



Online Vulnerability Scanner
User Manual

Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Acunetix Ltd.

Acunetix Online Vulnerability Scanner is copyright of Acunetix Ltd. 2004–2015.

Acunetix Ltd. All rights reserved.

<http://www.acunetix.com>

info@acunetix.com

Document version 4.0

Last updated: 2nd March 2015

Table of Contents

- Introduction
- Overview
- Registration and Evaluation
- Configuring Scan Targets
- Installing AcuSensor
- Launching Scans
- Analysing Scan Results
- Generating Reports
- Acunetix Reports
- Configuring Child Accounts
- Troubleshooting and Support

Introduction to Acunetix Web Vulnerability Scanner

Why You Need To Secure Your Web Applications

Website security is today's most overlooked aspect of securing an enterprise and should be a priority in any organization. Increasingly, hackers are concentrating their efforts on web-based applications – shopping carts, forms, login pages, dynamic content, etc. Accessible 24/7 from anywhere in the world, insecure web applications provide easy access to backend corporate databases and also allow hackers to perform illegal activities using the attacked sites. A victim's website can be used to launch criminal activities such as hosting phishing sites or to transfer illicit content, while abusing the website's bandwidth and making its owner liable for these unlawful acts.

Hackers already have a wide repertoire of attacks that they regularly launch against organizations including SQL Injection, Cross Site Scripting, Directory Traversal Attacks, Parameter Manipulation (e.g., URL, Cookie, HTTP headers, web forms), Authentication Attacks, Directory Enumeration and other exploits.

The hacking community is also very close-knit; newly discovered web application intrusions, known as Zero Day exploits, are posted on a number of forums and websites known only to members of that exclusive underground group. Postings are updated daily and are used to propagate and facilitate further hacking.

Web applications – shopping carts, forms, login pages, dynamic content, and other bespoke applications – are designed to allow your website visitors to retrieve and submit dynamic content including varying levels of personal and sensitive data.

If these web applications are not secure, then your entire database of sensitive information is at serious risk. A Gartner Group study reveals that 75% of cyber-attacks are done at the web application level.

Why are web applications vulnerable?

- Websites and web applications are easily available via the internet 24 hours a day, 7 days a week to customers, employees, suppliers and therefore also hackers.
- Firewalls and SSL provide no protection against web application hacking, simply because access to the website has to be made public.
- Web applications often have direct access to backend data such as customer databases.
- Most web applications are custom-made and, therefore, involve a lesser degree of testing than off-the-shelf software. Consequently, custom applications are more susceptible to attack.
- Various high-profile hacking attacks have proven that web application security remains the most critical. If your web applications are compromised, hackers will have complete access to your backend data even though your firewall is configured correctly and your operating system and applications are patched repeatedly.
- Network security defense provides no protection against web application attacks since these are launched on port 80 which has to remain open to allow regular

operation of the business. It is therefore imperative that you regularly and consistently audit your web applications for exploitable vulnerabilities.

The need for automated web application security scanning

Manual vulnerability auditing of all your web applications is complex and time-consuming, since it generally involves processing a large volume of data. It also demands a high level of expertise and the ability to keep track of considerable volumes of code used in a web application. In addition, hackers are constantly finding new ways to exploit your web application, which means that you would have to constantly monitor the security communities, and find new vulnerabilities in your web application code before hackers discover them.

Automated vulnerability scanning allows you to focus on the already challenging task of building a web application. An automated web application scanner is always on the lookout for new attack paths that hackers can use to access your web application or the data behind it.

Within minutes, an automated web application scanner can scan your web application, identify all the files accessible from the internet and simulate hacker activity in order to identify vulnerable components.

In addition, an automated vulnerability scanner can also be used to assess the code which makes up a web application, allowing it to identify potential vulnerabilities which might not be obvious from the internet, but still exist in the web application, and can thus still be exploited.

Acunetix Web Vulnerability Scanner

Acunetix Web Vulnerability Scanner is an automated web application security testing tool that audits your web applications by checking for vulnerabilities like SQL Injection, Cross site scripting and other exploitable vulnerabilities. In general, Acunetix Web Vulnerability Scanner scans any website or web application that is accessible via a web browser and uses the HTTP/HTTPS protocol.

Acunetix Web Vulnerability Scanner offers a strong and unique solution for analyzing off-the-shelf and custom web applications including those utilizing JavaScript, AJAX and Web 2.0 web applications. Acunetix has an advanced crawler that can find almost any file. This is important since what is not found cannot be checked.

How Acunetix Web Vulnerability Scanner Works

Acunetix Web Vulnerability Scanner works in the following manner:

1. Acunetix DeepScan analyses the entire website by following all the links on the site, including links which are dynamically constructed using JavaScript, and links found in robots.txt and sitemap.xml (if available). The result is a map of the site, which Acunetix Web Vulnerability Scanner will use to launch targeted checks against each part of the site.

Name	HTTP Result	Inputs	Title	Content Type
http://testphp.vulnweb.com/				
+	Ok (200)		Home of Acune...	text/html
+.idea	Ok (200)		Index of /.idea	text/html
+.admin	Ok (200)		Index of /admin	text/html
+.AJAX	Ok (200)		ajax test	text/html
+.Connections	Ok (200)		Index of /Conn...	text/html
+.CVS	Ok (200)		Index of /CVS	text/html
+.Flash	Ok (200)		Index of /Flash	text/html
+.hpp	Ok (200)	1	HTTP Paramete...	text/html
+.icons	Not Found...			text/html

Screenshot - Crawler Results

2. If Acunetix AcuSensor Technology is enabled, the sensor will retrieve a listing of all the files present in the web application directory and add the files not found by the crawler to the crawler output. Such files usually are not discovered by the crawler as they are not accessible from the web server, or not linked through the website. Acunetix AcuSensor also analyses files which are not accessible from the internet, such as *web.config*.
3. After the crawling process, the Web Vulnerability Scanner automatically launches a series of vulnerability checks on each page found, in essence emulating a hacker. Acunetix Web Vulnerability Scanner also analyses each page for places where it can input data, and subsequently attempts all the different input combinations. This is the Automated Scan Stage. If the AcuSensor Technology is enabled, a series of additional vulnerability checks are launched against the website. More information about AcuSensor is provided in the following section.

The screenshot displays the Acunetix Scan Results interface. On the left, a tree view shows 'Scan Thread 1 (http://testphp.vulnweb.com)' with 'Web Alerts (185)'. A list of vulnerabilities is shown, including 'Blind SQL Injection (15)', 'CRLF injection/HTTP response splitting', 'Cross Site Scripting (verified) (26)', 'Directory Traversal (verified) (3)', 'HTTP Parameter Pollution (2)', 'Macromedia Dreamweaver Remote', 'PHP allow_url_fopen enabled (1)', 'Script source code disclosure (1)', 'SQL injection (verified) (26)', 'Weak Password (1)', 'Application error message (6)', 'Backup files (2)', 'Directory Listing (14)', and 'Error message on page (7)'. On the right, a detailed view of the 'Blind SQL Injection' alert is shown, marked as 'Severity HIGH'. The 'Vulnerability description' states: 'This script is possibly vulnerable to SQL Injection attacks. SQL injection is a vulnerability that allows an attacker to alter backend SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters. This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.' The 'Affected items' section is also visible.

Screenshot - Scan Results

4. The vulnerabilities identified are shown in the Scan Results. Each vulnerability alert contains information about the vulnerability such as POST data used, affected item, http response of the server and more.
5. If AcuSensor Technology is used details such as source code line number, stack trace or affected SQL query which lead to the vulnerability are listed. Recommendations on how to fix the vulnerability are also shown.

6. Various reports can be generated on completed scans, including Executive Summary report, Developer report and various compliance reports such as PCI or ISO 270001.

Acunetix AcuSensor Technology

Acunetix's unique AcuSensor Technology allows you to identify more vulnerabilities than other Web Application Scanners, whilst generating less false positives. Acunetix AcuSensor indicates exactly where in your code the vulnerability is and reports additional debug information.

SQL injection (verified)Severity HIGH

Vulnerability description

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This vulnerability affects [/listproducts.php](#).

Discovered by: Scripting (Sql_Injection.script).

AcuSensor
TECHNOLOGY

Vulnerability details

Source file: [/hj/var/www/listproducts.php](#) line: **43**

Additional details:

```
SQL query: SELECT * FROM users WHERE uname='1ACUSTART'"C33MmACUEND' AND pass=''
"mysql_query" was called.
```

Attack details

Cookie input **login** was set to **1ACUSTART"C33MmACUEND**

[View HTTP headers](#)

[View HTML response](#)

Screenshot - AcuSensor pinpoints vulnerabilities in code

The increased accuracy, available for PHP and .NET web applications, is achieved by combining black box scanning techniques with feedback from sensors placed inside the source code. Black box scanning does not know how the application reacts and source code analyzers do not understand how the application will behave while it is being attacked. AcuSensor technology combines both techniques to achieve significantly better results than using source code analyzers and black box scanning independently.

The AcuSensor sensors can be inserted in the .NET and PHP code transparently. The .NET source code is not required; the sensors can be injected in already compiled .NET

applications! Thus there is no need to install a compiler or obtain the web applications' source code, which is a big advantage when using a third party .NET application. In case of PHP web applications, the source is readily available. To date, Acunetix is the only Web Vulnerability Scanner to implement this technology.

Advantages of using AcuSensor Technology

- Ability to provide more information about the vulnerability, such as source code line number, stack trace, affected SQL query.
- Allows you to locate and fix the vulnerability faster because of the ability to provide more information about the vulnerability, such as source code line number, stack trace, affected SQL query, etc.
- Significantly reduces false positives when scanning a website because it understands the behavior of the web application better.
- Alerts you to web application configuration problems which can result in a vulnerable application or expose sensitive information. E.g. If 'custom errors' are enabled in .NET, this could expose sensitive application details to a malicious user.
- Advises you how to better secure your web server settings, e.g. if write access is enabled on the web server.
- Detects more SQL injection vulnerabilities. Previously SQL injection vulnerabilities could only be found if database errors were reported, whereas now the source code can be analyzed for improved detection.
- Ability to detect SQL injection vulnerabilities in all SQL statements, including in SQL INSERT statements. Using a black box scanner such SQL injection vulnerabilities cannot be found. This significantly increases the ability for Acunetix Web Vulnerability Scanner to find vulnerabilities.
- Discovers all the files present and accessible through the web server. If an attacker gains access to the website and creates a backdoor file in the application directory, the file is found and scanned when using the AcuSensor Technology and you will be alerted.
- AcuSensor Technology is able to intercept all web application inputs and build a comprehensive list with all possible inputs in the website and test them.
- No need to write URL rewrite rules when scanning web applications which use search engine friendly URL's! Using the AcuSensor Technology the scanner is able to rewrite SEO URL's on the fly.
- Ability to test for arbitrary file creation and deletion vulnerabilities. E.g. Through a vulnerable script a malicious user can create a file in the web application directory and execute it to have privileged access, or delete sensitive web application files.
- Ability to test for email injection. E.g. A malicious user may append additional information such as a list of recipients or additional information to the message body to a vulnerable web form, to spam a large number of recipients anonymously.

