

Guide to Acunetix 360 Basics

Contents

3	Step 01 Learning the Basics
3	<i>Web Application Security Scanning Flow</i>
4	Step 02 Installation
4	<i>Acunetix 360 On-Premises</i>
4	<i>Acunetix 360 Online</i>
5	Step 03 Setting Up Your Team & User Permissions
6	Step 04 Adding Target Website Applications
6	<i>Verifying Ownership</i>
7	Step 05 Launching a Scan
7	<i>Using the Default Settings</i>
7	<i>Using Customized Settings</i>
8	Step 06 Reviewing Scan Results
8	<i>What Is Going on During Scanning?</i>
9	<i>What Information is Available Following the Scan?</i>
9	<i>What Should I Do with Detected Issues?</i>
10	Step 07 Creating A Scan Report
10	<i>Why Do We Need Reports?</i>
11	Support

1

LEARNING THE BASICS

Welcome to Acunetix!

Web security might seem like a daunting concept, but with Acunetix 360, you can start scanning target web applications immediately.

Acunetix 360 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 attackers. It also is designed to become a part of your complete cybersecurity environment and integrate with many other solutions.

ACUNETIX 360 LEADER IN ACCURACY

Acunetix 360 is one of the leaders in terms of accuracy and employs several different techniques aimed at reducing false positives. Acunetix 360 provides a Proof of Exploit, meaning that you can avoid wasting time on manual verifications. This enables you to spend time fixing vulnerabilities instead.

WEB APPLICATION SECURITY SCANNING FLOW

Acunetix 360 is one of the leaders in terms of accuracy and employs several different techniques aimed at reducing false positives. Acunetix 360 provides a Proof of Exploit, meaning that you can avoid wasting time on manual verifications. This enables you to spend time fixing vulnerabilities instead.

1 Knowing your web application

2 Preparing and configuring scans

3 Scanning your web applications

4 Reviewing and comparing scan results with previous scans

5 Fixing issues

6 Retesting fixed issues

7 Generating reports

A COMPLETE WEB SECURITY SOLUTION

Acunetix 360 is available Online or On-Premises. It allows you to scan multiple websites at the same time, provides dashboards that deliver an overview of the security state of your web applications, and lots of features to help you to scan websites, manage issues and run reports.

Helpful links for further information:

- [What is Acunetix 360?](#)
- [Web Application Security Scanning Flow](#)

INSTALLATION

Now that you know how Acunetix 360 works, here is a quick look into the deployment differences between Acunetix 360 On-Premises and Acunetix 360 Online.

ACUNETIX 360 ON-PREMISES

Acunetix 360 On-Premises is an edition that you install on your own infrastructure. The typical motivation behind this choice is to keep all the resulting data stored in-house.

For more details regarding the installation steps, start with [Installing and Configuring Acunetix 360 On-Premises](#).

Once the installation is complete, you can log in using the credentials created during the installation.

ACUNETIX 360 ONLINE

Acunetix 360 Online is a cloud-based web application security scanner. As soon as your license is activated, you will receive an invitation email. Simply click on the link in the invitation email to create your credentials, and then log in.

SYSTEM REQUIREMENTS

A complete installation of Acunetix 360 has 4 components, with the following recommended requirements:

Acunetix 360 Application Server

- Windows Server 2019 with IIS role and .NET Framework 4.7.2
- 2GHz Processor or faster
- 8Gb RAM or more
- 20Gb Disk space or more

Acunetix 360 Agent

- Windows Server 2019 with .NET Framework 4.7.2
- 2GHz Processor or faster
- 4Gb RAM or more
- 5Gb Disk space or more

Acunetix 360 Authentication Verifier

- Windows Server 2012 R2 with .NET Framework 4.7.2
- 2GHz Processor or faster
- 4Gb RAM or more
- 5Gb Disk space or more

Database Server

- Microsoft SQL Server 2012 or later
- 2GHz Processor or faster
- 4Gb RAM or more
- 6Gb Disk space or more

Edit Team Member

Name

Developer Demo - Marketing Sales

Email

demo-marketing@acunetix.com

Phone Number

🇺🇸 (201) 555-0123

Time Zone

(UTC+03:00) Istanbul

Date and Time Format

dd/MM/yyyy

Password

Confirm Password

A good password should contain 8 - 256 characters. As you mix lowercase/uppercase letters, digits and non-word characters it will become stronger. You are also encouraged to use a [pass phrase](#).

