Web Application Vulnerability Assessment with Nessus & Qualys, including Certificate View.

PRESENTED BY OKPERIRUISI LOUIS

6TH AUGUST, 2025

project objective

The aim of this project is to identify vulnerabilities in a web application using NESSUS and QUALYS to scan the web app, analyze the reports, and recommend a remediation plan. Additionally, Qualys was also used for Certificate View, which provides complete visibility into digital certificates and their configurations. This includes on-premises and cloud assets, enabling SSL/TLS certificate management.

Visit: https://www.tenable.com/downloads/nessus & click on Download

Downloads / Tenable Nessus

Tenable Nessus

1 Download and Install Nessus

Choose Download

Version

Nessus - 10.9.2

Platform

Windows - x86_64

Download

Checksum

Download by curl >

Docker >

Summary

Release Date: Jul 30, 2025

Release Notes:

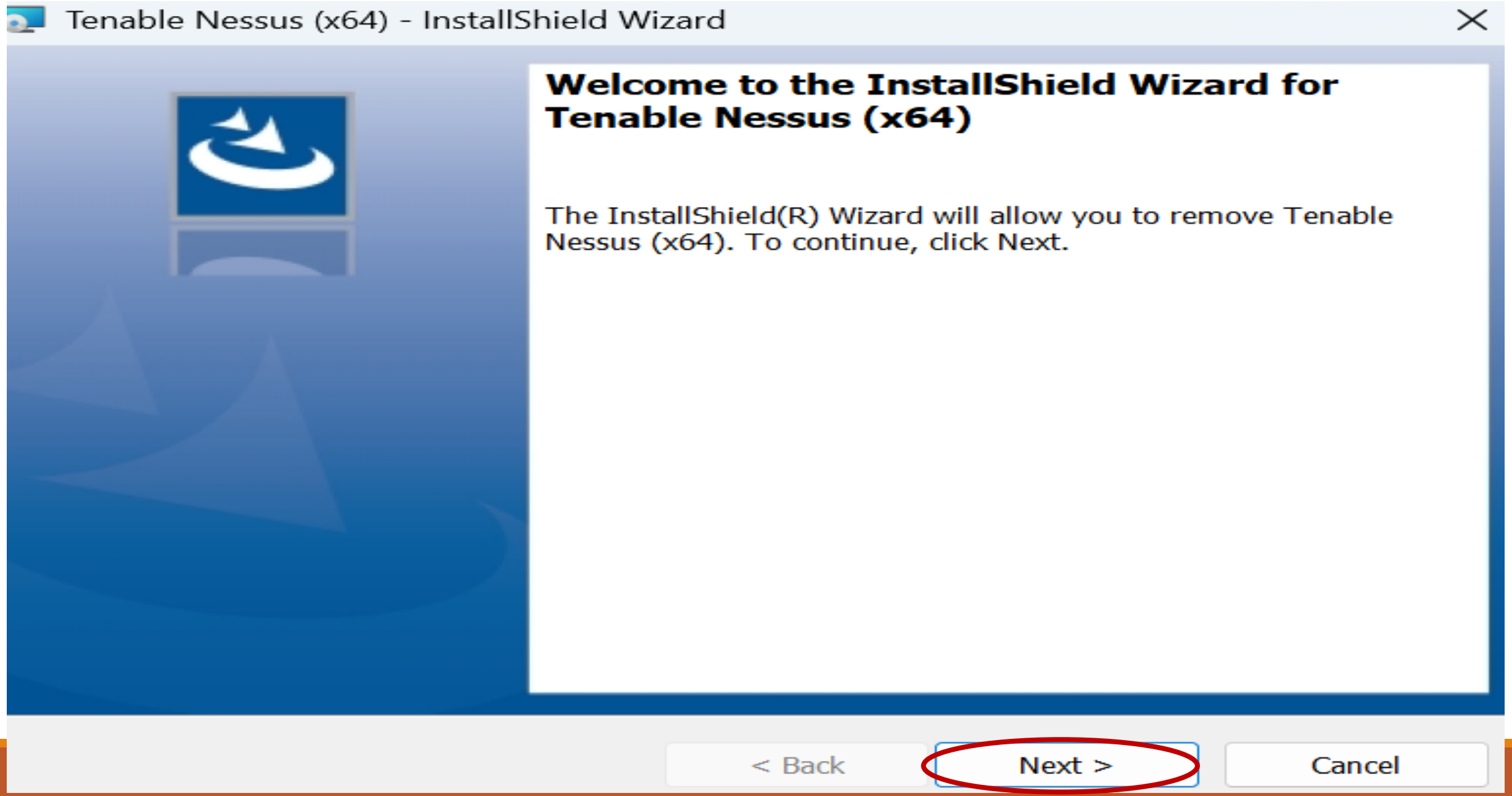
Tenable Nessus 10.9.2 Release Notes

Signing Keys:

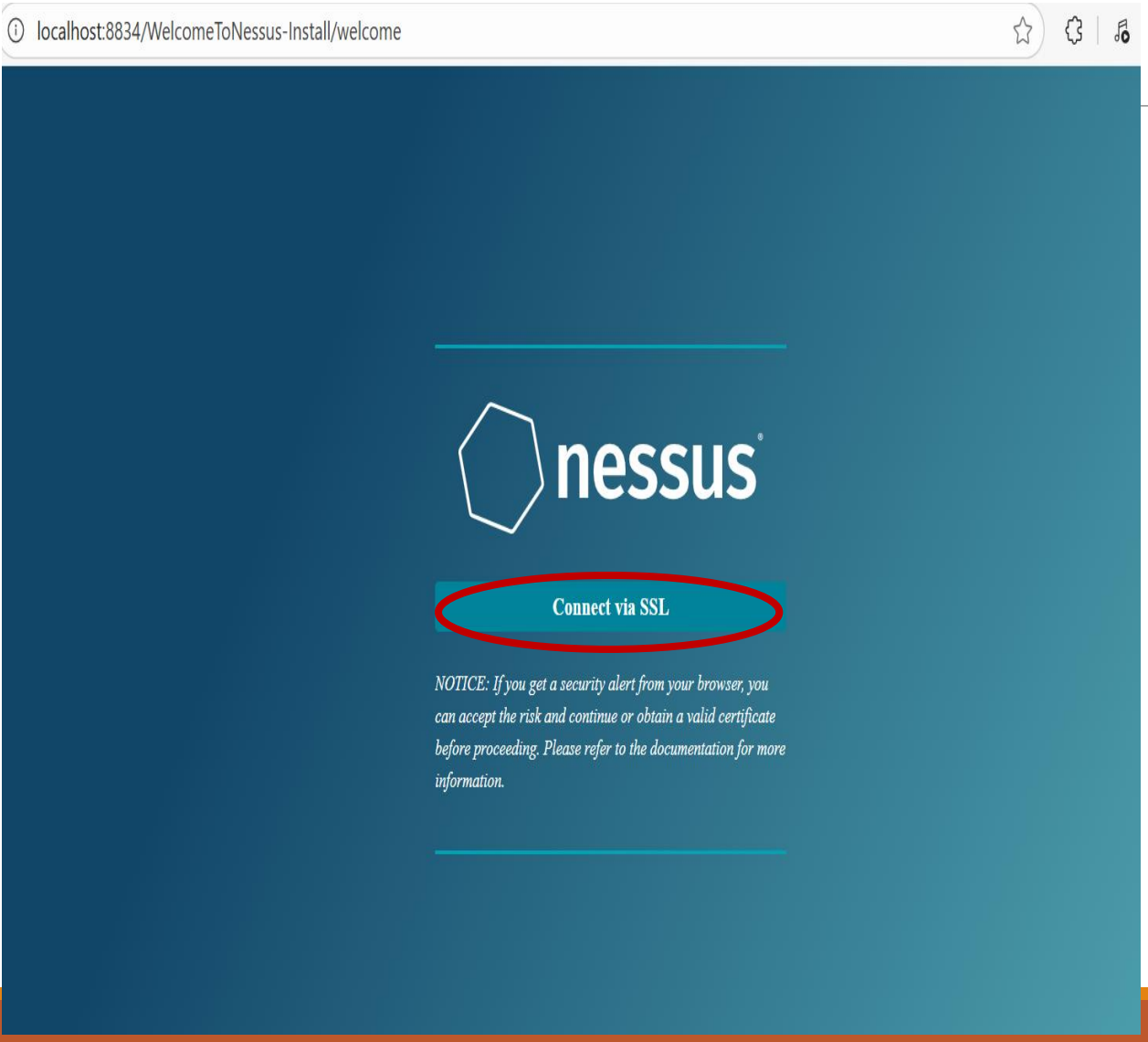
RPM-GPG-KEY-Tenable-4096 (10.4 & above)

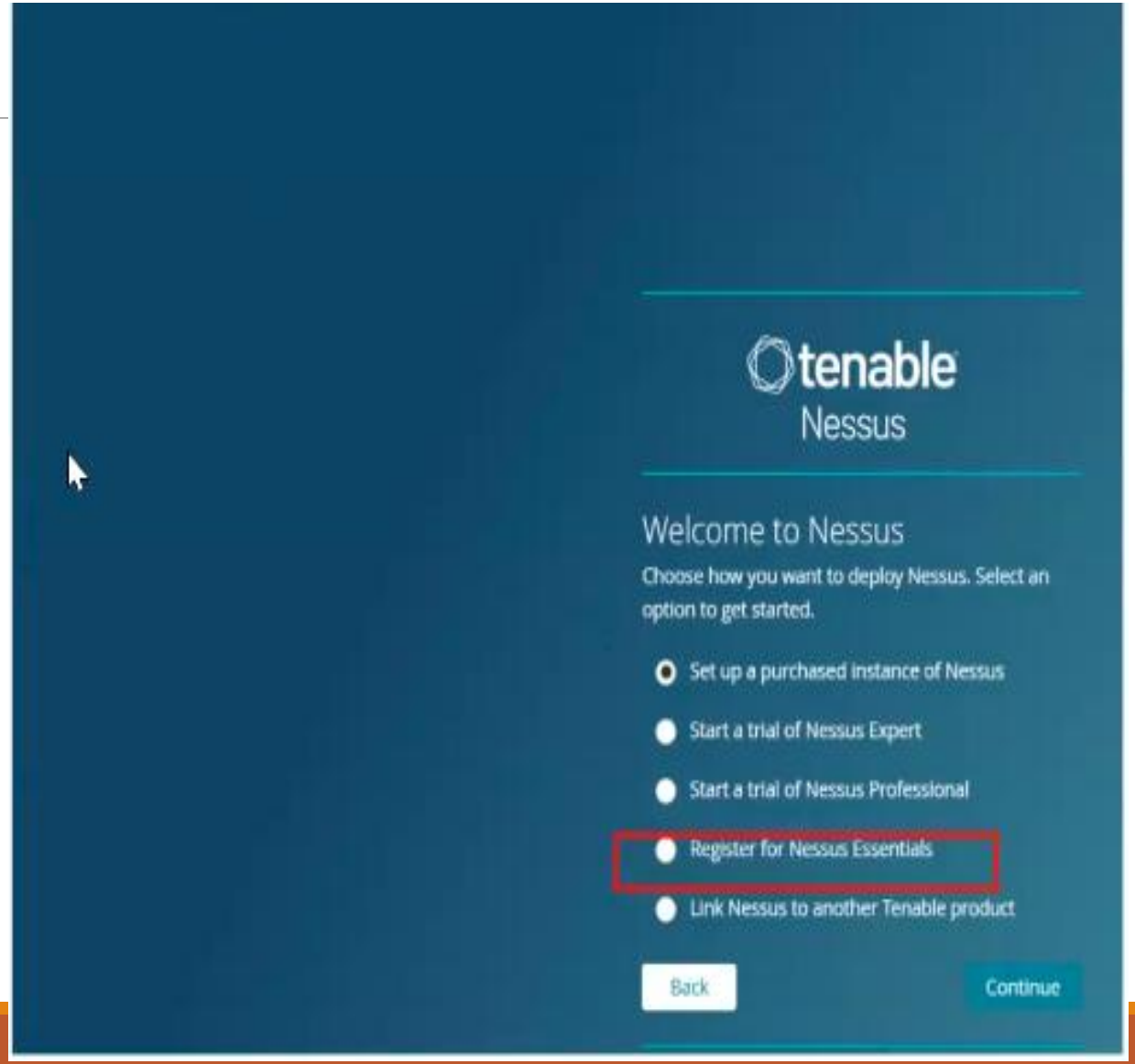
RPM-GPG-KEY-Tenable-2048 (10.3 & below)

After download, go to your download folder and run Nessus application, Click next

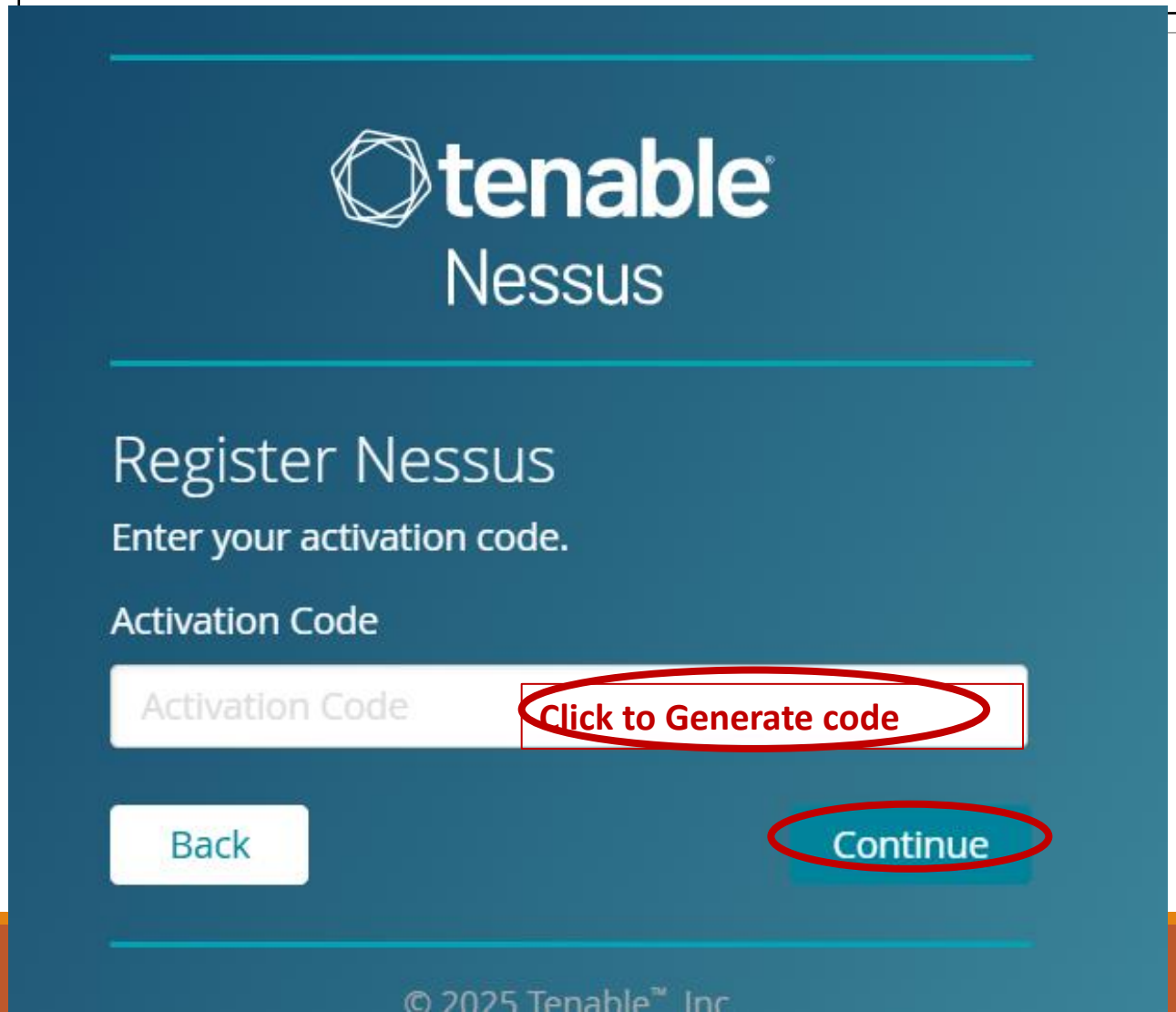


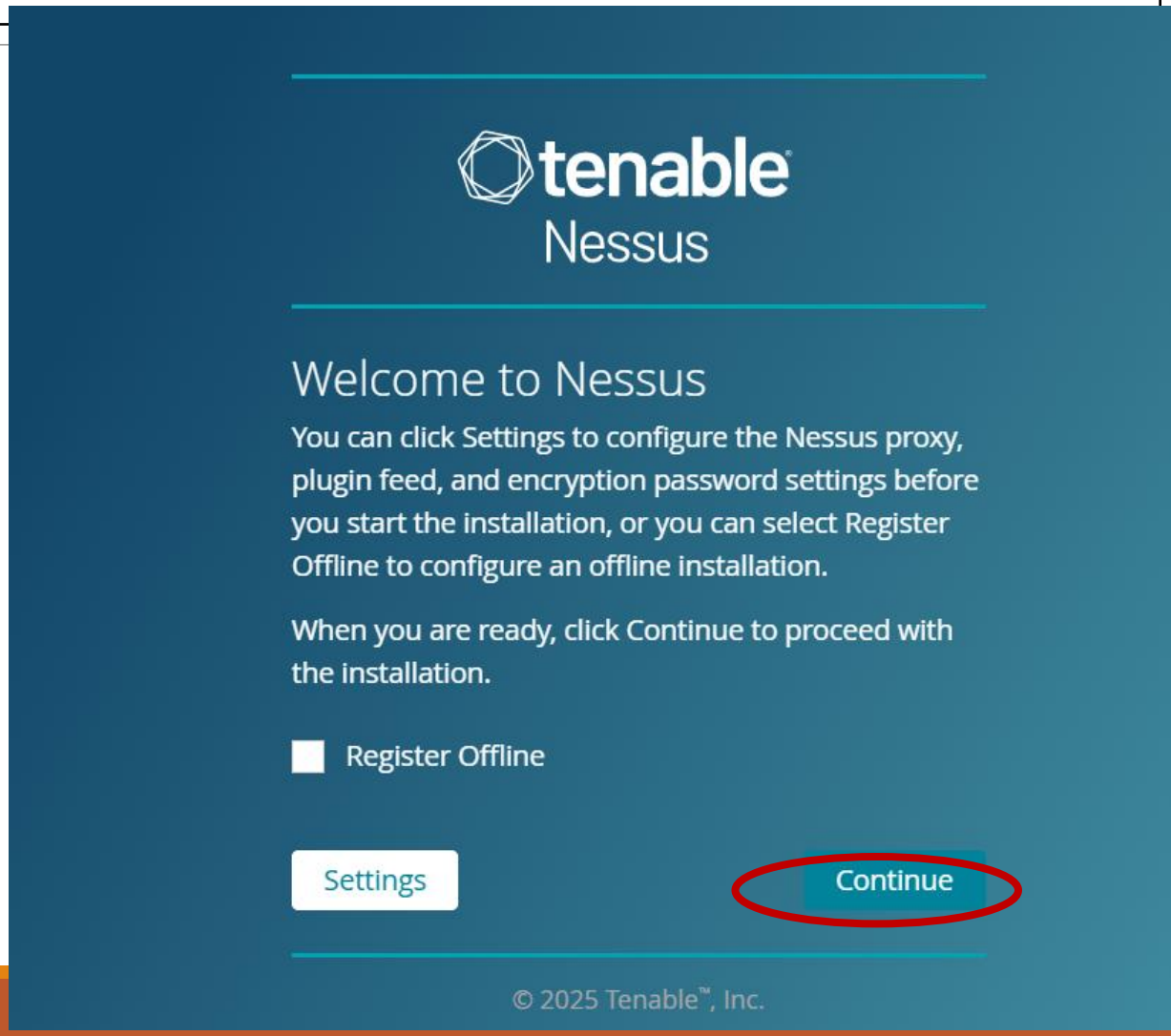
Installation Cont...