Network Vulnerability Scanning

As part of a website audit, Acunetix will execute a network security audit of the server hosting the website. This network security scan will identify any services running on the scanned server by running a port scan on the system. Acunetix will report the operating system and

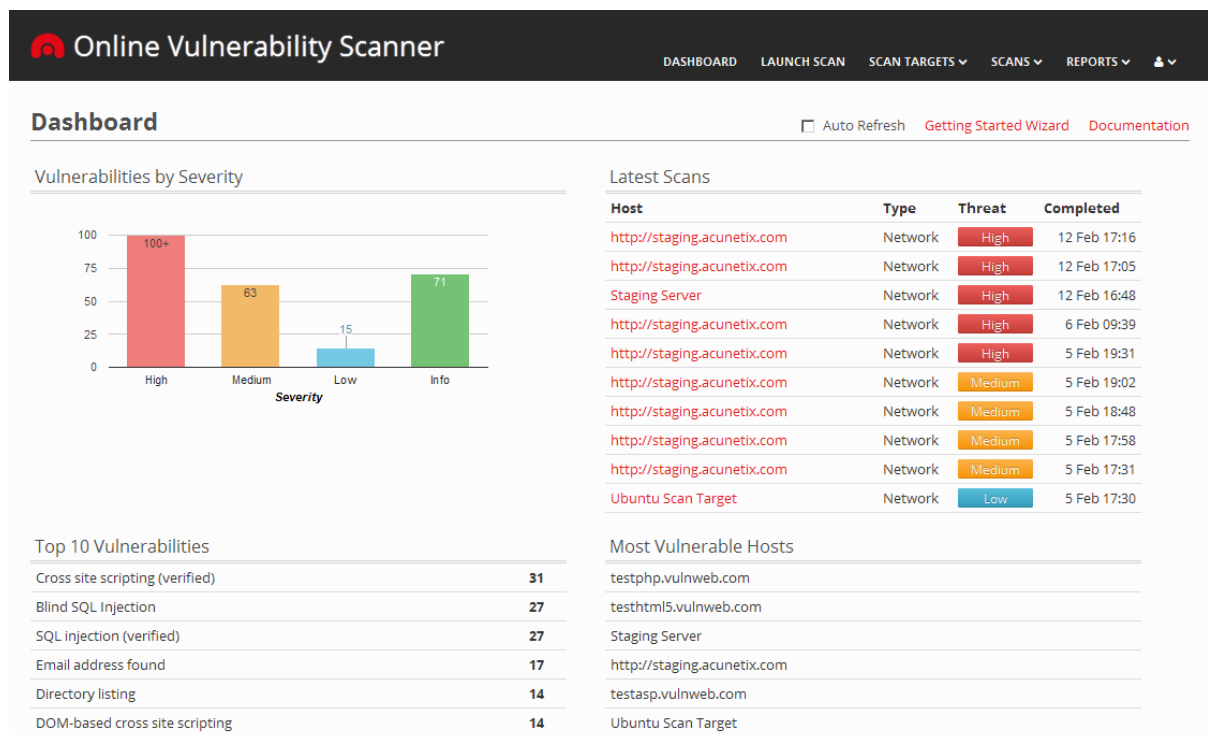
the software hosting the services detected. This process will also identify Trojans which might be lurking on the server.

The network vulnerability scan assesses the security of popular protocols such as FTP, DNS, SMTP, IMAP, POP3, SSH, SNMP and Telnet. Apart from testing for weak or default passwords, Acunetix will also check for misconfiguration in the services detected which could lead to a security breach. Acunetix will also check that any other servers running on the machine are not using any deprecated protocols. All these lead to an insecure system, which would allow an intruder to damage your web site and your reputation.

Acunetix Online Vulnerability Scanner (OVS) also integrates the popular OpenVAS network scanner to check for over 35,000 network vulnerabilities. During a network scan, Acunetix OVS makes use of various port probing and OS fingerprinting techniques to identify a vast number of devices, Operating Systems and server products. Numerous security checks are then launched against the products identified running on the scanned server, allowing you to detect all the vulnerabilities that exist on your perimeter servers.

Overview

Acunetix Online Vulnerability Scanner (OVS) is a highly effective solution which helps you to identify web and network vulnerabilities in your Internet-facing web sites, web applications and any other perimeter servers. Acunetix OVS consists of the following components:



Screenshot - Acunetix WVS User Interface

Dashboard

The dashboard provides a general overview of the security of your scan targets. From here, you can easily check:

- how many vulnerabilities have been detected, grouped by severity
- the threat level identified for recent scans
- the vulnerabilities that are identified most frequently
- the most vulnerable hosts
- upcoming scans

When you start using Acunetix OVS, you will be shown the Getting Started Wizard instead of the Dashboard.

Scan Targets

Online Vulnerability Scanner

DASHBOARD LAUNCH SCAN SCAN TARGETS SCANS REPORTS

Scan Targets

Scan Now Schedule a Scan Add Scan Target

Select the Scan Target(s) to be scanned.
All scans are done from **scanners.acunetix.com**. Please configure any firewalls / WAFs accordingly.

Unverified Scan Targets cannot be scanned. Check the *Status* column for more information.

<input type="checkbox"/>	Name ^	Host ^	Status	
<input type="checkbox"/>	Staging Server	http://staging.acunetix.com	Verified (full scans allowed)	
<input type="checkbox"/>	Test ASP	http://testasp.vulnweb.com	Demo (full scans allowed)	
<input type="checkbox"/>	Test HTML5	http://testhtml5.vulnweb.com	Demo (full scans allowed)	
<input type="checkbox"/>	Test PHP	http://testphp.vulnweb.com	Demo (full scans allowed)	
<input type="checkbox"/>	Ubuntu Scan Target	51.152.92.57	Partially Verified (Network scans allowed)	

Online Vulnerability Scanner © 2015 Acunetix Ltd.


Screenshot - Scan Targets list


This is where you configure the servers that you would like Acunetix OVS to scan. From the Scan Targets drop down, you can add Scan Targets, list all your Scan Targets and configure Scan Target Groups.

Launch Scans

This is where you can launch scans against your Scan Targets. Scan can be configured to occur immediately or scheduled to start at a later date. Scans can also be configured to recur on a regular basis (e.g. every week or every month).


Scans


















 Online Vulnerability Scanner

DASHBOARD LAUNCH SCAN SCAN TARGETS ▾ SCANS ▾ REPORTS ▾ 

Alerts (132) Knowledge Base (8) Severity [Generate Report](#)

Start Date 20 Jan 2015 11:52	Files 94	Requests 56145	Host Name http://testphp.vulnweb.com
End Date 20 Jan 2015 12:12	Directories 33	Avg. Response Time 119.06 ms	Scan Target Name Test PHP
Duration 0h 20m 0s	Variations 26	Responsive Yes	Scan Type Web



Name	Module
+  Blind SQL Injection (27)	Scripting (Blind_Sql_Injection.script)
+  CRLF Injection/HTTP response splitting (verified) (1)	Scripting (CRLF_Injection.script)
+  Cross site scripting (2)	Scripting (Remote_File_Inclusion_XSS.script)
+  Cross site scripting (verified) (27)	Scripting (XSS.script)
+  Directory traversal (verified) (2)	Scripting (Directory_Traversal.script)
+  HTTP parameter pollution (2)	Scripting (HTTP_Parameter_Pollution.script)
+  nginx SPDY heap buffer overflow (1)	Scripting (Version_Check.script)
+  Script source code disclosure (1)	Scripting (Script_Source_Code_Disclosure.script)
+  Server side request forgery (2)	Scripting (Server_Side_Request_Forgery.script)
+  SQL injection (verified) (27)	Scripting (Sql_Injection.script)
+  Weak password (1)	Scripting (Html_Authentication_Audit.script)
+  .htaccess file readable (1)	Scripting (htaccess_File_Readable.script)
+  Application error message (6)	Scripting (Error_Message.script)
+  Backup files (2)	Scripting (Backup_File.script)
+  Directory listing (14)	Scripting (Directory_Listing.script)
+  Error message on page (7)	Scripting (Text_Search_File.script)
+  HTML form without CSRF protection (5)	Crawler

Screenshot - Scan Results

You can view your scans from the Scans drop down. Here you can monitor the status of your current scans, view the scan results and the alerts for the scans that have completed and generate reports for your finished scans.

Reports

The screenshot shows the 'Online Vulnerability Scanner' interface. At the top, there is a navigation bar with links: DASHBOARD, LAUNCH SCAN, SCAN TARGETS, SCANS, and REPORTS. The 'REPORTS' section is active, showing a 'Saved Reports' page. Below the header, there are filters for 'Scan Target', 'Status', and 'Scan Type', all set to 'All'. A 'Filter' button is on the right. An information icon and text state: 'Below is the list of reports that have been generated in the past.' Below this is a table with 7 columns: Scan Date, Scan Type, Scan Profile, Scan Target, Report Type, Report Format, and Status. The table contains 10 rows of report data. Each row has a 'Download' link with an external icon. At the bottom, there is a footer with 'Online Vulnerability Scanner © 2015 Acunetix Ltd.' and social media icons.

Scan Date	Scan Type	Scan Profile	Scan Target	Report Type	Report Format	Status
17 Dec 2014 12:02	Web	XSS	Test ASP	Affected Items	PDF	Download
12 Nov 2014 10:50	Web	XSS	Test HTML5	Affected Items	PDF	Download
12 Nov 2014 10:49	Web	XSS	Test PHP	Affected Items	PDF	Download
17 Dec 2014 12:03	Network	Full Scan (safe checks)	Test ASP	Network Security Report	PDF	Download
17 Dec 2014 12:03	Network	Full Scan (safe checks)	Test ASP	Network Security Report	RTF	Download
17 Dec 2014 12:02	Web	XSS	Test ASP	Quick Report	PDF	Download
12 Nov 2014 10:49	Web	XSS	Test PHP	PCI 3.0	PDF	Download
12 Nov 2014 10:49	Web	XSS	Test PHP	Affected Items	RTF	Download
12 Nov 2014 10:50	Web	XSS	Test HTML5	Quick Report	PDF	Download

Screenshot - Saved Reports

Reports can be generated from the Reports drop down too. All the reports are stored in your account, and can also be accessed from the Reports section.

Profile

Here you can view and edit your user details. You can also request that your account details are verified by an Acunetix representative - this is required before you can launch network scans on your scan targets.

Registration

First, you need to register with Acunetix OVS before you can start running scans. If you have not already registered, visit

<http://www.acunetix.com/vulnerability-scanner/register-online-vulnerability-scanner/> to start your trial. Make sure that your details are correct as we will need these details in the manual review of your registration. Read and accept the Terms of Service and click the 'Register' button when done.

