Quick Start Guide.

FOR STANDARD AND PREMIUM

acunetix

Contents

Acunetix Quick Start Guide

LEARNING THE BASICS

Congratulations on joining Acunetix!
Web security might seem like a daunting concept. But with Acunetix, you can start scanning target web applications immediately.

Acunetix is an automated, yet configurable, web application security scanner. It enables you to scan websites, web applications and web services in order to detect vulnerabilities and other issues that may be useful to malicious hackers.

First, we recommend that you read the **Acunetix Introduction.**

INFORMATION

Acunetix provides, in many cases, proof that discovered vulnerabilities are real, significantly reducing false positives. Together with the speed of the Acunetix scanning engine (the fastest on the market), this means you avoid wasting time on manual verifications. This enables you to spend time fixing vulnerabilities instead.

WEB APPLICATION SECURITY

THE SCAN PLAN

A good way to bring security to your web applications is to follow a simple 6-point plan.

1. Understand your web application's underlying technologies and structure
2. Preparing and configuring targets
3. Scanning your web application
4. Resolving issues
5. Retesting fixed issues
6. Generating reports

Getting Started with Acunetix

INSTALLATION

There are two ways to use Acunetix:

- Acunetix Online is a cloud-based web application security scanner. You can simply log in by using the Account Administrator credentials you were supplied.

- Alternatively, you can download and install the Acunetix on-premises edition.
    - First check in with the Installing Acunetix guide to understand that your system has the minimum system requirements.
    - Proceed with installing Acunetix. Once it is installed and you have created your administrator user account, you can start using the application immediately.

ACTIVATING YOUR ACUNETIX INSTALLATION

After the installation, Acunetix needs to be activated using your license key . Simply log into the Acunetix web UI and navigating to the profile page of your account, where you will need to update your contact details. Insert your license key and proceed with product activation. With the on-premises edition, you can also choose to register your installation with the AcuMonitor service. Acunetix Online users will automatically make use of AcuMonitor. More details about License Activation can be found here.

INFORMATION

AcuMonitor is used to detect certain types of vulnerabilities, such Blind XSS, SSRF, XXE and other out of band vulnerabilities which can only be detected using an intermediary service. More information on AcuMonitor can be found here.

Product activation requires an internet connection.

ADDING TARGET WEBSITE APPLICATIONS

Now that you have installed Acunetix, you are almost ready to start scanning. Before you begin, it is important you understand how to add a target website, and, equally important, how to define the target to correctly match your website. Adding your target website before starting to scan is necessary so Acunetix knows which sites you want to scan, and how best to perform the scan to take a better snapshot of the web application's attack surface.

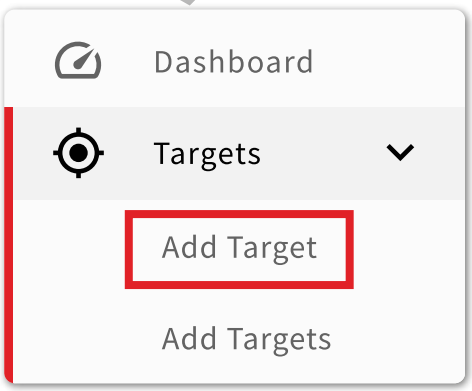
WARNING

Each target scanned counts towards your license; you cannot switch this site out for a different site you need to scan. To see a more complete description of how targets are counted towards your license, see **What is a Target**.

Acunetix Online users need to verify the ownership of their websites prior to scanning. For more details on this, see **Configuring Targets**.

ADDING THE TARGET IN ACUNETIX

Click on "Targets -> Add Target".



Enter the URL of your Target and a Description.

Click the "Save" button.

VERIFYING WEBSITE OWNERSHIP (Acunetix Online only)

You can Verify Ownership of a website by uploading a verification file into the root of the Target's URL. For Network scanning, there will be a one-time verification process where you may need to be contacted by Acunetix.

You can obtain more details about the verification process in **Configuring Targets**.

Ownership Verification is an important step, and you are recommended to act responsibly in this regard; specifically, you should keep in mind that your website will be attacked during the scan. You should also see **Is a Vulnerability Scan Invasive Enough to Damage my Site or Data?**.

AUTHENTICATION SETTINGS

Authentication settings are very important for a web application scan. Most web applications require a legitimate user to log in before allowing the user access to parts of the web application that are reserved to logged-in users. To scan these reserved parts of the web application, this authentication step must be configured within your

Target settings so the scanner can reach these components.

Authentication may be configured in one of two ways. The first option is to use the **Acunetix Auto-Login** feature; for most web applications using a simple login/logout mechanism, this will be sufficient. More complex login mechanisms will require additional configuration, which can be done using the Acunetix Login Sequence Recorder. For more details on this, see **Configuring Targets**.

WEB APPLICATION TECHNOLOGIES

Default configuration will allow you to use Acunetix for black-box scanning; this means that the scanning engine uses a large set of techniques to efficiently and effectively scan the target web application even without having "insider" knowledge of the server-side scripting engine being used. The engine will scan the web application, using multiple mechanisms to attempt to find flaws and vulnerabilities, much the same way as a malicious hacker would. The modern-day term for this is DAST, or Dynamic Application Security Testing.