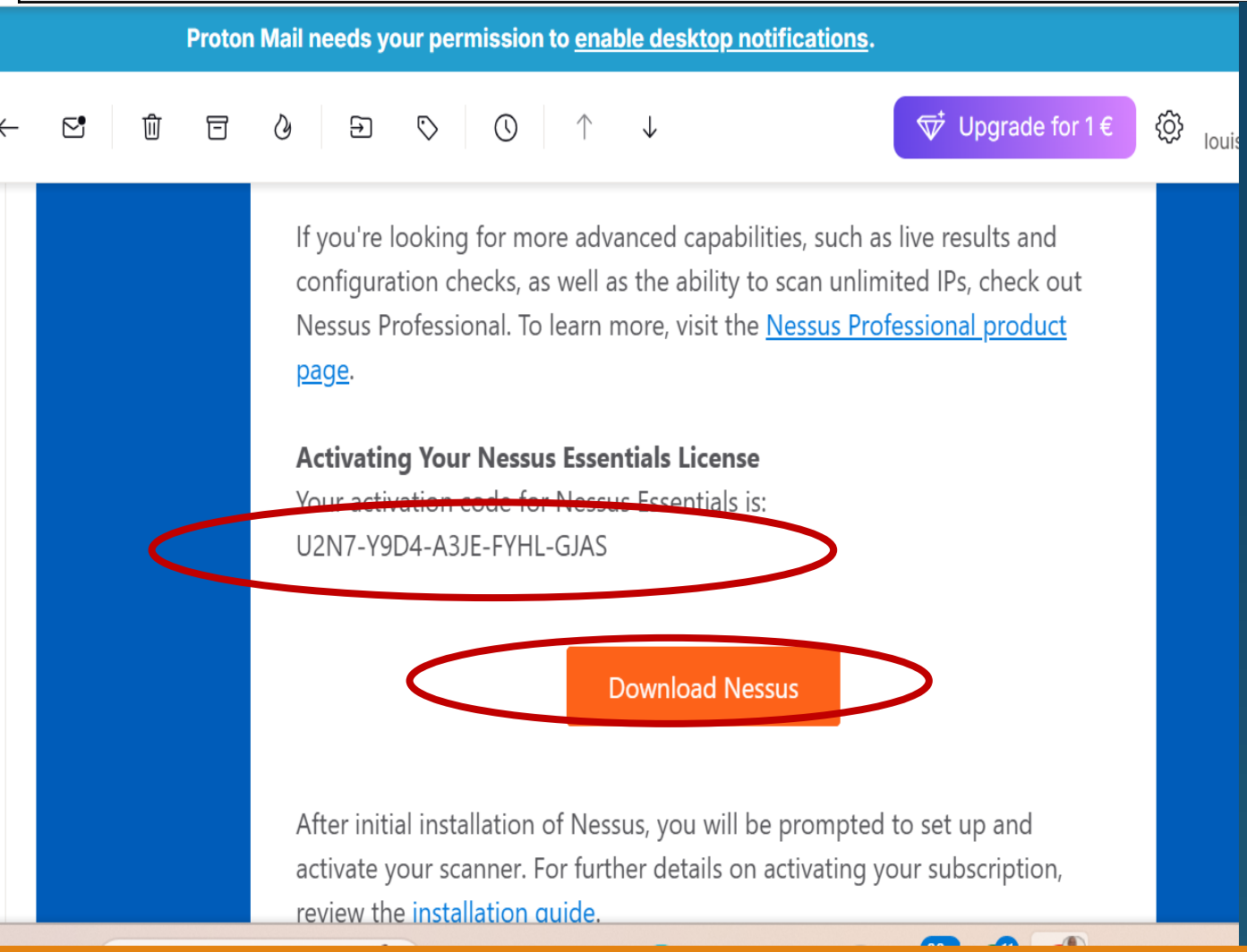


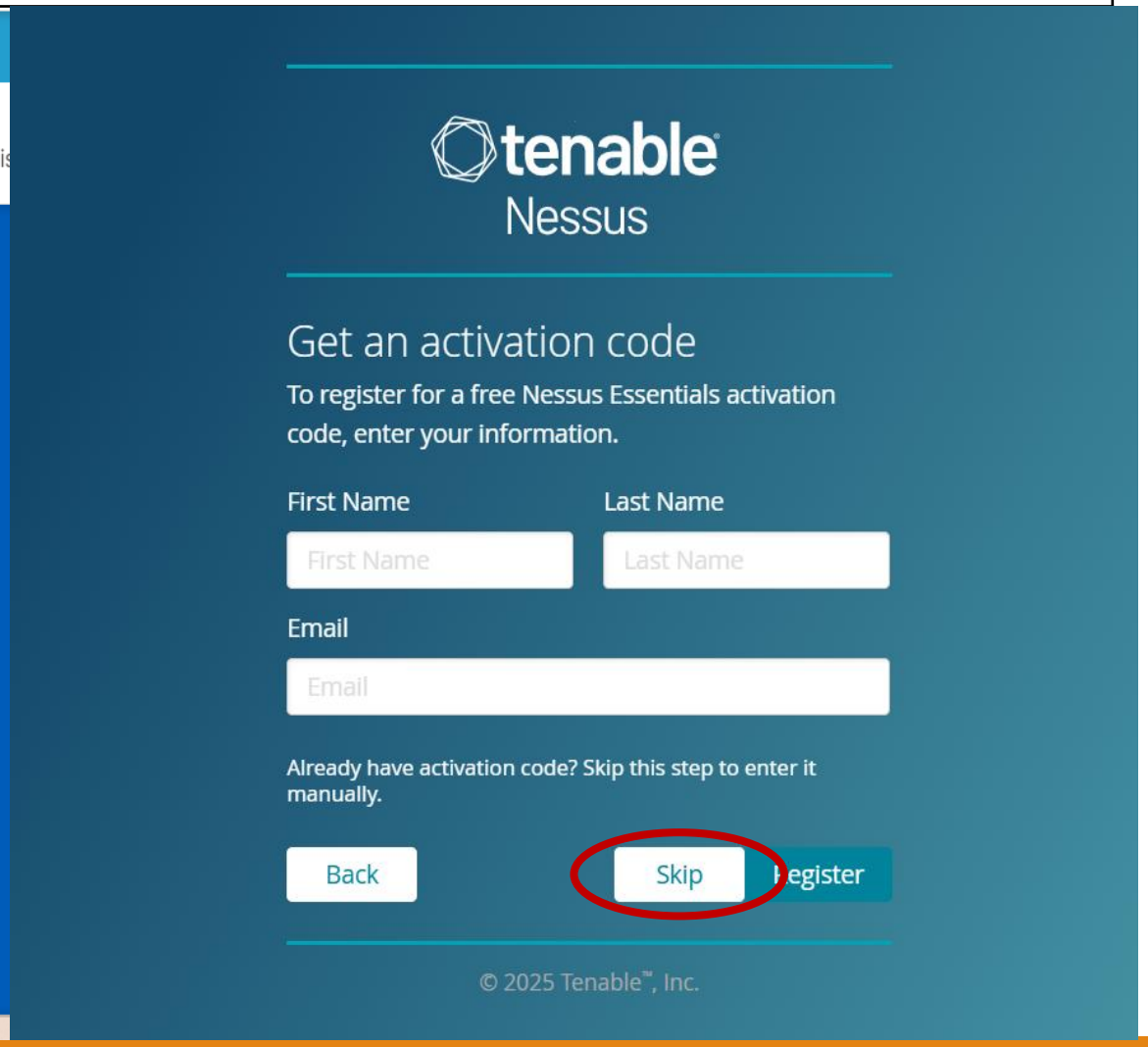
Installation Cont…… Click on “Generate code” and a code will be generated and send to your email as provided on the picture at the LHS, copy and paste the code on the provided field for the “Activate Code”, then click on “Continue” at the RHS picture.



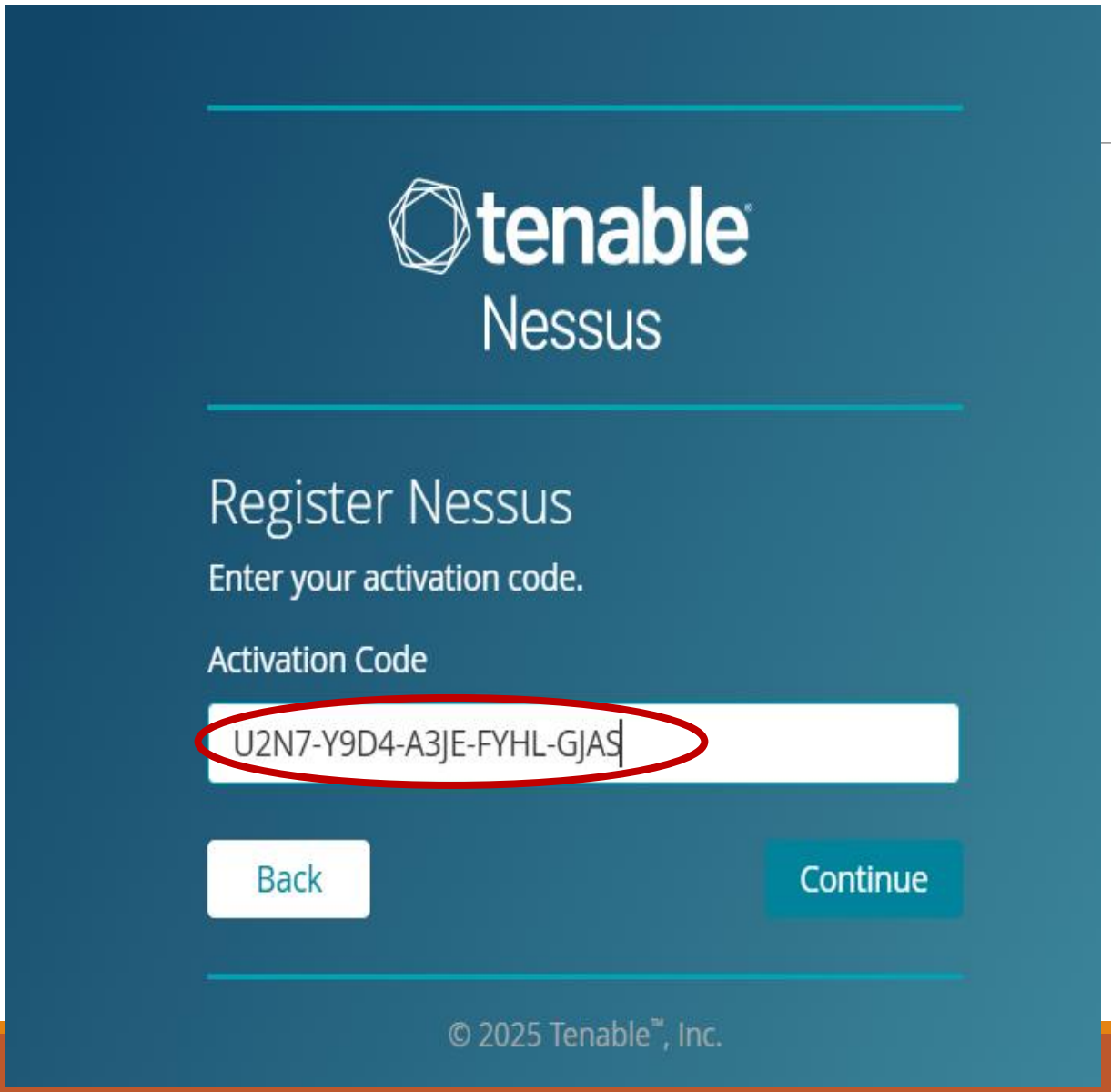


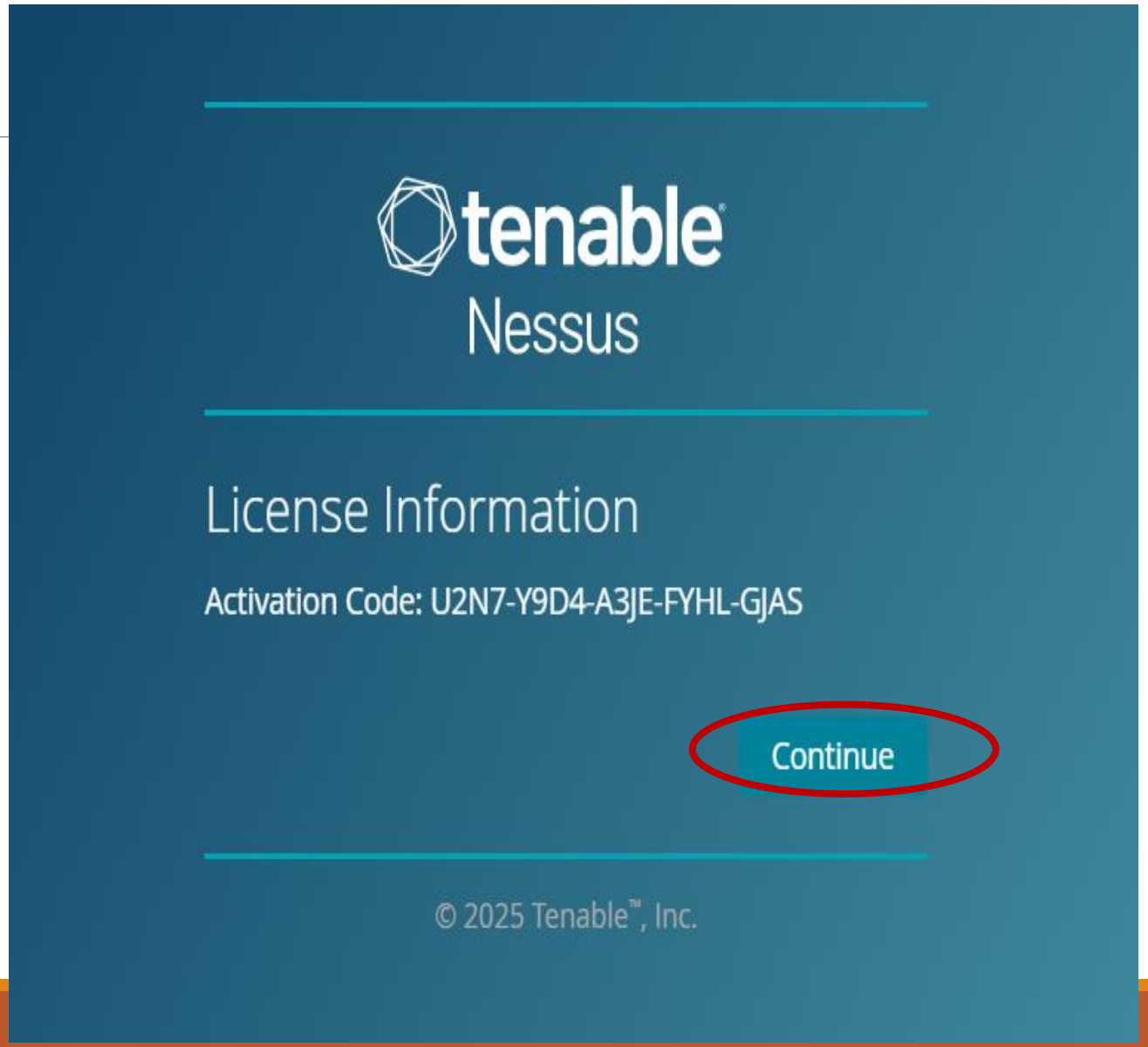
Installation Cont... copy the Activation Code and Click on **Download Nessus, and then** click on "**Skip**" at the picture at RHS since we have already generated the activation code.



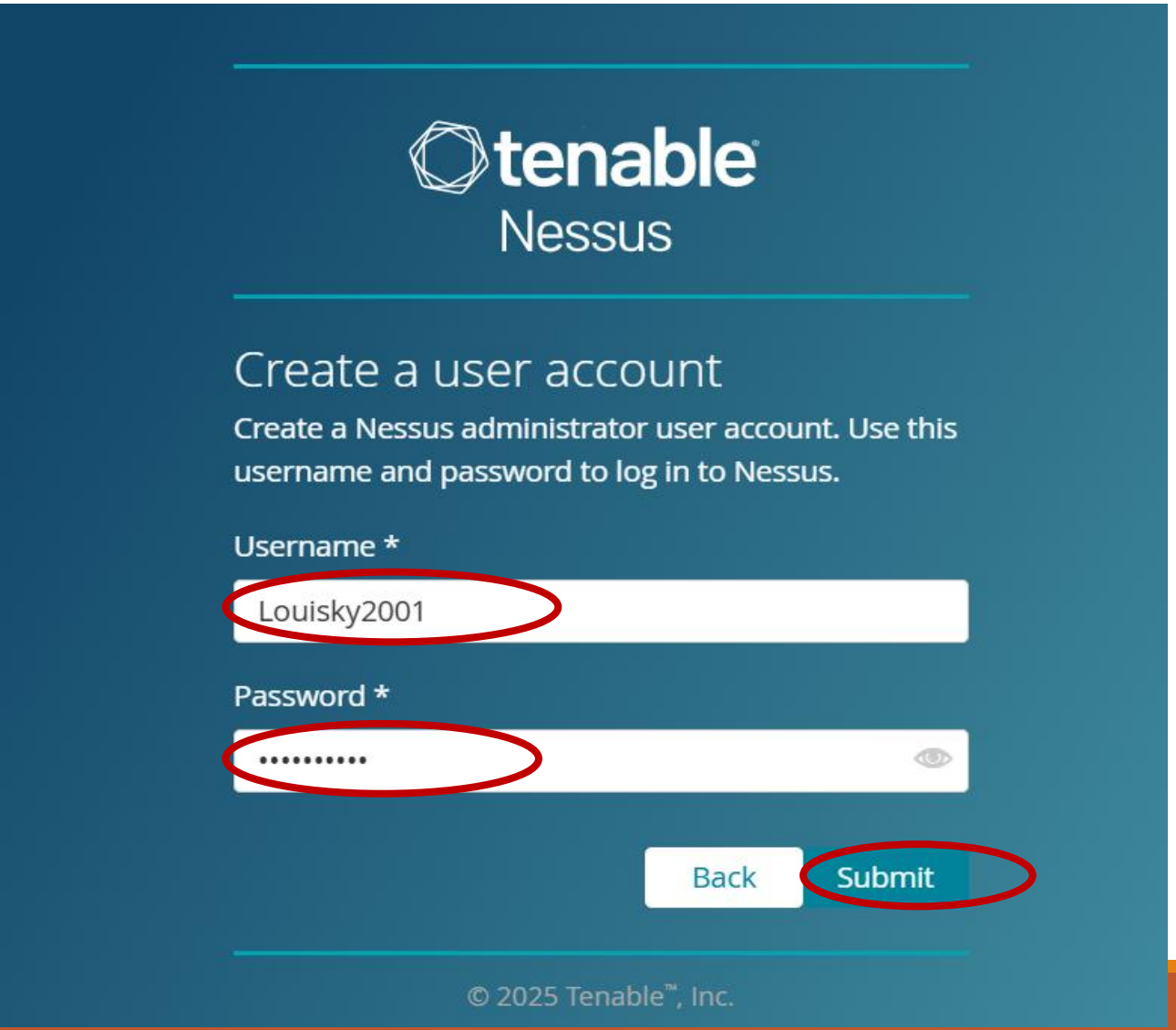


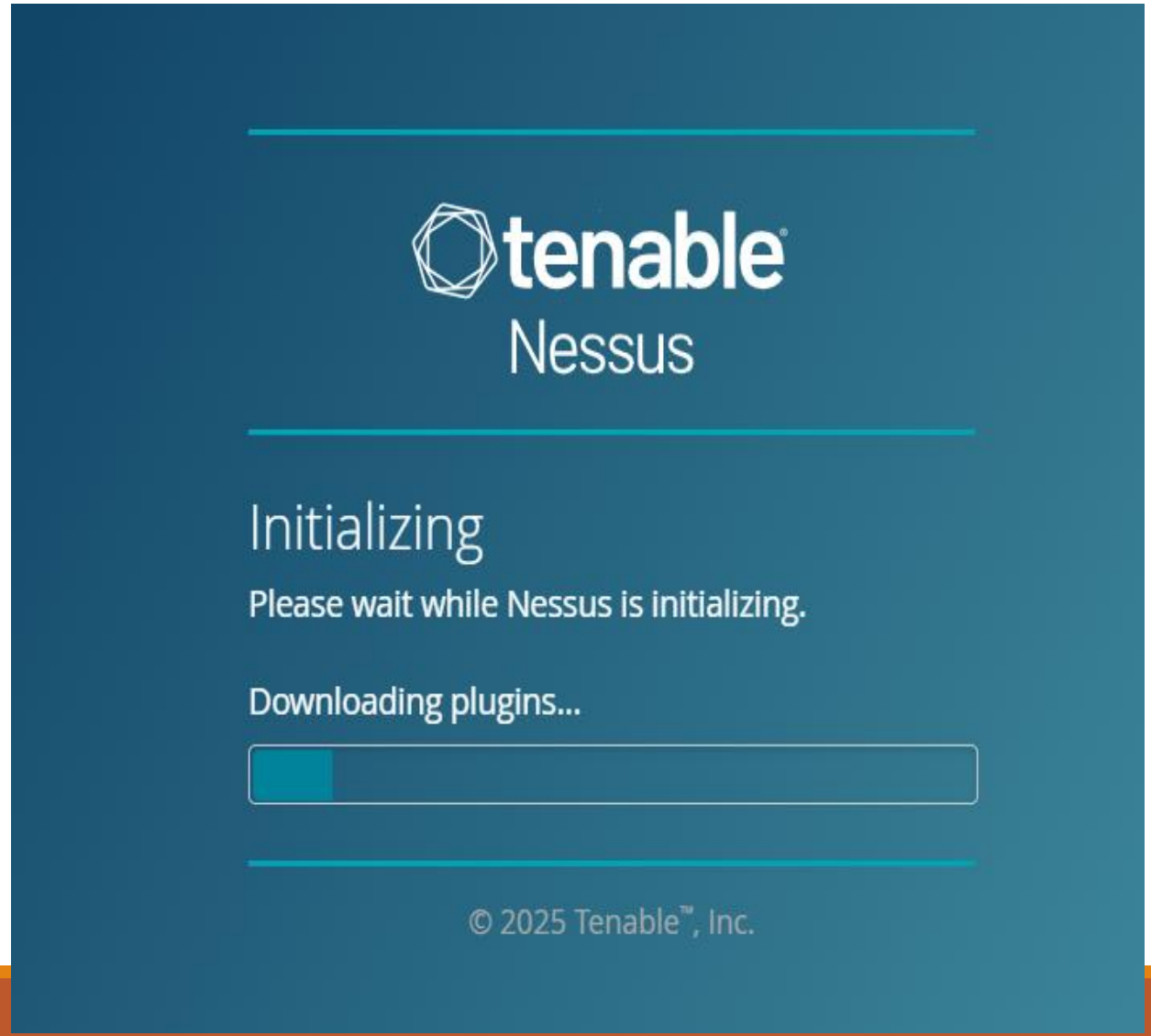
Installation Cont. After pasting the code, click on "**Continue**" on the page at RHS and LHS