A confirmation email will be sent to the email address provided. Click on the link in the email, to complete your registration. At this stage, you will be asked for a password which needs to be at least 8 characters, and contain 3 of the following – a number, a small letter, a capital letter and a special character (e.g. !@#\$%).

Important: All registrations are manually reviewed. Perimeter network scans are only made available for accounts where their details are confirmed to be correct.

Acunetix OVS Trial

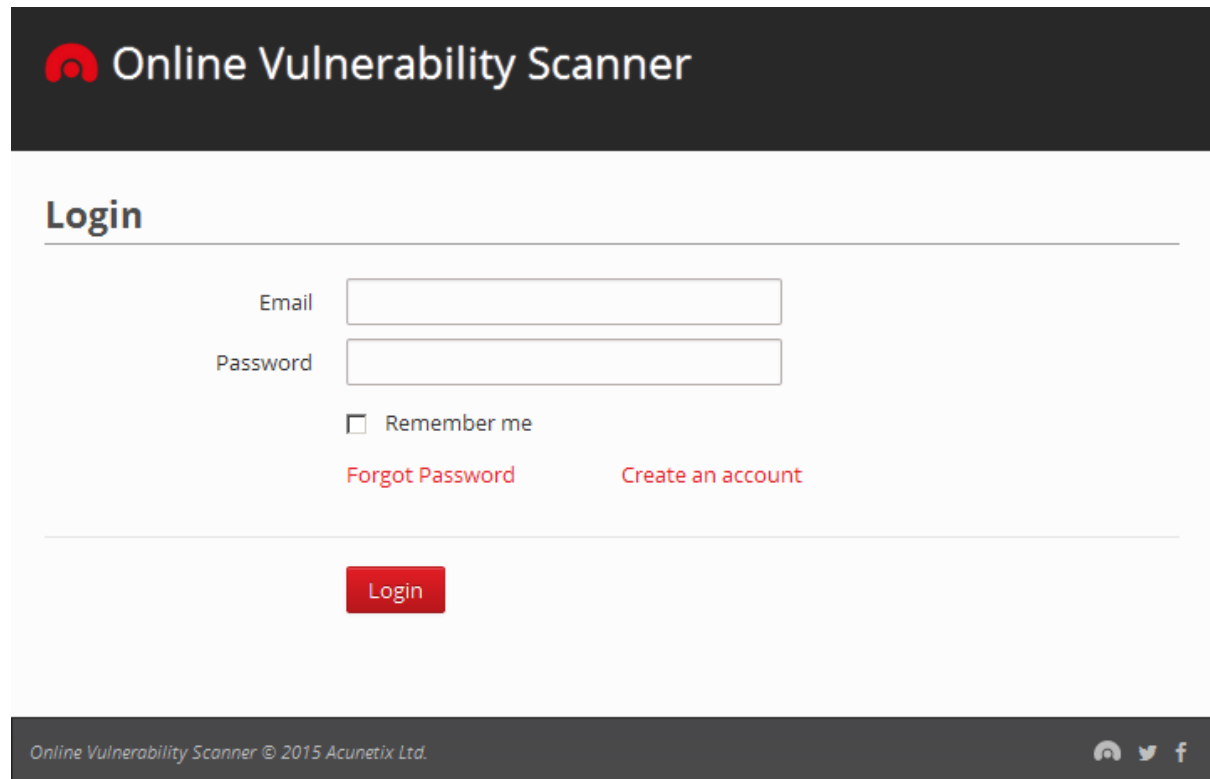
Your Acunetix OVS Trial starts the moment you confirm your account registration. The Acunetix OVS Trial is practically identical to the full version in functionality and features, but contains the following limitations:

- The Trial expires in 14 days
- You can configure up to 2 Scan Targets of your choice
- You can launch up to 2 FULL Network Scans against these Scan Targets
- You can launch up to 2 LIMITED Web Scans against these Scan Targets. You will be notified of the vulnerabilities detected, but the details, remediation advice and PDF reports will not be available. You can download the [Sample web reports](#).

You can also launch FULL web and network scans, by configuring any 2 of the following Acunetix test sites as Scan Targets and running scans against them.

- <http://testphp.vulnweb.com>
- <http://testasp.vulnweb.com>
- <http://testaspnet.vulnweb.com>
- <http://testhtml5.vulnweb.com>

Logging in



The screenshot shows the login interface for the Online Vulnerability Scanner. At the top, a dark header contains the Acunetix logo and the text "Online Vulnerability Scanner". Below this, the word "Login" is displayed in a large, bold font. The login form consists of two input fields: "Email" and "Password". Below the password field is a checkbox labeled "Remember me". Two links, "Forgot Password" and "Create an account", are positioned below the checkbox. A red "Login" button is centered at the bottom of the form. The footer of the page includes the text "Online Vulnerability Scanner © 2015 Acunetix Ltd." and social media icons for GitHub, Twitter, and Facebook.

Online Vulnerability Scanner

Login

Email

Password

☐ Remember me

[Forgot Password](#) [Create an account](#)

[Login](#)

Online Vulnerability Scanner © 2015 Acunetix Ltd.

Screenshot - Acunetix OVS Login Screen

You can log in to Acunetix OVS from <https://ovs.acunetix.com>. Use the email address and password that you provided during registration to log on to your Acunetix Online Vulnerability Scanner account.

Configuring Scan Targets

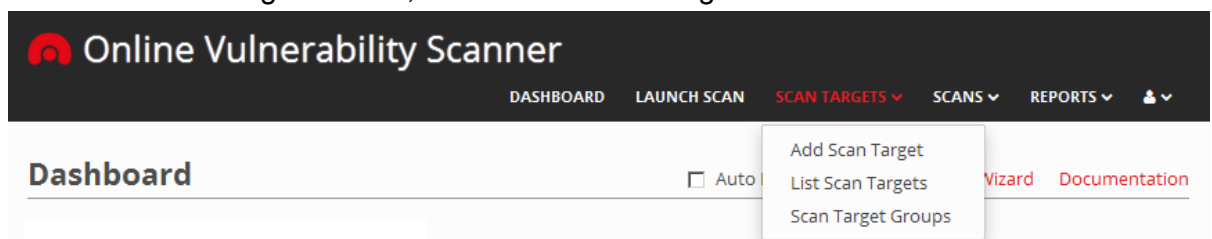
Scan Targets are the web and perimeter servers that you would like to scan using Acunetix OVS. These will need to be configured in Acunetix OVS before they can be scanned. Once configured, a scan target can be scanned repeatedly.

There are two types of Scan Targets that you can configure:

- **Web Scan Targets** – this is where your website and web applications are hosted. Both Network and Web Vulnerability scans can be launched against such scan targets.
- **Perimeter Network Scan Targets** – these are scan targets that host any other type of service exposed on the internet; such as your firewall, router, mail server, DNS server etc.

All scan targets can be configured from the 'Scan Targets' menu. The configuration of Network and Web Scan targets is very similar, and will only differ in the information provided for authentication purposes. Proceed as follows to create a new scan target:

1. From the 'Scan Targets' menu, select 'Add Scan Target'.



Screenshot - Add Scan Target option

2. Provide a name that will allow you to easily identify this scan target. You also have the option to provide a description of the scan target.

Add Scan Target

The screenshot shows the 'Add Scan Target' form with the 'General' tab selected. It contains three input fields: 'Name' with the value 'Acunetix Test Site', 'Description' with the value 'Acunetix PHP Test Site', and 'Host' with the value 'http://testphp.vulnweb.com'. Below the fields is a red 'Add Scan Target' button.

Screenshot - Configure Scan Target Details

3. Insert the URL of the website or web application, or the IP of the server you would like to scan.
4. Configure Web and/or Network Specific options (explained in the next section).
5. Click 'Add Scan Target' when complete.


Verifying Scan Target Ownership


Once you create a new scan target, you will be asked to verify ownership of the scan target. Scan target verification will depend on the type of scan that you intend to launch against the scan target.

In summary, web vulnerability scans require the unique verification file to be present in the root of the web server before a scan starts. This is required for all your scan targets against which you wish to run web scans.

Network vulnerability scans require that we verify your account details; a one-time process where you will be contacted by a member of our support team.


Scan Target Verification

 This Scan Target requires verification

 The Ownership of each Scan Target needs to be verified before scans can be launched against the Scan Target.
Web Scans require that you upload a unique file to the root of your web site.
Network Scans require that we confirm your contact details.

Web Scan Verification

INCOMPLETE


 Instructions:
1. Download the unique verification file.
2. You will need to upload this file to the root of your web site.
3. Click the Verify Scan Target button to complete verification.

Note: Web Scan Verification is done from scanners.acunetix.com. Please configure any firewalls and WAFs accordingly.

1. Download Verification File


2. Upload file to the root of your site

3. Verify Scan Target

Last Check Not checked yet
 **The ownership of the scan target has not been verified.**
[Contact us](#) if you need help verifying this Scan Target.

Network Scan Verification

INCOMPLETE

 Network Scans are only allowed after your account details have been manually verified. Confirm that your account details are correct, and request verification.

Proceed to verify my details

Screenshot - Scan Target Verification required

Web Scan Verification

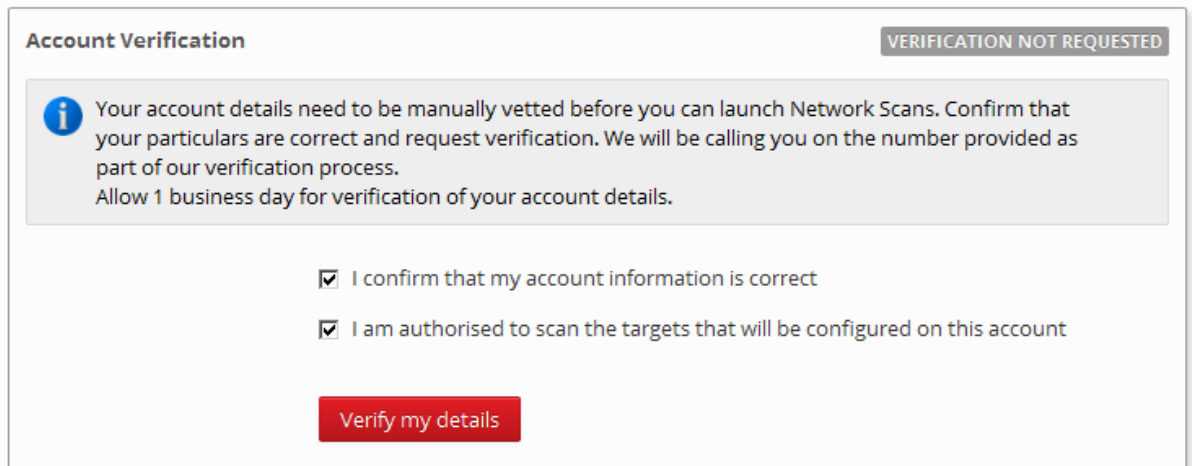
Web scan verification is a 3 step process.

