plugin is set to be more exhaustive and will enable testing of HTTP headers that are not synonymous with security flaws. For example, it would be exceptionally rare to find a vulnerability within an "Accept" HTTP header, however it's not impossible and therefore it is enabled by this profile.</p> <p>The Penetration Test profile also includes additional plugins designed for penetration testers and enables all safe exploit options.</p> <p>Since the Penetration test profile is exhaustive, it also takes longer to complete a scan (around 4 times longer than a standard scan).</p>
GDPR	<p>The General Data Protection Regulation or GDPR is legislation designed to protect privacy and data security of individuals within the EU and UK. The law affects anyone who works with Personally Identifiable Information (PII) even if the organisation resides outside the EU/UK. One of the most notable elements of the GDPR is the fines attached to non-compliance or failing to sufficiently protect PII data (4% of global turnover or €20,000,000, whichever is higher).</p> <p>The GDPR profile was created to help organisations audit their applications for compliance and identify vulnerabilities that could result in a data breach. Selecting this profile will prioritise high and critical impact vulnerabilities and enable specific GDPR checks such as:</p> <ul style="list-style-type: none"> • Identify PII collection through websites and applications. • Identify forms that are not compliant with GDPR standards (e.g. non-compliant consent collection). • Identify insecure communication of PII data. • Identify insecure storage of user passwords.

Profile	Description
Vulnerability / Attack Specific	<p>Several templates are also available to configure the scan for a specific technology stack or vulnerability. Selecting one of these templates will disable checks which are not relevant for the target environment. For example, running a WordPress scan will disable checks for technologies not typically found with WordPress such as ASP .NET.</p> <p>Templates are also created when a critical impact vulnerability is being widely exploited and needs to be detected as a matter of urgency. In each case, the vulnerability will be detected by selecting one of the generic profiles such as "Standard Scan", however should you wish to run an estate wide scan for one particular flaw, templates are provided for convenience.</p>

New Scan Advanced / Edit Scan

After selecting a scan template, or by selecting **New Scan Advanced**, the scan edit view is displayed. This view is used to configure scan targets, schedule scan start time, define permitted scan schedules and configure checks performed during the scan.



New Scan Load Scan Profile

You can initiate a new scan using this form. Please ensure that you only enter targets that you have permission to scan.

2 Scan Settings

Name

Scheduled Start Date

Repeat

No repeat

Tags

appcheck, pci, databases

☐ Auto rescan a vulnerability when fixed

3 Targets

By default AppCheck will crawl the **whole** of an application even when provided a target with a path such as "http://www.example.com/path". You can limit the scope to the crawler using the "|" (pipe) character at the end of a URL such as "http://www.example.com/path|"

Enter your url's and hosts, new line separated example:

http://www.example.com

www.example.com

Use the pipe character | to limit the crawling scope of a scan http://www.example.com/path|

3a

+ Assets Groups

Key to target types:

- Infrastructure
- Application
- Limited Crawl Application
- Out of Scope
- Unresolved
- Invalid

Creating a New Scan

When you create a new scan, you define a set of targets and rules options which set the scope for the scanner.

If you want to repeat a previous scan, you can click "Scan Again" next to the relevant scan.

It is useful to create scans for distinct business tasks (e.g. web-application only scans, logical service groups, one-off scan, etc.), since:

- this allows related scan results to be easily filtered for vulnerability resolution workflow;
- and each scan definition may be given its own periodic scheduling routine

GoScript

GoScript is a simple scripting language to define application workflows, such that the scanner may complete multi-stage authentication or flex other key user scenarios.

The following script would direct the scanner to complete a multi-stage authentication process:

```
go: https://myapp.com/Login
wait for: Enter credentials
username = user123
password = password123
click: Log In

wait for: Security Questions
Date of birth = 1/1/1980
Occupation = engineer
click: Continue

wait for: welcome
```

- (1) Load Scan Profile
Allows for the loading of pre-defined [scan profiles](#).
- (2) Scan Settings
Basic minimal settings required for a scan, details of which are [documented below](#).
- (3) Targets
What the scanner is to target for running scans against, more details on targets can be [found below](#).
 - o (3a) Copy and Paste Targets
 - o (3b) Import Asset Groups
Allows for the importing of targets from previously defined asset groups, these are collections of targets stored as a logical group for scanning and reporting.
 - o (3c) Target Types
Helpful information about the types of target included in this scan and their validity.
 - Infrastructure Target
 - Application Target
 - Limited Crawl Application Target
 - Out of Scope Target
 - Unresolvable Target
 - Invalid Target

Scan Configuration

Basic Settings

AppCheck has been setup in a way that the defaults are good for the vast majority of use cases, these settings will thoroughly test the majority of sites with little adjustment of the configuration options so that simply entering the intended scan target with the bare bones information needed to start a scan can get you underway.

Scan Settings

These are the most basic settings required for scanning, the options here should be fairly self-explanatory, we will cover them here for the sake of clarity.

Warning:

Editing scan configuration settings while a scan is presently running will not take effect until the next scan, this is because the configuration has already been sent out to a scan hub and has been consumed by a scan process, once a scan process has started there is no way presently to update a running configuration without impacting on the end results.

Scan Name

All scans require a name so that you can identify them later on, it's recommended to give scans meaningful names as later on once you have a number of scans running, it can be difficult to find and manage the results you are looking for, example "Production Apps" or "UAT Database".

Scheduled Start Date

Scan can either be started right away or started on a schedule, if you schedule a scan to start at a specific time and date the scan will be started then. The modification of a schedule will only take effect while a scan is running, you can include multiple windows against a single scan to allow for just about any conceivable scheduling arrangement.

Repeat

This controls how frequently a scan will repeat automatically at the above schedule time, if this scan definition is presently running then the repeat will be skipped till the next window.

Targets

Targets tell AppCheck what it is actually accessing/probing in order to test. Broadly they are broken down into two categories: **Application** and **Infrastructure**. The main distinction between the two is that Infrastructure targets fall into the category of known vulnerabilities and we are looking for signatures and version of known infrastructure software. Application vulnerabilities generally tends to fall into the unknown category due to them being custom written code. There is some small crossover between the two (for instance WordPress Core) but generally this is the distinction.

Application Targets

Application targets are web applications: these should start with a `http://` or `https://` and can either run on the standard ports or an additional port argument can be passed into the URL. For example <https://example.com:8080> would tell AppCheck to attack web application hosted on the domain example.com using protocol HTTPS on port 8080.

Limiting Web Application Scope (Scan specific URL only)

When performing a web application scan, you might want to either explicitly restrict a scan of a domain to a certain path (eg `www.example.com/path2/`), or to explicitly exclude a certain path from scanning (e.g. `www.example.com/static/`) whilst scanning all other paths on the domain.

Application targets can be set to a limited crawl target. What this means is AppCheck-NG will not scan outside of a given path (directory) in the URL. Normally when AppCheck-NG is crawling and attacking an application it attempts to crawl the entire domain.

Even if the scan target is given as <https://www.example.com/path1> AppCheck will use this as the **starting** point for scanning, but will crawl and then attack any other paths found via crawling or brute force discovery, including pages at eg `https://www.example.com/path2`

In some instances, this can be undesirable behaviour: for instance if you entered <http://www.example.com/app1> as a target, you may have the expectation that AppCheck-NG will only scan this page (and pages within that directory). However if you wish to scan **ONLY** that path and pages within it, you can limit the scope of the crawler with the “|” (pipe) character as a suffix (trailing character) in the scan target.

If you change your scan target to <http://www.example.com/app1|> (note trailing pipe character) then this will now only crawl and attack paths above within the `/app1` path/directory, leaving `/app2` and `/app2` and all other paths un-scanned.

Excluding Specific Web Application Crawl Targets (Exclude specific URL)

It is also possible to exclude a given path (and directories underneath it) using the **blacklist** feature in the scan configuration

Any URLs entered in this list (and directories underneath them) will be excluded/blacklisted from scanning.

Infrastructure Targets

Infrastructure targets are the hosts themselves and we are generally checking against all ports to see what services are available, checks will then be performed against that host to see what services and operating systems are running and if it matches any known vulnerability signatures. Any hostname, IP address, IP range or CIDR notation address is a permissible infrastructure target.

Excluding Specific IPs from infrastructure scanning

The **Blacklist Targets** section of a scan configuration can also be used to exclude specific IPs from within a scan target range from being scanned.

Other target types are informational:

Out Of Scope	indicates that this target does not fall within the permitted scanning scope of your license
Unresolved	indicates that the entered target cannot be resolve by the AppCheck external servers. This is often the case with internal applications as we resolve from a different set of servers to the scanning hubs. If the target has a DNS entry added into the hub management section that the central AppCheck service should now be able to resolve the target.
Invalid	targets are targets that make no sense to the scanner, they don't match any application, hostname or valid IP notations and are invalid and will be ignored

Advanced Settings

While AppCheck's default configurations are good for the vast majority of cases if you understand the inner working of your application there are plenty of useful configuration options to tune to get the best out of your scan.

It's strongly recommend that you read through this section and understand what each setting does before experimenting with any changes to the default configuration.

Web Application Scanning

Web application scanning is performed using a multi-phase approach in which the scan hubs:

1. Perform a discovery phase to determine the extent of the application footprint/attack surface via a combination of methods such as crawling (navigating through links from the main page), brute force discovery (guessing paths/URLs), examining files such as sitemap.xml, and others.
2. Perform an active phase of requests bearing attack payload to test discovered URLs for vulnerabilities such as Injection flaws.

Web Application Scan Options

This section contains tweaks and changes to the application scanner, there are many advanced options located in here many of them can have a direct impact on the time it takes to run a scan but could mean you are missing vulnerabilities by skipping important checks.

Web Application Scanner Settings

Enable Web Application Scanner☒

Allows the web application vulnerability scanning component of the scan to be enabled/disabled. You might disable this if you just want to run an infrastructure scan.

Scan Forms☐

Note, though recommended for finding vulnerabilities, scanning forms may cause disruption (e.g. generating contact email or application content).

Avoid Contact Forms☐

The scanner will try and avoid submitting data to contact forms.

Scanner Profile

Default

Enable the web application scanner

This will enable or disable the web application scanner, it will automatically re-enable if a web application is entered into the target field and has to be manually disabled again if it's not desired to run.

Scan Forms

This option enables scanning of forms and is recommended for best scan coverage.

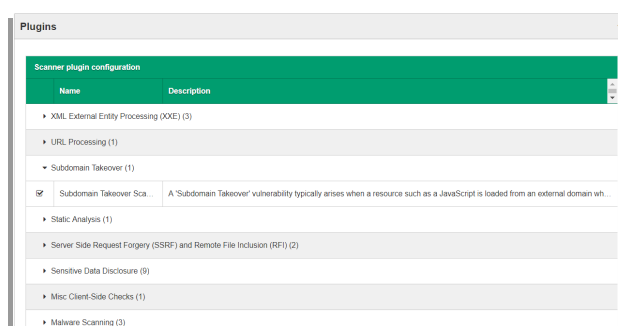
Avoid Contact Forms

This option is for users that wish to scan forms in production but are worried about the effect it could have on their contact forms if they have the inability to drop contact form submissions that match a given pattern. When AppCheck is testing an application, it needs to be able to submit payloads to forms and observe the responses it receives in order to decide if a given control is vulnerable. This includes contact forms, by checking this option AppCheck will drop any target that appears to be a contact form, however it is strongly recommend you implement controls around contact form emails to be able to fully test these.

Web Application Scan Plugins

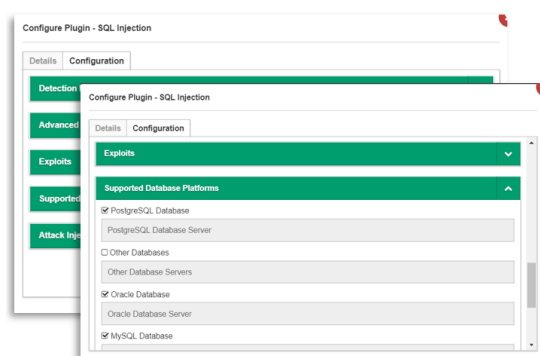
Expanding the *Plugins* menu under *Web Application Settings* allows you to configure each web application assessment module.

Plugins are grouped into categories and can be enabled and disabled by selecting the checkbox positioned at the side of each individual plugin.



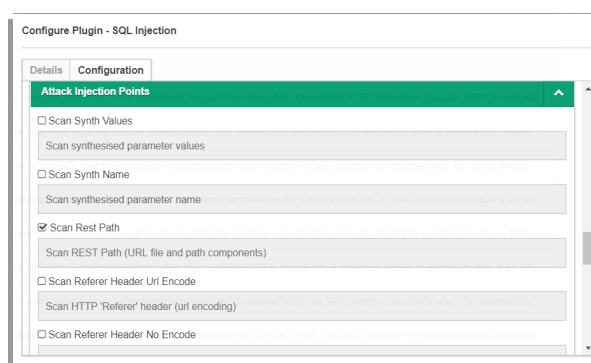
Each plugin has options unique to the specific test. Clicking on each plugin will open the configuration window and allow granular customisation of how each test is conducted.

Selecting a scan template such as “Standard Scan” or “Penetration Test” configures each of these options automatically. When selecting “New Scan Advanced” the default options are aligned to Standard Scan.



All plugins include a “Attack Injection Points” option which defines which portions of the HTTP request should be tested.

The values configured within this option have been set to their optimal values based upon the plugin and scan template chosen. However, advanced users may wish to alter configuration to suit their needs.



Authenticated Web Application Scanning

Some applications have special areas or functionality that are only available to users once they have authenticated, AppCheck is able to scan these types of applications by authenticating itself as a user and then scanning behind the authentication barrier.

Authenticated scanning is intelligent and is able to handle HTML-based login forms as well as BASIC authentication when encountered.

Authenticated Scanning ▼

Username

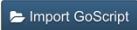
Password

☐ Show password

Login URL

OPTIONAL: Direct the scanner to use a particular login URL. This may fall outside of the scanning scope and is mainly useful for single-sign-on authentication.

GoScript



Complex authentication steps may be defined here using a simple GoScript - contact your consultant for advice if you think this beta option may be useful. See the tip panel on the right for an example.

Access Granted Keywords

Overrides the default Access Granted Keywords

Access Denied Keywords

Overrides the default Access Denied Keywords

Username, Password, Login URL

These are the minimum details that AppCheck requires to be able to authenticate with an application, in the vast majority of cases this is all you need and the mechanism should be smart enough to successfully authenticate in most cases.

Access Granted / Denied Keywords

AppCheck uses a combination of keyword detection and content variance to decide if authentication was successful, however these are not always 100% successful at establishing if that is the case. In these fields you can provide AppCheck with additional keywords that can be used as hints on the page to enable it to determine the authentication state.

NTLM Authentication

A Microsoft implementation of HTTP Basic authentication, usually only seen on IIS servers and is usually tied to internal LDAP account.

NTLM Authentication

NTLM Username

NTLM Password

☐ Show password

NTLM Login URL

OPTIONAL: Direct the scanner to use a particular login URL.