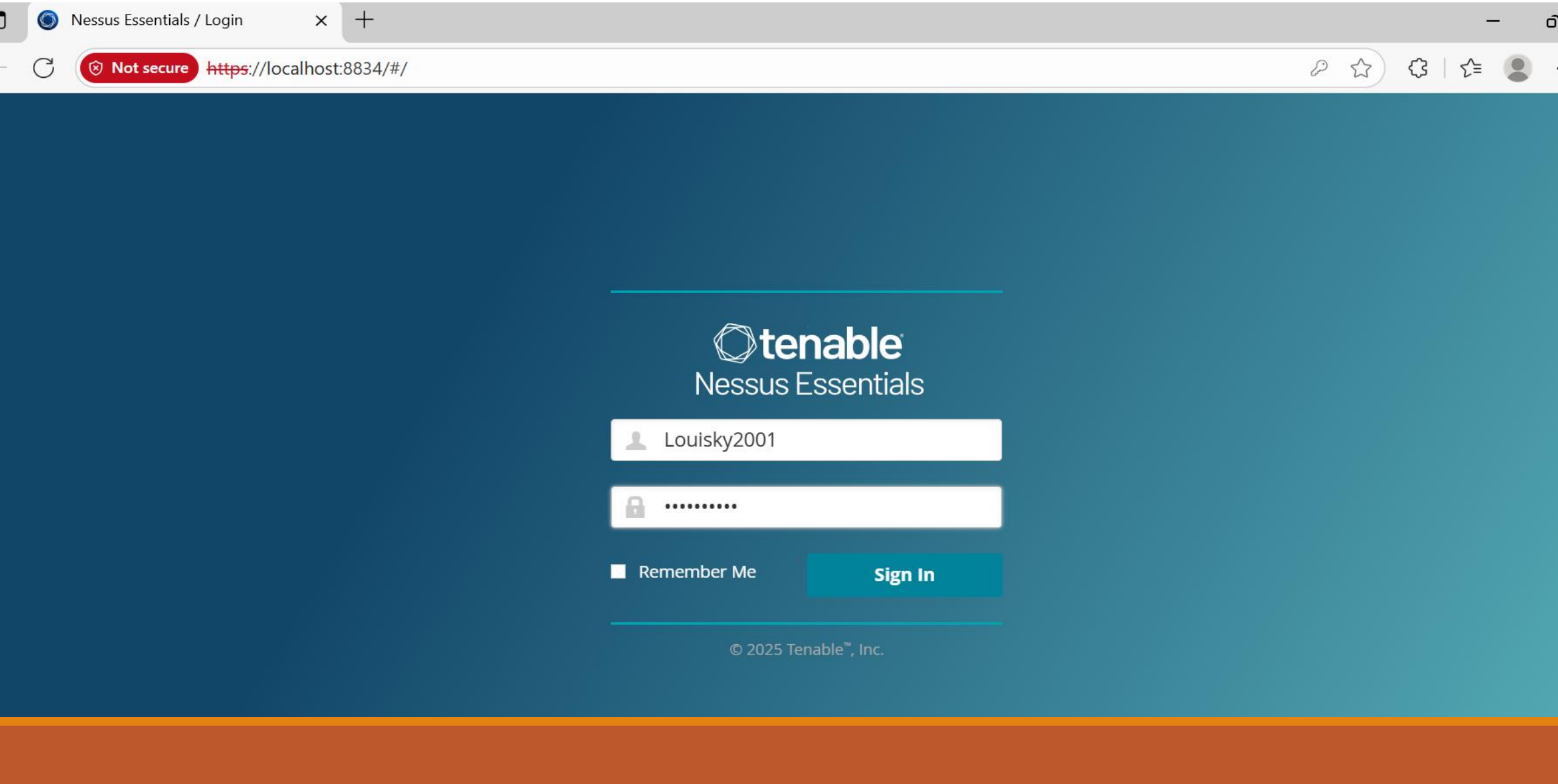


Installation Cont.. Enter your choice “**Username**” & “**Password**”, click “**Submit**”

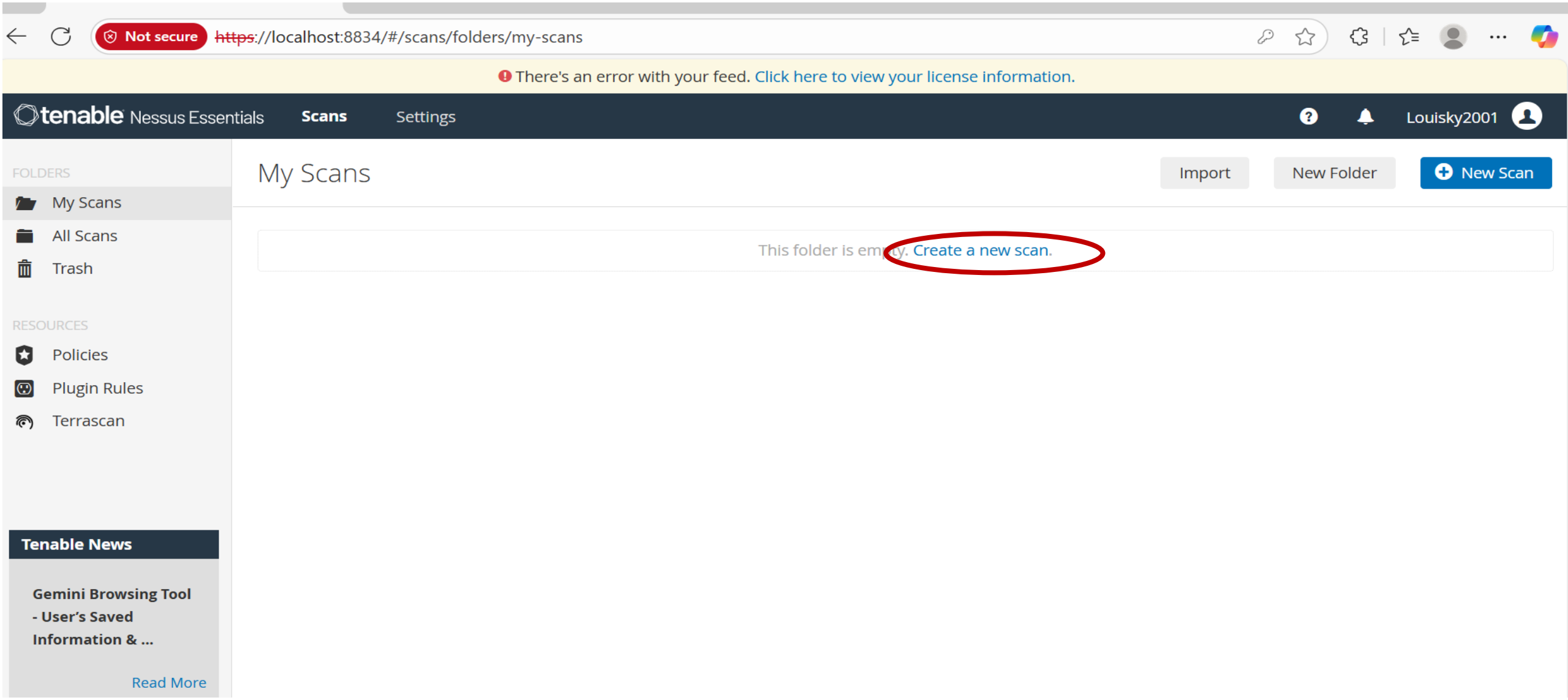




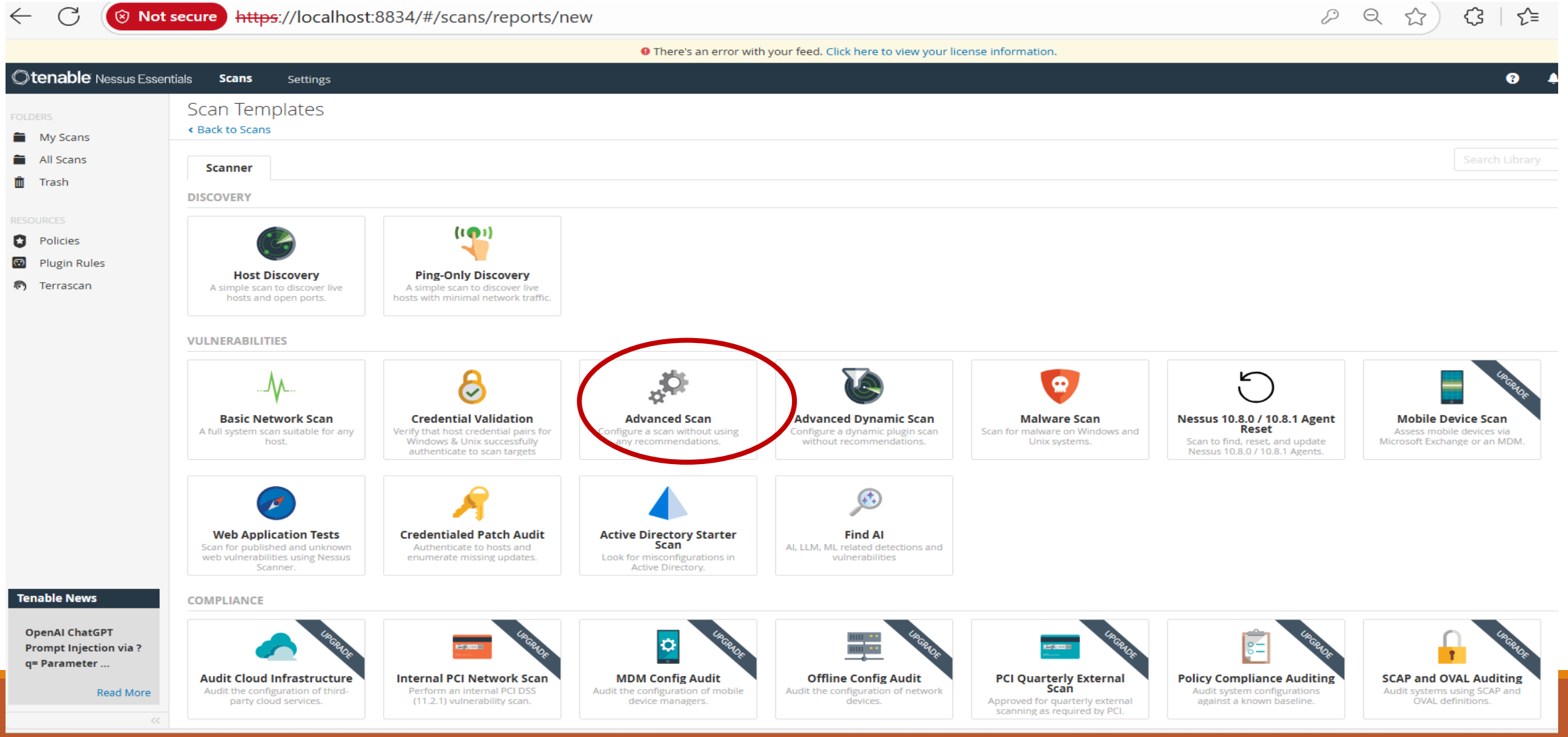
Login with your “**Username**” and “**Password**” to access Nessus Interface



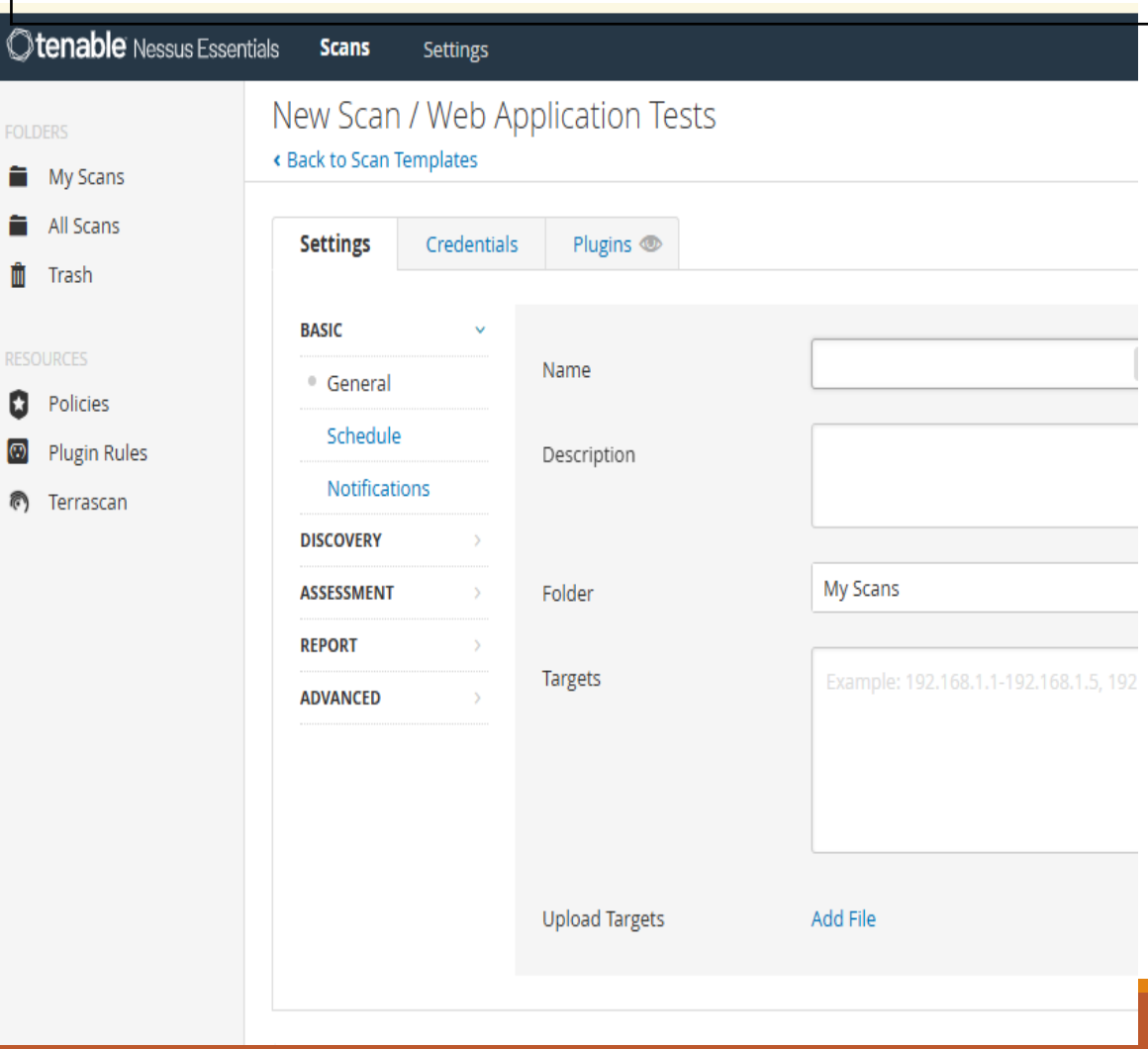
Click on "Create a New Scan"

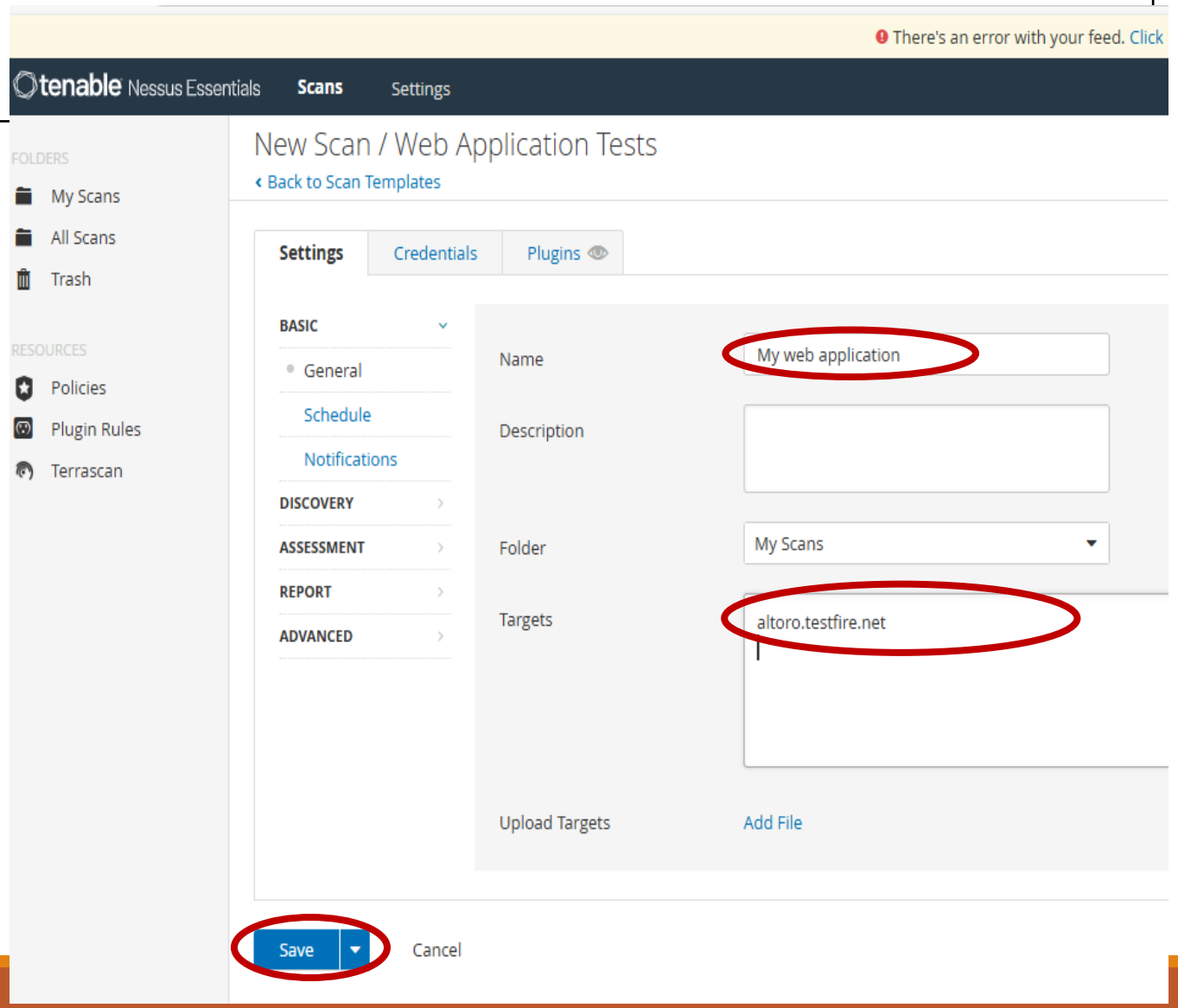


From the displayed Scan template, you can chose any area of your interest you want to scan e.g Vulnerabilities scanning, Compliance, and Assets Discovery. But in our case we click on Web App Test.