1. Download the unique verification file assigned to your new scan target.
2. Upload the verification file to the root of the site (using FTP for example).
3. From the configuration of the scan target in Acunetix OVS, click on 'Verify Ownership' to complete the verification process.

Note: The verification file needs to be kept in the root of the site, since Acunetix OVS will check for the verification file each time it scans the server.

Network Scan Verification

1. For network scans you will need to verify the authenticity of your account details, and request verification of your account details by an Acunetix representative.
2. From within the configuration of your scan target, in the Network Scan Verification, click 'Proceed to verify my details', or you can go directly to Account Settings > Profile.
3. Confirm that your account details are correct, and update as needed.



Account Verification VERIFICATION NOT REQUESTED

i Your account details need to be manually vetted before you can launch Network Scans. Confirm that your particulars are correct and request verification. We will be calling you on the number provided as part of our verification process.
Allow 1 business day for verification of your account details.

☒ I confirm that my account information is correct

☒ I am authorised to scan the targets that will be configured on this account

Verify my details

Screenshot - Verify account details

4. From within the Account Verification section, you can request the verification of your account details.
5. An Acunetix representative will get in touch with you within 24 hours to complete the verification.
6. Once your account details have been verified, you can launch network vulnerability scans on all your scan targets.

Contact us at support@acunetix.com if you require help with the verification process.

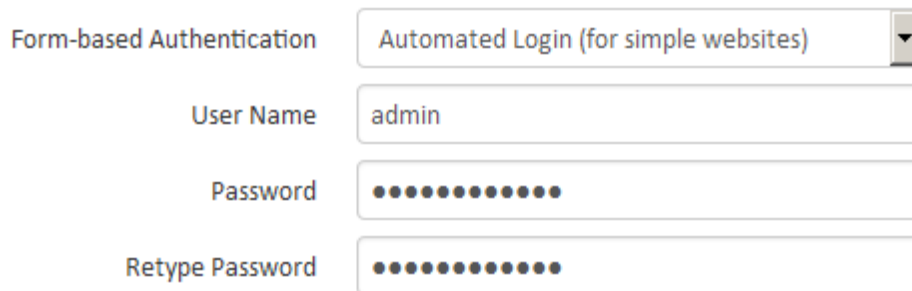
Note: When listing the scan targets, the Status column will indicate the verification status of each scan target configured. This will allow you to easily identify the ones that still need to be verified.

Web Server Scan Settings

In the web server scan settings, you can configure any authentication settings required to access restricted areas within the website. You can also generate a unique AcuSensor agent for your scan target.

Configuring Web Site Authentication

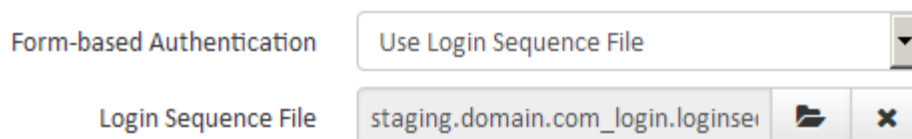
If the new scan target is a web application or a website, you might need to scan restricted areas within the web application. The information used to access the restricted area can be configured from the Web Server Scan Settings within the scan target's configuration.



The screenshot shows a web form titled "Form-based Authentication". It has a dropdown menu set to "Automated Login (for simple websites)". Below this are four input fields: "User Name" with the text "admin", "Password" with ten dots, "Retype Password" with ten dots, and a "Login" button.

Screenshot - Form-based Authentication - Automated Login

In most cases, you can select to use 'Automated Login (for simple web applications)'. You simply need to provide the Username and Password to access the restricted area. The scanner will automatically detect the login link, the logout link and the mechanism used to maintain the session active.



The screenshot shows a web form titled "Form-based Authentication". It has a dropdown menu set to "Use Login Sequence File". Below this is a text input field labeled "Login Sequence File" containing the text "staging.domain.com_login.loginseq". To the right of the input field are two buttons: a folder icon and a close icon (X).

Screenshot - Form-based Authentication using Login Sequence Recorder

For more complex web applications, which might be using a more elaborate login mechanism, you would need to [download](#) and use the Login Sequence Recorder to create a Login Sequence file (*.loginseq). This can then be uploaded and saved with your Web Scan Target settings. Information on how to use the Login Sequence Recorder can be found at <http://www.acunetix.com/blog/docs/acunetix-wvs-login-sequence-recorder/>

Generating and Installing AcuSensor

AcuSensor improves the scan results provided by Acunetix OVS by being able to identify all the pages on your website, increases the information about the vulnerabilities detected and decreases false positives.

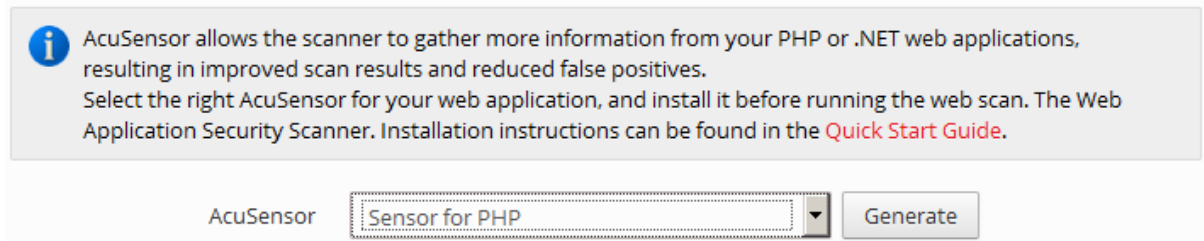
NOTE: Installing the AcuSensor Agent is optional. Acunetix Web Vulnerability Scanner is still best in class as a “black box” scanner but the AcuSensor Agent improves accuracy and vulnerability results.

The unique Acunetix AcuSensor Technology identifies more vulnerabilities than a black box Web Application Scanner while generating less false positives. In addition, it indicates exactly where vulnerabilities are detected in your code and also reports debug information.

Acunetix AcuSensor requires an agent to be installed on your website. This agent is generated uniquely for your website for security reasons. Acunetix AcuSensor can be used with PHP and .NET web applications.

Generating the AcuSensor files

1. From within the scan target's settings, scroll down to Web Scan Settings.



Screenshot - Generate AcuSensor files

2. In the AcuSensor section, select whether to generate AcuSensor for PHP or .NET.
3. Click the Generate button. You will be prompted to save the AcuSensor files.

Once you have generated and downloaded the unique AcuSensor files for your web application, you can proceed with [installing AcuSensor in your web application](#).

Network Server Scan Settings

You might also want to configure SSH credentials for your scan target. This will allow the Acunetix OVS network scanner to provide a more comprehensive network scans of the scan target.

Note: SSH credentials are optional. If no SSH credentials are provided, a full network scan can still be done using the same information that a hacker has.

Installing AcuSensor

Acunetix AcuSensor increases the efficiency of an Acunetix scan by improving the crawling, detection and reporting of vulnerabilities, while decreasing false positives. Acunetix AcuSensor can be used on .NET and PHP web applications.

Installing the AcuSensor Agent

NOTE: Installing the AcuSensor Agent is optional. Acunetix Web Vulnerability Scanner is still best in class as a “black box” scanner but the AcuSensor Agent improves accuracy and vulnerability results when scanning .NET and PHP web applications.

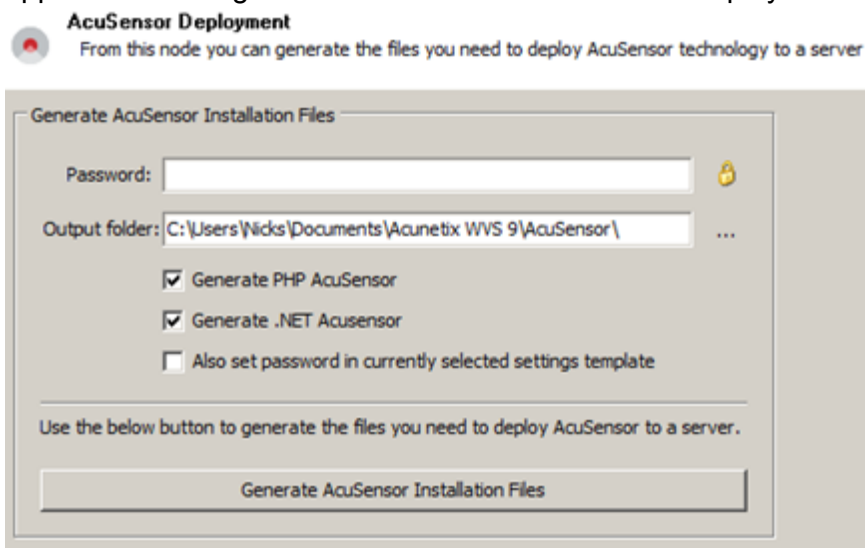
The unique Acunetix AcuSensor Technology identifies more vulnerabilities than a black box Web Application Scanner while generating less false positives. In addition, it indicates exactly where vulnerabilities are detected in your code and also reports debug information

Acunetix AcuSensor requires an agent to be installed on your website. This agent is generated uniquely for your website for security reasons.

Generating the AcuSensor files

First you will need to generate your unique AcuSensor files. Proceed as follows:

1. If using Acunetix WVS, open Acunetix WVS and navigate to the 'Configuration > Application Settings' node. Click on the 'AcuSensor Deployment' node.