INFORMATION

AcuSensor gets additional information from the server back end, at the time when Acunetix is scanning the web application. This additional information gives us a number of benefits:

- Line of code or stack trace indicating where vulnerability is created
- Greater precision and increased confidence in vulnerabilities detected
- Full web application coverage

A more advanced strategy we can use is IAST, or Interactive Application Security Testing, where Acunetix creates an **AcuSensor** agent file that can be deployed into a web application for some types of server-side scripting languages (JAVA, PHP, and .NET). Once AcuSensor is deployed, it works in tandem with the external Acunetix scanning engine, returning feedback in real-time for a much wider range of tests that can now be performed thanks to the synergy between the external scanner and the AcuSensor WITHIN the application.

You can get more detailed information about deploying the AcuSensor for **PHP**, **JAVA**, and **.NET**.

GROUPING YOUR TARGETS

If you are managing a large number of web sites or applications, it will benefit you to organize these websites or applications into logical groups for ease of management; you can later on assign a whole group of websites to a particular security staff member.

LAUNCHING A SCAN

Now that your targets are configured, you are ready to launch a scan. There are two ways to do this. You can either use the default settings, or you can configure them for an optimized and faster scan.

USING THE DEFAULT SETTINGS

Acunetix is an easy to use, automated web application security scanner. Depending on whether you want to check your web application for all vulnerabilities, or just for a subset of vulnerabilities, Acunetix provides a number of default scanning profiles, including:

- Full Scan
- High Risk Vulnerabilities
- Cross-site Scripting Vulnerabilities
- SQL Injection Vulnerabilities
- Weak Passwords
- Crawl Only
- Full Web and Network Scan
- Network Scan

...as well as the possibility to create a custom profile to run specific classes of tests as you may wish to perform.

The built-in Scan Profiles makes it easy to get started quickly. To understand the scan settings in more detail, start with **Creating a New Scan**.

INFORMATION

Remember that scan duration may vary depending on the size of the web application, the response time of the web application, and the security checks enabled in the Scan Profile you select.

REVIEWING SCAN RESULTS

Now that the scan has been launched, it's time to look into the **generated results**. In fact, the Scan page shows its findings even while the scan is in progress, exposing a list of all the vulnerabilities found so far, a hierarchical model of the structure of the web application discovered during the initial crawling stage of the scan, and a dashboard with a summary of the key pieces of information relevant to the scan.

Each vulnerability is listed, classified according to type, and described for eventual resolution by the development team - complete with the HTTP request made to the web server to identify the vulnerability, and the response received that contains the vulnerability.

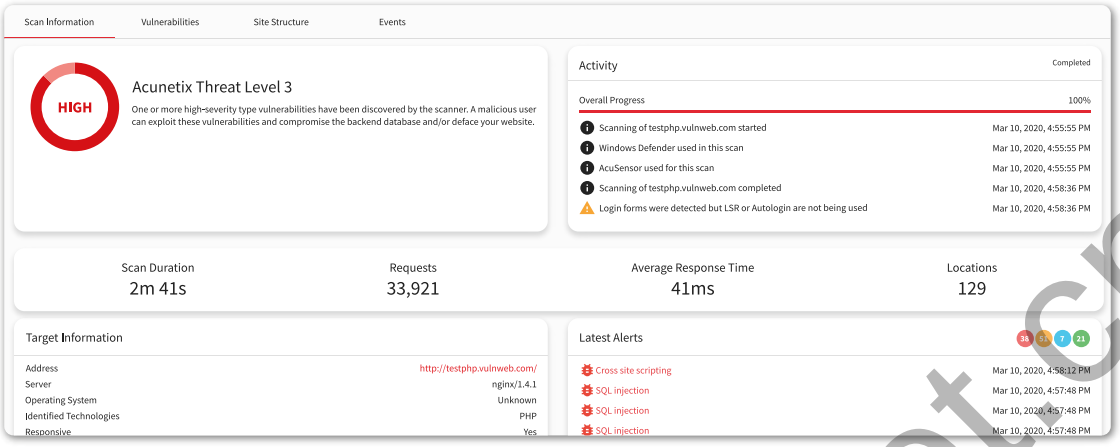
As you go through your first few scans of your web application, you can:

- Learn about vulnerability severity levels
- Gain an overview of the security state
- Check the scan summary and impacts
- Review the issues and remedies
- Fix the vulnerabilities and retest
- Update the status of the issues

In this section, we will discuss how vulnerabilities are categorised, how to interpret ongoing and completed scan results, and what to do once an issue has been identified and fixed.
Now is a good time to read up about **Vulnerability Severity Levels** and other classification nomenclature.

WHAT IS GOING ON DURING SCANNING?

During the scan phase, Acunetix is crawling and attacking discovered pages. The Scan summary page shows the results for a single website during the scan, and also after completion.