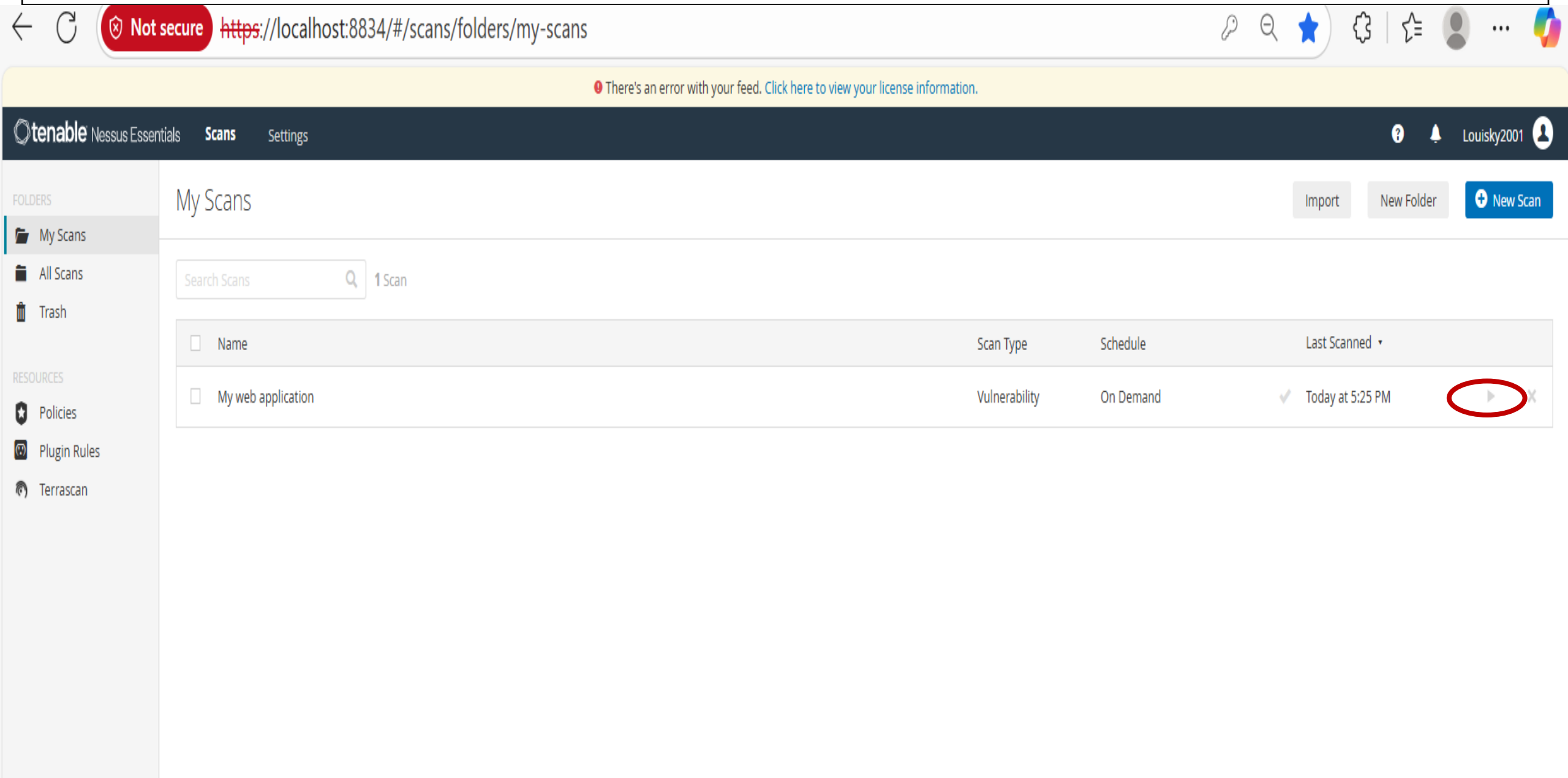


Web Application Scanning, Using Nessus. Fill-in any name of your choice in the "**name**" **field, and** Enter the **domain name or IP address only**, **without** http:// or https:// into the **TARGET** field, click **save and click Launch**

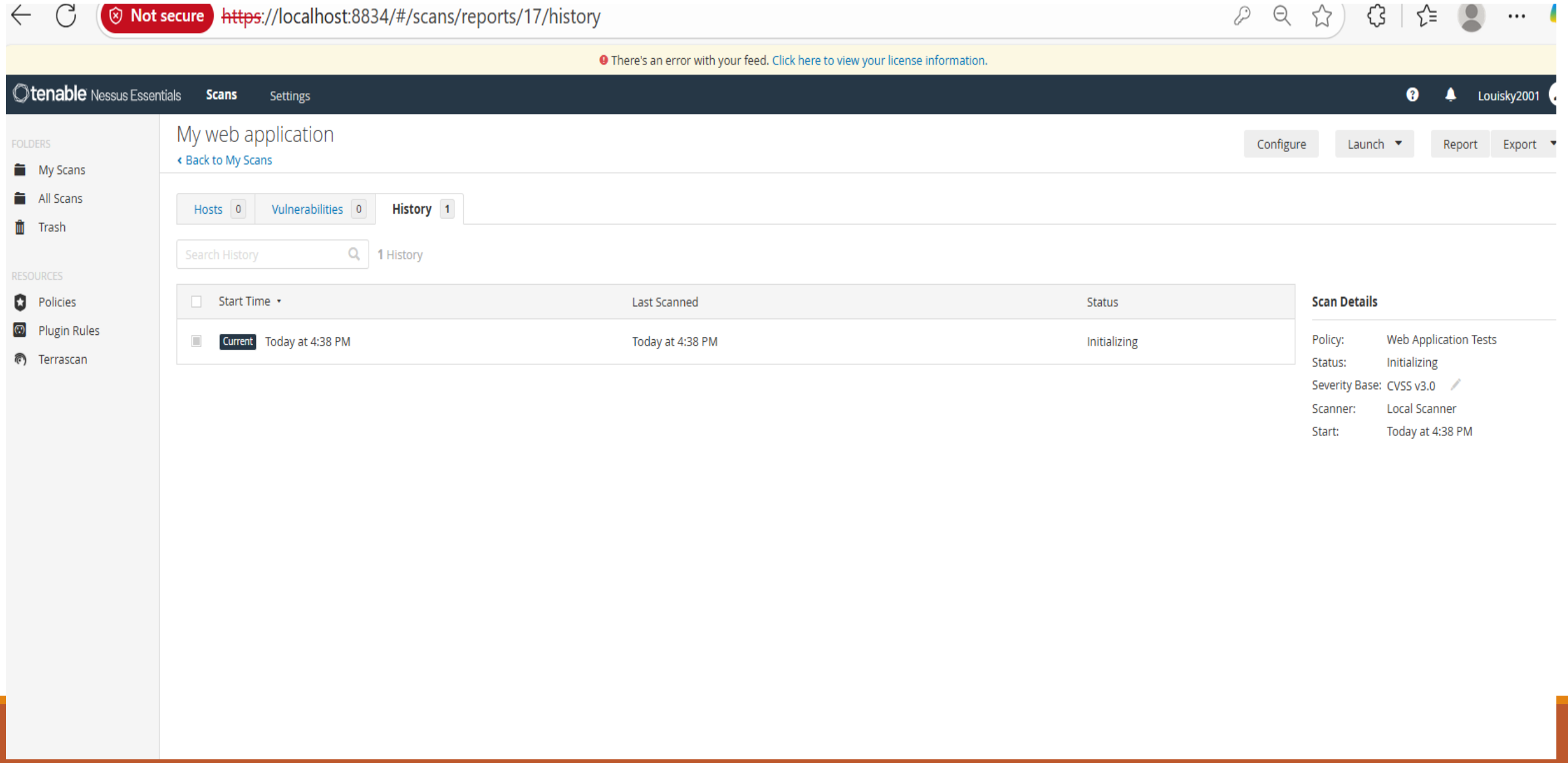




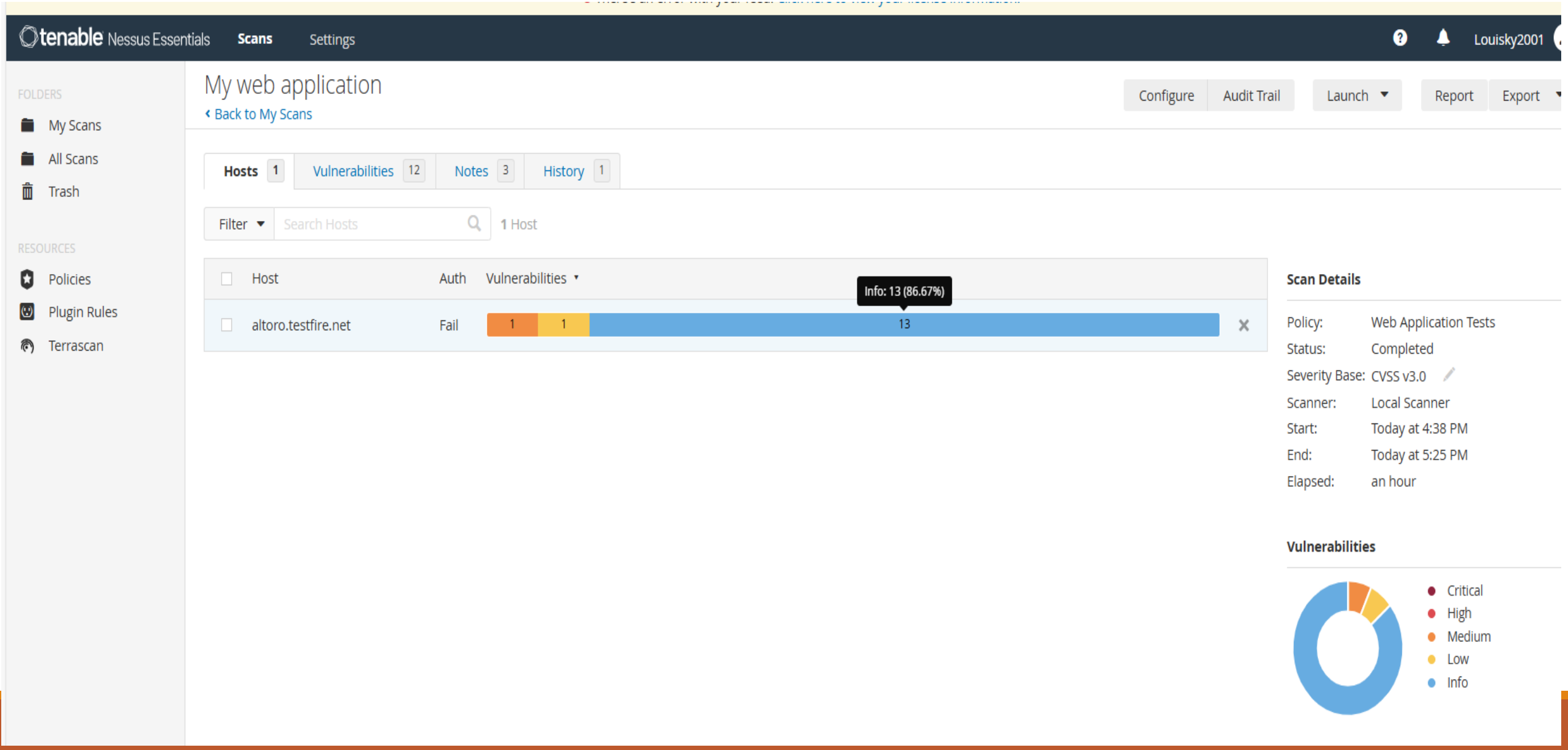
Click on the drop-down arrow to Launch the Scan



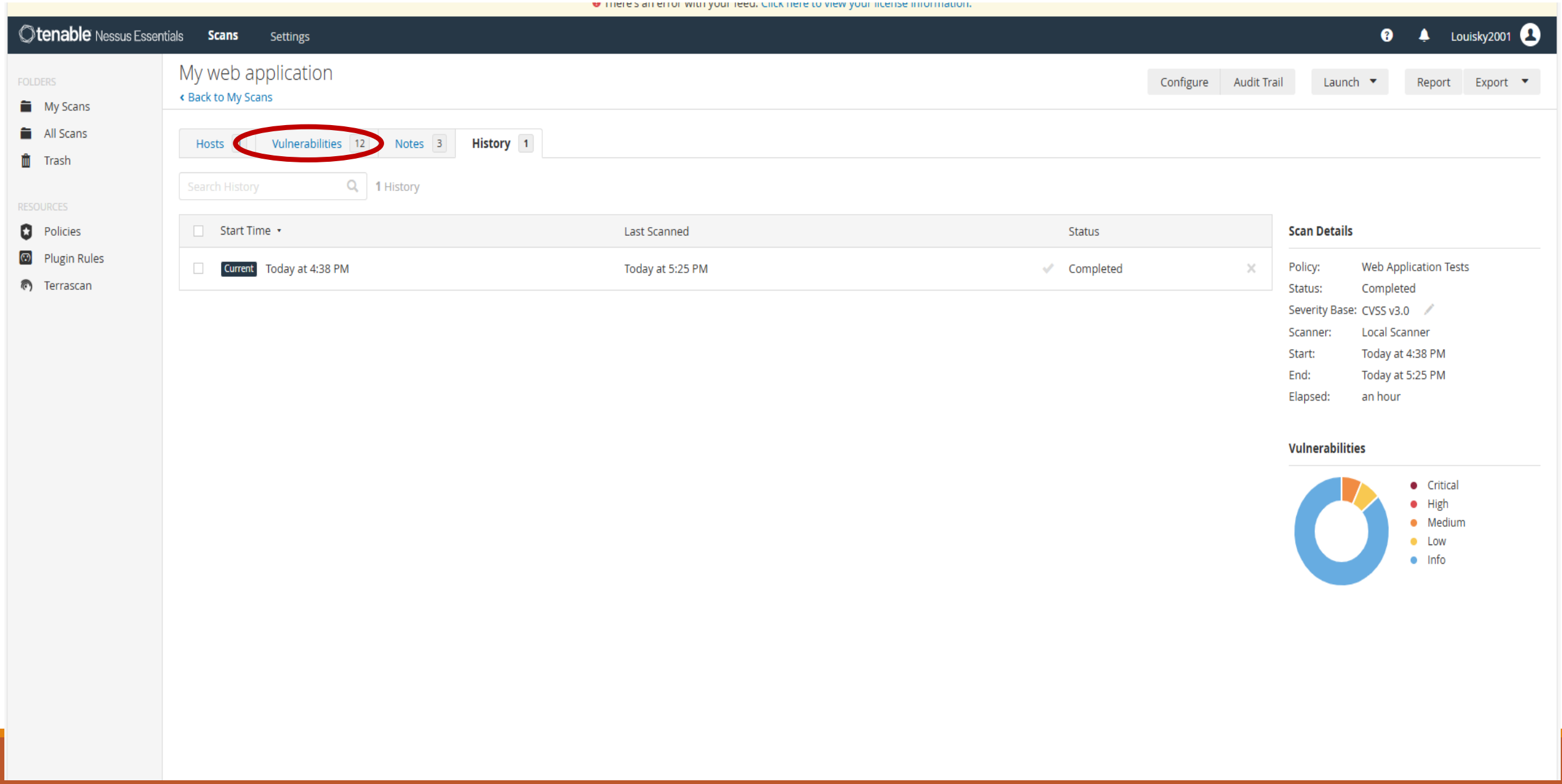
Initializing.....



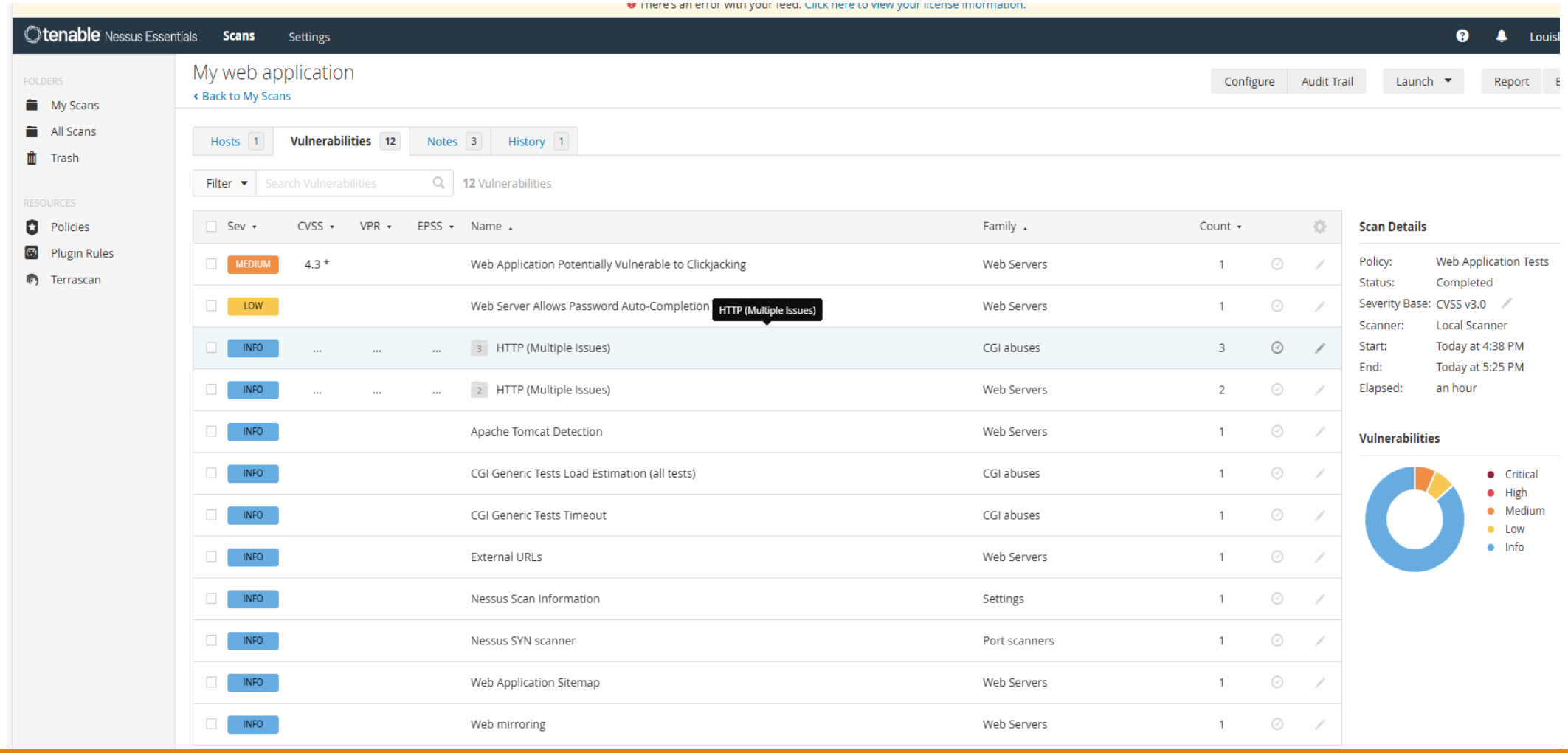
One (1) host, Eleven (11) Vulnerabilities were found, with Failed Authentication



Click on the "**VULNERABILITY TAB**" to see all the vulnerabilities in order of criticality.



Click on any of the vulnerability you want to analyze. In our case I clicked on the first vulnerability on the scanned result, whose severity is "**Medium**"



FOLDERS
My Scans
All Scans
Trash

RESOURCES
Policies
Plugin Rules
Terrascan

My web application / Plugin #85582

‹ Back to Vulnerabilities

Hosts 1 | Vulnerabilities 12 | Notes 3 | History 1

MEDIUM Web Application Potentially Vulnerable to Clickjacking

Description

The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.

X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.

Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.

Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.

Solution

Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response.
This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

See Also

http://www.nessus.org/u?399b1f56
https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet
https://en.wikipedia.org/wiki/Clickjacking

Output

```
The following pages do not use a clickjacking mitigation response header and contain a clickable event :

  - https://altoro.testfire.net/
  - https://altoro.testfire.net/feedback.jsp
  - https://altoro.testfire.net/index.jsp
  - https://altoro.testfire.net/login.jsp
  - https://altoro.testfire.net/search.jsp
```

To see debug logs, please visit individual host

Port ▲	Hosts
443 / tcp / www	altoro.testfire.net

Plugin Details

Severity:	Medium
ID:	85582
Version:	$Revision: 1.7 $
Type:	remote
Family:	Web Servers
Published:	August 22, 2015
Modified:	May 16, 2017

Risk Information

Risk Factor: Medium

CVSS v2.0 Base Score: 4.3

CVSS v2.0 Vector:
CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N

Reference Information

CWE: 693

Description of the Vulnerability

The remote web server does not include the X-Frame-Options or the Content-Security-Policy: frame-ancestors headers in its responses. This omission may leave the site vulnerable to clickjacking attacks, where users are tricked into clicking elements they can't see, potentially leading to unauthorized actions. X-Frame-Options is a widely supported browser header developed by Microsoft to help prevent such attacks. Content-Security-Policy (CSP) with frame-ancestors is a modern, W3C-backed alternative with growing browser support. These headers are currently the most effective and detectable automated defenses.

