

## Platform Overview



### Customisable Analytical Dashboard

The AppCheck Dashboard presents a fully configurable view of your current security posture. From here you can track remediation progress, spot vulnerability trends and instantly see which areas of your environment are most at risk.

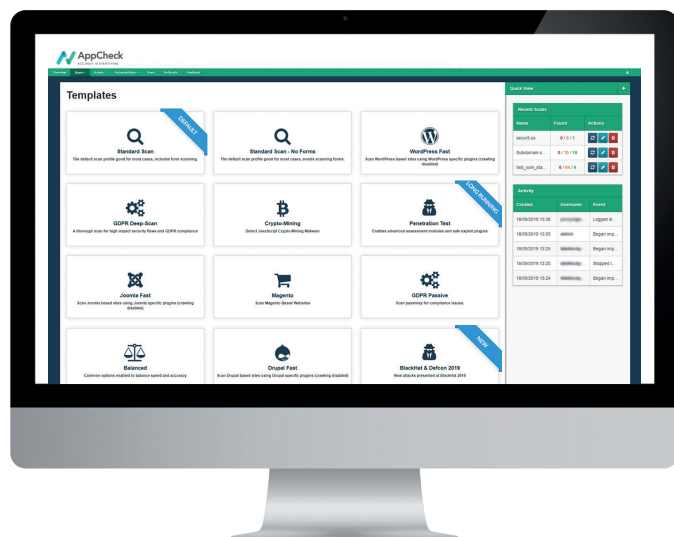
This can include but not limited to:

- > High, Medium, Low vulnerability tracker
- > Most vulnerable applications
- > Most vulnerable hosts
- > Fixed and Unfixed Vulnerabilities
- > OWASP Top 10 vulnerabilities
- > Recent Scans
- > Activity Logs
- > Impact Chart



### Scan Templates

Scans can be run in a few clicks using templates built by our security experts enabling the user to scan for specific vulnerabilities rather than requiring to run a full test. Tailor a scan to meet your needs and build from scratch using the profile editor.



This includes:

- > Scan templates built by experienced security experts
- > Constantly updated in line with changing security landscape
- > Run specific assessments
- > Increased scan speed
- > Scan for specific compliance vulnerabilities
- > Scan for CMS specific vulnerabilities
- > Tailor scan profiles towards your user requirements

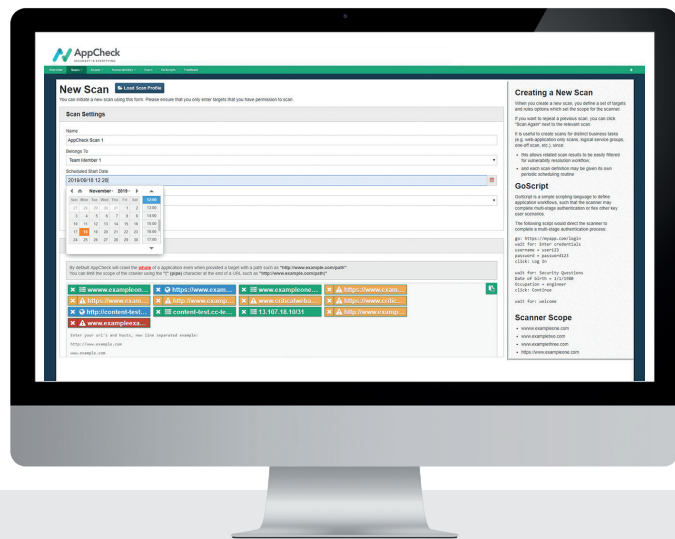
## Platform Overview



### Bespoke Scan Configuration

The AppCheck tool enables for simple scan configuration allowing the user to scan a URL or Infrastructure target within a matter of moments:

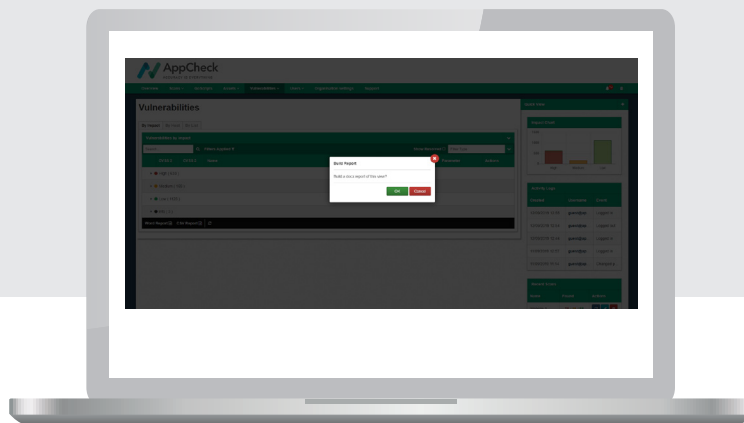
- > 'Import and remove' targets
- > Scan scheduling between specific dates and times
- > Authenticated testing
- > Form Testing
- > Customisable plug-ins



### One-click Reporting

Results can be exported as either a professional penetration testing report in Microsoft Word format or as a CSV file, with a single click. Results can also be exported in JSON format to allow easy integration with third-party tools.