If you are managing a suite of web applications, the Dashboard provides an overview of your web inventory, showing:

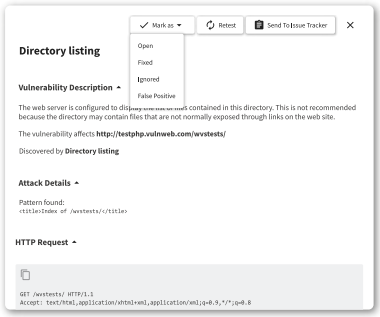
- statistics for the different vulnerability classifications
- a ranking of the web applications from most-to-least vulnerable
- a shortlist of the most commonly found vulnerabilities within the inventory
- trend charts to expose the efficiency and effectiveness of the remediation process

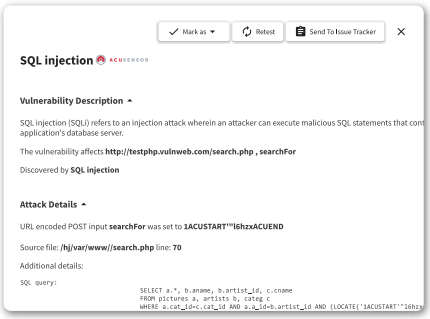
MANAGING DETECTED VULNERABILITIES

Once a list of vulnerabilities is obtained, the next task is to **manage issues found by Acunetix**.

- The list of vulnerabilities can be filtered and sorted to give priority to the items that are most relevant to the situation.
- If exposed vulnerability will take a long time to fix, it is possible to export vulnerabilities for import into top-tier Web Application Firewalls.
- Integration with Issue Trackers can be configured for easier tracking by developers.
- When a second or subsequent scan is performed, one can "Compare Scans" to identify which vulnerabilities are no longer present (fixed), and which still remain.

You can read up on **Managing Vulnerabilities** in more detail. Once a vulnerability is evaluated and possibly fixed, you can **Update the Status of a Vulnerability in Acunetix**.





REPORTING TO STAKEHOLDERS

Acunetix Reports allow you to inform stakeholders, such as management teams and regulatory bodies, about the state of your web applications' security. Reports can cover one or more scans, or one or more targets. Depending on the intended consumer of the report, different types of reports with varying levels of detail can be generated.

WHY DO WE NEED REPORTS?

Reports are important because:

- Developer teams need reports to work on discovered vulnerabilities
- Directors and Regulatory bodies need reports to show compliance
- Managers need reports to evaluate impact on running business, and prioritizing remediation tasks
- Support staff need reports to react to customer requests for assistance

WHY DO WE NEED REPORTS?

A number of built-in report formats are provided with Acunetix, including Developer and Executive Summary reports and compliance reports, such as HIPAA, OWASP Top 10, NIST SP800, PCI DSS, and others. You can get more information about the availability of different Types of Reports.

SETTING UP YOUR USERS AND PERMISSIONS

Now that you have added your first target, you can configure your users and access levels.

Setting up user permissions at the start ensures that users get access to the features they need to work on the websites they are responsible for, identifying and resolving security issues right away.

To set up your users and their access levels, go to Configuring Users. Each user can have one of 3 roles: Tech Admin, Tester, and Auditor. If a Tech Admin is assigned the "Access All Targets" right, then he also is able to add Targets to the system. This table summarizes the functionality assigned to each role.

	Tech Admin	Tester	Auditor
Scan Targets	Full Control	Scan	View
Scan Target Groups	Edit / Scan	Scan	View
Scans	View / Delete	View / Delete	View
Reports	Create / View	None	Create / View

EMAIL SETTINGS

Once you start using Acunetix, you want to be kept up-to-date with timely notifications. You can configure your SMTP server's address, port, from address, security protocol used, and any authentication as needed.

You will receive emails about, for example, product updates, completed scans or a monthly status update. This can be particularly useful to keep yourself updated with the results of your scheduled scans. You can find more information about Email Settings **here**.

NETWORK SCANNER

Acunetix can be configured to use OpenVAS to perform network scans of the Targets configured in Acunetix. When this is done, Network scans can be launched in the same way as web application scans. All the vulnerabilities - web and network, can be managed from the Acunetix portal. Installation of OpenVAS and the configuration of Acunetix to use the Network Scanner is explained **here**.

ISSUE TRACKERS

Acunetix supports sending vulnerabilities to an issue tracker; there is support for a number of platforms:

- Github
- Gitlab
- Azure Devops (Team Foundation Server)
- JIRA
- Bugzilla
- Mantis

Further information about integration with issue trackers can be found **here**.

MULTIPLE SCANNING ENGINES

The Acunetix Multi-engine setup is suitable for Enterprise customers who need to scan more than 10 websites or web applications simultaneously. This can be achieved by installing one Main Installation and multiple Scanning Engines, all managed from a central console.

You can find more detailed information on Multi-Engine setup **here**.

CUSTOM INTEGRATION VIA API

Acunetix includes an API which can be used to integrate Acunetix with other applications. The API allows you to create and scan Targets, retrieve scan results, and generate Acunetix reports. To investigate the API further, go **here**.