GoScript Authentication

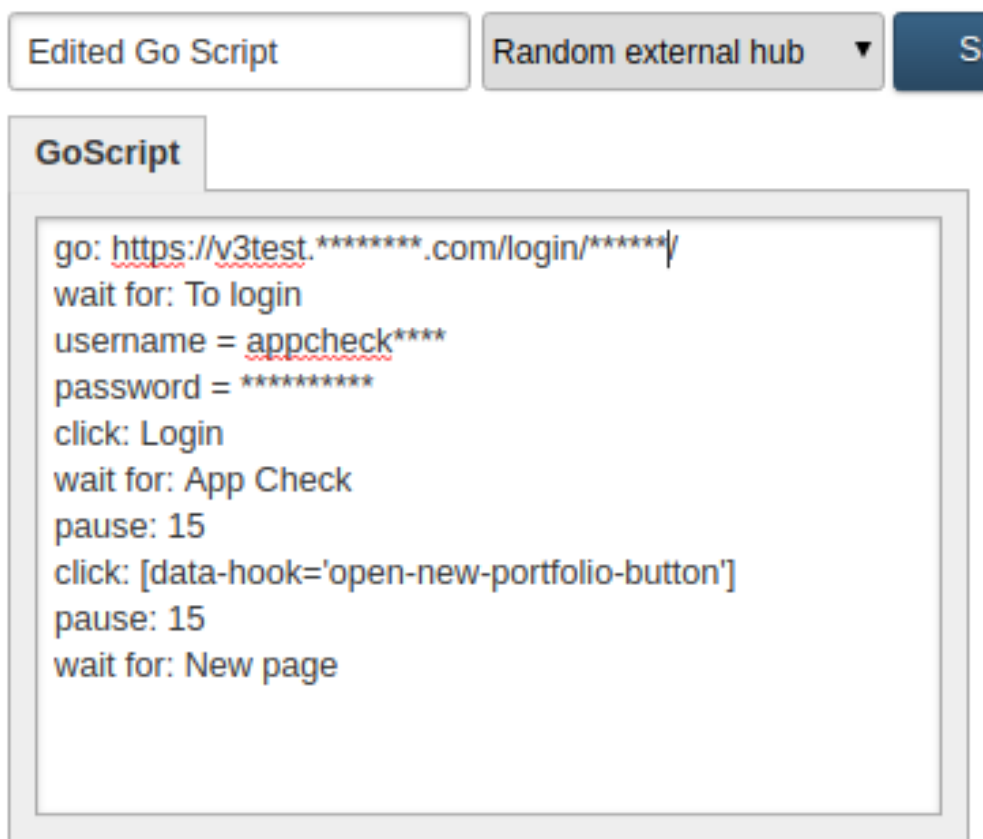
Users can also use GoScript for authenticating applications with a more complex authentication flow requiring multiple steps or other complications. Please see the separate GoScript section of this guide for more information on syntax and usage.

GoScript Journey Navigation

Sometimes you may want to test a web application that contains a form consisting of two or more “steps” that a customer must journey through, for example completing multiple sections of a form across different pages, with access to the second or third pages being restricted until valid input is entered into each of the preceding form fields.

It is difficult for an automated scanner such as AppCheck to always determine what constitutes valid input for early form fields that may allow it to progress through the form to a second or later page.

GoScript is AppCheck’s scripting language for navigating applications that require this kind of complexity, using five simple syntax commands. Please see the separate GoScript section of this guide for more information on syntax and usage.



Web API Scanning

Many web services are designed for automated computer to computer interaction as opposed to the human-readable web applications or web portals. These are generally provided via an Application Programming Interface (API) and AppCheck has been developed to be able to scan these too.

Presently AppCheck web application scanning supports the following API types:

- SOAP (Simple Object Access Protocol) XML APIs, preferably specified via WSDL (Web Service Description Language) files
- REST APIs, preferably specified via Swagger/OpenAPI specification files (JSON/YAML)

API Scanning ▼

Enable WSDL Discovery ☐

Used for discovering WSDL (Web Service Description Language) files

Access is supported via API access keys or Basic authentication headers.

Advanced WebApp Scan Settings

AppCheck has a number of advanced settings that can alter the depth of the scan taking place, tweaking these can either cut or extend the time it takes to scan an application. Disabling some of these options however can mean that you are not getting the coverage your application requires leading to missed vulnerabilities.

Scan HTTP and HTTPS

This option tells AppCheck to scan an application with HTTP and HTTPS as a single target, this is common for most modern applications and there are really only a few rare set of circumstances where this should be disabled. The most common case being that the HTTP and the HTTPS services serve up different applications.

Active Scan

Active scanning is when AppCheck is sending payloads to an application to actively see how it responds to evaluate it for vulnerabilities. This is in contrast to other phases of scanning which are all passive, this means that AppCheck isn't sending any payloads to the application and it is simply collecting information passively, for example software versions and checking for this existence of known vulnerable software.

Max Threads

By default, AppCheck runs 10 scanner threads, this is the maximum number of concurrent connections the scanner will have to your application throughout the scan. We have found this number to be optimal for the vast majority of applications, however if you are experiencing issues with the level of traffic to your application while scanning with AppCheck then this number can be reduced down to 1 concurrent connection.

Info:

While turning down the number of threads reduces the amount of traffic and server load that your application has to deal with, it also increases scanning time. It's recommended to only turn these settings down if this is causing disruption to your services.

Concurrency Level

This controls the number of scan processes to run for this scan, by default AppCheck runs a single process with the above specified number of threads. By increasing the concurrency level, you increase the number of process's that are running. It is useful to increase the concurrency when you have a lot of applications to scan at once as it can reduce the time it takes to complete these types of scan.

Info:

This is an advanced feature of AppCheck and due to the additional resource requirements for running these types of scans the feature is hidden by default. If you have a use case for this then speak to your account manager about getting it enabled.

Group URLs

Usually when a scan is conducted within AppCheck each target in scope is processed and scanned in sequence as this is the expected end user behaviour. However in some cases the targets provided are co-dependant or share functionality in some way, in this case it's useful to group these targets together as a single logical application. This means that a route to a vulnerable resource discovered in an application that refers to another application within scope that otherwise was uncrawlable or undetectable can be successfully uncovered and exploited.

Brute Force Discovery

Warning:

While this option can drastically decrease scan time on scans with multiple targets, it will not help against singular targets. Great care should also be taken when enabling this option to fully understand your infrastructure as while scan time can potentially be reduced, it can have a detrimental effect on your service if the load is not correctly spread across your servers.

This option enables the forced discovery of paths that may not be crawlable within the application, this usually covers things like hidden admin interfaces and other potentially sensitive resources that may not be well protected and could be insecure. Disabling this can potentially decrease scan time as resources are no longer being wasted on paths that don't exist however it also means potentially missing serious security flaws.

Password Guessing List

AppCheck maintains a list of approximately 10,000 common passwords as seen during manual penetration testing engagements, these have a high probability of occurring in the wild when we attempt to perform brute-force checks against an application. From time to time however an organisation may have a specific set of passwords that are used internally or during the development life-cycle that were not meant to make it out into production. In this field you can include additional passwords for AppCheck to attempt to brute-force and feedback on.

DOM-XSS Checks

This setting controls the use of real browsers to detect and confirm XSS vulnerabilities, disabling this option can result in faster scan times but will miss this class of vulnerability.

Scan REST Paths

Many modern web applications use the application path as a means to pass predictable structured variables to the application, skipping this check will result in a quicker scan time but will miss vulnerabilities in these predictable paths.

Scan Parameter Names

This setting instructs AppCheck to attack parameter names as well as values in the search for vulnerabilities, examples of this would be the parameter name maps to a database column name that is injected into a query without filtering. Disabling this option will decrease scan time but will miss these vulnerabilities.

Seeded Targets

This is an advanced scanner option and is used to guarantee that a target makes it into the attack phase of a scan. This can be useful when just wanting to quickly confirm a target is free of vulnerabilities or when a target cannot actually be reached by the crawler. For example, you could enter <http://www.example.com/hard/target/?1=1> and this would seed the scanner so that this target will make it into the attack phase of the scan.

Cyber Essentials Checks

This option enables some extended checks aimed at helping organisations perform additional checks to tighten up prior to going for cyber essentials, these checks include additional password credential checks against any login portals discovered during the scan as well as additional information in the results geared towards remediating issues that would be flagged as cyber essentials failures.

Scan Only GoScripts / GoScript

Enabling this option tells AppCheck to disable it's crawling engines and only attack content discovered from GoScript workflows. This is useful if there is only a requirement to scan a very specific workflow in an application and not the whole application.

The script required for the workflow can be populated below or loaded from an existing GoScript already saved and tested within the [GoScript view](#).

HTTP Headers

This is an advanced section and controls if AppCheck is to attack the headers sent in application requests. Sometimes headers can be missed out from being validated correctly as the developer didn't expect them to be abused in the same way as other parameters that are user controllable within the browser are. The downside to these increased header checks are the increased scan time required to iterate these.

HTTP Headers ▼

Referrer ☐

Include the referrer in the list of testable headers

Cookie ☐

Include the cookie in the list of testable header

User Agent ☐

Include the user-agent string in the list of testable header

All others ☐

Test all possible HTTP headers

Custom HTTP Headers

Add custom HTTP headers here to be used in all scanner requests, one per line, in the same style as in an HTTP request. Note, a header declared here will *overwrite* that header if already in a request.
For example...
Referer: http://www.example.com (will override)
Custom-View: secret (custom will be included in every request)

Referrer

This option tells AppCheck to attack the referrer header with payloads while actively scanning.

Cookie

This option tells AppCheck to attack cookie keys and values with payloads while actively scanning as well as the cookie header it's self.

User Agent

This is a common one to be overlooked in basic analytics tracking, this option enables the user agent to be attacked with payloads during the attack phase of scanning.

All Others

Send payloads to all headers during the attack phase of a scan.

Custom HTTP Headers

This option allows you to enter in custom headers that will be used when sending each request to the target application. These headers will override the default headers used by AppCheck in all requests apart from when that header is being attacked. Custom headers are used for a variety of reasons most often is to identify AppCheck to an application or for authentication.

Dev Settings

These options are usually hidden and are normally only exposed to enable experimental features within AppCheck which we feel may be of benefit when scanning your application. Documentation for these isn't typically available as they are subject to change and are documented once promoted into the main scanner configuration, if you have development options exposed in your scan settings it will have followed a call with technical support and the required feature will have been explained then.

Infrastructure Scanning

The infrastructure scanning settings permit the configuration of the infrastructure scanning portion of the test. Infrastructure scanning is generally **passive** in that it performs port scans and makes requests to a range of ports, without an attack payload, looking for information returned in the returned data or metadata signature that indicates versions of operating system and applications that may be vulnerable based on known published vulnerabilities (CVEs).

Infrastructure Scanner Settings

Run infrastructure scanner first

☐

Run the infrastructure scan first i.e. before the web application scan.

Vulnerability Scanner

Enable vulnerability scanner

☒

Allows the vulnerability scanning component of the scan to be enabled/disabled. You might disable this if you just want a quick port scan.

Port Scanner

Infrastructure Scanning Options

Run infrastructure scanner first

By default, AppCheck will run the application scanner before the infrastructure scanner. While the infrastructure scanner is faster to run than the application scanner, if we haven't been whitelisted correctly on a firewall it does have a tendency to cause the scan hub to be blocked when the port scan runs and starts looking for vulnerable services. If AppCheck is correctly whitelisted it can be useful to enable the infrastructure scanner to run first to be able to get feedback on vulnerabilities early into a scan.

Vulnerability Scanner Settings

For scanning from the public scanning hubs there is only the option to enable or disable the vulnerability scanner; for internal hub customers there are more options exposed here. This is because outside the firewall the number of applications exposed is typically much more limited when compared to the internal environment where a greater range of checks are required. These additional options are documented in the internal hub documentation.

Credentialed Infrastructure Scanning

Credentialed Infrastructure Scanning is one of the options only exposed for scans configured to use internal scan hubs.

AppCheck is able to perform credentialed infrastructure scanning to access a host via SSH (Linux, Unix, MacOS X) or SMB/WMI (Windows) and check for vulnerabilities that cannot be determined from scanning a host remotely across the network, i.e. missing patches. The effectiveness of the tests are dependent upon the user permissions of the account being used, with an admin account preferable.

Scanning via a Domain Account is possible, and a separate guide for this is available in our online knowledgebase at <https://appcheck.zendesk.com/hc/en-us/articles/360011113914-Credentialed-Infrastructure-Scanning>

Port Scanning

The port scanner is a light weight wrapper around nmap and runs independently of the infrastructure scanner to provide parity. It's configured by default to get good results in most situations, and can be configured to run more or less checks. It is important however that you understand the options selected before starting a scan as some things can drastically increase the time it takes to run a port scan.

Enabled

Enables or disables the port scanner from running

Rapid host discovery

Uses ICMP ping packets to detect if a host is live or not, this is a quick way to discover a host however a large number of firewalls will block these packets by default which results in the host registering as down. Enable this if you know these packets will make it through your firewall.

Dead host detection

This is used to detect if a host is down and report on it in the scan results, this involves using a number of timeouts to confirm the host is truly unavailable. This increases scan time as the port scanner has to start with the assumption that every host is up and cannot rely on the host discovery.

Ports to scan

The default option here is the 1,000 most common service ports, other options include the 10 and 100 most common going up to the most populate 10,000 and all 65,536 ports. In most cases the 1,000 and 10,000 most common ports are sufficient and all 65,536 should only be scanned if trying to confirm a change on an obscure port.

Additional ports to scan (TCP)

If not scanning the full 65,536 port range then you can elect to scan additional obscure ports here and they will be included in with the above selected range.

UDP Scan

By default, AppCheck only checks TCP ports, UDP port scanning can be enabled with this option however there are a few things to be taken into consideration before enabling this option.

- Unlike TCP, UDP is stateless.
- This means unlike TCP there is no connected and disconnected state and there isn't even a guarantee of reply following sending a packet to a service.
- Services can only be detected by the request timing out.
This means that to detect a UDP service you have to timeout the response from the server following sending a packet and repeat that a couple of times in case the packet was lost. All this means it can take considerably more time to detect a UDP service over a TCP service multiplied by the number of ports being scanned.

Combine the above with the dead hosts detection and a moderate size IP range and a scan that could have taken minutes can take days. UDP applications and services are typically things like VoIP and live streaming video where the loss of a single packet is irrelevant to the overall flow of content and re-transmission is more expensive than just forgetting about it.

Additional Ports to scan (UDP)

Same as the above TCP option apart from it adds ports to the UDP scan scope.

Port Scan Depth

This controls the level of fingerprinting the port scanner goes into once a port has been identified to be open, the options are as follows.

- Discover ports only
This option will only check for open ports and will assume these are running the service that's typically meant to be running on that port
- Discover ports and service details
This option discovers ports as above and then attempts to fingerprint the service running on that port, this is useful to identify services that are running on a none standard port.
- Discover ports and service details with OS fingerprinting
Does the above and also attempts to identify the underlying OS at the same time, it will present back a list of possible OS's with a probability for each.

Port scan timings

This option controls how long to wait for a response before assuming the port is dead and moving on, longer timings should lead to more accurate results but the scan will take longer to complete. More aggressive timings will mean a scan completes faster but there is a chance of missing some services if no response is received in time.

TCP Scan method

There is a choice here between half open SYN scanning and performing a full TCP connect. In most cases a SYN scan should be fine however some firewalls block or purposefully do not respond to these packets in which case a full TCP connection is required to confirm that a port is open. Full TCP handshakes take longer than SYN packets so using this option will increase scan time.

Scanning Window Settings

The scanning window controls when a **running** scan is permitted to run, automatically pausing and resuming a scan as it exits and enters the scanning window. Multiple scanning windows can be in effect to meet complex scheduling requirements and times are permitted to wrap, so 12:00 to 09:00 will wrap to the following day.

Scanning Window Settings ▼

Permitted Scanning Times
Add Schedule+

Start

End

9 : 0

17 : 0

Days

Sun	Mon	Tue	Wed	Thu	Fri	Sat
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

remove✕

Scheduled times can be used to set windows to control at what times the scanner will run, for example 09:00 AM to 17:30 PM Monday to Friday and 00:00 AM to 00:00 AM Saturday and Sunday Note: Changing the schedule on a already running scan will not take effect until the scan is next run.

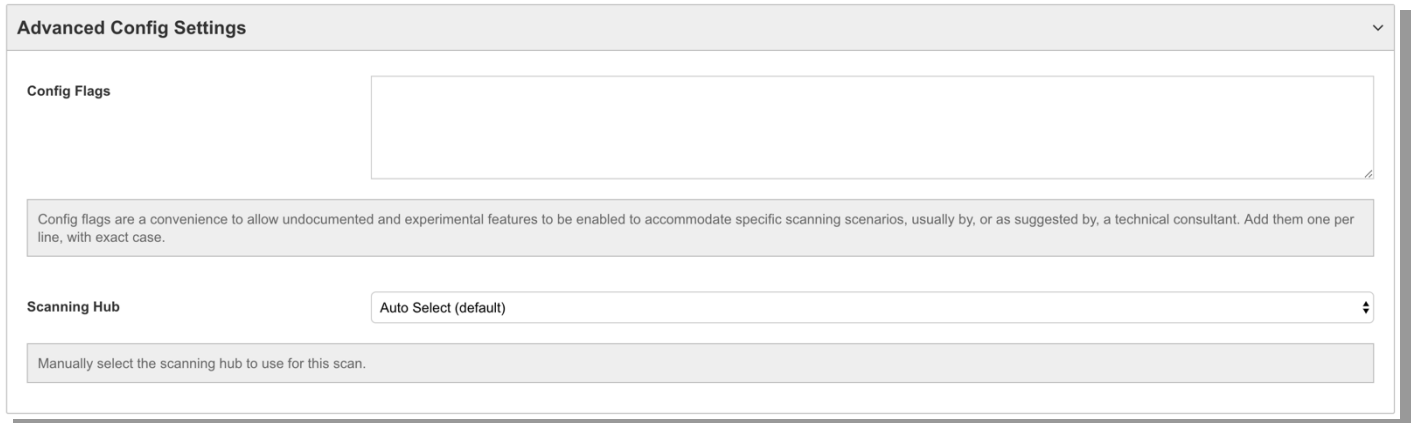
Warning:

Scanning windows will not automatically start a scan you will need to set a **Scheduled Start Date** as described in the basic scan settings. A schedule will also not automatically resume a scan that has been manually paused, giving the end user control over the schedule window.