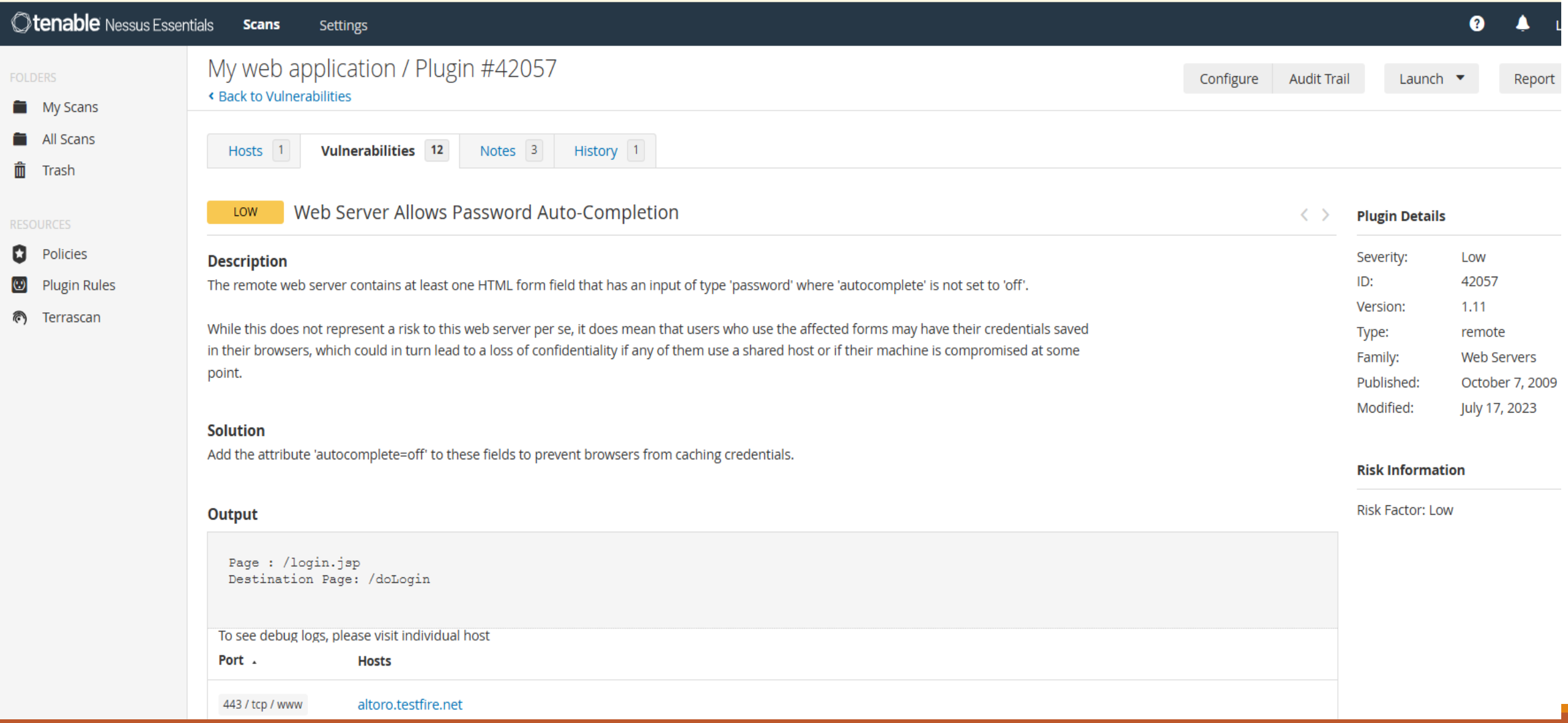
However, false positives may occur if other protections like frame-busting JavaScript are used or if the page doesn’t handle sensitive actions.

Solution to the Vulnerability

Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response. This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

The Output	Risk Information
The following pages do not use a clickjacking mitigation response header and contain a clickable event : - https://altoro.testfire.net/ - https://altoro.testfire.net/feedback.jsp - https://altoro.testfire.net/index.jsp - https://altoro.testfire.net/login.jsp - https://altoro.testfire.net/search.jsp	Risk Factor: **Medium** CVSS **v2.0** Base Score: **4.3** CVSS v2.0 Vector: CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N

Let us look at the next vulnerability, whose severity is LOW



Description of the Vulnerability

The remote web server contains at least one HTML form field that has an input of type 'password' where 'autocomplete' is not set to 'off'.

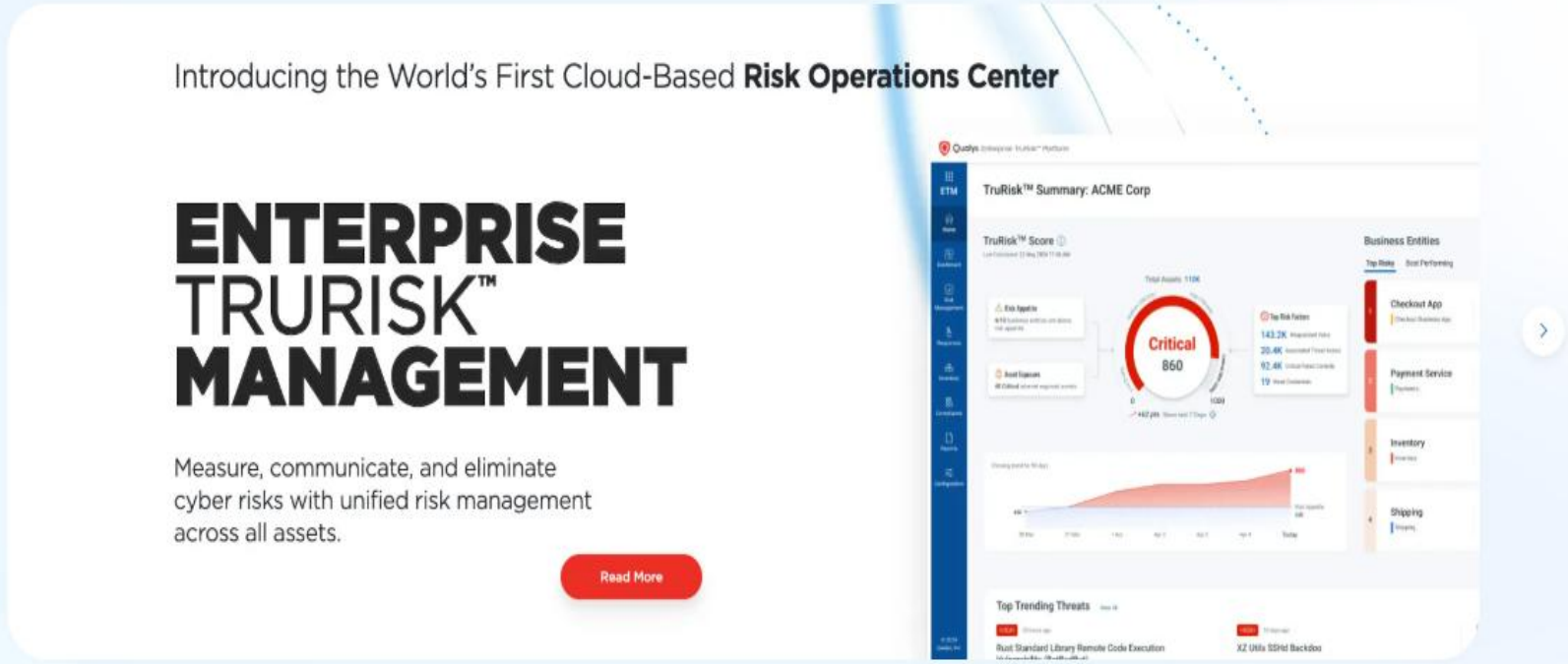
While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or if their machine is compromised at some point.

Solution to the Vulnerability

Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.

The Output	Risk Information
Page : /login.jsp Destination Page: /doLogin	Risk Factor: Low

WEB APPLICATION SCAN, USING QUALYS



Qualys

vmeru5lk

••••••••••

Forgot Password

Please wait...

Don't have an account? Sign up

Platform Status | Contact Support

Login FAQs | Trust Center | Qualys Blog | Privacy

Upcoming Events View all Events

14 Aug

Patch Tuesday Webinar August 2025: This Month in Vulnerabilities and Patches

7:00 PM - 8:00 PM UTC-08:00

Latest Announcements

New

Qualys Unveils Industry's First Agentic AI-Powered Risk Operations Center Delivering Autonomous Risk... 4 Days Ago 4 Aug

Qualys. Enterprise TruRisk™ Platform

Modules | Help | Louis OKPERIRUISI | Log out

Welcome back Louis

Thank you for using Qualys.
We'd love to hear your feedback ›

To learn more about the other applications in the Qualys Suite ›

You have 23 applications available in your subscription

Administration
Manage Application Users and Permissions
Visit now

Certificate View
Analyse and manage SSL/TLS certificates and vulnerabilities
Visit now

Cloud Agent
Stay updated with network security by deploying agents on your hosts
Visit now

Connectors
Discover Resources that are present in your cloud account
Visit now

Container Security
Discover, track, and continuously protect Containers and Images
Visit now

Continuous Monitoring
Set up monitoring and alerting of new security risks
Visit now

Custom Assessment and Remediation
Script orchestration and execution for custom assessment, response and remediation
Visit now

CyberSecurity Asset Management
Identify security gaps and manage asset health across your hybrid IT environment
Visit now

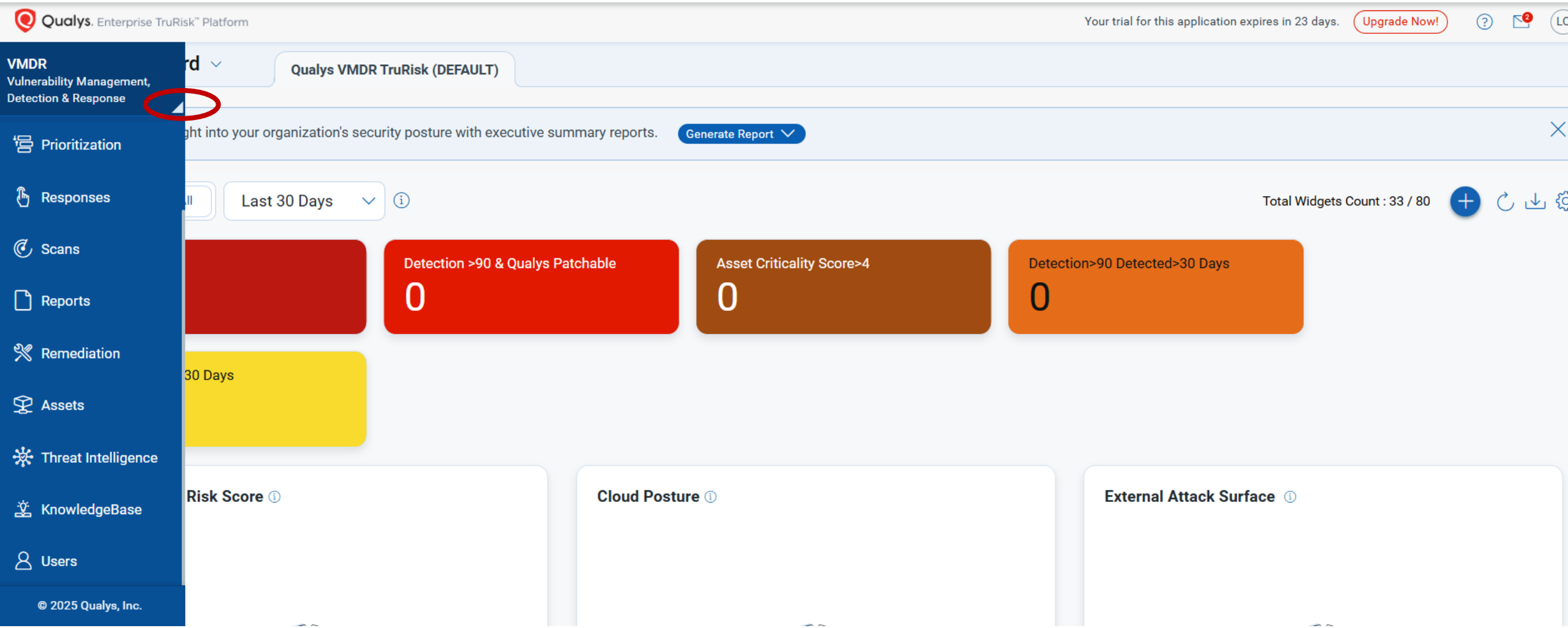
Global AssetView
Maintain full, instant visibility of all your global IT

Network Passive Sensor
Gain continuous, real-time visibility of all assets

Patch Management
Deploy patches to your systems

PCI Compliance
Achieve compliance with the PCI Data Security

Click on the drop-down arrow at the top LHS, and select " **TotalAppSec**" from the appeared list



Qualys. Enterprise TruRisk™ Platform

Web Malware Detection

Help | Louis OKPERIRUISI | Log out

PA SCA **Policy Audit**
Define and monitor IT security standards aligned with regulations

SAQ **Security Assessment Questionnaire** Trial
Automate risk and compliance through questionnaire campaigns

PCI **PCI Compliance**
Achieve compliance with the PCI Data Security Standard (DSS)

APPLICATION SECURITY (2)

TAS **TotalAppSec**
Unified application risk management solution designed to secure modern web applications and APIs

MD **Web Malware Detection**
Scan and Monitor Your Sites for Malware Infections

SENSOR MANAGEMENT (4)

CA **Cloud Agent**
Stay updated with network security by deploying agents on your hosts

PS **Network Passive Sensor** Trial
Gain continuous, real-time visibility of all assets

Get Started

QualysGuard MDS Video Series ›
The Malware Detection Service videos can help you quickly get to know MDS. The videos provide a quick high level overview, show off the new Web 2.0 UI features that make it so easy to use, and also provide task oriented step by step instruction for the most common workflows. The videos are short and to the point so you will be able to get right to work after watching them.

MDS Introductory Content ›
This content will help you learn more about the Malware Detection Service (MDS). Documentation, screenshots and links to content provide you with resources to ensure your organization can take advantage of all the features of MDS Enterprise Edition.

Join the Qualys MDS Community ›
Come join other MDS users on the QualysGuard community where you can get updates on new MDS features that are being planned, get answers to questions and find other MDS related resources.

2.apps.qualys.eu/portal-front/module/mds/#

TAS
TotalAppSec

Home

Dashboard

Discovery

Applications

Configuration

Scans

Detections

Reports

Knowledge Base

Import and Start Scanning Immediately

Scan external and internal applications and API's without installing any software

Import Webapps & API's

Supported Files TXT CSV

Visit Dashboard

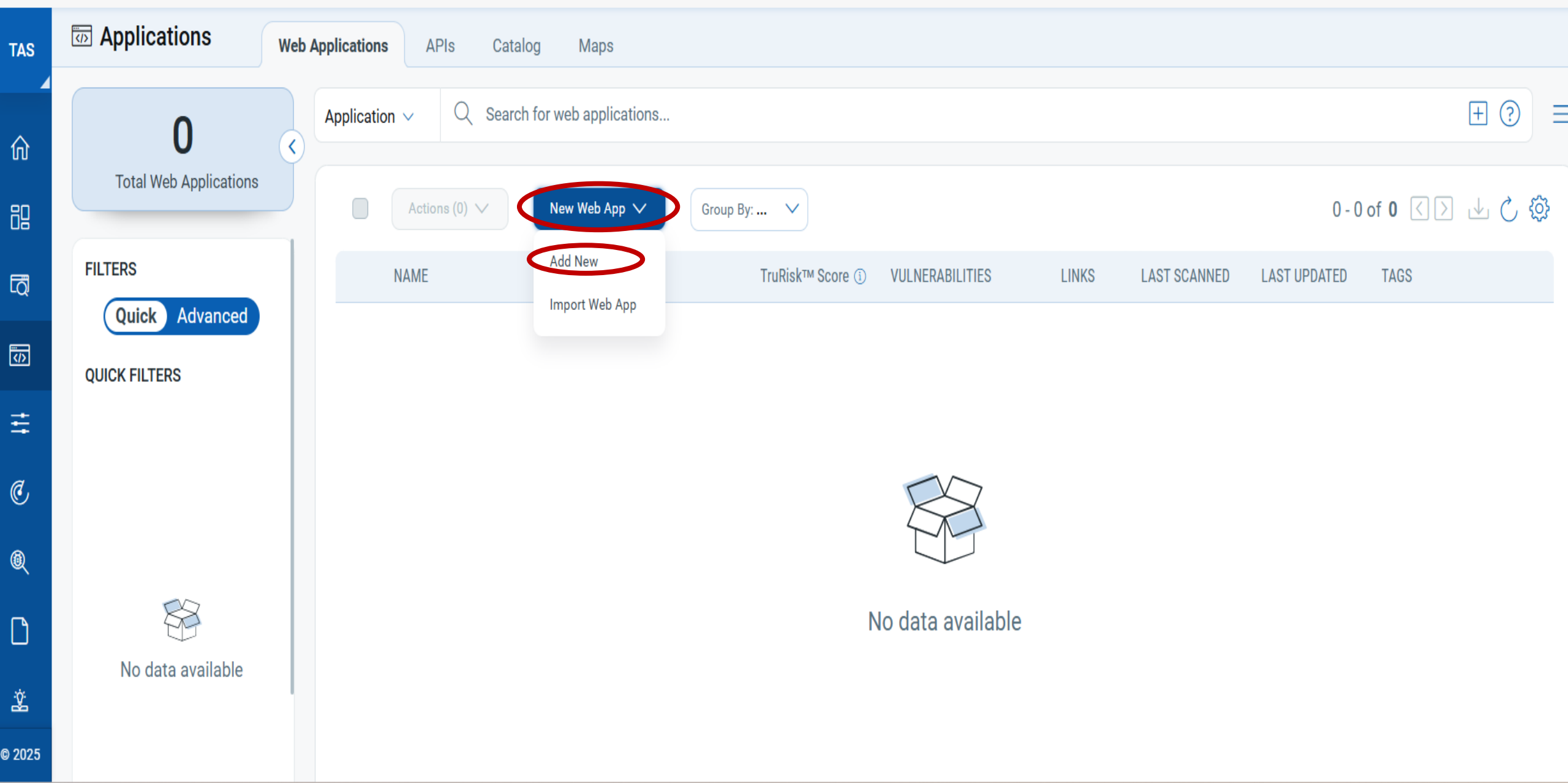
Total Web Applications and API's

High Risk Webapps & APIs

Webapps & APIs w/ Malwares

Vulnerable webapps & API's

Click on the drop down at the front of “New Web App” and click “Add New”



Qualys. Enterprise TruRisk™ Platform

← Add New: **Web Application**

Step **1**/5

- **Basic Information**
- Crawl Settings
- Default Scan Settings
- Additional Configurations
- Review & Confirm

Provide the basic information for the Web Application.

Name *

My Web-App Scan

235 characters remaining

Web Application URL or Swagger file URL *

http:// altoro.testfire.net/

2028 characters remaining

Custom Attributes

Name *

4000 characters remaining

Value *

4000 characters remaining

Add

Clear Selection | Remove Selected

NAME	VALUE

Cancel

Next

← Add New: **Web Application**

Step **2**/5

- Basic Information
- **Crawl Settings**
- Default Scan Settings
- Additional Configurations
- Review & Confirm

Crawl Settings

Web Application URl(or Swagger file URL)

http://altoro.testfire.net/

Crawl Scope

Limited at or below URL hostname (altoro.testfire.net)

Scope will be limited to the hostname within the URL: **http://altoro.testfire.net/**using HTTP or HTTPS and any port.All links discovered on the **altoro.testfire.net** domain will be in scope.For example, all links discovered in **http://altoro.testfire.net/support/** and **https://altoro.testfire.net/logout/** will be in scope.Links outside the **altoro.testfire.net** domain are not in scope.This means, for example, links like **http://cdn.altoro.testfire.net** will not be in scope.

Explicit URLs to Crawl/ REST paths and Parameters/ SOAP WSDL Location

Crawl Links

Robots txt file

Cancel Previous Next

Qualys. Enterprise TruRisk™ Platform

← Add New: **Web Application**

Step **3**/5

- Basic Information
- Crawl Settings
- **Default Scan Settings**
- Additional Configurations
- Review & Confirm

Default Scan Settings

Select Option Profile.

Create Record

Select Scanner Appliance

(•) External ( ) Individual ( ) Tags (Scanner Pool)

[ ] Lock this scanner appliance for this application.

Cancel Scan Option ⓘ

Do not Cancel Scan test

Crawl Settings

[ ] Progressive Scanning ⓘ

Cancel | Previous | Next

← Add New: **Web Application**

Step **4**/5

- Basic Information
- Crawl Settings
- Default Scan Settings
- **Additional Configurations**
- Review & Confirm

Additional Configurations

Configure additional settings for the scan.

Authentication Records

Select one or more authentication records to be used for scanning this Web Application. Each record defines one or more authentication methods – Basic, Server, NTLM.

Header Injection

Enter headers that need to be injected by the scanning service to scan the web application in the <header>: <text>. You can enter multiple headers, each header in a separate line.