Screenshot – AcuSensor Deployment settings node

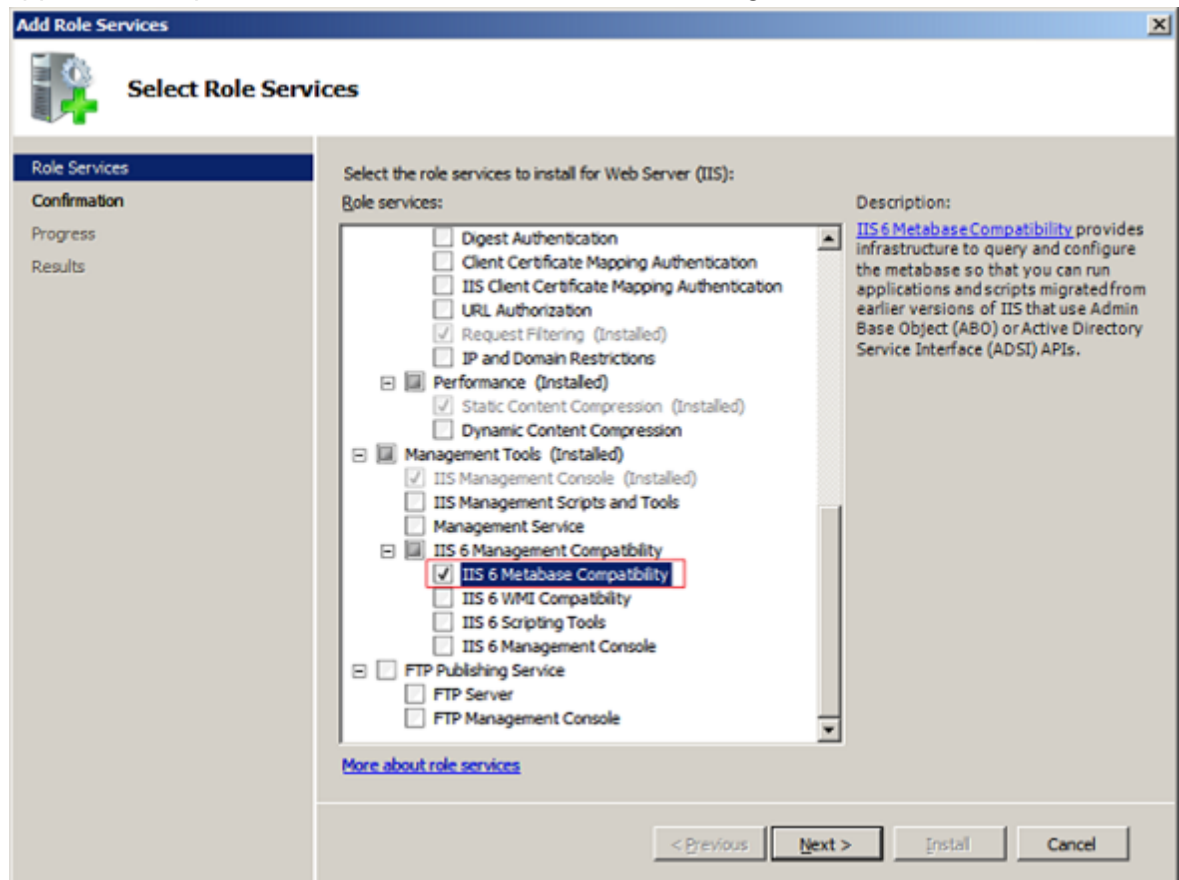
2. If using Acunetix Online Vulnerability Scanner, you can generate the AcuSensor files from the Scan Target's configuration. From Acunetix OVS, change to Scan Targets > List Scan Targets > Click on the Scan Target's name. Skip to step 6.
3. Enter a password or click on the padlock icon to randomly generate a password unique to the AcuSensor file.
4. Select 'Also set password in currently selected settings template' to store the password specified in the scan settings template.
5. Specify the path where you want the AcuSensor files to be generated.
6. Select whether to generate files for a PHP website or a .NET website.
7. Click on **Generate AcuSensor Installation Files** to generate the files.

8. Depending on if you are using an ASP .NET or a PHP website, use one of the following procedures to install the AcuSensor files.

Installing the AcuSensor agent for ASP .NET Websites

The AcuSensor agent will need to be installed in your web application. This section describes how to install AcuSensor in an ASP.NET web application.

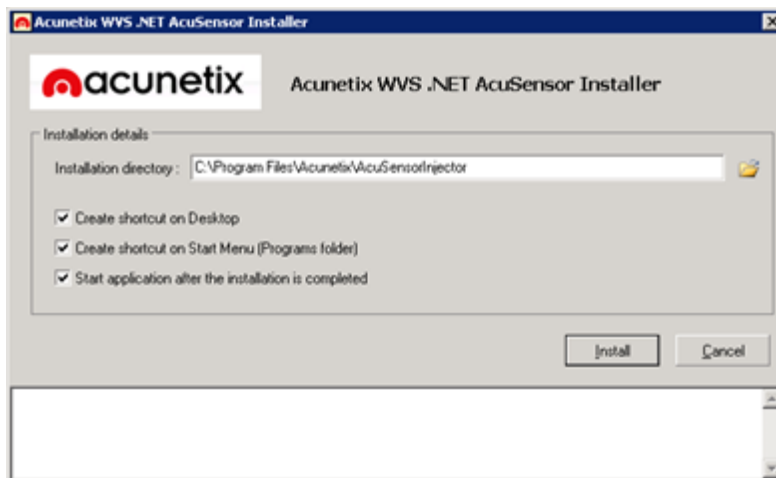
1. **Install Prerequisites on the server hosting the website:** The AcuSensor installer application requires Microsoft .NET Framework 3.5 or higher.



Screenshot - Enable IIS 6 Metabase Compatibility on Windows 2008

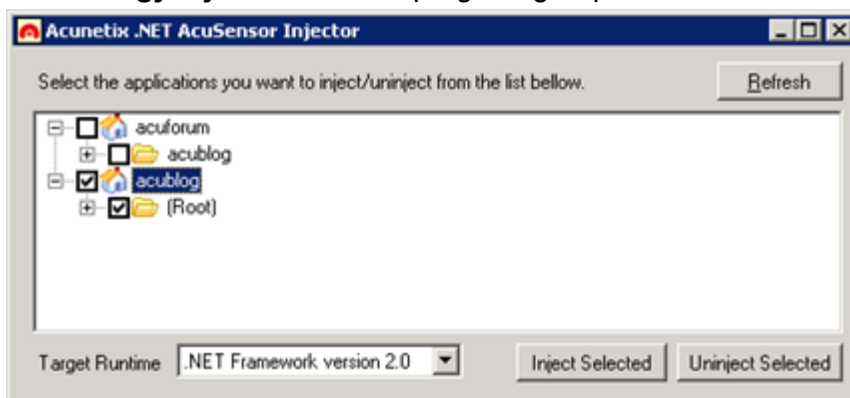
On Windows 2008, you must also install IIS 6 Metabase Compatibility from 'Control Panel > Turn Windows features On or Off > Roles > Web Server (IIS) > Management Tools > IIS 6 Management Compatibility > IIS 6 Metabase Compatibility' to enable listing of all .NET applications running on server.

2. Copy the AcuSensor installation files to the server hosting the .NET website.



Screenshot – Acunetix .NET AcuSensor Agent installation

3. Double click **Setup.exe** to install the Acunetix .NET AcuSensor agent and specify the installation path. The application will start automatically once the installation is ready. If the application is not set to start automatically, click on **Acunetix .NET AcuSensor Technology Injector** from the program group menu.



Screenshot – Acunetix .NET AcuSensor Technology Agent

4. On start-up, the Acunetix .NET AcuSensor Technology Installer will retrieve a list of .NET applications installed on your server. Select which applications you would like to inject with AcuSensor Technology and select the Framework version from the drop down menu. Click on **Inject Selected** to inject the AcuSensor Technology code in the selected .NET applications. Once files are injected, close the confirmation window and also the AcuSensor Technology Injector.

Note: The AcuSensor installer will try to automatically detect the .NET framework version used to develop the web application so you do not have to manually specify which framework version was used from the Target Runtime drop down menu.

Installing the AcuSensor agent for PHP websites

This section describes how to install AcuSensor in an ASP.NET web application.

1. Locate the PHP AcuSensor file of the website you want to install AcuSensor on. Copy the **acu_phpaspect.php** file to the remote web server hosting the web application.

The AcuSensor agent file should be in a location where it can be accessed by the web server software. Acunetix AcuSensor Technology works on websites using PHP version 5 and up.

2. There are 2 methods to install the AcuSensor agent, one method can be used for Apache servers, and the other method can be used for both IIS and Apache servers.

Method 1: Apache .htaccess file

Create a .htaccess file in the website directory and add the following directive:

php_value auto_prepend_file '[path to acu_phpaspect.php file]'.

Note: For Windows use 'C:\sensor\acu_phpaspect.php' and for Linux use '/Sensor/acu_phpaspect.php' path declaration formats. If Apache does not execute .htaccess files, it must be configured to do so. Refer to the following configuration guide: <http://httpd.apache.org/docs/2.0/howto/htaccess.html>. The above directive can also be configured in the *httpd.conf* file.

Method 2: IIS and Apache php.ini

1. Locate the file 'php.ini' on the server by using *phpinfo()* function.
2. Search for the directive **auto_prepend_file**, and specify the path to the acu_phpaspect.php file. If the directive does not exist, add it in the php.ini file:
auto_prepend_file="[path to acu_phpaspect.php file]"
3. Save all changes and restart the web server for the above changes to take effect.

Testing your AcuSensor Agent

To test if the AcuSensor agent is working properly on the target website, do the following:

1. In the **Tools Explorer**, Navigate to 'Configuration > Scan Settings' node and select the AcuSensor node.
2. Enter the password of the AcuSensor agent file which was copied to the target website.
3. Click **Test AcuSensor installation on a Specific URL**. A dialog will prompt you to submit the URL of the target website where the AcuSensor Agent file is installed. Enter the desired URL and click **OK**.

Changing the AcuSensor Password

If you need to change the password used by the AcuSensor agent on your website, you will need to re-generate the AcuSensor Files and reinstall them on your website.

Perform the following if you are using a .NET website:

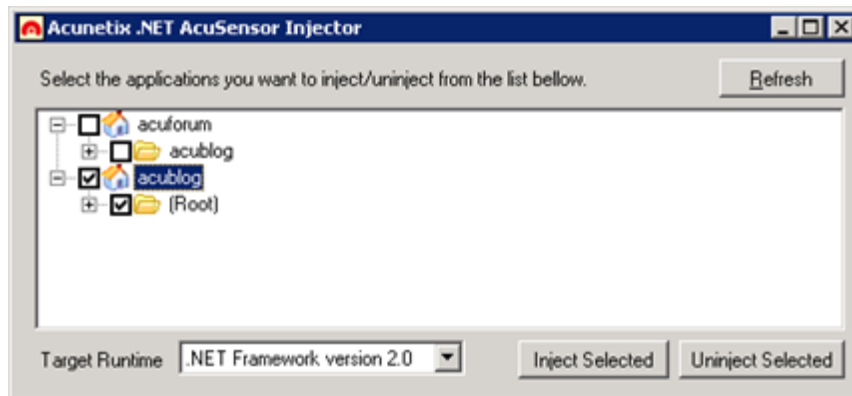
1. Use the procedure in the next section to Disable and Uninstall the AcuSensor agent.
2. Configure a new password.
This step can be omitted if you are using Acunetix Online Vulnerability Scanner, since a new unique and secure password is automatically generated each time the AcuSensor files are generated. The unique password is stored with the Scan Target's settings.
3. Click on Generate AcuSensor installation files.
4. Proceed with installing the new AcuSensor files. If you are using a PHP web application, you will just need to overwrite the old **acu_phpaspect.php** with the new **acu_phpaspect.php** file.

Disabling and uninstalling AcuSensor

To uninstall and disable the sensor from your web site:

AcuSensor for ASP .NET websites

1. Browse to the installation directory where the AcuSensor Agent was been installed
2. Open AcuSensorInjector.exe.



Screenshot - Select website and click Uninject Selected

3. Select the website where the AcuSensor agent is installed and click on 'Uninject' to remove the AcuSensor Agent from the site.
4. Close AcuSensorInjector.exe
5. From the same directory, double click uninstall.exe to uninstall the AcuSensor Agent files.