Scans can be paused for a maximum of 14 days, after this period the scan is automatically aborted.

Advanced Scan Configuration

Advanced optimisation options are available within here which allow behavioural or special features to be used by the scanner.



The screenshot shows the 'Advanced Config Settings' window. It has a title bar with a close button. Inside, there's a 'Config Flags' section with a large text area for input. Below this is a grey box with explanatory text: 'Config flags are a convenience to allow undocumented and experimental features to be enabled to accommodate specific scanning scenarios, usually by, or as suggested by, a technical consultant. Add them one per line, with exact case.' Below that is a 'Scanning Hub' section with a dropdown menu currently set to 'Auto Select (default)'. At the bottom is another grey box with text: 'Manually select the scanning hub to use for this scan.'

Config Flags

These are special flags that can be passed to the scanner, which enable or disable features within the scanner some of the most useful flags are documented below.

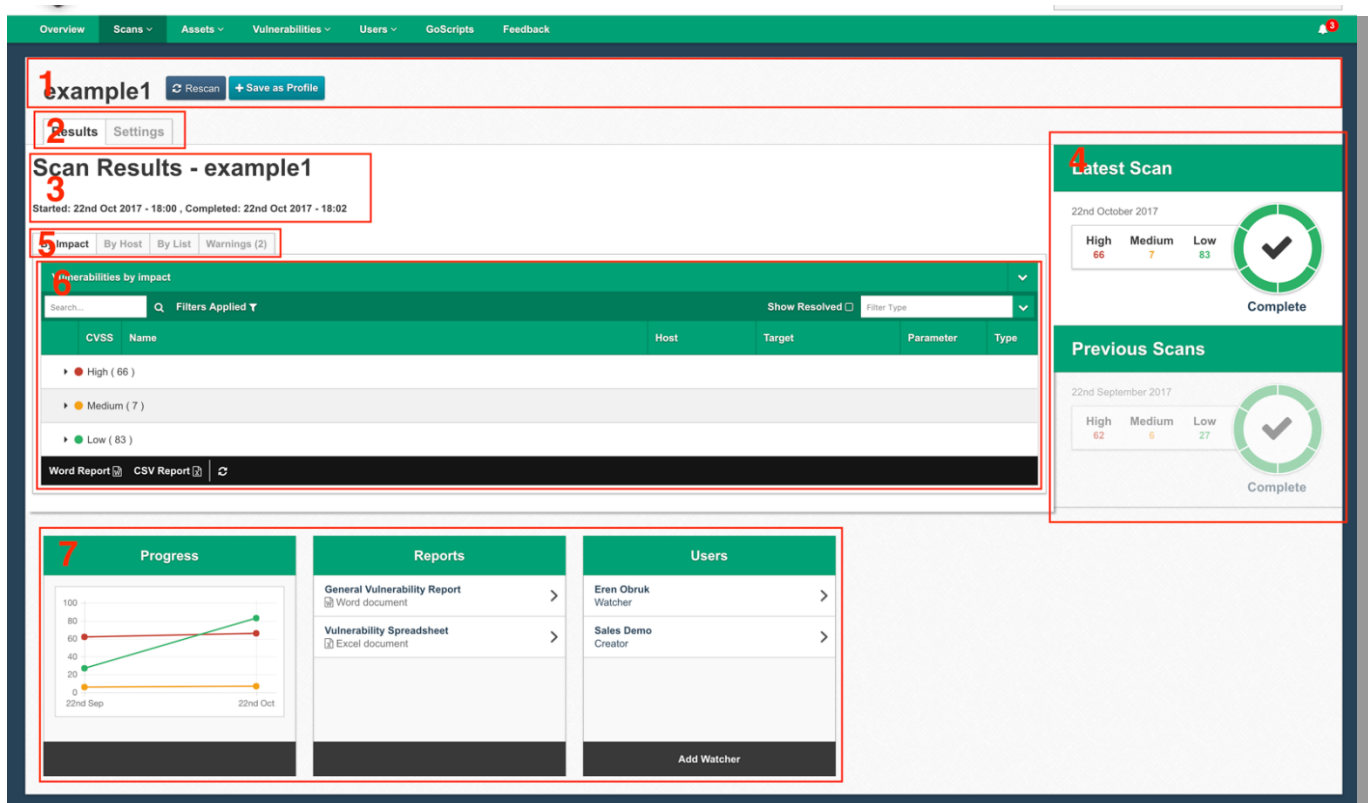
- **low_hanging_vulns**
This config flag prevents the scanner from running a discovery phase of the scan. So the attack surface can only be determined through crawling and no hidden content will be discovered. The crawl time is also limited which drastically reduces the potential attack surface of a scan. During the attack phase the scanner only looks for common cases of vulnerabilities and does not go through edge cases.
- **!phased**
Runs all the plugins at once as opposed to in distinct phases, can mean early results faster as targets are being attacked at the same time they are being crawled.
- **global_auth**
Allows the scanner to deal with a double layer authentication barrier, where an application is protected by basic auth and then a application level authentication barrier.

Scanning Hub

AppCheck will at the time of scheduling select the best hub for the present scan config based on resources available and if the scope appears to be internal or external, however in some instances the user may want to instruct AppCheck on which hub to use, such as forcing an external target to be run from an internal hub or to use a hub that has experimental features available. This option allows the user to be more selective about where a scan is to run, if available the user can select from any public hub, when used in conjunction with an internal hub option scans between public and private hubs where available.

Scan Results

The scan results pages are available from when a scan starts running, these contain the latest and previous results of all scans run with the current scan configurations settings. Within here are tools useful for vulnerability management which is covered later in this document as well as an overview on remediation progress and access to scan reports.



- (1) Header Controls
Contains the scan configuration name and action buttons
 - o Start Scan / Rescan
 - o Pause
 - o Resume
 - o Abort
 - o Save as Profile
- (2) View Tabs
Switch the current view between the results for this scan and the settings this scan was configured with.
- (3) Scan name and duration
The name of the scan and information about the duration of the scan.
- (4) Previous scan results
Past runs of this scan configuration, as well as a summary of the results and the end status of the scan.
- (5) Results view tabs
Used to switch the vulnerability results view to different overviews for managing vulnerabilities.
- (6) Current vulnerability view

The current vulnerability management view, more details on this in the managing vulnerabilities section.

- 7) Report controls
Reporting controls showing an overview on remediation of this scan configuration, report download buttons and who is watching this scan and will receive status updates.

Scan Report Groups

Scan report groups allow you to take the results of multiple scan configurations and group them together as a single logical group for the purpose of reporting and vulnerability management.

Scan Report Groups + New Group				
<input type="text" value="Search..."/> Q				
Created	Group Name	User	Tags	Actions
31/08/2016 09:46	Example Group	Moqueed N		Edit Delete
06/09/2016 09:16	New Report Group	Sales Demo		Edit Delete
03/08/2017 11:36		Sales Demo		Edit Delete
17/08/2017 15:42	Fake Group scans	Sales Demo		Edit Delete
17/08/2017 15:57		Sales Demo		Edit Delete
<div> ⏪ ⏩ Limit 10 Page 1 of 1 ⏴ ⏵ 🔄 </div> <div>Showing 1 to 5 of 5 records</div>				

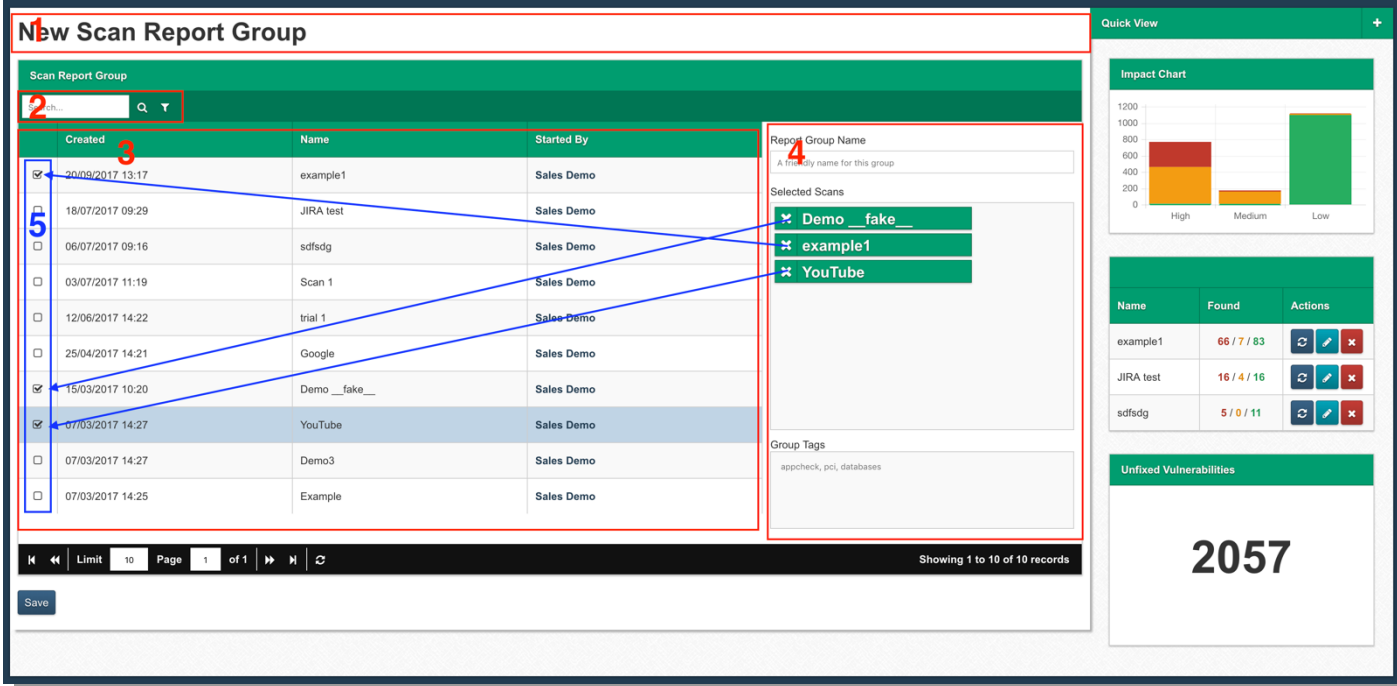
The interface is a fairly straight forward table management, with options to create a new report group, edit a report group, view results and delete a report group.

Info:

Deleting a report group will not remove scan configurations or vulnerabilities so you are free to experiment here and can create multiple overviews incorporating the same scan configurations.

New Group / Edit Group

This view controls the creation and editing of report groups, this interface is fairly straight forward presenting an editor of all the scans configurations that have been run to date, you can then allocate a name to the result group and select which scans are included for easy searching.



The screenshot shows the 'New Scan Report Group' interface. It includes a search bar (2), a table of scan configurations (3) with checkboxes (5), a form for the report group name (4), and a sidebar with an impact chart, a table of found vulnerabilities, and a total count of 2057 unfixed vulnerabilities.

Created	Name	Started By
20/09/2017 13:17	example1	Sales Demo
18/07/2017 09:29	JIRA test	Sales Demo
06/07/2017 09:16	sdfsdg	Sales Demo
03/07/2017 11:19	Scan 1	Sales Demo
12/06/2017 14:22	trial 1	Sales Demo
25/04/2017 14:21	Google	Sales Demo
15/03/2017 10:20	Demo __fake__	Sales Demo
07/03/2017 14:27	YouTube	Sales Demo
07/03/2017 14:27	Demo3	Sales Demo
07/03/2017 14:25	Example	Sales Demo

Name	Found	Actions
example1	66 / 7 / 83	[Refresh] [Edit] [Delete]
JIRA test	16 / 4 / 16	[Refresh] [Edit] [Delete]
sdfsdg	5 / 0 / 11	[Refresh] [Edit] [Delete]

- (1) Title Section
- (2) Scan configuration search and filter controls
- (3) List of scan configurations
All scan configurations run to date
- (4) Entry form
Edits the scan configurations included in the group.
- (5) Scan check boxes
This is linked to the scan edit form and is bi-directional

Report Group Name

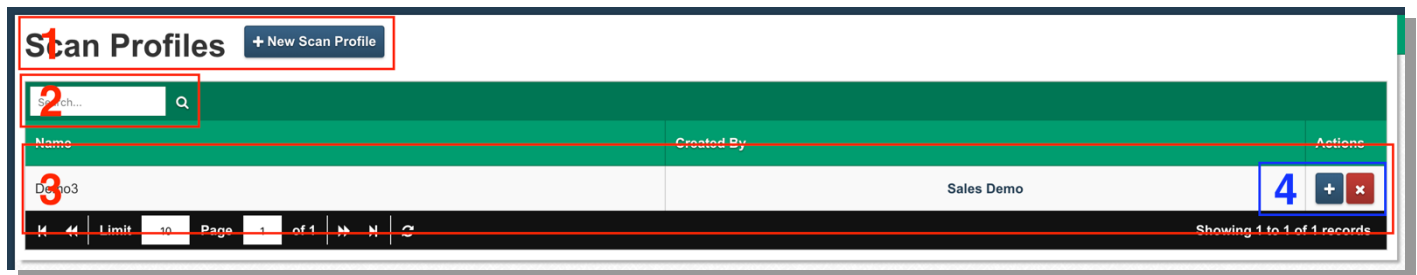
The name to be used to identify this report group, try and enter a name that is unique for this report group so it's easy to identify later.

Selected Scans

This shows an overview of the scans that have been presently selected, removing these will uncheck the scans in the scan configurations list to the left.

Scan Profiles

Scan profiles are a means to be able to apply a preselected series of settings to a number of scan configurations, the settings for profiles is almost identical to that of the scan configurations apart from they are missing target and scheduling controls which are considered to be unique to a scan configuration.



- (1) Action header, New scan profile
- (2) Search bar
Search for existing scan profiles
- (3) Saved Profiles
List of scan profiles for the current search result, clicking on these will open the edit scan profile view.
- (4) Profile actions
 - o Apply Profile
Applies this scan profile to a new auto named scan configuration
 - o Delete Profile
Removes this scan profile, this action cannot be undone.

New Scan Profile / Edit Scan Profiles

The settings here are nearly identical to those in the new scan / edit scan view please refer to [this section](#) for details on available options.

Organisation Settings

The “Organisation Settings” tab contains a single field permitting you to add a notification URL:

Scan Finished (notification URL)
<input type="text"/>
<input type="button" value="Update"/>

If populated, then on scan completion, AppCheck will post a message to the notification URL. AppCheck sends scan notification emails by standard to all watchers configured on the scan, via email. However the notification URL feature permits the notification to be integrated into customer’s own monitoring or other solutions.

Vulnerabilities

Vulnerabilities are at the very heart of AppCheck and we pride ourselves on not only aiming to be at the forefront of vulnerability discovery and accuracy, but also in providing a leading vulnerability management platform.

Vulnerabilities within AppCheck are signed with a unique signature upon identification, this makes tracing them and avoiding duplication very simple. For instance, if an XSS vulnerability is picked up against a target in one scan and then is discovered again against the same target in another scan, then that becomes just another instance of the same vulnerability. This means that any workflow action to remediate that vulnerability will actually remediate it in both scans minimising the amount of administration required to stay on top of your discovered vulnerabilities.

The following sections describe vulnerability management, within AppCheck and presents you with a number of options of how this information can be viewed and managed.

Vulnerabilities broadly fall into two categories **Infrastructure** and **Application**. Infrastructure vulnerabilities are typically off the shelf vendor software with known vulnerabilities and resolution is typically updates and patches. Application vulnerabilities are unknown vulnerabilities and they require uncovering, resolution is typically custom code fixes.