- > Includes simple JSON data API to retrieve raw vulnerability data for use in third party applications
- > Download custom filtered results and view via HTML, Docx or CSV
- > PCI and UK Government PSN compatible formats



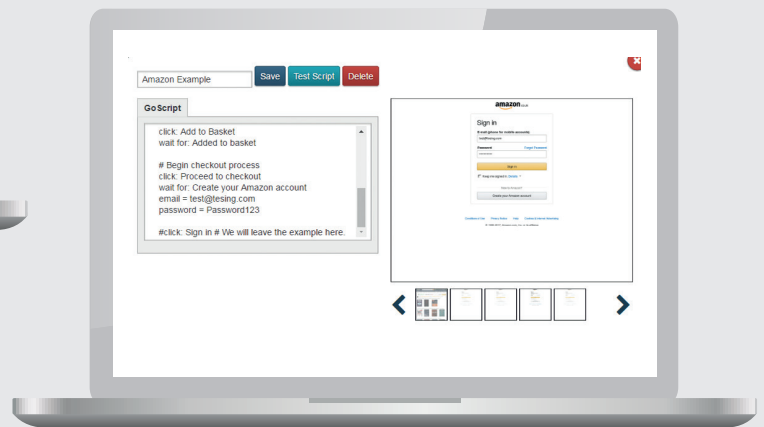
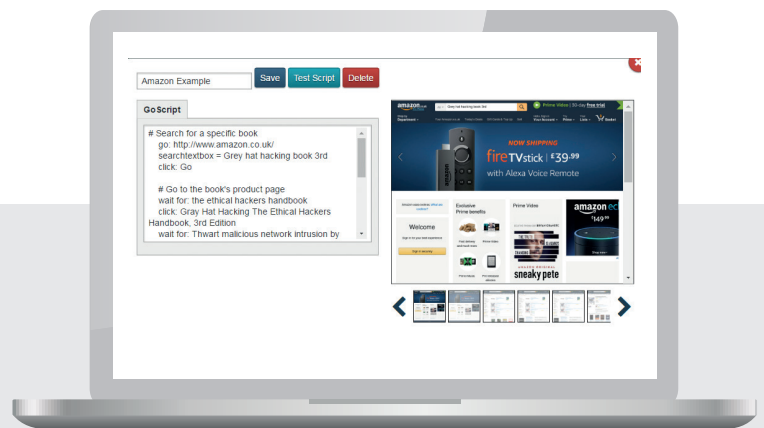
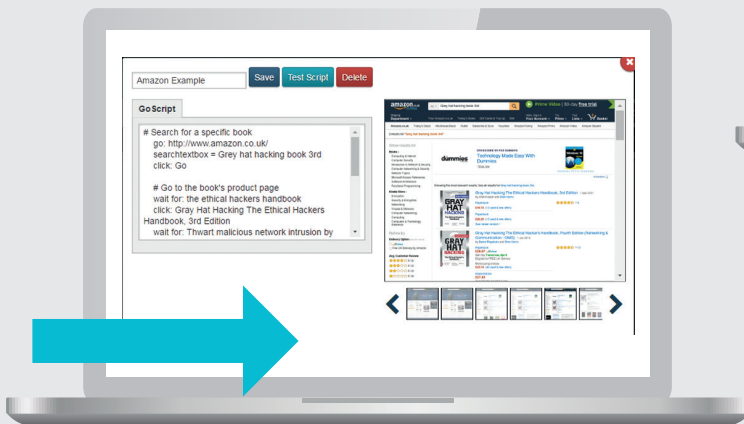