Note: If you uninstall the Acunetix .NET AcuSensor Technology Injector without un-injecting the .NET application, then the AcuSensor code will not be removed from your .NET application.

AcuSensor for PHP

1. If method 1 (.htaccess file) was used to install the PHP AcuSensor, delete the directive: **php_value auto_prepend_file="[path to acu_phpaspect.php file]"** from .htaccess
2. If method 2 was used to install the PHP AcuSensor, delete the directive: **auto_prepend_file="[path to acu_phpaspect.php file]"** from php.ini.
3. Finally, delete the Acunetix AcuSensor PHP file: acu_phpaspect.php.

Note: Although the Acunetix AcuSensor agent requires authentication, it is recommended that the AcuSensor client files are uninstalled and removed from the web application if they are no longer in use.

Launching Scans

After configuring your scan targets, you are ready to launch scans for web and network vulnerabilities. This can be done as follows:

1. From Acunetix OVS, click 'Launch Scan'.
2. Select one or more scan targets that you would like to scan.
3. Click 'Scan Now'. You can also schedule scans by selecting 'Schedule a Scan'.

Scan Now

i Select the type of scan required, confirm the Scan Targets and click Launch Scan.

Web Vulnerability Scan Full Scan

Network Vulnerability Scan Full Scan (safe checks)

☐ I confirm that I am fully authorised to scan the targets shown below

Reports

i Optional: Automatically generate reports after the scan is done.

Web Reports Choose... PDF

Network Reports Choose... PDF

Targets 1 scan target

Name	Host	Status
http://staging.acunetix.com	http://staging.acunetix.com	Verified (full scans allowed)

Launch Scan Cancel

Screenshot - Scan a Target

4. You will then be asked to select the type of scan you want to perform.
For example, if you only require a network scan, select 'No web scan' in the 'Web Scanning Profile' list, and select one of the scanning profiles in the 'Network Scanning Profile' list. Check the Scanning Profiles section for more information.
5. You can optionally have a report automatically generated after the scan is finished.
6. Finally, click on the 'Launch Scan' button to have your scan(s) queued. You will be taken to the All Scans list, which allows you to monitor the progress of the scans requested.

Notes:

1. Scans can only be initiated against your scan targets after they have been verified. Check the Verifying Scan Target Ownership section in [Configuring Scan Targets](#). We might need to contact you to perform further verification.
2. It is recommended to launch both web and network scans against a website.
3. Some scans, especially those performed on large websites may take a long time to complete. You will be notified by email when the scan has finished.
4. All our scans are launched from 'scanners.acunetix.com'. It is recommended that you whitelist this host on your firewall. If this is not done, your firewall might block all the connections made by Acunetix OVS, invalidating the scans.
5. If you launch multiple scans against the same scan target at the same time, Acunetix OVS will queue the scans so that only one scan is executed at a time. This is done to prevent overloading the scanned server with requests.

Scanning Profiles

A *Scanning Profile* is a logical grouping of checks that Acunetix OVS performs to scan for a specific category of vulnerabilities (such as Cross-Site Scripting, SQL Injection, CSRF, etc.). Below is a list of scanning profiles with a short description about each:

Web Scanning Profiles


- Full Scan
Use the Full Scan profile to launch a scan using all the checks available in Acunetix OVS.
- High Risk Alerts
The High Risk Alerts scanning profile will only check for the most dangerous web vulnerabilities.
- Cross-Site Scripting (XSS)
The XSS scanning profile will only check for Cross-Site Scripting vulnerabilities.
- SQL Injection
The SQL Injection scanning profile will only check for SQL Injection vulnerabilities.
- Weak Passwords
The Weak Passwords Scanning profile will identify forms which accept a username and password and will attack these forms.
- Cross-Site Request Forgery (CSRF)
The CSRF scanning profile will only check for Cross-Site Request Forgery vulnerabilities.

Network Scanning Profiles

- Full Scan (safe checks)
This scanning profile can be used for most network scans. It will perform a full scan, but avoids running invasive checks which might cause problems with the scanned server.
- Full Scan (incl. invasive checks)
Use this scanning profile to run a more comprehensive scan, including the invasive checks available in Acunetix OVS. Ideally, execute scans using this scanning profile just before you put the server in production, or during off-peak hours.


Scans performed using this scanning profile can hinder the performance of the scan target, and might also cause it to go offline.















Review Scan Results

 Online Vulnerability Scanner

DASHBOARD LAUNCH SCAN SCAN TARGETS ▾ SCANS ▾ REPORTS ▾ 👤 ▾

Alerts (132) Knowledge Base (8) Severity All severity levels ▾ [Generate Report](#)

Start Date	20 Jan 2015 11:52	Files	94	Requests	56145	Host Name	http://testphp.vulnweb.com	
End Date	20 Jan 2015 12:12	Directories	33	Avg. Response Time	119.06 ms	Scan Target Name	Test PHP	
Duration	0h 20m 0s	Variations	26	Responsive	Yes	Scan Type	Web	

Name	Module
+  Blind SQL Injection (27)	Scripting (Blind_Sql_Injection.script)
+  CRLF injection/HTTP response splitting (verified) (1)	Scripting (CRLF_Injection.script)
+  Cross site scripting (2)	Scripting (Remote_File_Inclusion_XSS.script)
+  Cross site scripting (verified) (27)	Scripting (XSS.script)
+  Directory traversal (verified) (2)	Scripting (Directory_Traversal.script)
+  HTTP parameter pollution (2)	Scripting (HTTP_Parameter_Pollution.script)
+  nginx SPDY heap buffer overflow (1)	Scripting (Version_Check.script)
+  Script source code disclosure (1)	Scripting (Script_Source_Code_Disclosure.script)
+  Server side request forgery (2)	Scripting (Server_Side_Request_Forgery.script)
+  SQL injection (verified) (27)	Scripting (Sql_Injection.script)
+  Weak password (1)	Scripting (Html_Authentication_Audit.script)
+  .htaccess file readable (1)	Scripting (htaccess_File_Readable.script)
+  Application error message (6)	Scripting (Error_Message.script)
+  Backup files (2)	Scripting (Backup_File.script)

Screenshot - Scan results

Once the scan has finished, Acunetix OVS will send you an email with a summary of the results and a link allowing you to access the scan results directly. The scan results show the start and end date of the scan, the duration of the scan and all the alerts that have been identified during the scan. The AcuSensor logo is also displayed when the scan detects and makes use of AcuSensor during a web scan.

Alerts (vulnerabilities) discovered

One of the key components of the scan results is the list of all vulnerabilities found in the scan target during the scan. Depending on the type of scan, these can be either Web Alerts or Network Alerts, and the alerts are categorized according to 4 severity levels:



High Risk Alert Level 3 – Vulnerabilities categorized as the most dangerous, which put the scan target at maximum risk for hacking and data theft.



Medium Risk Alert Level 2 – Vulnerabilities caused by server misconfiguration and site-coding flaws, which facilitate server disruption and intrusion.



Low Risk Alert Level 1 – Vulnerabilities derived from lack of encryption of data traffic or directory path disclosures.



Informational Alert – These are items which have been discovered during a scan and which are deemed to be of interest, e.g. the possible disclosure of an internal IP address or email address, or matching a search string found in the Google Hacking Database, or information on a service that has been discovered during the scan.

Depending on the type of vulnerability, additional information about the vulnerability is shown when you click on an alert category node:

- **Vulnerability description** - A description of the discovered vulnerability.
- **Affected items** - The list of files or components which are affected by the alert.
- **The impact of this vulnerability** – Level of impact on the website, web server or perimeter server if this vulnerability is exploited.
- **Attack details** - Details about the parameters and variables used to test for this vulnerability. E.g. for a Cross Site Scripting alert, the name of the exploited input variable and the string it was set to will be displayed. You can also find the HTTP request sent to the web server and the response sent back by the web server (including the HTML response).
- **How to fix this vulnerability** - Guidance on how to fix the vulnerability.
- **Detailed information** - More information about the reported vulnerability.
- **Web references** - A list of web links providing more information on the vulnerability to help you understand and fix it.

Grouping of Vulnerabilities

Name	Module
+ Blind SQL Injection (27)	Scripting (Blind_Sql_Injection.script)
+ CRLF injection/HTTP response splitting (verified) (1)	Scripting (CRLF_Injection.script)
+ Cross site scripting (2)	Scripting (Remote_File_Inclusion_XSS.script)
- Cross site scripting (verified) (27)	Scripting (XSS.script)

Affects	Parameter
+ /404.php	
+ /AJAX/showxml.php	mycookie
+ /comment.php	name
+ /guestbook.php	login
+ /guestbook.php	text
+ /guestbook.php	name

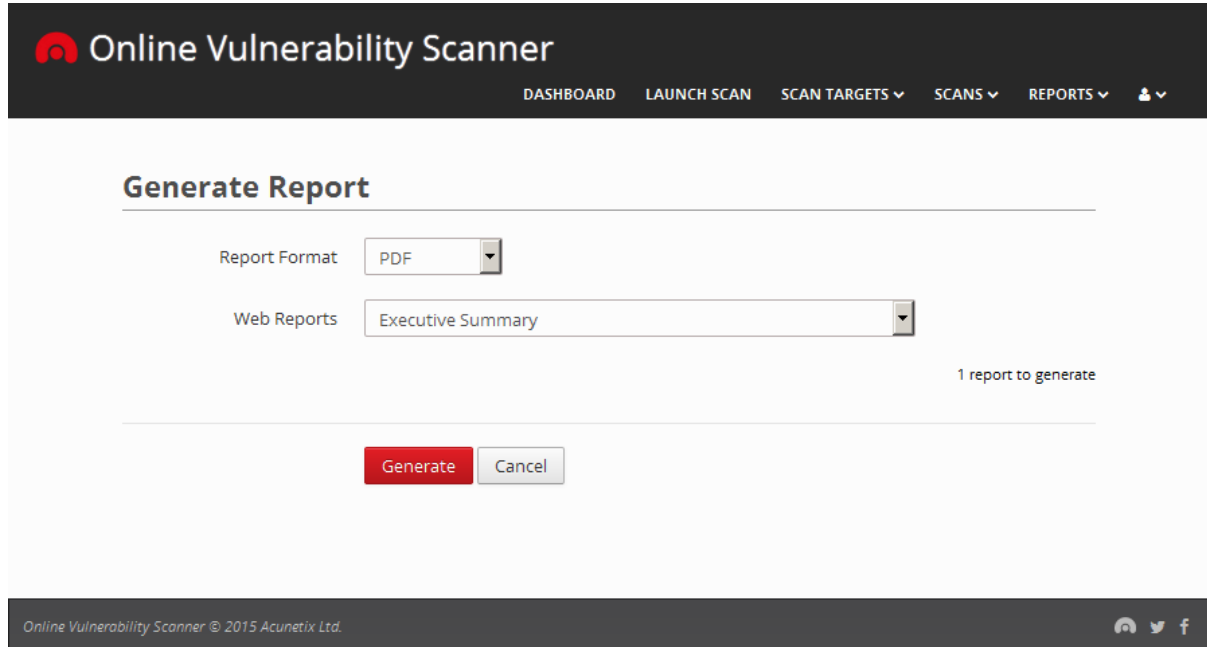
Screenshot – Grouping of vulnerabilities

If the same type of vulnerability is detected on multiple pages, the scanner will group them under one alert node. Expanding the alert node will reveal all the vulnerable pages. Expand further to view the vulnerable parameters for the selected page.