Vulnerability Organisation

Vulnerabilities are generally managed in one of three places, each of these provides slight variations on how the vulnerability information is organised helping to provide a workflow that works for your organisation.

1. Within a scan configuration
2. Vulnerabilities menu
3. From within a report group

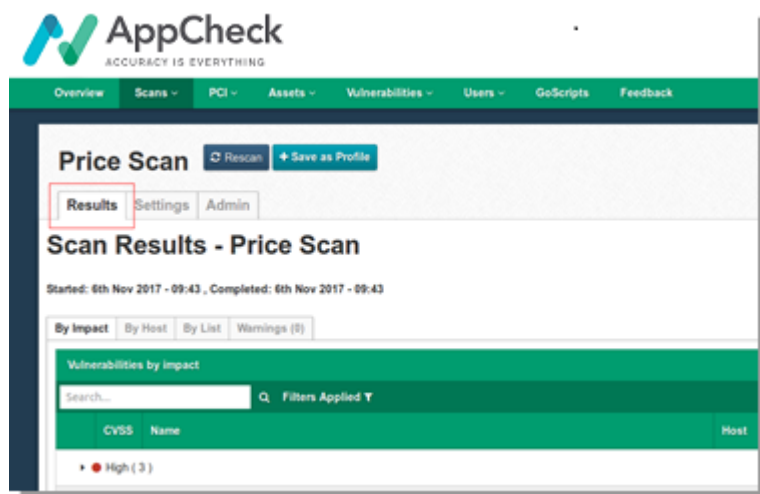
Vulnerabilities within a scan configuration

Clicking any row from the **All Scans / My Scans** menu should open up the scan results view, in here the latest vulnerabilities discovered in a scan and vulnerabilities discovered in previous runs of that scan configuration can be managed.

The scan results view

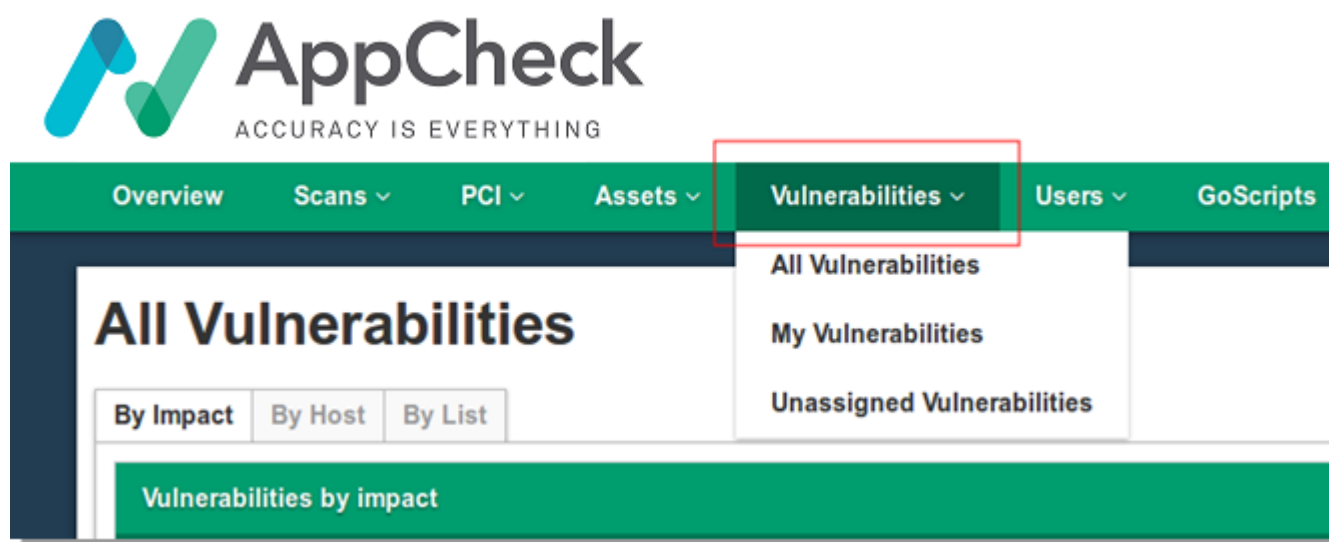
Upon entering the scan results view vulnerabilities are managed from the results tab which should be active by default.

For details on the other tabs and actions within the scan results view please see the **Scan Results** section of this [document](#).



All Vulnerabilities

The Vulnerabilities menu can be accessed via the top-level navigation bar, this presents a global view on vulnerabilities aggregated from all scan results. These lists exclude any duplication as mentioned previously in [this document](#) as vulnerabilities within AppCheck are uniquely signed.



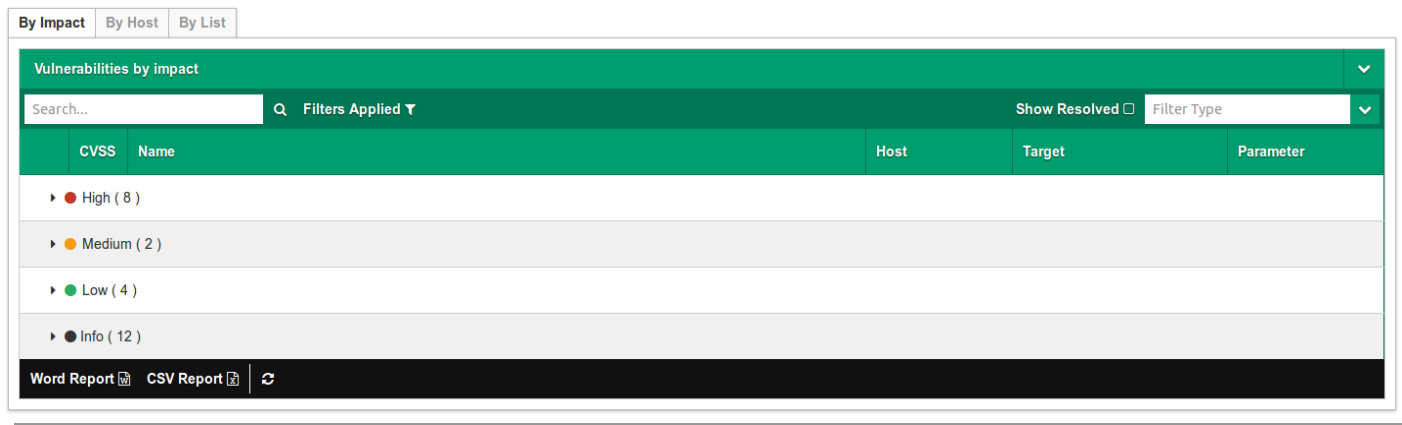
- All Vulnerabilities
Lists all vulnerabilities found across all scans run by your organisation
- My Vulnerabilities
Lists all vulnerabilities assigned to you.
- Unassigned Vulnerabilities
Lists all vulnerabilities not assigned to a user.

Report Groups Vulnerabilities

As documented in the **report groups** section of [this document](#), report groups are set up to provide an overview of multiple scan configurations and allows the vulnerabilities of these joint scans to be managed from there.

Vulnerability Management

Vulnerabilities are managed via the vulnerabilities tables, this component is replicated in all vulnerability management screens to provide a consistent means to manage vulnerabilities across all the available views.



CVSS	Name	Host	Target	Parameter
High (8)				
Medium (2)				
Low (4)				
Info (12)				

Word Report CSV Report

Vulnerability Table

The vulnerability table allows the user to search and filter a list of vulnerabilities and provides access to the vulnerability information screen and provides access to the vulnerability workflows. This information is presented as a series of common views which alters the organisation of vulnerabilities for easy viewing.

Vulnerability group tabs

By Impact

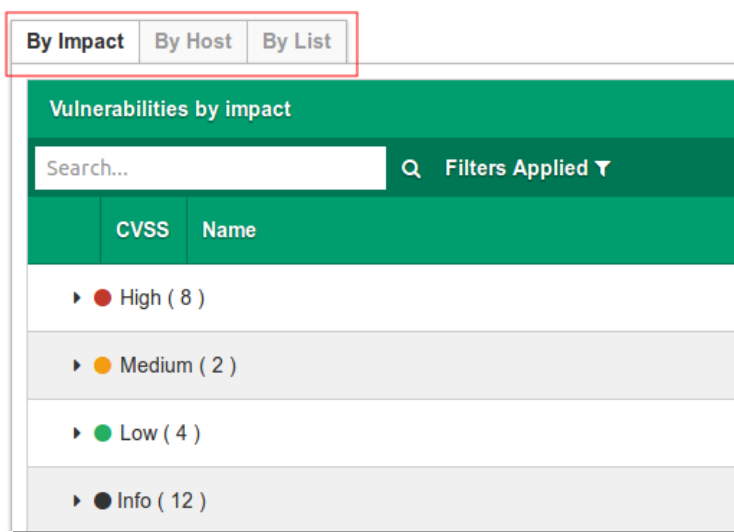
This view groups the vulnerabilities by the impact of threat they represent, **High**, **Medium**, **Low** and **Info**.

By Host

This view organises vulnerabilities by the host they were discovered on sorted by impact.

By List

This view lists all vulnerabilities in the present view, by default it's organised by impact but can be sorted and filtered.



CVSS	Name	Host	Target	Parameter
High (8)				
Medium (2)				
Low (4)				
Info (12)				

Word Report CSV Report

Data display

Depending upon the selected vulnerability grouping (see Vulnerability [group tabs](#)), vulnerabilities are displayed in a hierarchical manner leaf nodes being vulnerability entries. By default the groups are collapsed:

Vulnerabilities by impact		
<input type="text" value="Search..."/>		<input type="button" value="Q"/> Filters Applied <input type="button" value="T"/>
	CVSS	Name
▶ ● High (8)		

Expanding a group lists the vulnerability types and the number of instances found (shown in brackets).

▼ ● High (8)
▶ Server-Side Template Injection (1)
▶ Sentinel: XXE Injection Detected (1)
▶ Reflected Cross-site Scripting (JS Execution) (3)
▶ Reflected Cross-site Scripting (CONFIRMED) (1)
▶ Flash Cross Site Scripting via getURL (1)
▶ Flash Cross Site Scripting via ExternalInterface.call (1)

Further expansion of this will list the vulnerability entries, will present a table like view with similar layout and sorting to the vulnerabilities list view.

▼	CVSS	Name	Host	Target	Parameter
▼ ● High (8)					
▼ Server-Side Template Injection (1)					
<input type="checkbox"/>	8.3	● Server-Side Template Injection	localhost	/template_injection/server_si...	query.data

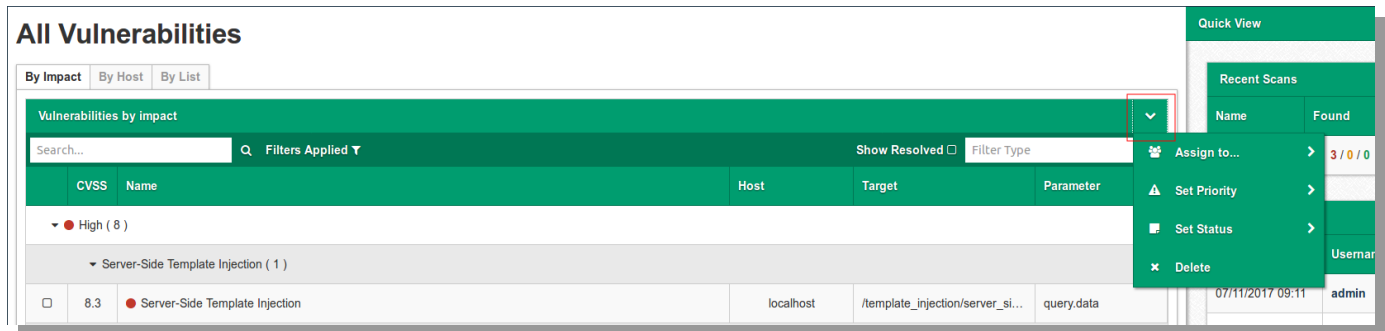
Data fields

Referring to the above image we have the following data fields:

- The first field is a checkbox used for bulk actions (see [Bulk actions](#)).
- CVSS: CVSS score for the vulnerability
- Name: name of the vulnerability with additional info in brackets ([see additional info](#))
- Host: Fully Qualified Domain Name (FQDN) or IP address where the vulnerability was found
- Target: URL path/port/service of the vulnerability
- Parameter: the vulnerable request parameter (if applicable)

Bulk actions

The bulk actions drop down menu provides a number of actions to apply across a number of selected vulnerabilities (selected via checkbox on first field).



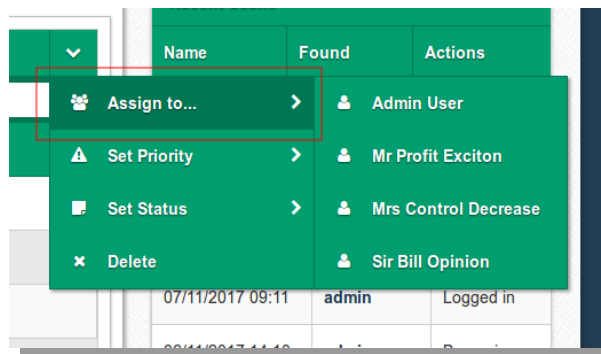
The screenshot shows the 'All Vulnerabilities' page with a table of vulnerabilities. A dropdown menu is open, showing the following actions:

- Assign to...
- Set Priority
- Set Status
- Delete

The table has columns: CVSS, Name, Host, Target, and Parameter. The first row shows a vulnerability with CVSS 8.3, Name 'Server-Side Template Injection', Host 'localhost', Target '/template_injection/server_si...', and Parameter 'query.data'.

Assign to

The "Assign to" action will assign selected vulnerabilities to the user selected in the "Assign to" sub-menu:



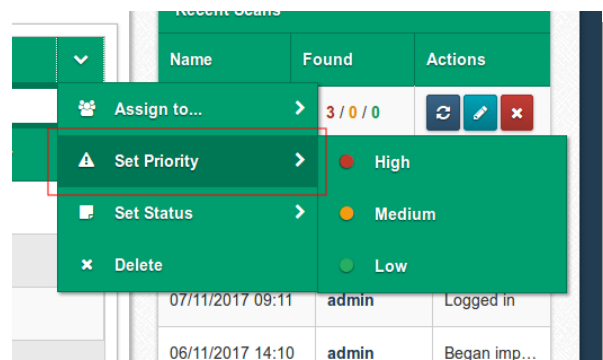
The screenshot shows the 'Assign to' sub-menu with the following options:

- Admin User
- Mr Profit Exciton
- Mrs Control Decrease
- Sir Bill Opinion

Set Priority

The "Set Priority" action will change the priority of the selected vulnerabilities to one of (accessed via its sub-menu), by default AppCheck will assign a priority that matches the impact of the vulnerability discovered.

- **High**
- **Medium**
- **Low**



The screenshot shows the 'Set Priority' sub-menu with the following options:

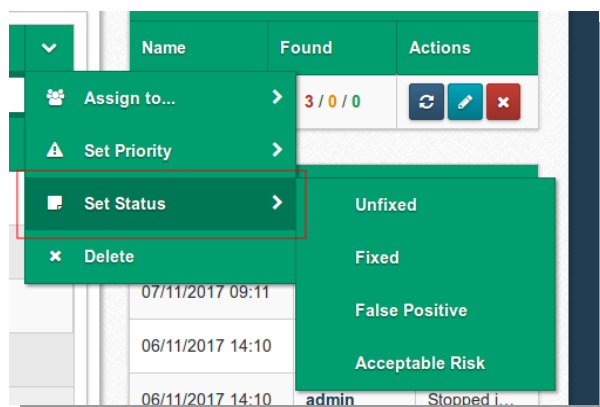
- High
- Medium
- Low

Set Status

The "Set Status" action will change the status of selected vulnerabilities to one of:

- Unfixed
- Fixed
- False Positive
- Acceptable risk

See [workflow](#) for more information.