## GoScript

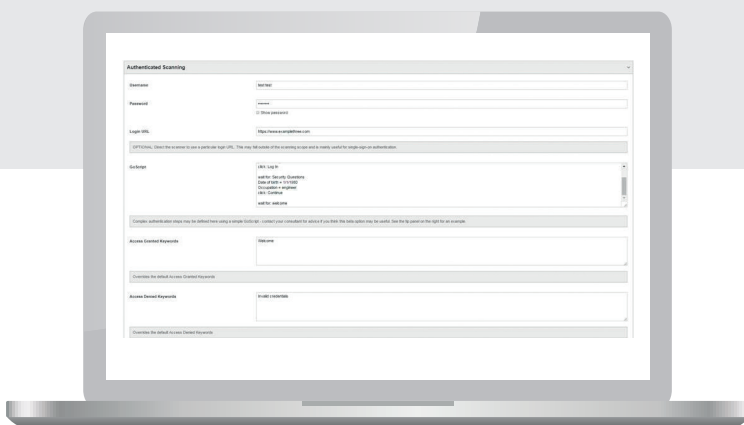
GoScript is a simple scripting language that defines application workflows, so that the scanner can flex key user journeys and can also be implemented to complete multi-stage authentication.

- > GoScript enables AppCheck to crawl complex applications
- > Enabling the tool to navigate an app as a human would
- > Fuzzing for vulnerabilities throughout the workflows
- > Authenticated scanning options for logins

Fig1: The workflow for purchasing a product on Amazon



- > Fig 1, illustrates selective screenshots of a GoScript mapping the user workflow of purchasing a product on Amazon.
- > Full example can be found on our YouTube channel: Simply search 'AppCheck GoScript Demo'.



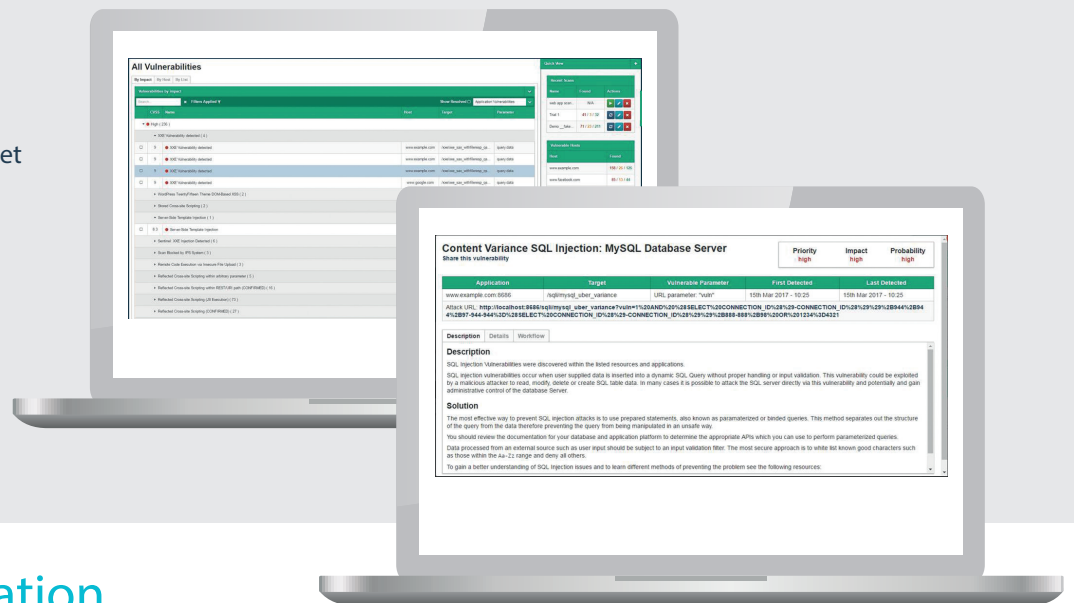
## Platform Overview



### Managing Vulnerabilities

AppCheck's vulnerability management platform enables each user to manage vulnerabilities discovered across the business in a variety of ways. The vulnerability management platform is completely customisable and has been specifically designed for the user to view and prioritise the vulnerabilities that matter most to them. Vulnerabilities can be managed by:

- > Web App, Infrastructure
- > OWASP, CVSS
- > Impact, Priority, Likelihood
- > Host Name, Parameter, Target
- > Specific vulnerability



### Remediation

AppCheck's technical analysis and information gives the user the exact detail and parameter of all vulnerabilities discovered, enabling IT teams to easily locate any flaws that are detected. Additionally, remediation advice is very clear and simple to follow, allowing users to quickly fix any vulnerabilities that are discovered.

- > Breakdown of where and when the vulnerability was discovered
- > Technical description of discovered vulnerabilities
- > Details of the exact attack used
- > Simple to follow remediation advice