User Account Status

User State

Enabled Disabled

Access Type

☒ API Access

Account Permissions

☐ Application Administrator
☐ Account Administrator
☐ Manage Websites

Scan Permissions

☐ Start Scans
☒ View Scan Reports
☒ Manage Issues
☒ Manage Issues (Restricted)

Website Groups

☒ Select All
☐ Select None
☒ Inverse Selection

Filter Website Groups

Start typing to filter the website groups

☐ Default
☒ Marketing Sites

Checked Scan and Website management permissions apply to the selected website groups.

3

SETTING UP YOUR TEAM & USER PERMISSIONS

Now that you have logged in to your Acunetix account, let's look at how to set up your team and user permissions.

ADMINISTRATIVE ACCESS REQUIRED

Management of Teams and User Permissions is restricted to Administrator-level users only.

Setting up user permissions at the beginning means that the relevant users will have access to the relevant features. They can get started detecting and fixing vulnerabilities immediately.

1. To set up your team, go to **Managing Team Members in Acunetix 360**.
2. For each team member, you also need to **Configure User Permissions in Acunetix 360**. The **User Permissions Matrix in Acunetix 360** will help you understand what each permission enables users to do.

USERS WITH ADMINISTRATOR PERMISSIONS CAN CREATE AND MANAGE TEAMS

Name	Email	User State	2FA Enabled	
Erman Ates	erman.ates@acunetix.com	Enabled	No	
Maria K. Hoffman	MariaKHoffman@acunetix.com	Enabled	Yes	Edit
Debra W. Young	DebraWYoung@acunetix.com	Enabled	No	Edit
Willie C. Murray	WillieCMurray@acunetix.com	Enabled	No	Edit
Joey L. Derosa	JoeyLDerosa@acunetix.com	Enabled	Yes	Edit

Export to CSV New Team Member My Account

Displaying 5 of 5 items

ADDING TARGET WEBSITE APPLICATIONS



Now that you have set up your team and user permissions, it is important to understand how to add a target website. Adding your target website before launching a scan is a necessary step so that Acunetix knows which sites you would like to scan.

Important Licensing Information

1. Acunetix 360 licensing revolves around the number of targets that you enter into the system. Once a domain name has been scanned, it counts towards your license; you cannot switch out a site that has already been scanned for a different site you need to scan.
2. Remember to delete any domain names added during your Acunetix 360 trial.
3. Keep in mind that you can change your domain names only once a year.

Acunetix 360 Online users need to verify the ownership of this website prior to scanning. If you have multiple websites to scan, you can contact the Acunetix support team to whitelist your account. This will enable you to scan all your websites without ownership verification.

Adding A Website

1. Click  Website, then *New Website*
2. Complete the *Name*, *URL* and other information.
3. Click 

VERIFYING OWNERSHIP

You can Verify Ownership of a Website by HTML File Upload, Meta Tag Verification, TXT Records in DNS Verification or Email Verification. You can do this in the Manage Websites window. Complete the relevant fields. Follow the instructions in [Verifying Website Ownership](#).

We recommend that you act responsibly and make sure that you are authorised to scan the website first. Remember that during the scan your website will be attacked. See [Do Acunetix Scans Damage Web Applications?](#)

LAUNCHING A SCAN

Your target websites are all set up and 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 360 is an easy to use, automated web application security scanner. It provides many default configurations including: Default Scan Policy with built-in Security Checks, Report Policy, Maximum Scan Duration, Scan Scope, Heuristic URL Rewrite Mode, and Notifications. This makes it easy to get started quickly. To understand the scan settings in detail, start with [Creating a New Scan](#).