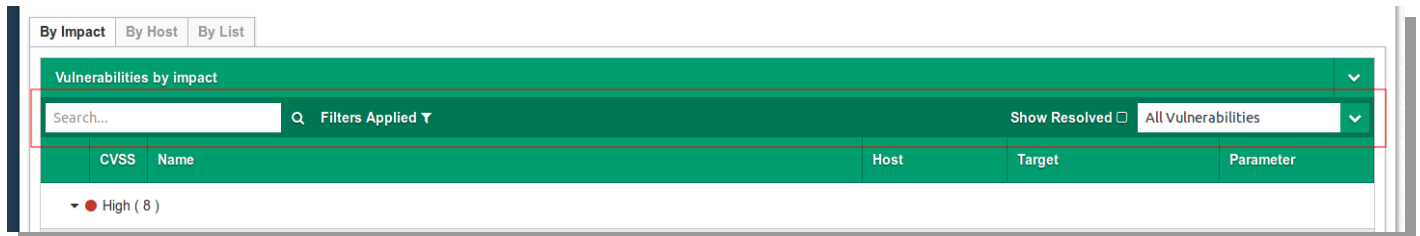
Delete

The "Delete" action will delete the selected vulnerabilities

Vulnerability search and filtering

The search and filter bar is useful for producing a list of vulnerabilities according to a set of criteria.

Search field

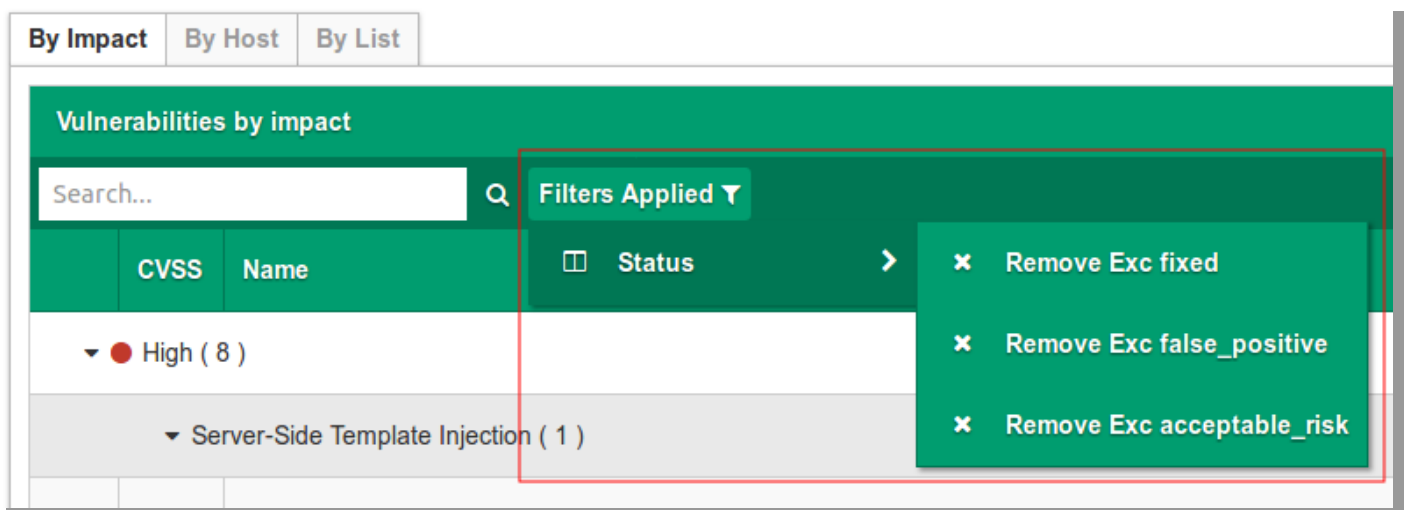


The search field will return a list of vulnerabilities where the search term is contained within the following fields for a vulnerability entry:

- Name
- Host
- Target
- Parameter

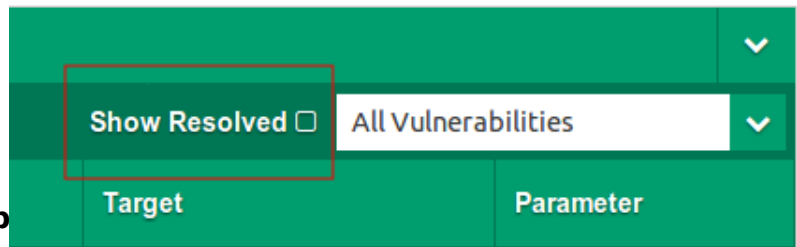
Filters Applied

Filters Applied displays the default list of filters applied to the list of vulnerabilities. These filters can be removed and in doing so will update the list of displayed vulnerabilities.



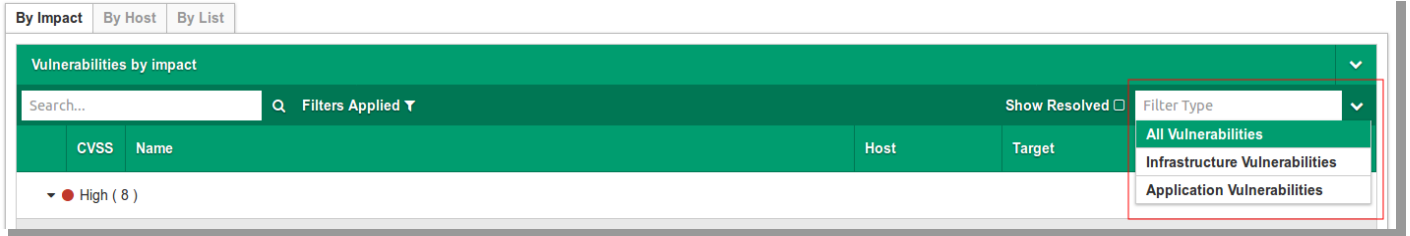
Show Resolved

Ticking this check-box will update the vulnerability list to display items marked as "resolved" (see [Vulnerability workflow](#))



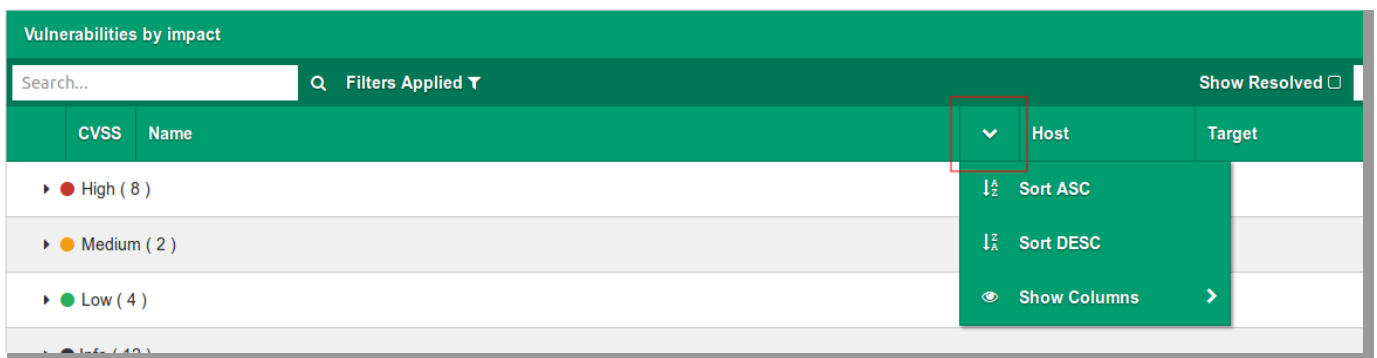
Infrastructure/application vulnerabilities

The infrastructure / application vulnerability drop-down menu will only display vulnerabilities for the selected type i.e. selecting "Application Vulnerabilities" will exclude infrastructure vulnerabilities from the displayed list.

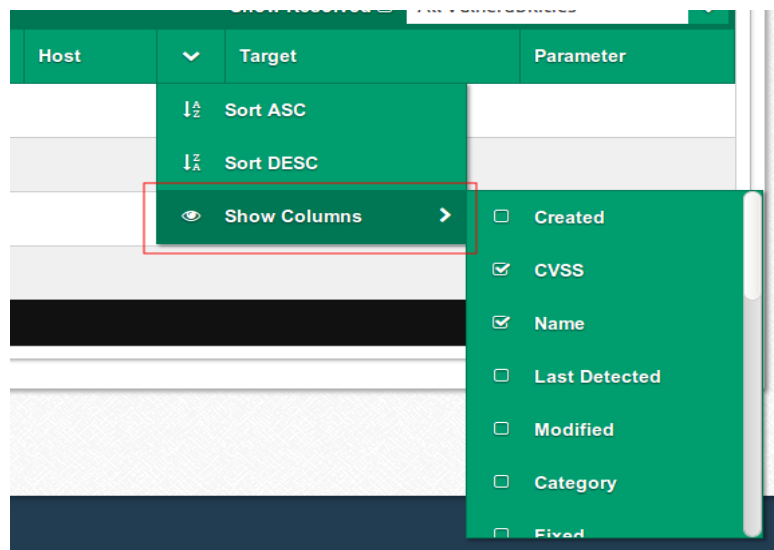


Column sorting

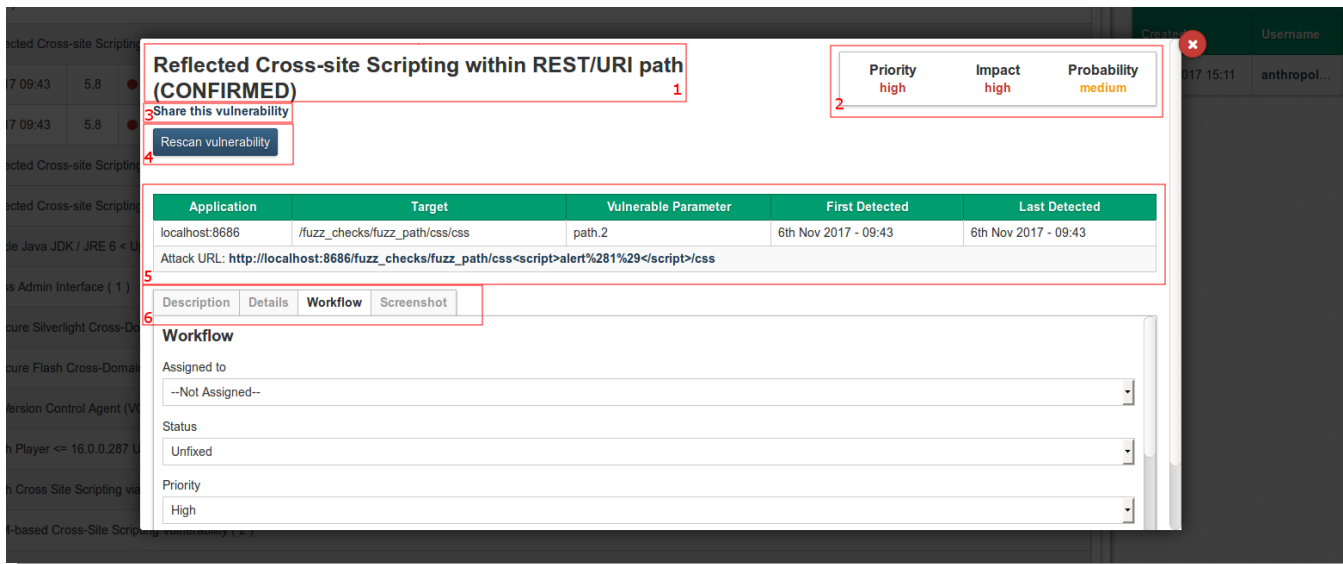
Selecting the drop down menu that appears on hovering over a column header will allow you to sort that column ascending or descending:



Additionally further columns can be displayed on the table by ticking the corresponding check-box in the "Show Columns" sub-menu:



Vulnerability information screen



Reflected Cross-site Scripting within REST/URI path (CONFIRMED)

Share this vulnerability | Rescan vulnerability

Application	Target	Vulnerable Parameter	First Detected	Last Detected
localhost:8686	/fuzz_checks/fuzz_path/css/css	path.2	6th Nov 2017 - 09:43	6th Nov 2017 - 09:43

Attack URL: `http://localhost:8686/fuzz_checks/fuzz_path/css<script>alert%281%29</script>/css`

Description | Details | **Workflow** | Screenshot

Workflow

Assigned to: --Not Assigned--

Status: Unfixed

Priority: High

Clicking an entry in the vulnerability table will display the vulnerability's information screen

This screen provides further information not displayed in the vulnerability listing table and provides additional access to a functionality i.e. adding notes to the vulnerability changing its status and assigning it to another user within the organisation.

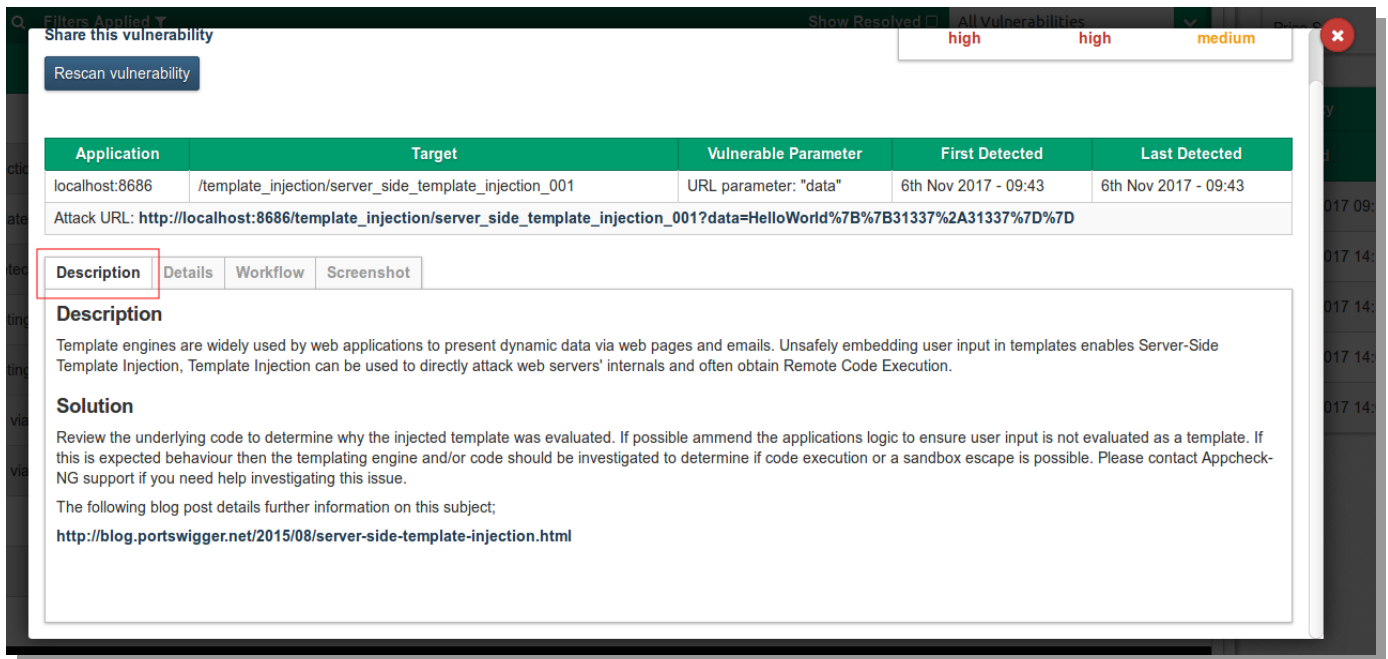
- (1) Vulnerability title
This is the title of the vulnerability, additional information may appear in brackets.
- (2) Severity
Displays the severity of the vulnerability, which is made up of the following attributes:
 - Priority
 - Impact
 - Probability
- (3) Share this vulnerability
This link provides a URL to a separate page containing the vulnerability's information.
- (4) Rescan vulnerability
This will start a new scan using only the AppCheck plugins that discovered the vulnerability. This option is only available for some vulnerabilities, at the time of writing it's mostly limited to application vulnerabilities.
- (5) Vulnerability details table
Application: Fully Qualified Domain Name (FQDN) or IP address where the vulnerability was found
 - Target: URL path/port/service of the vulnerability
 - Parameter: the vulnerable request parameter (if applicable)
 - First Detected: The date the vulnerability was first detected for the application
 - Last Detected: The date the vulnerability was last detected for the application i.e. on a rescan
 - Attack URL: The URL where the vulnerability was discovered and example payload.
- (6) Detail/Action tabs
These tabs group further information and functionality regarding the vulnerability, the following tabs will only display if applicable to the vulnerability:

- o Details
- o Screenshot

Description

The description may consist of two parts:

- Description: A general description of the vulnerability
- Solution (if applicable): Provides steps to mitigate the vulnerability



The screenshot displays the AppCheck interface for a vulnerability report. At the top, there are filters and a 'Rescan vulnerability' button. Below this is a table with columns: Application, Target, Vulnerable Parameter, First Detected, and Last Detected. The table shows a vulnerability on localhost:8686 targeting the path /template_injection/server_side_template_injection_001, with the vulnerable parameter being the URL parameter 'data'. The attack URL is provided as http://localhost:8686/template_injection/server_side_template_injection_001?data=HelloWorld%7B%7B31337%2A31337%7D%7D. Below the table, there are tabs for Description, Details, Workflow, and Screenshot. The 'Description' tab is selected, showing a detailed explanation of the vulnerability and a solution. The solution advises reviewing the underlying code to ensure user input is not evaluated as a template and provides a link to a blog post for further information.