Web App Endpoint Definition

Select any one Option. If this field is empty, the value is considered as null.

Set up Exclusion Lists

Global exclusions can be configured as global settings. Choose whether to use global exclusions and add more exclusions for this web app if you like.

Default DNS Override

Select one or more DNS override records with mappings to be used for scanning.

Cancel Previous Next

Click on the drop-down to chose Vulnerability

Qualys. Enterprise TruRisk™ Platform

← Add New: **Web Application**

Step **5**/5

- Basic Information
- Crawl Settings
- Default Scan Settings
- Additional Configurations
- **Review & Confirm**

Review & Confirm

Basic Information Edit

Name	My Web-App Scan
URL	http://altoro.testfire.net/

Custom Attributes

ATTRIBUTES	VALUES

No data available.

Cancel | Previous | Create Web Application | Create Web Application and Launch Scan

← Add New: **Web Application**

Step **5**/5

- Basic Information
- Crawl Settings
- Default Scan Settings
- Additional Configurations
- **Review & Confirm**

Review & Confirm

Basic Information Edit

Name	My Web-App Scan
URL	http://altoro.testfire.net/

Custom Attributes

ATTRIBUTES	VALUES

No data available.

Discovery

Vulnerability

Cancel | Previous | Create Web Application | Create Web Application and Launch Scan

Qualys. Enterprise TruRisk™ Platform

← Launch New Scan: **Vulnerability**

Step **1**/3

- **Basic Details**
- Scan Settings
- Review And Confirm

Basic Information

Provide the basic information for the scan.

Name *

My Web-App Scan - Aug 8, 2025

227 characters remaining

Scan Target

(•) Names ( ) Tags

Select Name or Tag to include the applications you want to scan.

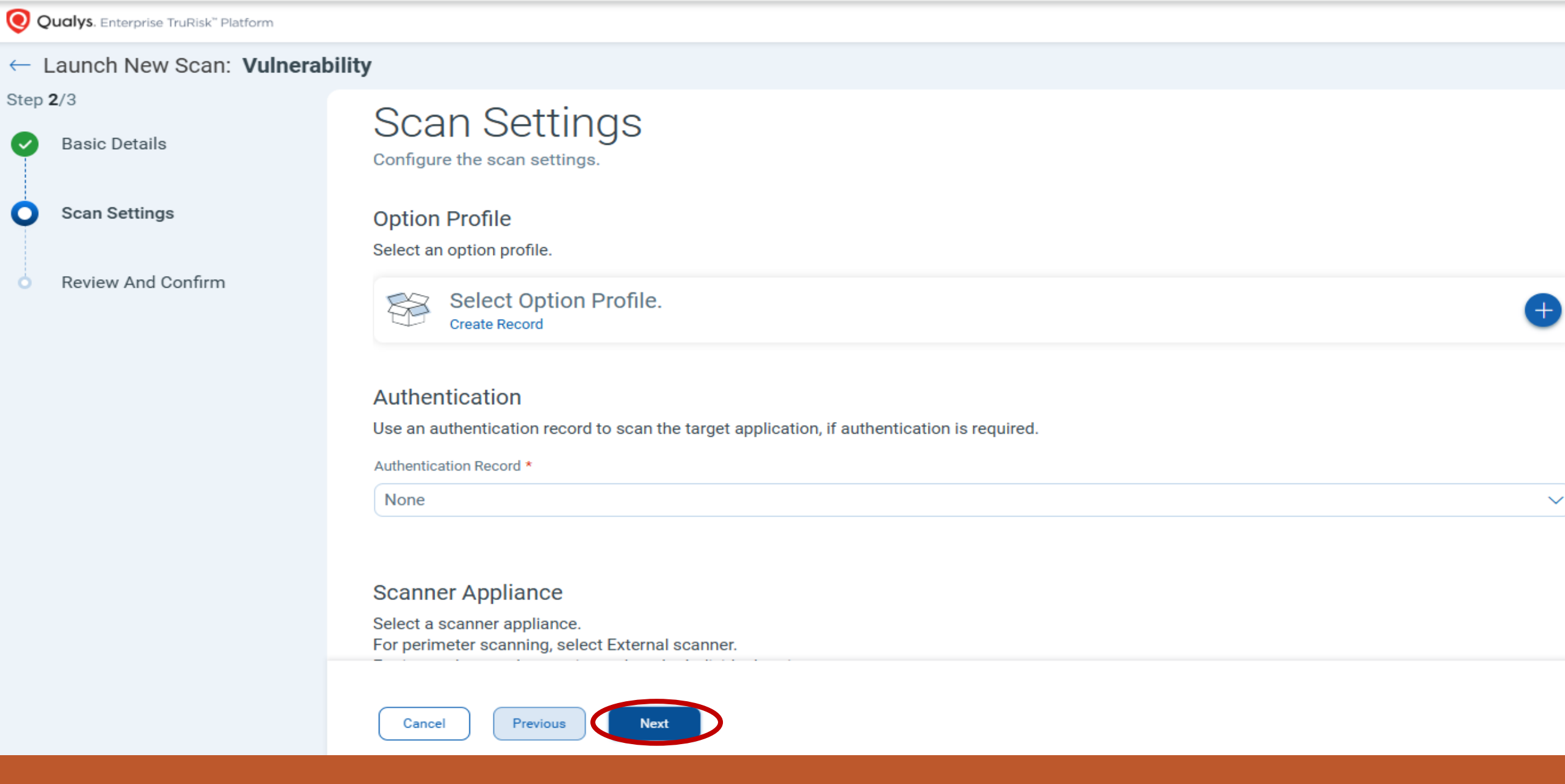
Applications

Clear Selection | Remove Selected

	NAME
	My Web-App Scan

Cancel Next

Click on “Create Record” and chose “Initial WAS Options”



← Add New: **Option Profiles**

Step **2**/5

- Profile Details
- **Scan Parameter**
- Search Criteria
- Comments
- Review And Confirm

Scan Parameter

Provide details for scan settings.

General Settings

Define form action URI and form field names. This results in crawling of all forms having same fields but with different action URI.

Form Submission *

( ) None ( ) Post ( ) Get (•) Post & Get

Form Crawl Scope

When enabled, we will calculate form uniqueness using form action URI in addition to form field names. This results in crawling of all forms having same fields but having different action URI.

[ ] Include form action URI in form uniqueness calculation.

Maximum Links To Crawl * ⓘ

1000

User Agent

Cancel Previous Next

Qualys. Enterprise TruRisk™ Platform

← Add New: **Option Profiles**

Step **3**/5

- Profile Details
- Scan Parameter
- **Search Criteria**
- Comments
- Review And Confirm

Search Criteria

Provide criteria for search during the web application scan.

Detection Scope

Select the scope of detections for the web application scan with this profile. Specify if the scan should perform a full assessment for all WAS detections, or if the scan shall focus on the specific WAS detections/vulnerabilities.

Detection *

Everything

- Core
- Categories
- Custom Search Lists
- XSS Power Mode
- Everything

Sensitive Content

Credit Card Numbers

Cancel | Previous | Next

Qualys. Enterprise TruRisk™ Platform

← Add New: **Option Profiles**

Step **4**/5

- Profile Details
- Scan Parameter
- Search Criteria
- **Comments**
- Review And Confirm

Comments

Add comments for this Option Profile

Enter a new comment

2048 characters remaining

Cancel | Previous | Next

Qualys. Enterprise TruRisk™ Platform

← Add New: **Option Profiles**

Step **5**/5

- Profile Details
- Scan Parameter
- Search Criteria
- Comments
- **Review And Confirm**

Review And Confirm

Basic Information

Name
initial WAS option

Owner
Louis OKPERIRUISI(vmeru5lk)

Default Option Profile
Disabled

Tags
-

Scan Parameter

General Settings

Form Submission
GET and POST

Form Crawl Scope
Disabled

Maximum links to test in scope
1000

User Agent
-

Request Parameter Set
Initial Parameters

Document Type
Enabled

Crawl Settings

Enhanced Crawling

SmartScan

SmartScan Depth

Cancel | Previous | **Create Option Profile**

← Launch New Scan: **Vulnerability**

Step **2**/3

- Basic Details
- **Scan Settings**
- Review And Confirm

Scan Settings

Configure the scan settings.

Option Profile

Select an option profile.

Option Profile

Create Record | Change

NAME
initial WAS option

☐ Make the selected profile the default profile for this application.

Authentication

Use an authentication record to scan the target application, if authentication is required.

Cancel | Previous | **Next**

Qualys. Enterprise TruRisk™ Platform

← Launch New Scan: **Vulnerability**

Step **3**/3

- Basic Details
- Scan Settings
- Review And Confirm

Review And Confirm

Basic Details

Name
My Web-App Scan - Aug 8, 2025

Scan Target

Type
Names

Web Application
My Web-App Scan

Scan Settings

Scanner Information

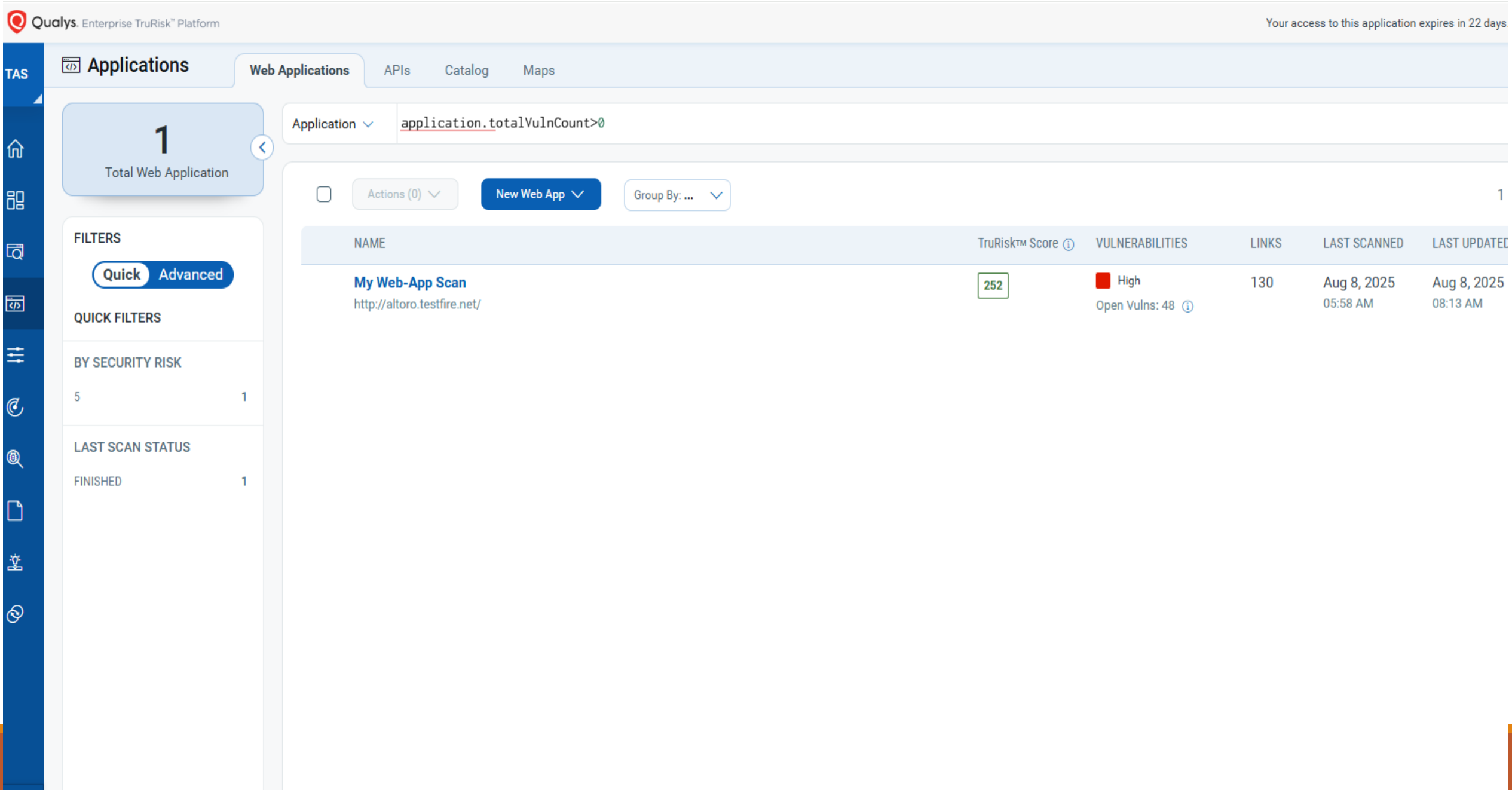
Scanner Appliance Type
External

Option Profile

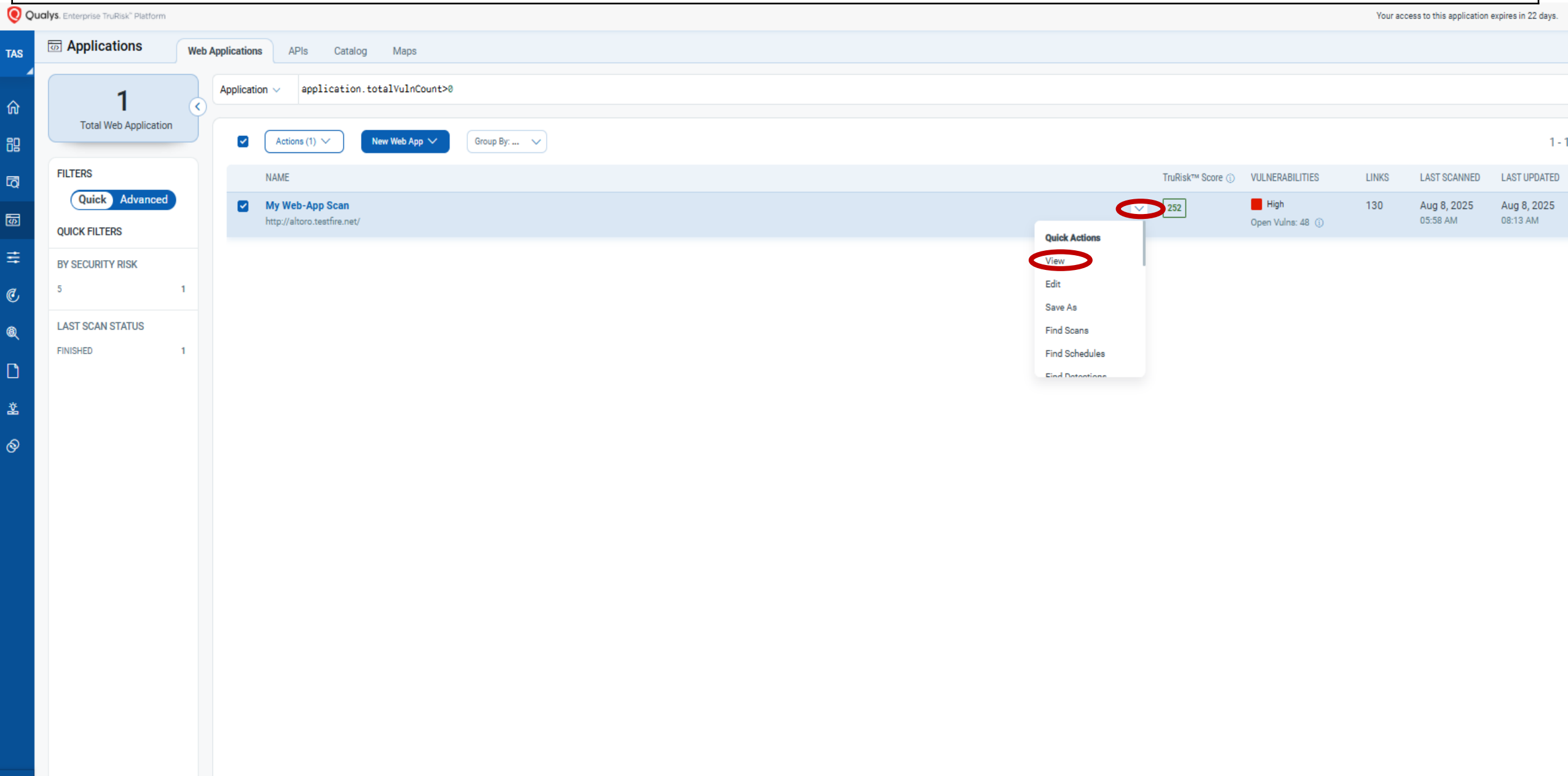
Option Profile
initial WAS option

Scan Option
Use this profile if the application has no default profile assigned

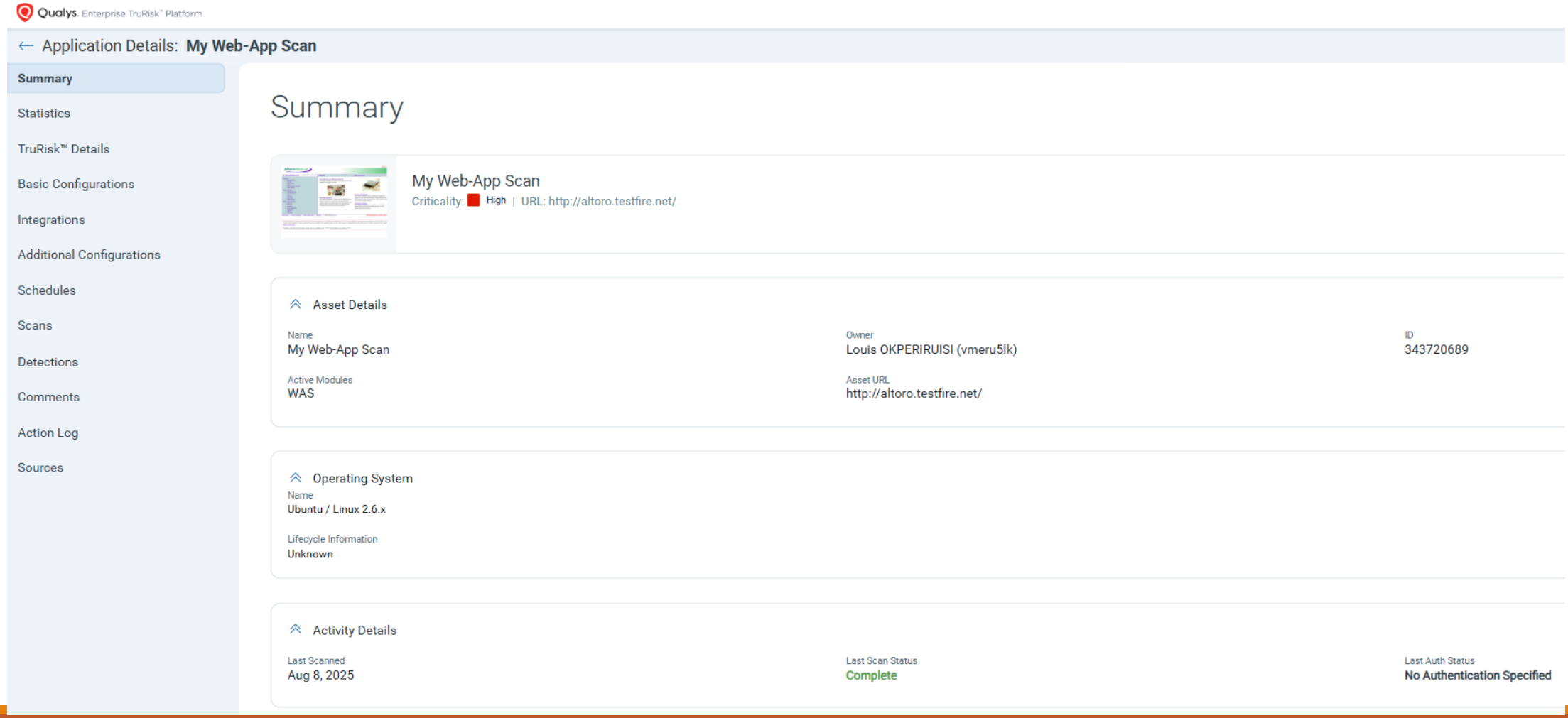
Cancel | Previous | Launch Scan


Qualys. Enterprise TruRisk™ Platform
Your access to this application expires in 22 days
TAS
Applications
Web Applications
APIs
Catalog
Maps
1
Total Web Application
Application
application.totalVulnCount>0
Actions (0)
New Web App
Group By: ...
1
FILTERS
Quick
Advanced
QUICK FILTERS
BY SECURITY RISK
5
1
LAST SCAN STATUS
FINISHED
1
NAME
TruRisk™ Score
VULNERABILITIES
LINKS
LAST SCANNED
LAST UPDATED
My Web-App Scan
http://altoro.testfire.net/
252
High
Open Vulns: 48
130
Aug 8, 2025
05:58 AM
Aug 8, 2025
08:13 AM

Click on the drop-down and select “view”



The panel at the LHS of the screen shows detailed overview of the scanned application that can be review for more detailed about the scanned Application. Let us start with the "Summary"



Summary, Cont…

TOP 10 VULNERABLE URLS

URL	VULNERABILI…
http://altoro.testfire.net/	6
http://altoro.testfire.net/sendFeedback	5
http://altoro.testfire.net/doLogin	4
http://altoro.testfire.net/feedback.jsp	2
http://altoro.testfire.net/index.jsp?content=..%2F..%2F..%2F..%2F..%2F..%2F..%2FWindows%2FSystem32%2Fdrivers%2Fetc%2Fh	2
http://altoro.testfire.net/index.jsp?content=..%2F..%2F..%2F..%2F..%2F..%2F..%2FWindows%2FSystem32%2Fdrivers%2Fetc%2Fh	2
http://altoro.testfire.net/login.jsp	2
http://altoro.testfire.net/search.jsp	2
http://altoro.testfire.net/index.jsp	1
http://altoro.testfire.net/index.jsp?content=%3C%0a%0dscript%20a%3D4%3EqssUH1Z5mf4%3D7%3C%0a%0d%2Fscript%3E	1

Statistics Overview of the entire scan.