Vulnerabilities Detected by AcuMonitor

An Acunetix OVS web scan will make use of AcuMonitor to detect certain vulnerabilities such as Blind XSS, Email Header Injection, and certain types of SSRF, XXE and Host Header Attacks. AcuMonitor can only detect some of these vulnerabilities after the scan has finished. When this happens, AcuMonitor will update the scan results with the new vulnerabilities detected and you will receive an email notifying you that the scan results have been updated. More information on AcuMonitor can be found at <https://www.acunetix.com/websitesecurity/acumonitor-next-generation-web-vulnerability-scanning/>.

Generating Reports



The screenshot shows the 'Online Vulnerability Scanner' web interface. At the top is a dark navigation bar with the logo and title 'Online Vulnerability Scanner', and a menu with links: DASHBOARD, LAUNCH SCAN, SCAN TARGETS, SCANS, REPORTS, and a user icon. Below this is a 'Generate Report' section with a title and a horizontal line. It contains two dropdown menus: 'Report Format' set to 'PDF' and 'Web Reports' set to 'Executive Summary'. To the right of these is the text '1 report to generate'. At the bottom of the section are two buttons: a red 'Generate' button and a grey 'Cancel' button. The footer of the page is dark and contains the text 'Online Vulnerability Scanner © 2015 Acunetix Ltd.' and social media icons for GitHub, Twitter, and Facebook.

Screenshot - Generate a Report

Once a scan is finished, you can generate a report for the scan. Proceed as follows:

1. When reviewing the results of a scan, you can select 'Generate Report' for that specific scan.
2. Choose the Report Format, which can be either PDF or RTF
3. Choose the report that you would like to generate. The reports available are described [here](#).
4. Click the 'Generate' button.
5. You will then be taken to the Saved Reports. The report might take a few seconds to generate. Click 'Refresh' to check if the report is ready to download. Reports are generally available in less than 10 seconds.

You can also generate reports in bulk via 'Reports' > 'Generate Reports'. Here you will be presented with a list of all your scans. Select the scans you would like to report on, choose the Report Format, the Type of Report and then click 'Generate'.

Acunetix Reports

The following is a list of the reports that can be generated from Acunetix Web Vulnerability Scanner (WVS) and Acunetix Online Vulnerability Scanner (OVS):

Affected Items Report

Availability: OVS and WVS

The Affected Items report shows the files and locations where vulnerabilities have been detected during a scan. The report shows the severity of the vulnerability detected, together with other details about how the vulnerability has been detected.

Developer Report

Availability: OVS and WVS

The Developer Report is targeted to developers who need to work on the website in order to address the vulnerabilities discovered by Acunetix Web Vulnerability Scanner. The report provides information on the files which have a long response time, a list of external links, email addresses, client scripts and external hosts, together with remediation examples and best practice recommendations for fixing the vulnerabilities.

Executive Report

Availability: OVS and WVS

The Executive Report summarizes the vulnerabilities detected in a website and gives a clear overview of the severity level of vulnerabilities found in the website.

Quick Report

Availability: OVS and WVS

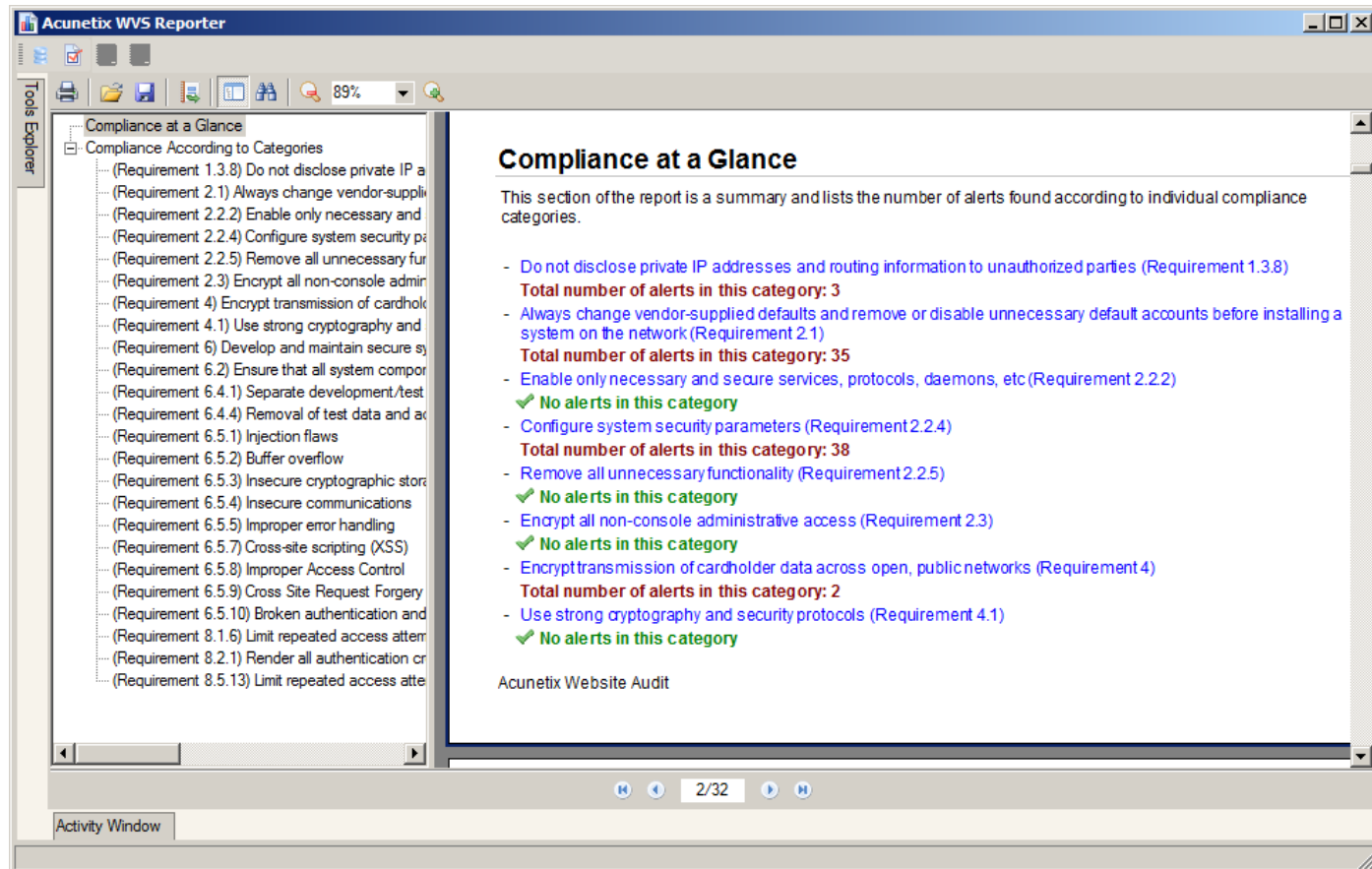
The Quick Report provides a detailed listing of all the vulnerabilities discovered during the scan.

Network Security Report

Availability: OVS only

The Network Security Report provides detailed security information about the perimeter network server scanned by Acunetix Online Vulnerability Scanner. This information is very useful for a network security auditor or pen tester who is tasked with analysing the security of the perimeter network.

Compliance Reports



Screenshot – PCI Compliance Report

Compliance Reports are available for the following compliance bodies and standards:

CWE / SANS - Top 25 Most Dangerous Software Errors

Availability: OVS and WVS

This report shows a list of vulnerabilities that have been detected in your website which are listed in the CWE / SANS top 25 most dangerous software errors. These errors are often easy to find and exploit and are dangerous because they will often allow attackers to take over the website or steal data. More information can be found at <http://cwe.mitre.org/top25/>.

The Health Insurance Portability and Accountability Act (HIPAA)

Availability: OVS and WVS

Part of the HIPAA Act defines the policies, procedures and guidelines for maintaining the privacy and security of individually identifiable health information. This report identifies the vulnerabilities that might be infringing these policies. The vulnerabilities are grouped by the sections as defined in the HIPAA Act.

International Standard - ISO 27001

Availability: OVS and WVS

ISO 27001, part of the ISO / IEC 27000 family of standards, formally specifies a management system that is intended to bring information security under explicit management control. This report identifies vulnerabilities which might be in violation of the standard and groups the vulnerabilities by the sections defined in the standard.

NIST Special Publication 800-53

Availability: OVS and WVS

NIST Special Publication 800-53 covers the recommended security controls for the Federal Information Systems and Organizations. Once again, the vulnerabilities identified during a scan are grouped by the categories as defined in the publication.

OWASP Top10 2013

Availability: OVS and WVS

The Open Web Application Security Project (OWASP) is web security project led by an international community of corporations, educational institutions and security researchers. OWASP is renown for its work in web security, specifically through its list of top 10 web security risks to avoid. This report shows which of the detected vulnerabilities are found on the OWASP top 10 vulnerabilities.

Payment Card Industry (PCI) standards

Availability: OVS and WVS

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard, which applies to organizations that handle credit card holder information. This report identifies vulnerabilities which might breach parts of the standard and groups the vulnerabilities by the requirement that has been violated.

Sarbanes Oxley Act

Availability: OVS and WVS

The Sarbanes Oxley Act was enacted to prevent fraudulent financial activities by corporations and top management. Vulnerabilities which are detected during a scan which might lead to a breach in sections of the Act are listed in this report.

