Acunetix Integrations

Acunetix integrates with 3rd party applications, making it easier to track and protect against the vulnerabilities identified by Acunetix. The Acunetix scan results can be used by the following Issue Trackers and WAFs, and Acunetix can also be used as part of a Continuous Integration environment.

Issue Trackers

An Issue tracker is a powerful and essential tool in the Software Development Life Cycle (SDLC) of almost any software project. It helps development teams streamline collaboration and manage their work without getting lost in an endless stream of emails and PDF reports.

Acunetix can send vulnerabilities as issues to the following Issue Trackers:

- Microsoft TFS
- JIRA
- GitHub (Including an Acunetix Jenkins plugin)

Web Application Firewalls (WAFs)

Acunetix integrates with popular WAFs to automatically create the appropriate Web Application Firewall rules to protect web applications against attacks targeting vulnerabilities that the scanner finds. This allows you to temporarily prevent exploitation of high-severity vulnerabilities until you are able to fix them.

Acunetix can export scan data to the following Web Application Firewalls (WAFs):

- Imperva SecureSphere.
- F5 BIG-IP Application Security Manager.
- FortiWeb WA

Continuous Integration (CI)

The Acunetix plugin for Jenkins, the popular open source Continuous Integration (CI) and automation platform, allows development and operations teams to identify and track web application vulnerabilities early on in the Software Development Life Cycle (SDLC), and crucially, before they make it into production. The Acunetix Jenkins Plugin integrates seamlessly with the Jenkins' build process, triggering automated Acunetix scans as part of the web application's build process inside of the Jenkins CI platform.

The Acunetix Jenkins Plugin enables you to:

- Trigger Acunetix scans from within Jenkins upon each build.
- Trigger Acunetix scans with built-in or custom Scan Types to only scan for specific vulnerabilities.
- Configure Jenkins to fail a build (and optionally abort the scan) as soon as a specific threat-level (high, medium or low severity) is reached.
- Automatically generate reports saved within Jenkins.