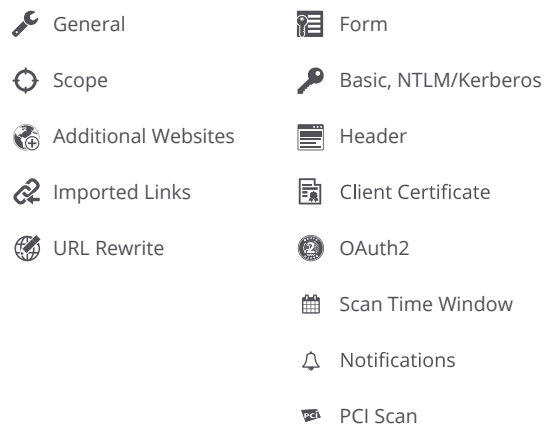
SCAN DURATION

Remember that scan duration may vary depending on the size of the web application and the security checks enabled in the Scan Policy you've selected.

USING CUSTOMIZED SETTINGS

Authentication and Scope settings are very important for a web application scan. If you enter the proper configurations, Acunetix 360 will fine tune itself automatically. However, in some cases, you may want to consider customizing scans by configuring further scan settings.

For example, many web applications have sections reserved only for authorized (signed-in) users. In these cases, you can configure various authentication methods, to make sure Acunetix 360 has access to those sections, and can conduct scanning there too. See [Types of Scans](#) for more scanning options.



To understand each setting and how to configure it, see [Acunetix 360 Scan Options Fields](#).

CUSTOM SCAN PROFILES

If you decide to configure some or all of these options in Acunetix 360, you can save your configuration as a Scan Profile (see [Overview of Scan Profiles](#)) to reuse it for future scans. Saved Scan Profiles are available by clicking the gear icon.

6

REVIEWING SCAN RESULTS

Now that you've launched your scan, you are ready to review the scan results. Reviewing scan results in the Issues and Dashboard windows is important for several reasons.

In the Issues window, you can see a list of each individual issue and where it was found. You can find out about the varying types of findings detected on your scanned websites, not just the vulnerabilities. Some of these include information that may be useful to attackers.

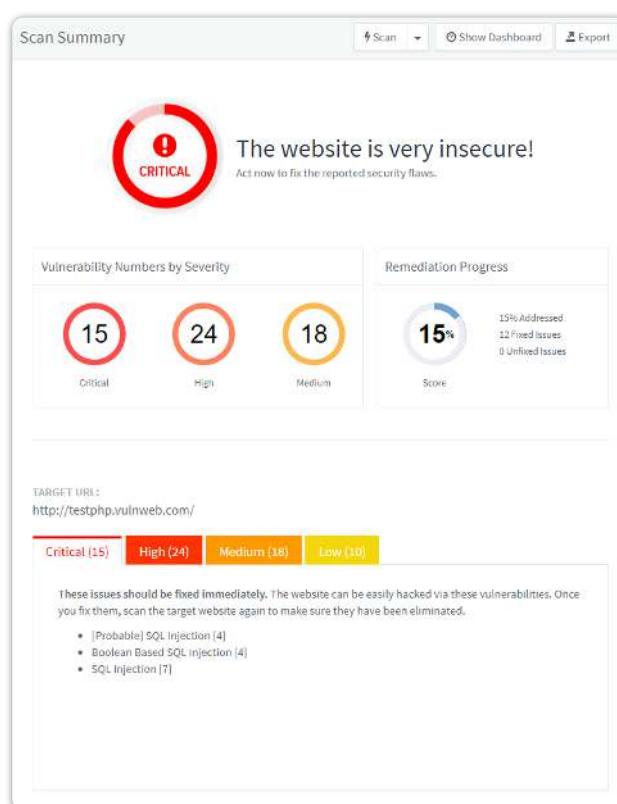
- 1 Learn vulnerability severity levels
- 2 Gain an overview of the security state
- 3 Check the scan summary and impacts
- 4 Review the issues and remedies
- 5 Fix the vulnerabilities and retest
- 6 Update the status of the issues

In this section, you will learn how we categorise detected vulnerabilities, how to interpret ongoing and completed scan results, and what to do once you have fixed an issue.