Qualys. Enterprise TruRisk™ Platform

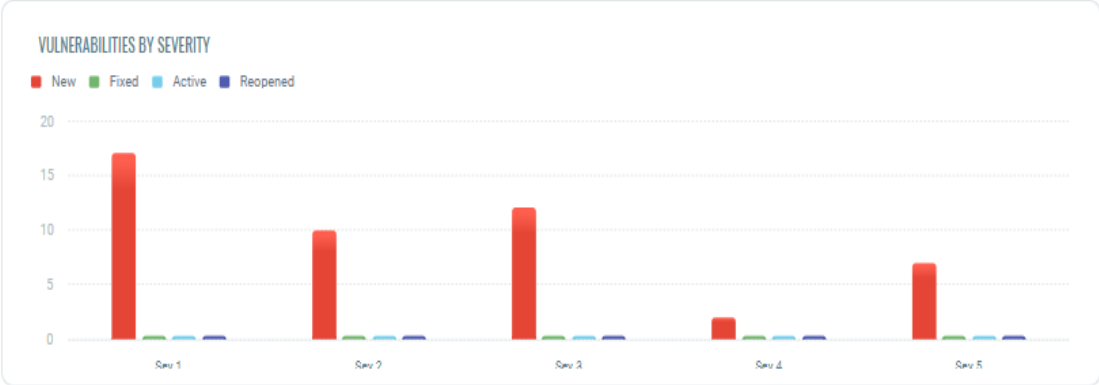
← Application Details: **My Web-App Scan**

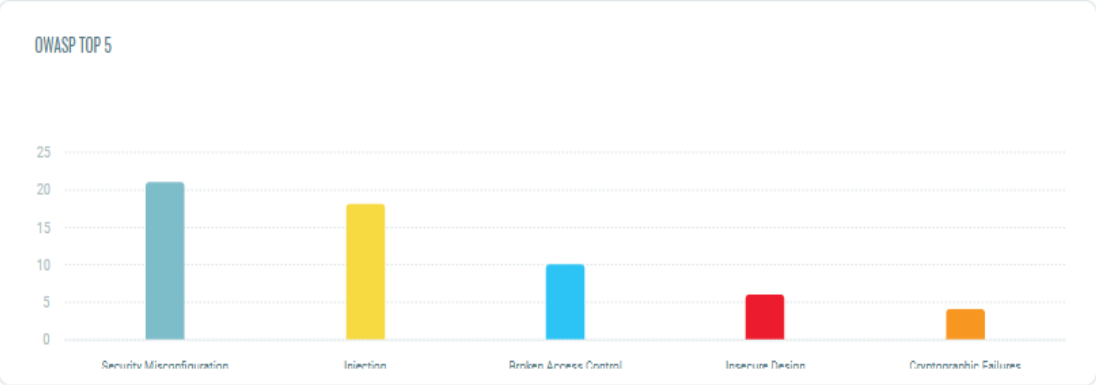
- Summary
- **Statistics**
- TruRisk™ Details
- Basic Configurations
- Integrations
- Additional Configurations
- Schedules
- Scans
- Detections
- Comments
- Action Log
- Sources

Basic Configuration

Actions

Vulnerabilities	Sensitive Content	Information Gathered
48	0	50





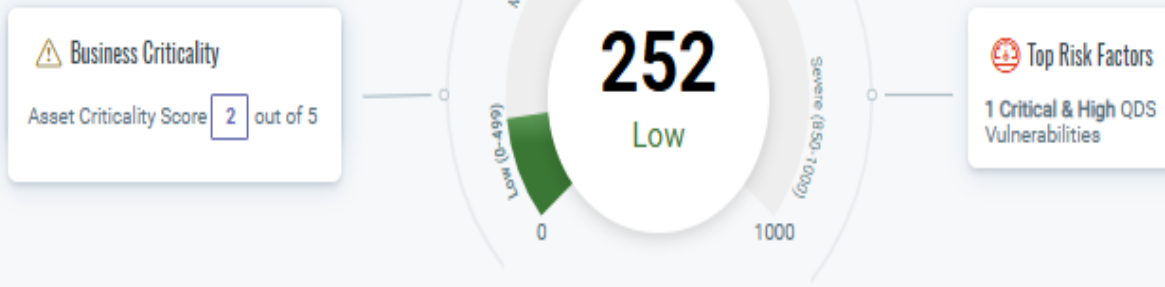
TruRisk Details

Qualys. Enterprise TruRisk™ Platform

← Application Details: **My Web-App Scan**

- Summary
- Statistics
- **TruRisk™ Details**
- Basic Configurations
- Integrations
- Additional Configurations
- Schedules
- Scans
- Detections
- Comments
- Action Log
- Sources

TruRisk™ Score and its Contributing Factors



Risk Calculation

Formula	**TruRisk™ Score** = MIN(ACS * (w_c* Avg(QDS_c) * np.power(Count(QDS_c), 1/100) + w_h* Avg(QDS_h) * np.power(Count(QDS_h), 1/100) + w_m* Avg(QDS_m) * np.power(Count(QDS_m), 1/100) + w_l* Avg(QDS_l) * np.power(Count(QDS_l), 1/100)), 1000)
Calculation	**TruRisk™ Score = (252)** = 2*{(1.0*100*(1^0.01))+(0.6*0*(0^0.01))+(0.4*50*(29^0.01))+(0.2*27*(18^0.01))}

TruRisk Details (Detections) cont.. Click on the "**QDS**" to have a complete overview of the vulnerability

Qualys. Enterprise TruRisk™ Platform

← Application Details: **My Web-App Scan**

- Summary
- Statistics
- **TruRisk™ Details**
- Basic Configurations
- Integrations
- Additional Configurations
- Schedules
- Scans
- Detections
- Comments
- Action Log
- Sources

Detections

only detection with QDS > 0 are shown.

1 - 48 of **48**

STATUS	QID	NAME	QDS	GROUP	LAST DETECTED	AGE	PATCH	SEVERITY
New	150360	**EOL/Obsolete Software: Adobe Flash Content Detected** http://altoro.testfire.net/subscribe.swf	100	INFO	Aug 8, 2025 05:58 AM	0	-	
New	150520	**Web Server Information Disclosure** http://altoro.testfire.net/search.jsp	55	INFO	Aug 8, 2025 05:58 AM	0	-	
New	150049	**Weak Credentials Vulnerability** http://altoro.testfire.net/doLogin	55	INFO	Aug 8, 2025 05:58 AM	0	-	
New	150263	**Insecure Transport** http://altoro.testfire.net/	55	INFO	Aug 8, 2025 05:58 AM	0	-	
New	150520	**Web Server Information Disclosure** http://altoro.testfire.net/	55	INFO	Aug 8, 2025 05:58 AM	0	-	
New	150053	**Login Form Is Not Submitted Via HTTPS** http://altoro.testfire.net/doLogin	55	INFO	Aug 8, 2025 05:58 AM	0	-	
New	150079	**Slow HTTP headers vulnerability** http://altoro.testfire.net/search.jsp	55	INFO	Aug 8, 2025 05:58 AM	0	-	
New	150001	**Reflected Cross-Site Scripting (XSS) Vulnerabilities** http://altoro.testfire.net/sendFeedback	50	XSS	Aug 8, 2025 05:58 AM	0	-	
New	150084	**Unencoded characters** http://altoro.testfire.net/index.jsp?content=%3C%0a%0dscript%20a%3D4%3Eqssgv25k9bV%3D7%3C%0a%0d%2Fscript%3E&job=OperationalRiskManager%3ARiskManagement	50	XSS	Aug 8, 2025 05:58 AM	0	-	
New	150084	**Unencoded characters** http://altoro.testfire.net/sendFeedback	50	XSS	Aug 8, 2025 05:58 AM	0	-	
New	150124	**Clickjacking - Framable Page** http://altoro.testfire.net/login.jsp	50	INFO	Aug 8, 2025 05:58 AM	0	-	
New	150001	**Reflected Cross-Site Scripting (XSS) Vulnerabilities** http://altoro.testfire.net/index.jsp?content=%3CEMBED%20SRC%3D%2F%2Flocalhost%2Fq7U7x1Mxr.swf%20AllowScriptAccess%3Dalways%3E%3C%2FEMBED%3E&job=Teller%3AConsumaerBanking	50	XSS	Aug 8, 2025 05:58 AM	0	-	
New	150022	**Server Error Message** http://altoro.testfire.net/index.jsp?content=..%2F..%2F..%2F..%2F..%2F..%2F..%2FWindows%2FSystem32%2Fdrivers%2Fetc%2Fhosts%00	50	INFO	Aug 8, 2025 05:58 AM	0	-	
New	150159	**Session Cookie Set over Non-HTTPS Connection**						

← Detection Details: **EOL/Obsolete Software: Adobe Flash Content Detected**

Detection Detail

Actions

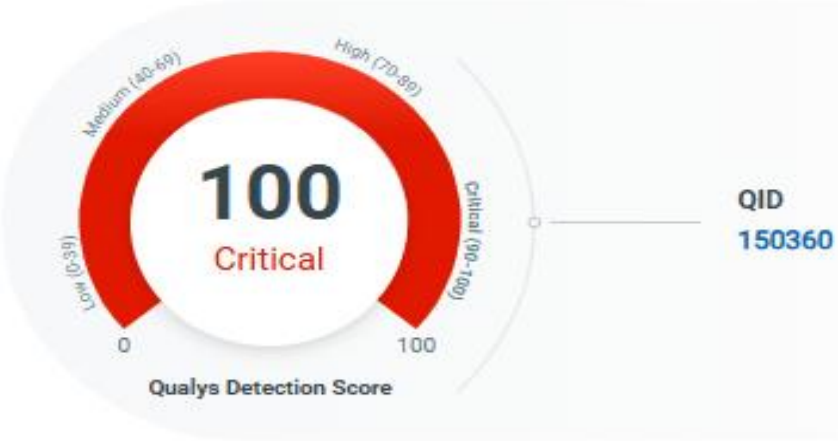
EOL/Obsolete Software: Adobe Flash Content Detected

QID: 150360 | Status: **New** | Severity: | Group: INFO

URL: http://altoro.testfire.net/subscribe.swf

Findings & Recommendations | DETECTION DETAILS | History & Comments | **QDS DETAILS**

Contributing Factors



QID
150360

Details

Finding #:	32045200
Unique #:	79f5af6d-1f3f-4540-9980-e64844c3df2f
Patch #:	-
Group:	Information Disclosure
CWE:	CWE-1104
CVE:	-
OWASP Web Appli... :	A6 Vulnerable and Outdated Components
CISA Known Explo... :	False
CVSS V3 Base:	9.8
CVSS V3 Temporal:	8.7
CVSS V3 Attack V... :	Network
CVSS V3 Vector S... :	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Authentication:	Not Used
Web Application:	My Web-App Scan
Times Found:	1
First Time Detected:	Aug 8, 2025 05:58 AM GMT+01:00
Last Time Detected:	Aug 8, 2025 05:58 AM GMT+01:00
Last Time Tested:	Aug 8, 2025 05:58 AM GMT+01:00

The Scan shows the “**THREAT**”, “**IMPACT**”, and “**REMENDIATION**” to the vulnerability

← Detection Details: **EOL/Obsolete Software: Adobe Flash Content Detected**

Detection Detail

EOL/Obsolete Software: Adobe Flash Content Detected
QID: 150360 | Status: **New** | Severity: | Group: INFO
URL: http://altoro.testfire.net/subscribe.swf

Findings & Recommendations DETECTION DETAILS History & Comments QDS DETAILS

Threat
Description
Adobe Flash content has been identified on this web application. Adobe Flash Player reached End Of Life (EOL) on 31 December 2020.

Impact
Description
As of 12 January 2021, Adobe has blocked all Flash content from running on Adobe Flash Player. For additional details on Adobe Flash Player EOL: https://www.adobe.com/in/products/flashplayer/enterprise-end-of-life.html#:~:text=As%20previously%20announced%20in%20July,Player%20beginning%2012%20January%202021

Solution
Description
Adobe recommends removing Flash content and/or migrating it to alternative technologies.
For more details refer to: https://www.adobe.com/in/products/flashplayer/enterprise-end-of-life.html#:~:text=As%20previously%20announced%20in%20July,Player%20beginning%2012%20January%202021
https://blog.qualys.com/vulnerabilities-research/2020/12/21/adobe-flash-player-reaches-end-of-life-on-december-31-2020

This is a “**MEDIUM**” Vulnerability, and we will click on the findings & recommendation for more details as well.

Qualys. Enterprise TruRisk™ Platform

← Detection Details: **Web Server Information Disclosure**

Detection Detail

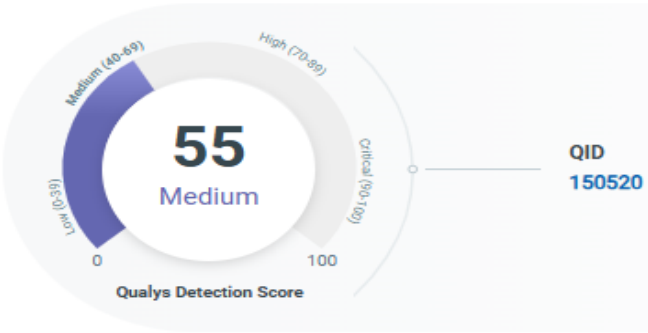
Web Server Information Disclosure

QID: 150520 | Status: **New** | Severity: | Group: INFO

URL: http://altoro.testfire.net/search.jsp

Findings & Recommendations | DETECTION DETAILS | History & Comments | QDS DETAILS

Contributing Factors



QID
150520

Additional Insights

Technical Attributes

CVSS Score
7.5

CISA known exploitable
-

EPSS Score
-

CISA Due Date
-

Temporal Attributes

Exploit Code Maturity (ECM)
-

Associated Malware (0)
-

Real Threat Indicators (RTI) / Exploit Type
No_patch,Easy_exploit

Threat Actor (0)

Remediation

Zero Day

Details

Finding #:	32045216
Unique #:	c54590ce-969c-432c-8c85-de93c9cc4742
Patch #:	-
Group:	Information Disclosure
CWE:	CWE-200
CVE:	-
OWASP Web Appli... :	A5 Security Misconfiguration
CISA Known Explo... :	False
CVSS V3 Base:	7.5
CVSS V3 Temporal:	6.9
CVSS V3 Attack V... :	Network
CVSS V3 Vector S... :	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Authentication:	Not Used
Web Application:	My Web-App Scan
Times Found:	1
First Time Detected:	Aug 8, 2025 05:58 AM GMT+01:00
Last Time Detected:	Aug 8, 2025 05:58 AM GMT+01:00
Last Time Tested:	Aug 8, 2025 05:58 AM GMT+01:00

The Scan shows the “**THREAT**”, “**IMPACT**”, and “**REMENDIATION**” to the vulnerability

Detection Detail

Web Server Information Disclosure

QID: 150520 | Status: **New** | Severity: | Group: INFO

URL: http://altoro.testfire.net/search.jsp

Findings & Recommendations DETECTION DETAILS History & Comments QDS DETAILS

Threat

Description

The target application discloses the Web Server software version via the "Server:" token sent in HTTP response header.

QID Detection Logic:

This QID sends a GET request to the target application and determines the Web Server version disclosed in the "Server:" token.

Impact

Description

Revealing the specific software version of the server may allow the server machine to become more vulnerable to attacks against software that is known to contain security holes.

Solution

Description

Customers are advised to modify the HTTP response header of the target application to not disclose detailed information about the underlying web server. Server implementers are encouraged to make this field a configurable option.

Choosing Between Nessus and Qualys for Web Application Scanning

- **Nessus** is a powerful vulnerability assessment tool known for its broad coverage, detailed reports, and strong detection of misconfigurations and known vulnerabilities. It is flexible, easy to set up, and suitable for organizations wanting full control over scans. However, it may require more manual configuration for web application–specific tests and remediation tracking.

- **Qualys Web Application Scanning (WAS)** is a cloud-based solution with deep web app crawling, automated vulnerability detection, and strong integration with compliance workflows. It excels in large-scale, continuous scanning and integrates well with cloud environments, though it may offer less flexibility for highly customized, internal-only testing without proper configuration.

Best Choice:

- For **comprehensive network and host vulnerability scanning with web app checks included**, **Nessus** is ideal.
- For **dedicated web application scanning with automation, scalability, and compliance tracking**, **Qualys WAS** is the stronger option.

Certificate View with QUALYS

Visit: https://www.qualys.com/certview/ to sign up

qualys.com/certview/

ction to clou... | SOC Types and Role... | QuillBot AI | EndPoint Security -... | Log Management -... | The Hacker News |... | Cyber Security Webi... | BrightTALK Cyberse...

Qualys. Platform Solutions Customers Resources Support More Community Login Contact Us Try Now

Qualys CertView.

Don't ever let your digital certificates expire.

Qualys CertView is totally free, and there's no software to download or install.

Sign Up Now to Get Your TruRisk Report for Free

Work email

Create your account

By submitting this form, you consent to Qualys' privacy policy.

Hey there! What questions can I answer for you?

Qualys CertView.

Don't ever let your digital certificates expire.

Qualys CertView is totally free, and there's no software to download or install.

Sign Up Now to Get Your TruRisk Report for Free

zeporo@fxzig.com

Louis

OKPERIRUISI

ovomeru limited

IT Support

07019710421

1-250

Nigeria

By submitting this form, you consent to Qualys' privacy policy.

Hey there! What questions can I answer for you?

Your Qualys CertView account has been created.

Thank you for signing up. You will receive an automated email with login instructions. We hope you enjoy this free service and will help spread the word!

Webinar

Take Control of Your Digital Certificates Globally: Assess and Monitor Security Implementation

Watch on demand ›

Getting started videos

Get more details on CertView and how to use it.

Watch videos ›

Related products

Qualys Certificate Inventory – Inventory TLS/SSL digital certificates on a global scale.

Qualys Certificate Assessment – Assess your digital certificates and TLS configurations.

Your temporary email address

zeporo@fxzig.com Copy

Autorefresh in 9 Refresh Change

Inbox

"Qualys Inc." <mail-info@qualys.com>

"Qualys Inc." <mail-info@qualys.com>

Qualys CertView: Thank You for Si... 8/16/2025

Qualys CertView - Welcome! Hello Louis, Thank ...

"Qualys Inc." <mail-info@qualys.com>

Qualys CertView: Thank You for Signing Up

Qualys.

Copy OTP For Activation

Your temporary email address

zeporo@fxzig.com Copy

Autorefresh in 10 Refresh Change

Inbox

"Qualys Inc" <qualys@qualys.net>
Qualys Registration -- Start Now 8/16/2025
Welcome Email – Qualys Web Application Secur...

"Qualys Inc." <mail-info@qualys.com>
Qualys CertView: Thank You for Si... 8/16/2025
Qualys CertView - Welcome! Hello Louis, Thank ...

"Qualys Inc" <qualys@qualys.net>

Qualys Registration -- Start Now

Username

vmeru5lk1

OTP Code

382539

This code is only valid for 72 hours. If the OTP Code is expired, please use the "Activate Your Account > Resend" option to generate a new OTP code.

Reference

Your temporary email address

zeporo@fxzig.com Copy

Autorefresh in 13 Refresh Change

Inbox

"Qualys Inc" <qualys@qualys.net>
Qualys Registration -- Start Now 8/16/2025
Welcome Email – Qualys Web Application Secur...

"Qualys Inc." <mail-info@qualys.com>
Qualys CertView: Thank You for Si... 8/16/2025
Qualys CertView - Welcome! Hello Louis, Thank ...

"Qualys Inc" <qualys@qualys.net>

Qualys Registration -- Start Now

Please click the following link and enter your OTP code.

Activate Your Account

After you activate your account, you will be redirected to your trial login page.
You can then use your username and password to log in.

Qualys.

Hello Louis

Verify Your Information

Before proceeding, verify the information below and ensure you have read the Service Agreement Terms and Conditions.
Note: Fields marked with (*) are mandatory.