DISA STIG Web Security

Availability: OVS and WVS

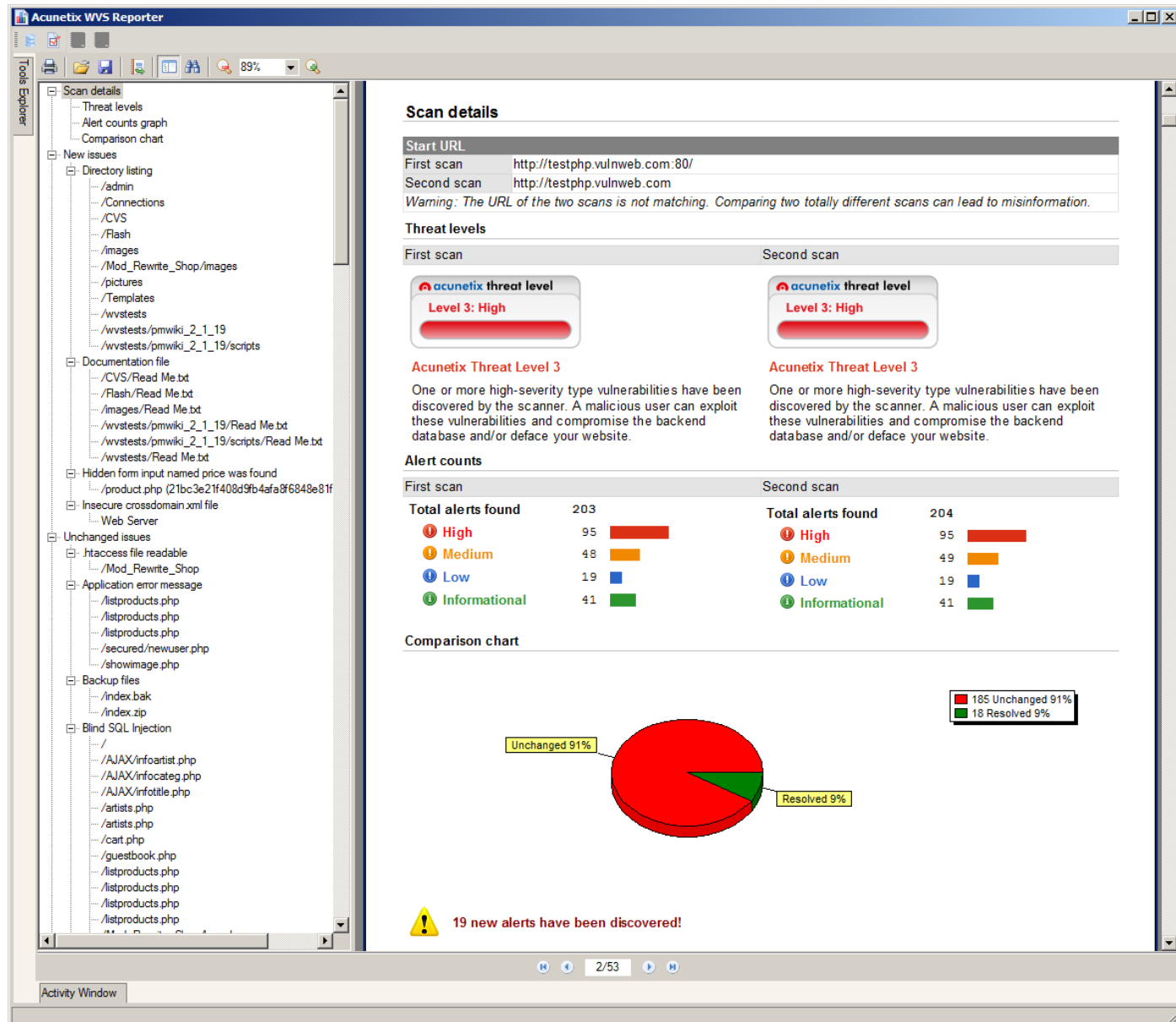
The Security Technical Implementation Guide (STIG) is a configuration guide for computer software and hardware defined by the Defense Information System Agency (DISA), which part of the United States Department of Defense. This report identifies vulnerabilities which violate sections of STIG and groups the vulnerabilities by the sections of the STIG guide which are being violated.

Web Application Security Consortium (WASC) Threat Classification

Availability: OVS and WVS

The Web Application Security Consortium (WASC) is a non-profit organization made up of an international group of security experts, which has created a threat classification system for web vulnerabilities. This report groups the vulnerabilities identified on your site using the WASC threat classification system.

Scan Comparison Report



Screenshot – Scan Comparison Report

Availability: WVS only

The Scan Comparison Report allows the user to track the changes between two scan results for the same application. This report will highlight resolved, unchanged and new vulnerabilities, making it easy to track development changes affecting the security of your web application.

Monthly Vulnerabilities Report

Availability: WVS only

This statistical report correlates the data from the scans performed in a specific month, and reports on the vulnerabilities identified during that month.

Configuring Child Accounts

The scanning and reporting tasks of scan targets can be delegated to other people within the organisation using Child Accounts. These Child Accounts are Acunetix OVS users which can be given permissions to create scan targets, scan them or report on them, all through your Root account. The original account retains control over which child accounts can access which specific scan targets and functionalities.

Note: This feature is only available to licensed users.

Child Account Roles

When creating a child account, you need to select a role for the user. There are 4 roles that you can choose from, which are Tech Admin, Tester / Auditor, Tester or Auditor. Depending on the role selected, the user will be able to create, edit, scan and delete Scan Targets, view scans and generate reports. The following table summarises the permissions available for each role

User Role	Tech Admin	Tester (Only)	Auditor (Only)	Tester / Auditor
Scan Targets	Full Control	Verify / Scan / AcuSensor	View	Verify / Scan / AcuSensor
Scan Target Groups	Edit / Scan	Scan	View	Scan
Scans	View / Delete	View / Delete	View	View / Delete
Reports	Create / View	None	Create / View	Create / View

Creating a Child Account

To create a Child Account:

1. From your Account menu (top right), select Users.
2. Click the Create button to create a new child user on your account
3. Insert the email address, name and surname of the new child account.
4. Select the Role for the new user. Child Account Roles are explained above.

- Click Create to create the new user

Online Vulnerability Scanner

DASHBOARDLAUNCH SCANSCAN TARGETS ▾SCANS ▾REPORTS ▾

Manage User

All Users

Edit Profile

Email

charlotte@company.com

Name

Charlotte

Surname

Hall

User Role

Auditor/Tester

Learn more

 about configuring child accounts.

Update

Configure Access

Access All Scan Targets ☐

Scan Target Groups

Name	Description	Allow Access
Business Unit A		<input checked="" type="checkbox"/>
Business Unit B		<input type="checkbox"/>
Business Unit C		<input type="checkbox"/>

Scan Targets

Name	Host	Status	Allow Access
Business Unit A Website	http://sbu1.company.testing123.com	Verified (full scans allowed)	<input type="checkbox"/>
Business Unit B Staging	http://staging.sbu2.company.testing123.com	Verified (full scans allowed)	<input checked="" type="checkbox"/>
Business Unit B Website	http://sbu2.company.testing123.com	Verified (full scans allowed)	<input type="checkbox"/>
Business Unit B WIKI	http://wiki.sbu2.company.testing123.com	Verified (full scans allowed)	<input type="checkbox"/>
Business Unit B WIKI2	http://wiki2.sbu2.company.testing123.com	Partially Verified (Network scans allowed)	<input type="checkbox"/>
Business Unit C Test site	http://test.sbu3.company.testing123.com	Verified (full scans allowed)	<input type="checkbox"/>
Business Unit C Website	http://www.sbu3.company.testing123.com	Verified (full scans allowed)	<input type="checkbox"/>

Online Vulnerability Scanner © 2015 Acunetix Ltd.

- After you create the user, you will need to permissions to specific Scan Targets or Scan Target Groups. You can also choose to give access to all Scan Targets on your account (keeping in mind the Role selected for the user)
- Click Update after configuring access to the Scan Targets.

Notes

- When a user is given access to all Scan Targets, the user will maintain access to all new Scan Targets created thereafter.
- When a user is given access to a Scan Target Group, the user will retain access to the Scan Targets that are added to the Scan Target Group thereafter. Similarly, the

user will lose access to the Scan Targets that are removed from the Scan Target Group.

- Tech Admins can create new Scan Targets and they can decide to add them to Scan Target Groups on which they have privileges.

Managing Child Accounts

Online Vulnerability Scanner

DASHBOARDLAUNCH SCANSCAN TARGETS ▾SCANS ▾REPORTS ▾

Users

Refresh

Email	Name	Surname	All Access	Roles		
tom@company.com	Tom	Peterson	<input type="checkbox"/>	Auditor Tester	Disable	Remove
chris@company.com	Chris	Jones	<input checked="" type="checkbox"/>	Tech Admin	Disable	Remove
charlotte@company.com	Charlotte	Hall	<input type="checkbox"/>	Auditor Tester	Disable	Remove
daniel@company.com	Daniel	Davies	<input type="checkbox"/>	Tech Admin	Enable	Remove
peter@company.com	Peter	Smith	<input checked="" type="checkbox"/>	Tester	Disable	Remove
joe@company.com	Joe	Doe	<input type="checkbox"/>	Tech Admin	Disable	Remove

Create

Online Vulnerability Scanner © 2015 Acunetix Ltd.

You can manage all your Child Accounts from the Users option. From here, you can instantly review the roles given to each user. You can also give access to all Scan Targets to individual users, Disable users and Remove users from your account.

Auditing Child Accounts

Online Vulnerability Scanner

DASHBOARDLAUNCH SCANSCAN TARGETS ▾SCANS ▾REPORTS ▾

Activity Log

Refresh

User

Group

Severity

Filter

All

All

All

User	Group	Type	Severity	Remote IP	Date ▾
+ chris@company.com	Targets	Target added to group	Info	165.150.196.54	12 Nov 2014 15:47
+ chris@company.com	Targets	Target added to group	Info	165.150.196.54	12 Nov 2014 15:47
+ chris@company.com	Targets	Target added to group	Info	165.150.196.54	12 Nov 2014 15:47
+ chris@company.com	Account	Logged in	Info	165.150.196.54	12 Nov 2014 15:46
+ joe@company.com	Targets	Target created	Info	50.213.160.50	12 Nov 2014 15:46
+ joe@company.com	Account	Logged in	Info	50.213.160.50	12 Nov 2014 15:44

The Master Account can audit all the actions done by all the Child Accounts. This can be done from the Activity Log, which can be accessed from the Account menu. Child accounts will have access to a similar Activity Log, however this will only show the activities that they have affected.

The Activity Log can be filtered by User, Type of log and Log Severity.

Troubleshooting and Support

User Manual

The most common queries can be answered by consulting this user manual.

Frequently Asked Questions

Our support team maintains a list of frequently asked questions at <http://www.acunetix.com/support/faq/>.

Acunetix Blog

We highly recommend that you follow our security blog by browsing to: <http://www.acunetix.com/blog/>.

Request Support

If you encounter persistent problems that you cannot resolve, we encourage you to contact the Acunetix Support team via email at support@acunetix.com. Please include any information you think is useful to help us diagnose your issue, such as information on the web technologies being used, screenshots showing the problem etc. Please include also the license key information in the support email.

We will do our best to answer your query within 24 hours or less, depending on your time zone.

Knowledge base / Support page

You can also explore the Acunetix knowledge base and other support options by browsing to: <http://www.acunetix.com/support/>.

Acunetix Facebook page

Join us on Facebook for the latest product and industry updates: <http://www.facebook.com/Acunetix>.