First, read up on [Vulnerability Severity Levels](#), so you can understand how we categorise detected vulnerabilities in scan results (by severity). This will help you prioritize which ones to tackle first.

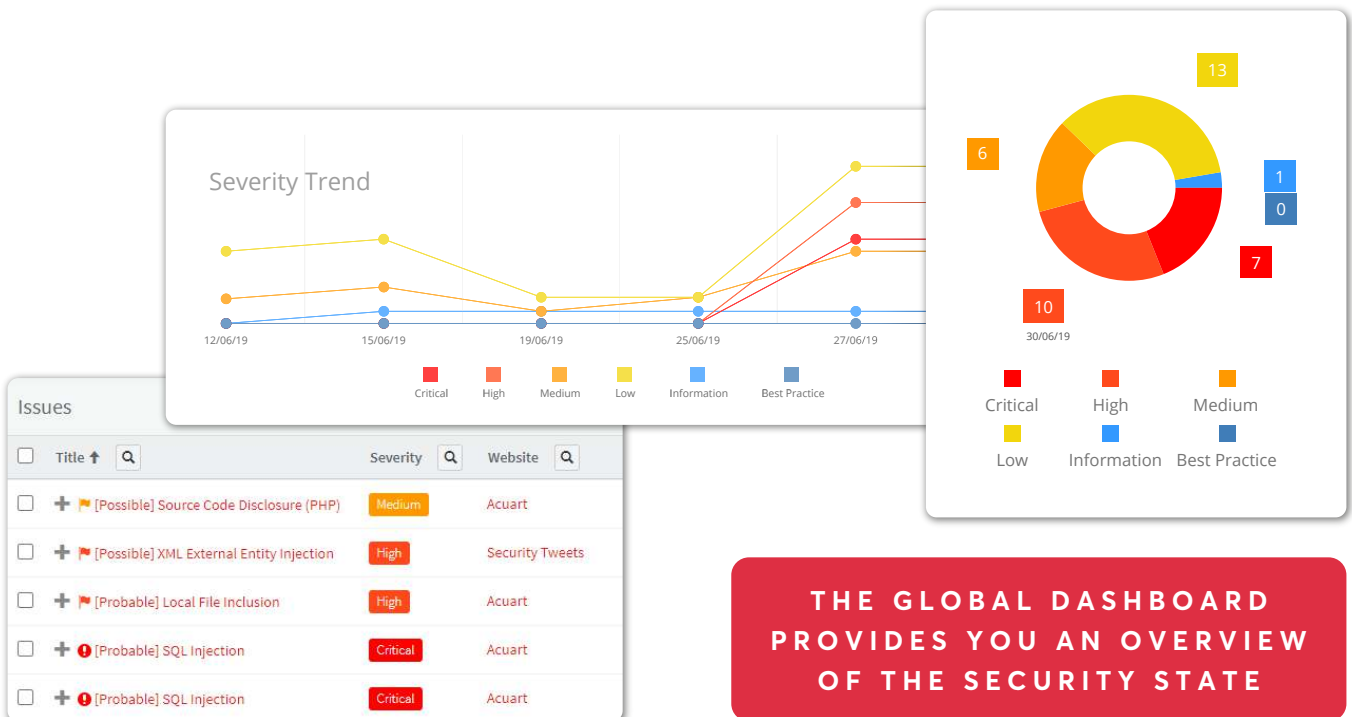
WHAT IS GOING ON DURING SCANNING?

- Acunetix 360 is crawling and attacking discovered pages.
- Start with [Viewing the Scan Summary Dashboard in Acunetix 360](#) to see the discovered issues during scanning.



WHAT IS GOING ON DURING SCANNING?

You can view the dashboards again; or you can gain an overview of the security state of all your web applications by [Viewing the Global Dashboard in Acunetix 360](#); or you can get a detailed view of all issues found by [Viewing Issues in Acunetix 360](#).



WHAT SHOULD I DO WITH DETECTED ISSUES?

- First, have a look at [Managing Issues](#).
- Next, move on to [Fixing a Vulnerability and Updating the Status of an Issue in Acunetix 360](#).