Application	Target	Vulnerable Parameter	First Detected	Last Detected
localhost:8686	/template_injection/server_side_template_injection_001	URL parameter: "data"	6th Nov 2017 - 09:43	6th Nov 2017 - 09:43

Attack URL: http://localhost:8686/template_injection/server_side_template_injection_001?data=HelloWorld%7B%7B31337%2A31337%7D%7D

Description

Template engines are widely used by web applications to present dynamic data via web pages and emails. Unsafely embedding user input in templates enables Server-Side Template Injection. Template Injection can be used to directly attack web servers' internals and often obtain Remote Code Execution.

Solution

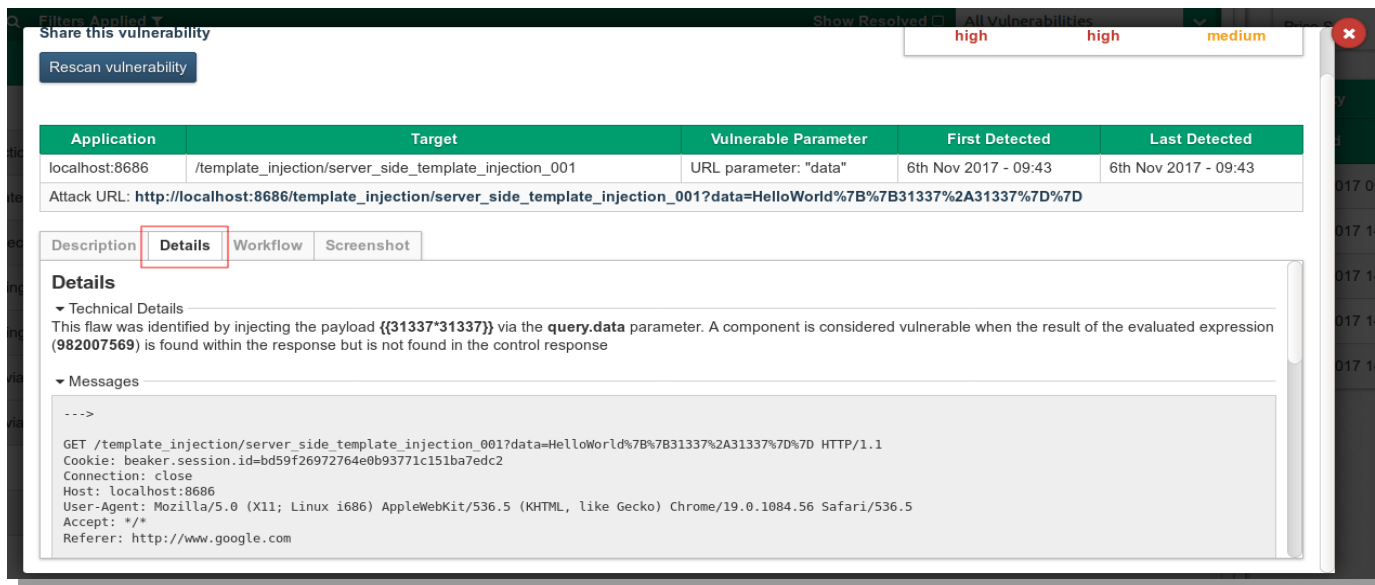
Review the underlying code to determine why the injected template was evaluated. If possible amend the applications logic to ensure user input is not evaluated as a template. If this is expected behaviour then the templating engine and/or code should be investigated to determine if code execution or a sandbox escape is possible. Please contact Appcheck-NG support if you need help investigating this issue.

The following blog post details further information on this subject;

<http://blog.portswigger.net/2015/08/server-side-template-injection.html>

Details

Contains technical details specific to the vulnerability found in the application. This is useful for manually confirming a vulnerability and providing further information about how it was detected and how it can be resolved.



Share this vulnerability

Rescan vulnerability

high high medium

Application	Target	Vulnerable Parameter	First Detected	Last Detected
localhost:8686	/template_injection/server_side_template_injection_001	URL parameter: "data"	6th Nov 2017 - 09:43	6th Nov 2017 - 09:43

Attack URL: http://localhost:8686/template_injection/server_side_template_injection_001?data=HelloWorld%7B%7B31337%2A31337%7D%7D

Description Details Workflow Screenshot

Details

▼ Technical Details

This flaw was identified by injecting the payload `{{31337*31337}}` via the `query.data` parameter. A component is considered vulnerable when the result of the evaluated expression (`982007569`) is found within the response but is not found in the control response

▼ Messages

```

--->
GET /template_injection/server_side_template_injection_001?data=HelloWorld%7B%7B31337%2A31337%7D%7D HTTP/1.1
Cookie: beaker.session.id=bd59f26972764eb93771c151ba7edc2
Connection: close
Host: localhost:8686
User-Agent: Mozilla/5.0 (X11; Linux i686) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Accept: */*
Referer: http://www.google.com

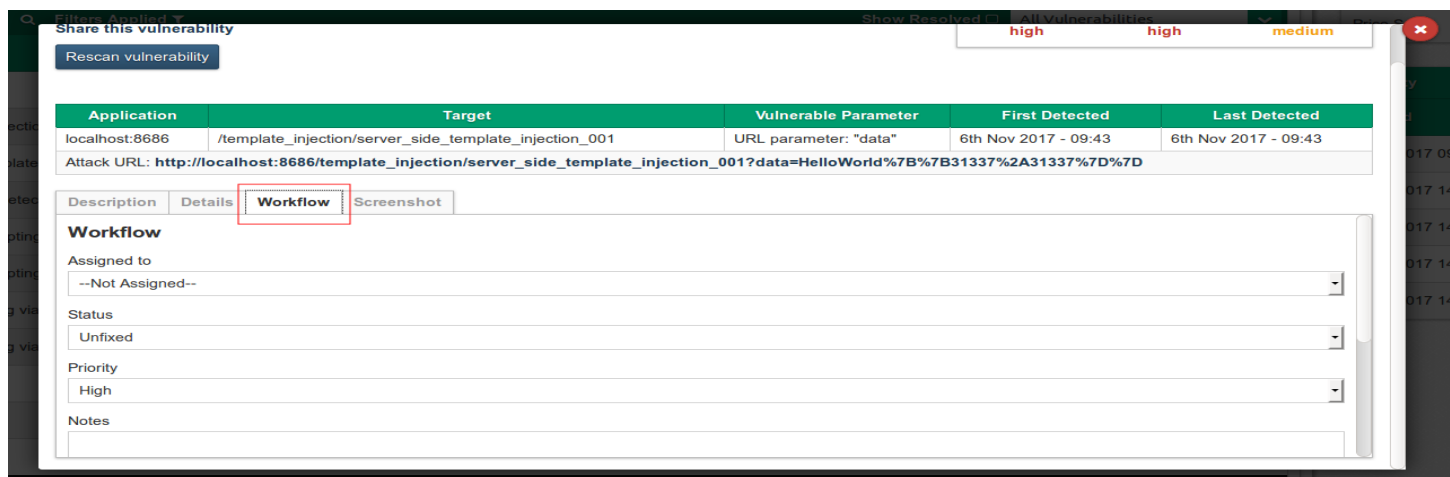
```

Workflow

The workflow tab provides a form to help manage vulnerabilities i.e. assigning the vulnerability to a user.

Workflow fields:

- Assigned: Person in your organisation the vulnerability is assigned to.
- Status: The status of the vulnerability (useful for filtering in the vulnerability listing table).
- Priority: Priority of the vulnerability, choose from: High, Medium, Low
- Notes: A text field for adding any notes to the vulnerability



Share this vulnerability

Rescan vulnerability

high high medium

Application	Target	Vulnerable Parameter	First Detected	Last Detected
localhost:8686	/template_injection/server_side_template_injection_001	URL parameter: "data"	6th Nov 2017 - 09:43	6th Nov 2017 - 09:43

Attack URL: http://localhost:8686/template_injection/server_side_template_injection_001?data=HelloWorld%7B%7B31337%2A31337%7D%7D

Description Details Workflow Screenshot

Workflow

Assigned to

--Not Assigned--

Status

Unfixed

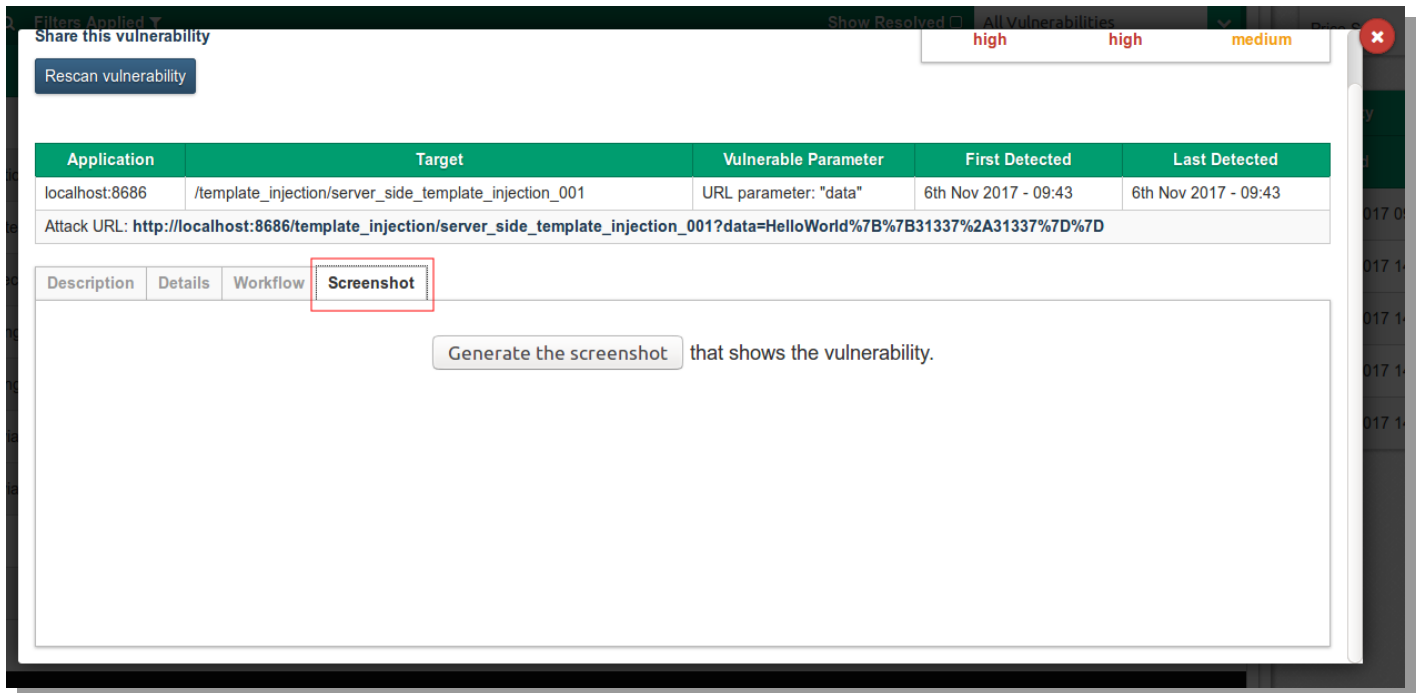
Priority

High

Notes

Screenshot

Generate a screen-shot of the page containing the vulnerability, useful for manually confirming a vulnerability.



Filters Applied ▼ Show Resolved ☐ All Vulnerabilities

Share this vulnerability high high medium

Rescan vulnerability

Application	Target	Vulnerable Parameter	First Detected	Last Detected
localhost:8686	/template_injection/server_side_template_injection_001	URL parameter: "data"	6th Nov 2017 - 09:43	6th Nov 2017 - 09:43

Attack URL: http://localhost:8686/template_injection/server_side_template_injection_001?data=HelloWorld%7B%7B31337%2A31337%7D%7D

Description Details Workflow **Screenshot**

Generate the screenshot that shows the vulnerability.

User Management

The **Users** tab/view permits the setup and management of one or more individuals and groups permitted to access your organisation's data. User management makes use of Role-Based Access Control (RBAC) to provide granular application permission.

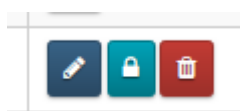
User Roles & RBAC (Role-Based Access Control)

Basic Role-Based Access Control (RBAC) is provided through the user of three tiers of user:

<i>Super-admin</i>	(not typically available for customer configuration)
Admin	High-privilege user able to perform actions including: <ol style="list-style-type: none"> 1. Setup additional users 2. Setup User Groups/Grant Permissions 3. Access to all results 4. All Permissions 5. Add further watchers to scans
User	Can be added to the user group to be given certain permissions (example: commence a scan, vulnerability management) Restricted visibility of scan results

Registered Users & User Management

The list of users can be seen on the main page of the **Users** view. Actions possible for each user are listed to the right and include (for admin users) **Edit**, **Disable User**, and **Delete User**



User Activity Logs

Clicking into a user account record will display a list of activity for that customer, including actions triggered by login

Sales Demo Edit			
Activity			
Search...			
Created	Object	Description	State
19/04/2016 10:43	User: Sales Demo	logged in	
19/04/2016 10:52	User: Sales Demo	logged out	
19/04/2016 11:21	User: Sales Demo	logged in	
19/04/2016 11:34	User: Sales Demo	logged in	
19/04/2016 11:48	User: Sales Demo	logged out	
19/04/2016 11:54	User: Sales Demo	logged out	
19/04/2016 12:04	User: Sales Demo	logged in	
19/04/2016 12:37	User: Sales Demo	logged out	
19/04/2016 15:12	User: Sales Demo	logged out	
19/04/2016 15:12	User: Sales Demo	logged in	
Limit 10 Page 1 of 226 Refresh			

Adding a New User

To add a new user click the **+ New User** button and enter in the user's details:

New User

Name

Email Address

Set user's password?
☐

User Role

User

Disable user?
☐

Update

User Groups

It is possible (and recommended) to add your users to one or more defined **User Groups** that map to e.g. different business units within your organisation. Once a User Group is defined, it can be:

- Populated with one or more users; and
- Tied to one or more scan definitions

In this way, you can grant different view horizons of scan configurations and vulnerability reports to different working groups from within your organisation, in a single AppCheck organisational account.

User group: Customer Group Maintain Old Behaviour details

Name	Can Run Scan	Can Pause Scan	Can Abort Scan	Can Create Scan	Can Edit Scan	Can Delete Scan	Can Edit Workflow
Customer Group Maintain Old Behaviour	✓	✓	✓	✓	✓	✓	✓

Users Scans

Search...



Name	Email	Role	Last Online
------	-------	------	-------------

Asset Management

The **Assets** view allows you to define a list of all assets (IP addresses, Fully Qualified Domain Names (FQDNs) and URLs (web addresses)) that reflect all the internet-facing systems and services that you wish to target for scanning.

All Assets + New Asset			
<input type="text" value="Search..."/> Q			
Asset	Description	Application	In Scope
http://www.google.co.uk	Added with group customer google assest	✓	✗
www.google.co.uk	Added with group customer google assest	✗	✗
https://www.google.co.uk	Added with group Google.co.uk Group	✓	✗

To start targetting a new system or service for scanning, it is not necessary to add an asset in the asset view manually, you can simply:

- Request via Technical Support that the new asset is added to your account scope; and then
- Add the domain/IP/URL as a target in your scan definition

However, asset management via the **Assets** view is recommended since it has several advantages:

- Provides a simple overview of all targeted assets across all scans
- Allows you to add a description for each asset or asset group, assigning a more memorable human-meaningful name as an *aide memoir*.
- Clearly indicates if each asset is in your account scope or not
- Allows you to group assets into groups so that they can be more easily managed and updated as they change over time, as well as mapping asset groups to scan targets for easier scan configuration setup and management.