The screenshot shows the details of a Cross-site Scripting (CSC) issue. The issue is marked as **CONFIRMED** and **HIGH**. The URL is `http://testphp.vulnweb.com/listproducts.php?cat=%3cscript%3enetsparker(0x008A30)%3c%2fscript%3e`. The parameter name is `cat` and the parameter type is `GET`. The attack pattern is `<script>netsparker(0x008A30)</script>`. The issue is marked as **Retestable** with a green checkmark.

Vulnerability Details

Acunetix 360 detected Cross-site Scripting, which allows an attacker to execute a dynamic script (*JavaScript, VBScript*) in the context of the application. This allows several different attack opportunities, mostly hijacking the current session of the user or changing the look of the page by changing the HTML on the fly to steal the user's credentials. This happens because the input entered by a user has been interpreted as HTML/JavaScript/VBScript by the browser. Cross-site scripting targets the users of the application instead of the server. Although this is a limitation, since it allows attackers to hijack other users' sessions, an attacker might attack an administrator to gain full control over the application.

Parameters

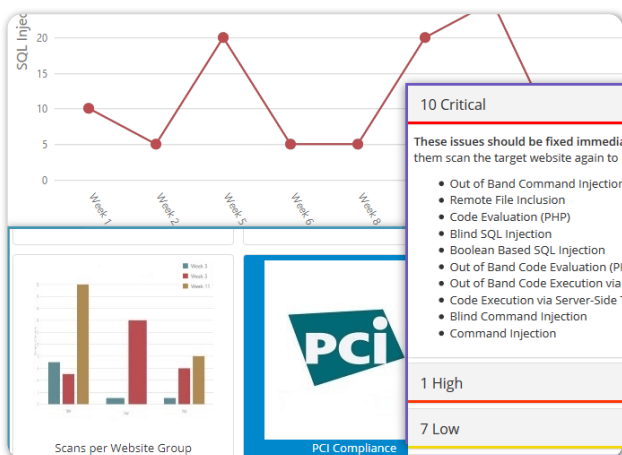
Parameter Name	Parameter Type	Attack Pattern
cat	GET	<script>netsparker(0x008A30)</script>

CREATING A SCAN REPORT

Now that you have reviewed your scan results, you can create various types of reports. Reporting is the last stage of the Web Application Security Scanning Flow and an important one, because it gives different users and departments all the information they need to take care of in their areas of responsibility.

WHY DO WE NEED REPORTS?

Managers need security reports that cover basic information on discovered issues and possible impacts. For further information see [Why Do We Need Reports?](#)



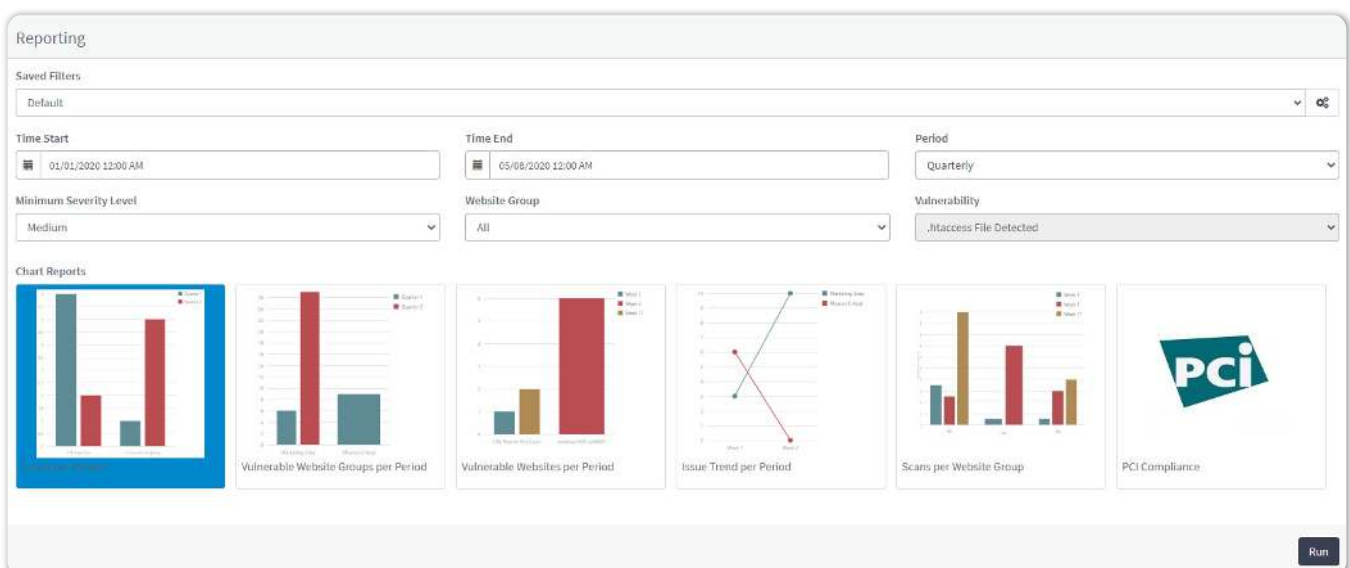
Acunetix 360 allows you to generate PCI compliance reports, approved by an ASV (Approved Scanning Vendor).

- **Built in Reports** - Including generic Trend and Status security reports
- **Report Templates** - For generating and downloading reports, including compliance reports
- **Statistical Reports**

Developers require more detailed information in order to begin fixing detected vulnerabilities.

In addition to [Reviewing Scan Results](#) you can also generate a [Detailed Scan Report](#).

**REPORTS HELP YOU MEET
COMPLIANCE REGULATIONS
SUCH AS ISO 27001,
HIPAA AND PCI.**



Integration with Desktop Tools

Acunetix and Netsparker are sister brands owned by Invicti Security. This relationship brings an additional entitlement; Acunetix 360 users also get a license to use Netsparker Standard.

Integration between Acunetix 360 and Netsparker Standard allows any scanning data compiled by Netsparker Standard to be imported into Acunetix 360; this additional data will be combined and used with the other data inside Acunetix 360.

Integration with DevOps, SDLC, and Other Systems

Acunetix 360 is a complete web application security solution that integrates with your existing environments, such as issue trackers, vulnerability management systems, and CI/CD platforms. This allows you to fully incorporate web app security into your Software Development Life Cycle (SDLC).

Acunetix 360 provides integration features for a very wide range of related tools and services in the following areas:

- Issue Tracking
- Project Management
- Continuous Integration
- Continuous Development
- Communications
- APIs
- Single Sign-On Providers
- Web Application Firewalls

For a more complete list of the available integrations, check out [What Systems Does Acunetix 360 Integrate With?](#)

SUPPORT

If you need help with anything mentioned in this guide, contact support@acunetix.com.

ABOUT ACUNETIX

Acunetix is a global web security leader. As the first company to build a fully dedicated and fully automated web vulnerability scanner, Acunetix carries unparalleled experience in the field. The Acunetix web vulnerability scanning platform has been recognized as a leading solution multiple times. It is also trusted by customers from the most demanding sectors including many fortune 500 companies.

Our mission is to provide you with a trustworthy web security solution that protects all your assets, aligns with all your policies, and fits perfectly into your development lifecycle. The Acunetix platform frees up your security team resources. It can detect vulnerabilities that other technologies would miss because it combines the best of dynamic and static scanning technologies and uses a separate monitoring agent. It is your platform of choice for comprehensive web vulnerability assessment and vulnerability management.



WHERE TO FIND US

Stay up to date with the latest web security news.

Website. www.acunetix.com

Acunetix Web Security Blog. acunetix.com/blog

Facebook. facebook.com/acunetix

Twitter. twitter.com/acunetix

CONTACT INFORMATION

Acunetix (Europe and ROW)

Tel. +44 (0) 330 202 0190

Fax. +44 (0) 30 202 0191

Email. sales@acunetix.com

Acunetix (USA)

Tel. (+1) 737 241 8773

Fax. (+1) 737 600 8810

Email. salesusa@acunetix.com