Appendices

Appendix A - GoScripts

GoScript is an advanced and unique feature of the AppCheck application scanner, combining the power of automated scanning with the guidance of a human to work through complex processes and pass validation where other scanners fail.

GoScript is useful to perform the following actions.

- Get past authentication barriers including single sign on and 2 factor
- Drive complex workflows such as sign-ups, purchases and data entry. As a user would passing validation to test deeper in the application
- Allows scanning of single page applications, going through targeted processes as opposed to clicking blindly
- Testing specific areas of a workflow

GoScript has a simple easy to understand and use language consisting of just five basic instructions and a single advanced instruction. Using these you are able to build up some very complex interactions mirroring the way a user would navigate the application by providing a series of instructions for the crawler to follow.

Basic Instructions

go:	Go to the given URL	go: http://www.example.com
wait for:	Wait for a given unique string	wait for: welcome
pause:	Wait for a given number of seconds	pause: 15
=	Set the value of a field	username = joe
click:	Find a page element and trigger a click	click: Log In
press:	Hit the enter key	Press: enter

Advanced Instructions

js:	Execute a snippet of JavaScript	js: \$('div.richtext').val('test'
-----	---------------------------------	-----------------------------------

AppCheck users have the option to edit any changes once the changes have been done, users have the option of “Test Script” to verify that the script is working via the screenshots provided.

Amazon Example

Random external hub

Save

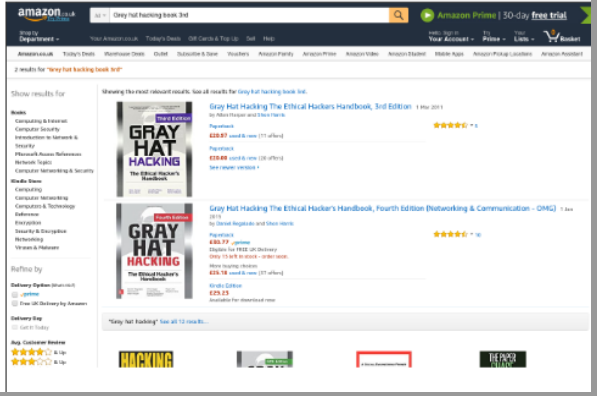
Test Script

Delete

GoScript

```
# Search for a specific book
go: http://www.amazon.co.uk/search?searchtext=Grey+hat+hacking+book+3rd+click:Go

# Go to the book's product page
wait for: the ethical hackers handbook
click: Gray Hat Hacking The Ethical Hackers Handbook, 3rd Edition
wait for: Thwart malicious network intrusion by
```



Appendix B - Two-Factor authentication with Google Authenticator

If your organisation has been set up to use two-factor authentication you will be presented with a set-up screen on your initial login:

Set up Authenticator

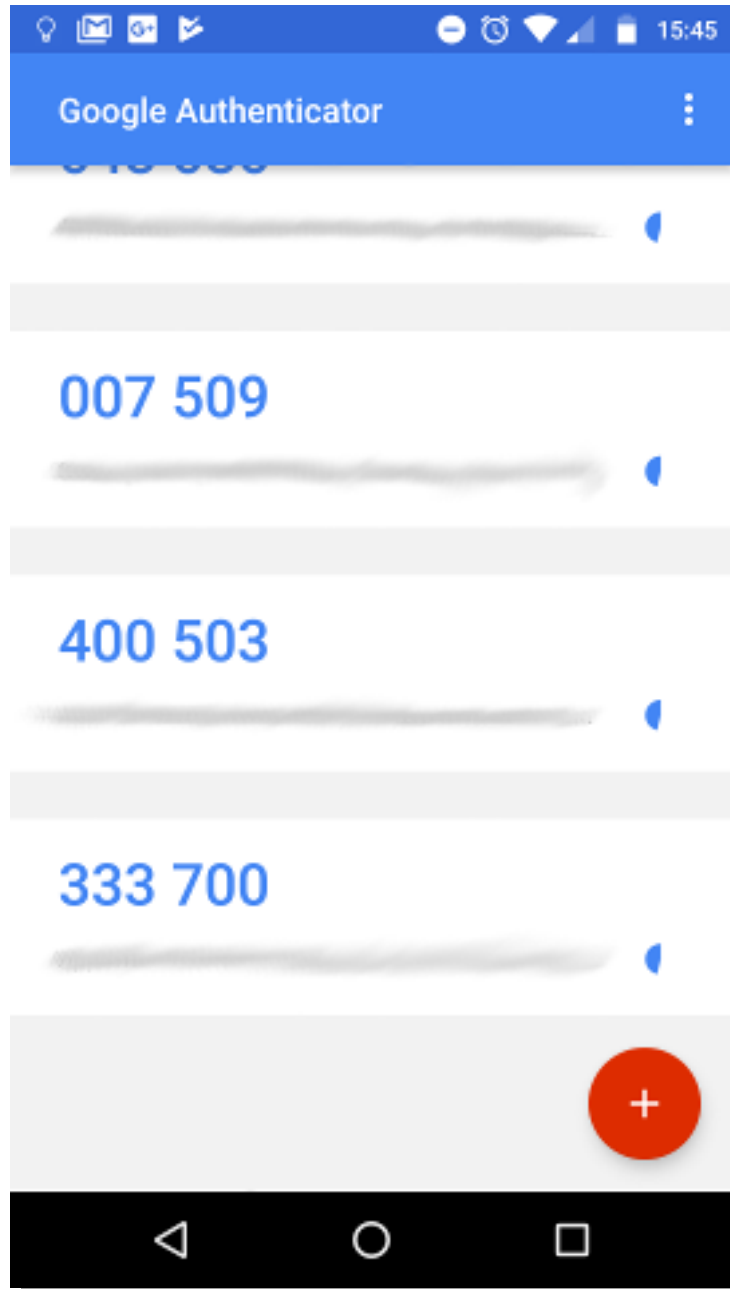
- Get the Google Authenticator App
 - Android: **Google Play**
 - iPhone: **iTunes**
- Add the secret key to the Google Authenticator App
 - Scan the QR code
 - or enter the key: **2SVIJC4RGBKAFL7X** and select "time-based" as method for this account.
- Enter the 6-digit code

Validation Code

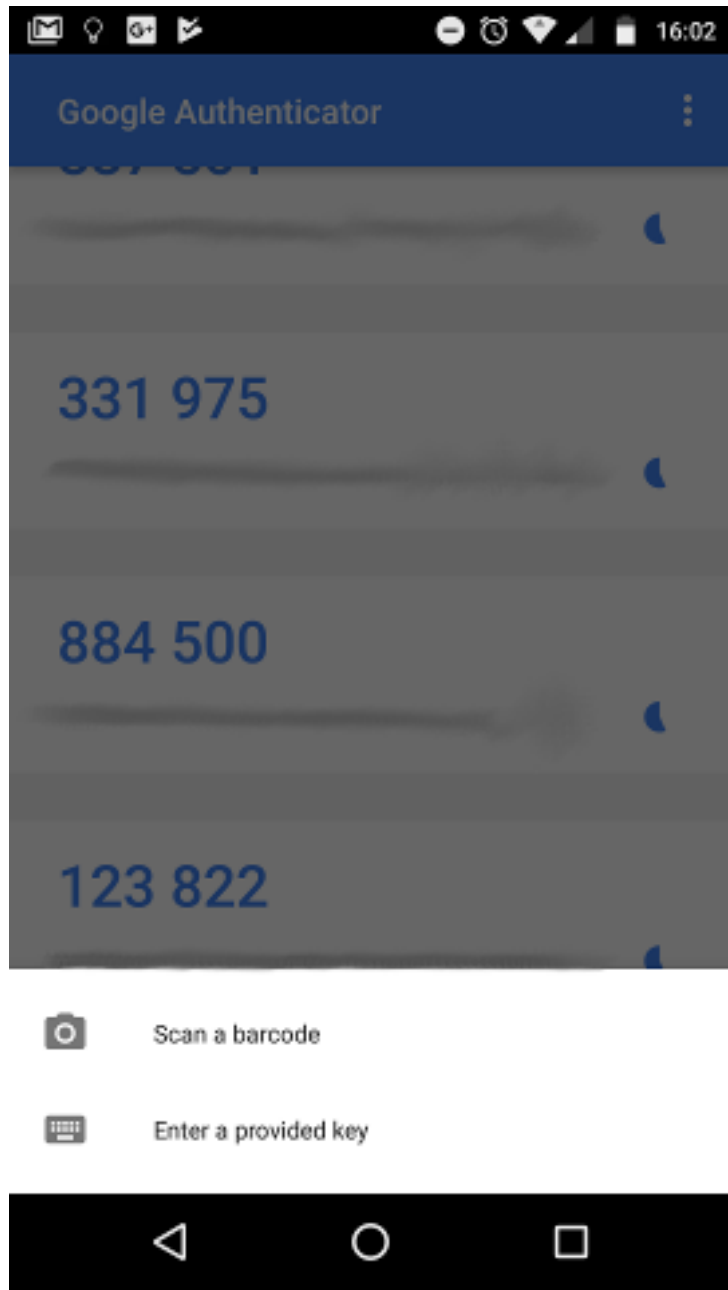
Verify

The first step is to download the Google Authenticator App, the set-up screen provides links to download this for Android or IOS (iPhone) based devices.

Once downloaded open the Google Authenticator App and click the red disc with the plus sign in the lower right corner:



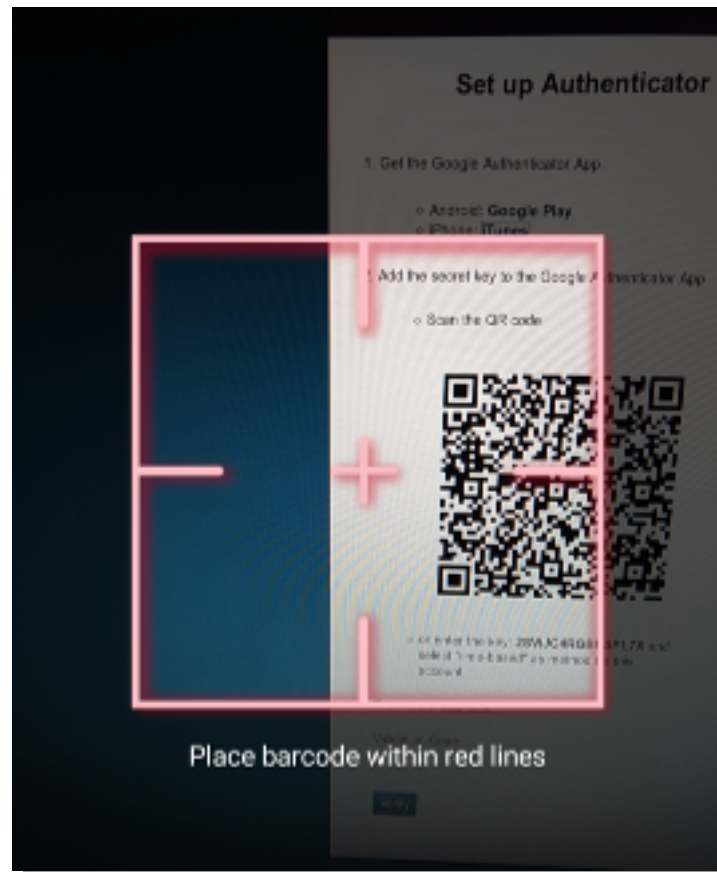
This will bring up options to either “Scan a barcode” or “Enter a provided key”



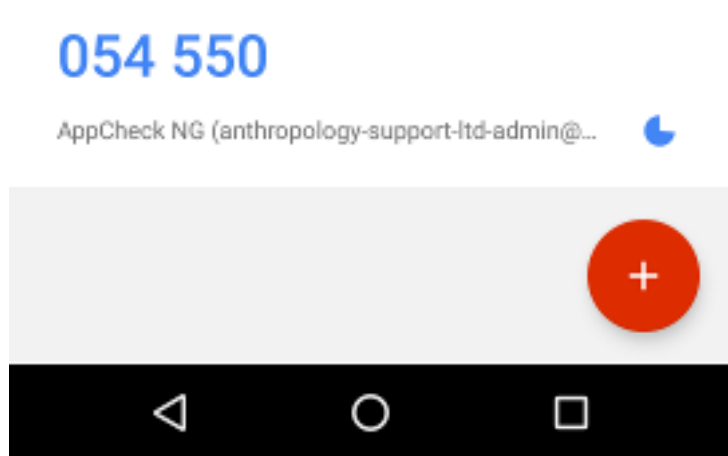
AppCheck allows the choice of scanning a barcode or entering a key.

Scan a barcode

If you wish to scan the barcode on the AppCheck two-factor setup screen select the “Scan a barcode” option in Google Authenticator and point your phone camera at the barcode on screen:

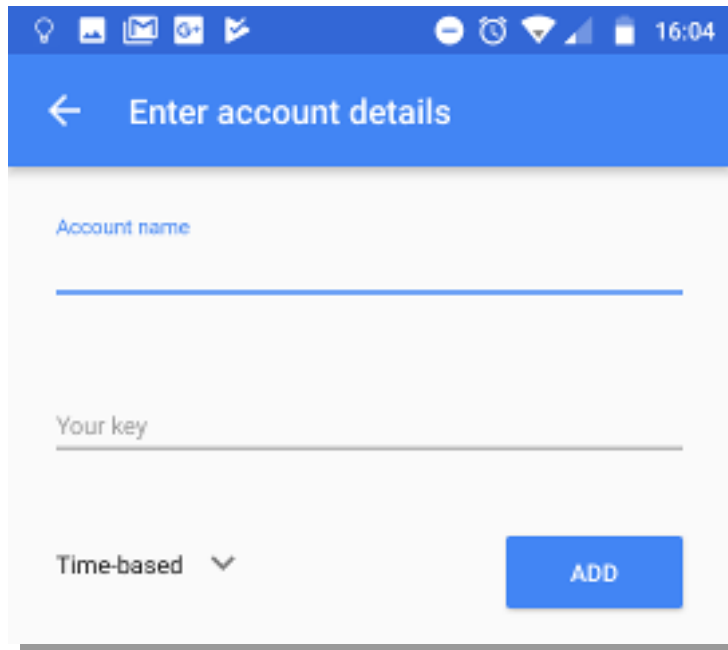


This will add an entry, in Google Authenticator, for your AppCheck user:



Enter a provided key

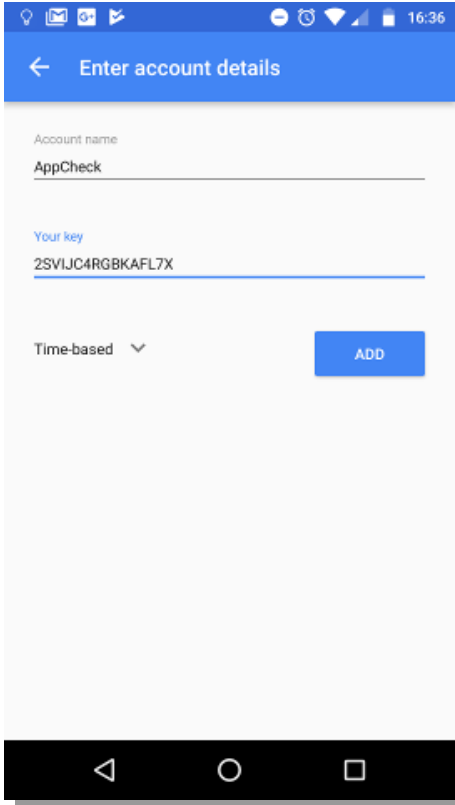
If you wish to set up 2-factor auth with the key provided on the set-up page select “Enter a provided key” in Google Authenticator. You will be presented with this screen:



Using the key supplied on the set-up page:



Enter this into Google Authenticator with an appropriate **Account name** i.e. “AppCheck” and then click *ADD*:



Enter account details

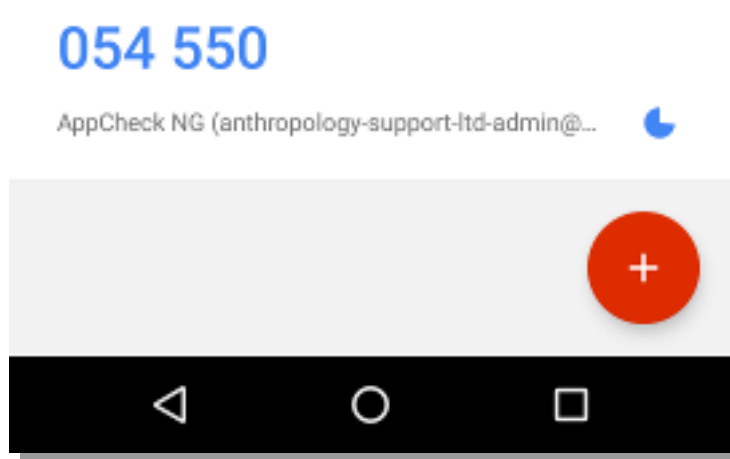
Account name
AppCheck

Your key
2SVIJC4RGBKAF7X

Time-based ▼

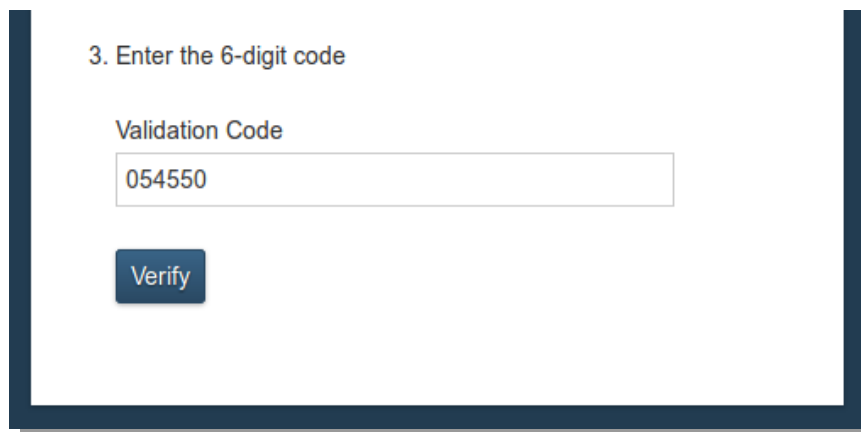
ADD

This will add an entry, in Google Authenticator, for your AppCheck user:

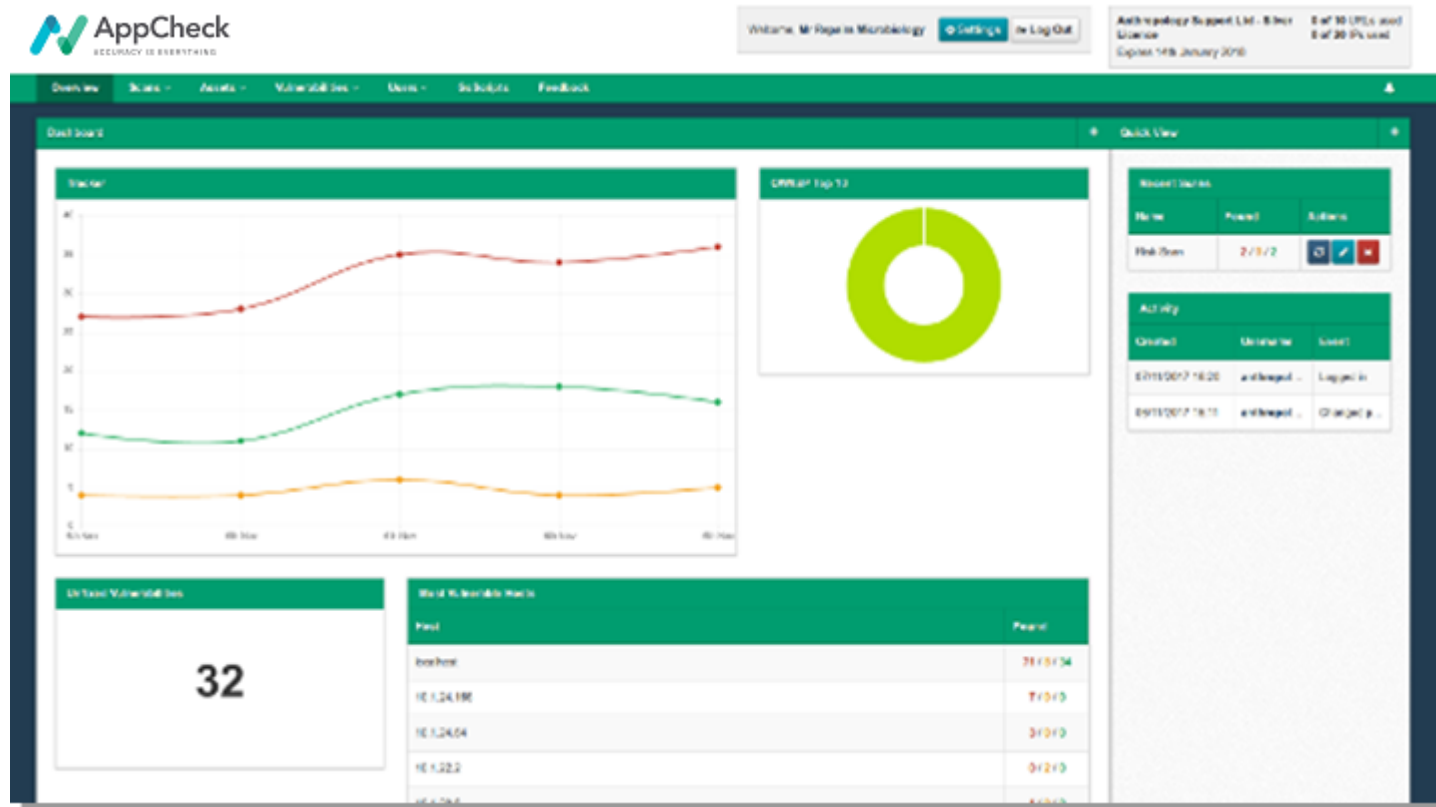


Completing Set-up

To complete set-up enter your 6-digit two-factor code (in this example **054550**) into the “Validation Code” field and click the “Verify” button.

A screenshot of a web-based form. The heading '3. Enter the 6-digit code' is at the top. Below it, the label 'Validation Code' is positioned above a text input field. The input field contains the text '054550'. Below the input field is a dark blue button with the word 'Verify' in white text.

You will successfully login to your account.




If the validation code is incorrect you will receive an error:

Incorrect code, try again

Set up Authenticator

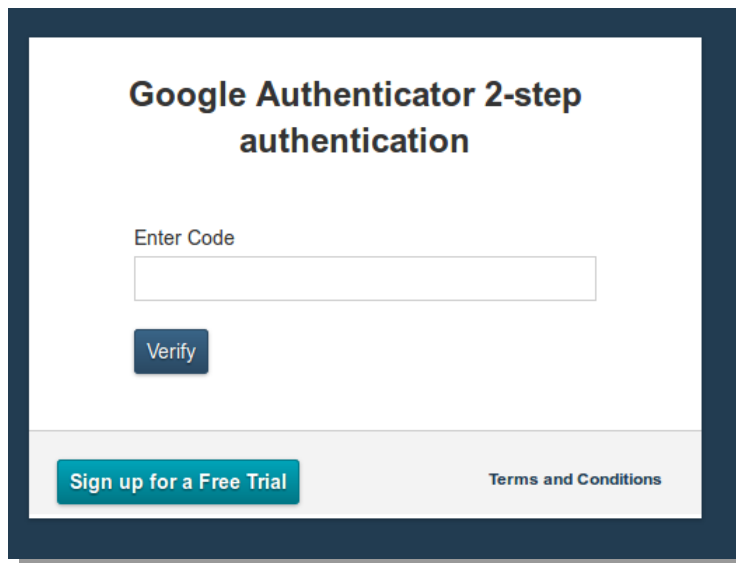
1. Get the Google Authenticator App
 - Android: [Google Play](#)
 - iPhone: [iTunes](#)
2. Add the secret key to the Google Authenticator App
 - Scan the QR code



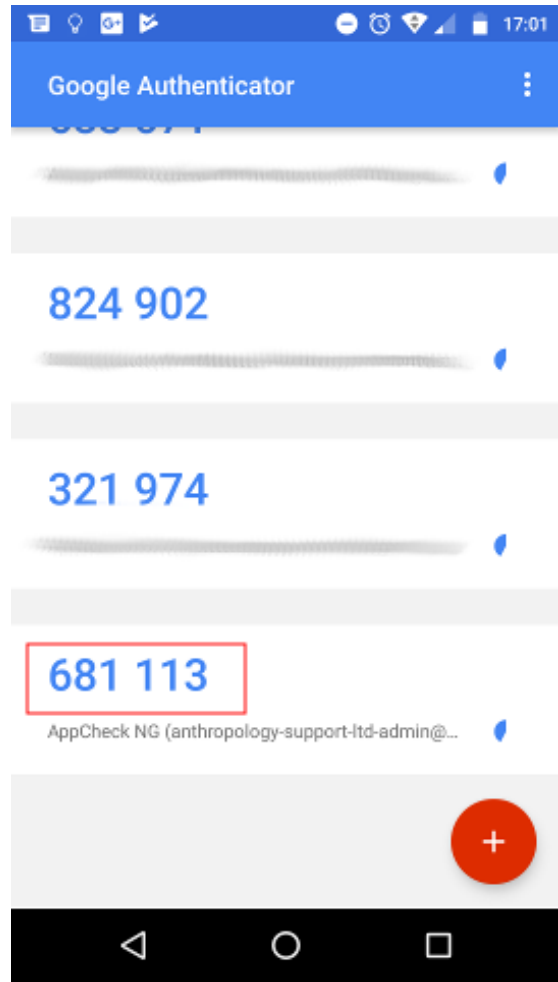
N.B. The 2-factor code is time based and so changes every 30 seconds and is refreshed on screen in the Google Authenticator app, be aware that if the code changes before entering into the “Validation Code” field on the set-up page the code will be deemed invalid and will produce the above error.

Future Logins

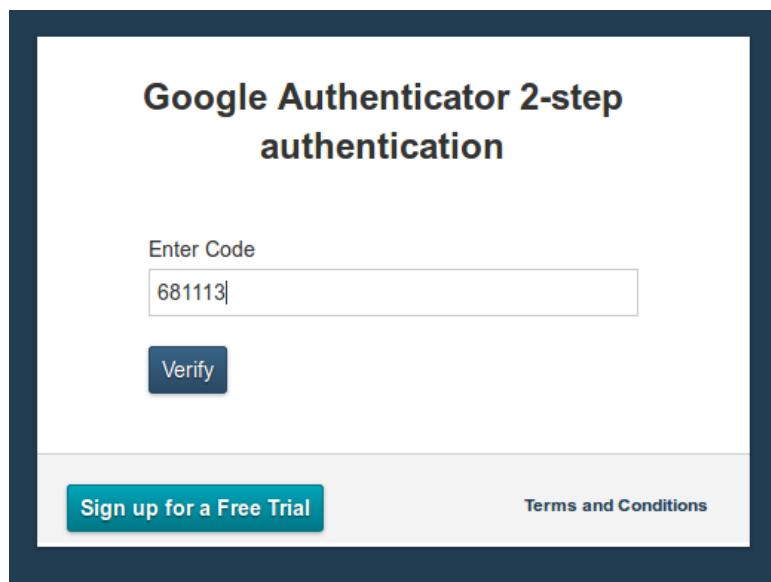
On future logins you will be presented with a 2-factor authentication form after entering your username and password:

A screenshot of a web-based 2-step authentication form. The form has a dark blue border. At the top, it says "Google Authenticator 2-step authentication" in bold. Below that is a label "Enter Code" above a text input field. Under the input field is a dark blue button with the word "Verify" in white. At the bottom of the form, there is a light gray bar containing two links: "Sign up for a Free Trial" in a teal box and "Terms and Conditions" in a smaller, dark blue font.

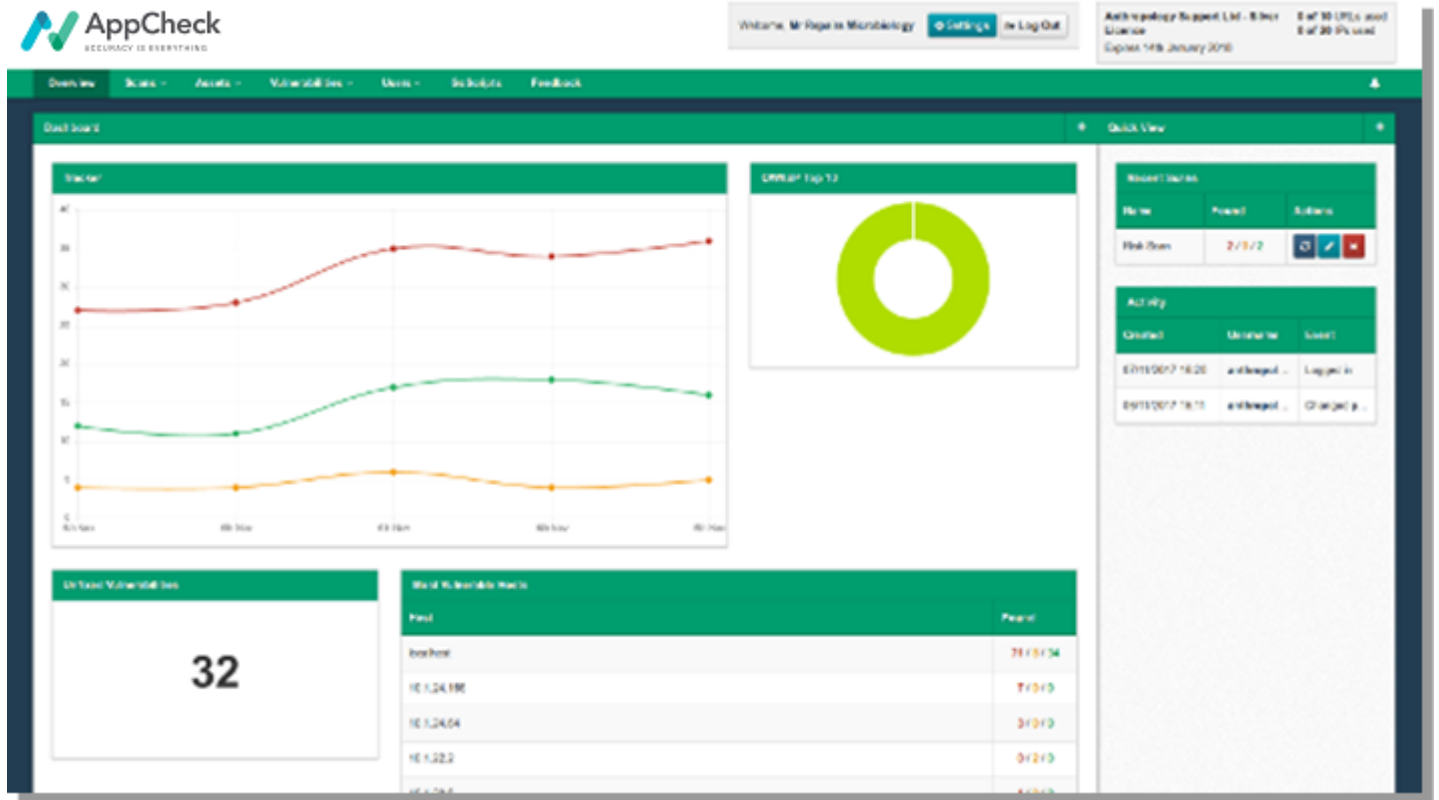
Open the Google Authenticator application and enter the code associated with your AppCheck account, i.e. **681113**:



Enter the code into the **Enter** Code field and click *Verify*:

A screenshot of the Google Authenticator 2-step authentication screen. The screen has a white background with a dark blue border. At the top, the text 'Google Authenticator 2-step authentication' is displayed in bold. Below this, there is a text input field labeled 'Enter Code' containing the code '681113'. A dark blue button labeled 'Verify' is positioned below the input field. At the bottom of the screen, there is a teal button labeled 'Sign up for a Free Trial' and a link labeled 'Terms and Conditions'.

You will be successfully logged in in:



If

the code is incorrect you will be presented with an error.

N.B. The 2-factor code is time based and so changes every 30 seconds and is refreshed on screen in the Google Authenticator app, be aware that if the code changes before entering into the "Enter Code" field on the authentication page the code will be deemed invalid and will produce the above error.