Personal Information

Prefix: Select

First Name: Louis

Last Name: OKPERIRUISI

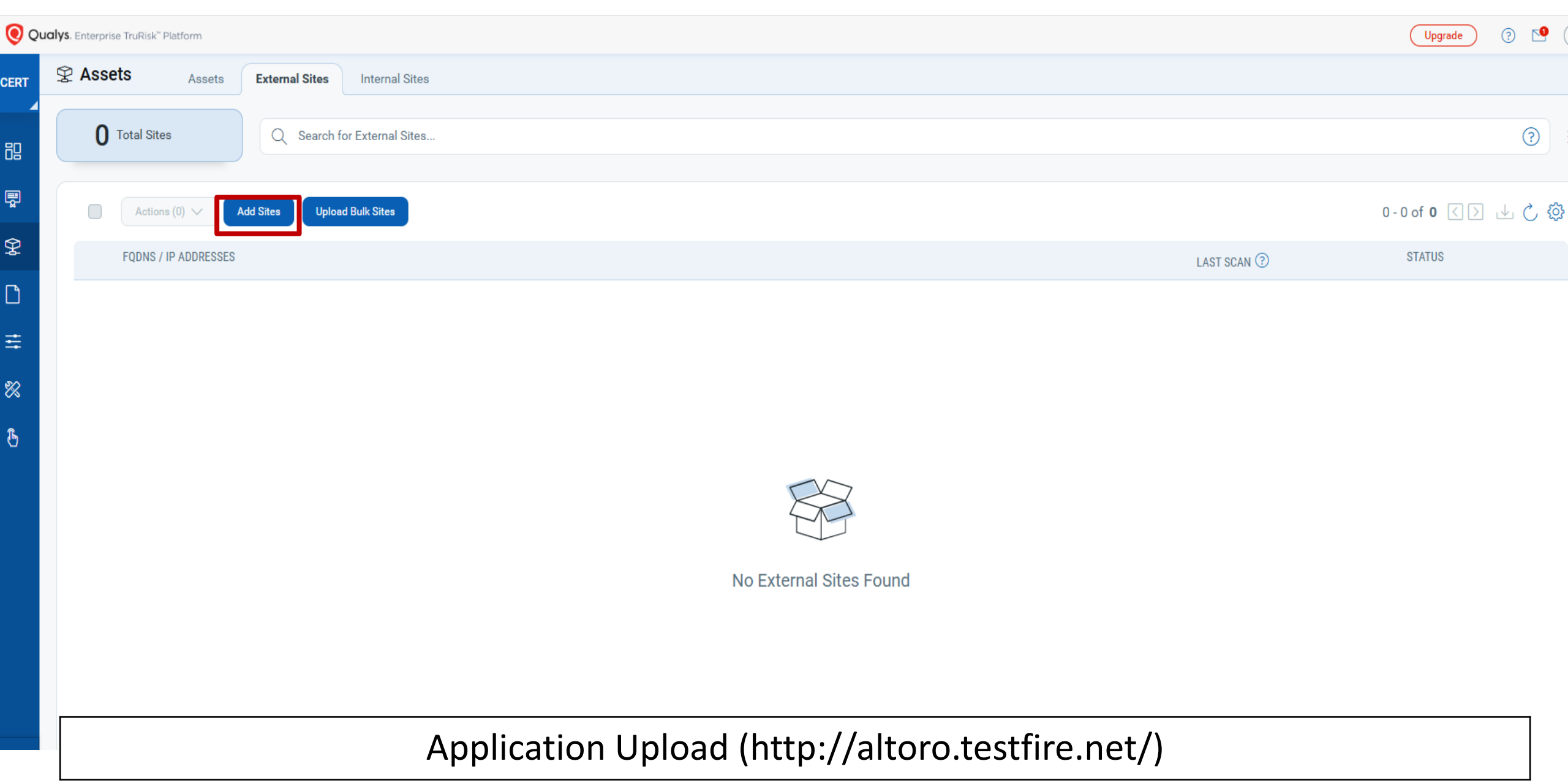
Title: *
IT Support

Contact Information

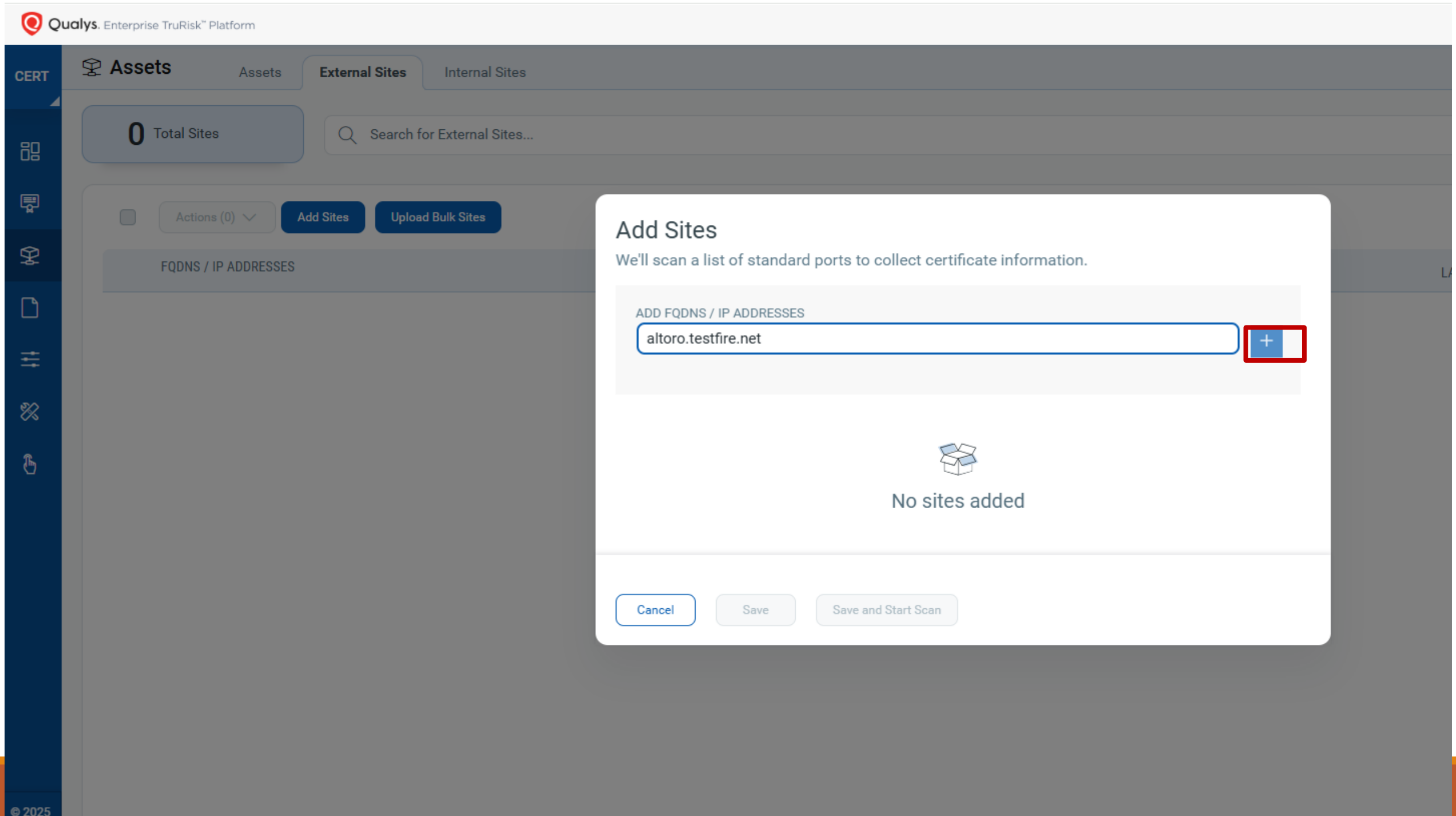
Email:
zeporo@fxzig.com

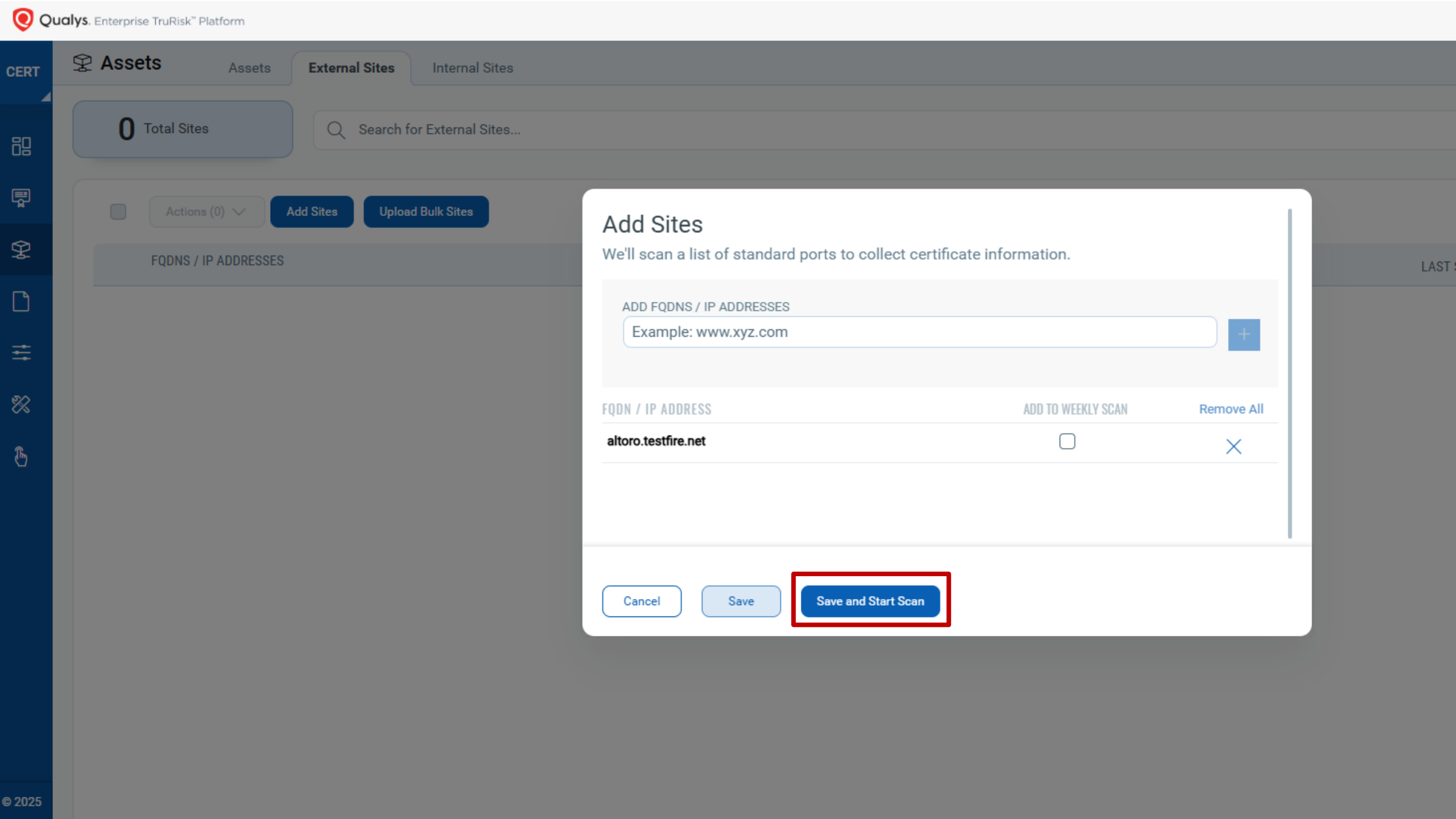
Contact Number:
07019710421

Fax:
Enter Fax Number

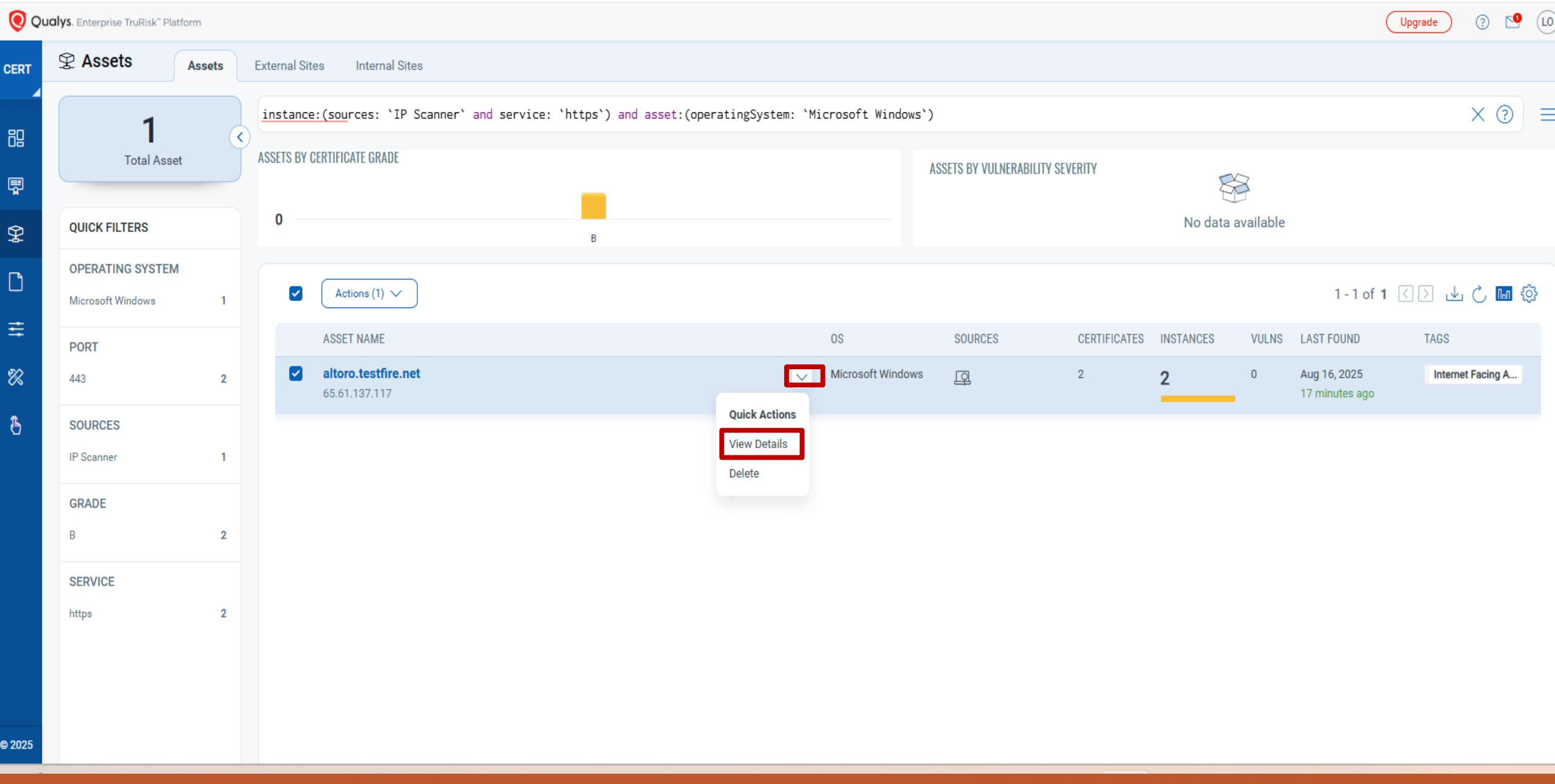


Application Upload (http://altoro.testfire.net/)


Qualys. Enterprise TruRisk™ Platform
CERT
Assets
Assets
External Sites
Internal Sites
0 Total Sites
Search for External Sites...
Actions (0)
Add Sites
Upload Bulk Sites
FQDNS / IP ADDRESSES
Add Sites
We'll scan a list of standard ports to collect certificate information.
ADD FQDNS / IP ADDRESSES
altoro.testfire.net
+
No sites added
Cancel
Save
Save and Start Scan
© 2025


Qualys. Enterprise TruRisk™ Platform
CERT
Assets
Assets
External Sites
Internal Sites
0 Total Sites
Search for External Sites...
Actions (0)
Add Sites
Upload Bulk Sites
FQDNS / IP ADDRESSES
LAST
Add Sites
We'll scan a list of standard ports to collect certificate information.
ADD FQDNS / IP ADDRESSES
Example: www.xyz.com
FQDN / IP ADDRESS
ADD TO WEEKLY SCAN
Remove All
altoro.testfire.net
Cancel
Save
Save and Start Scan
© 2025

Two Certificate Discovered, Click On View Details.



← Asset Details: **altoro.testfire.net**

INVENTORY
- Asset Summary
- System Information
- Network Information
- Open Ports
- Installed Software

SECURITY
- Vulnerabilities
- Certificates

SOURCES
- Summary
- CAPS
- Agent Summary

Asset Summary

altoro.testfire.net

Criticality Score: 2

OS: Microsoft Windows | Hardware: Unknown Manufacturer / Model

Identification

Hostname altoro.testfire.net	FQDN altoro.testfire.net	NetBIOS Name -
IPv4 Addresses 65.61.137.117	IPv6 Addresses -	Asset ID 348897938
Host ID 176261402		

Activity

Last User Login -	Last System Boot -	Created On 23 minutes ago 07:00 AM
Last Updated 9 minutes ago 07:14 AM	Last Activity -	

Last Location

← Asset Details: **altoro.testfire.net**

INVENTORY
- Asset Summary
- System Information
- Network Information
- Open Ports
- Installed Software

SECURITY
- Vulnerabilities
- Certificates

SOURCES
- Summary
- CAPS
- Agent Summary

Certificate Instances

Search for certificates...

CERTIFICATE NAME	SOURCES	PORT	PROTOCOL	SERVICE	GRADE
Sectigo RSA Domain Validation Secure ...		443	TLSv1,TLSv1.2,TLSv1.1	https	B Grade Summary
demo.testfire.net		443	TLSv1,TLSv1.2,TLSv1.1	https	B Grade Summary

← Certificate Details: Sectigo RSA Domain Validation Secure Server CA

- Information
- Hosts
- Certificate Path
- Raw
- Activity Log

Certificate Information

Valid

Sectigo RSA Domain Validation Secure Server CA

Expires in 1963d 17h 34m by Jan 1, 2031 12:59 AM

Issued by USERTrust RSA Certification Authority

Renew

Issued to

Name:	Sectigo RSA Domain Validation Secure Server CA
Organization:	Sectigo Limited
City:	Salford
State:	Greater Manchester
Country:	GB

Issued by

Name:	USERTrust RSA Certification Authority
Organization:	The USERTRUST Network
Country:	US

Fingerprints

Fingerprint:	7FA4FF68EC04A99D7528D5085F94907F4D1DD1C5381BACDC832ED5C960214676
Parent Fingerprint:	E793C9B02FD8AA13E21C31228ACCB08119643B749C898964B1746D46C3D4CBD2

Revocation Information

OCSP:	http://ocsp.usertrust.com
CRL:	http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl
Status:	Not Revoked

Certificate Details:

Serial Number:	7d5b5126b476ba11db7...
Certificate Type:	Intermediate
Key:	RSA 2048 bits
Signature Algorithm:	SHA384withRSA
First Found:	Aug 16, 2025
Last Found:	Aug 16, 2025

Key Usage:

Key Usage:	Digital signature Key certificate signing CRL signing

Validity:

Valid From:	Nov 02, 2018
Valid To:	Jan 01, 2031

← Certificate Details: **Sectigo RSA Domain Validation Secure Server CA**

Information
Hosts
Certificate Path
Raw
Activity Log

Host Instances

Host Instances Breakdown

Hosts	Instances
1	1

Search for Hosts...

1 - 1 of 1

ASSET NAME	SOURCES	PORT	PROTOCOL	SERVICE	LAST FOUND	GRADE
altoro.testfire.net 65.61.137.117		443	TLSv1,TLSv1.2,TLSv1.1	https	Aug 16, 2025	B Grade Summary

← Certificate Details: **Sectigo RSA Domain Validation Secure Server CA**

Information

Hosts

Certificate Path

Raw

Activity Log

Certificate Path

Valid

USERTrust RSA Certification Authority

Valid from Feb 01, 2010 to **Jan 19, 2038**

Issued by USERTrust RSA Certification Authority

Valid

Sectigo RSA Domain Validation Secure Server CA

Valid from Nov 02, 2018 to **Jan 01, 2031**

Issued by USERTrust RSA Certification Authority

First found: Aug 16, 2025

Last found: Aug 16, 2025

Demo.testfire.net Certificate's details

Qualys. Enterprise TruRisk™ Platform

← Certificate Details: **demo.testfire.net**

- **Information**
- Hosts
- Certificate Path
- Raw
- Activity Log

Certificate Information

demo.testfire.net

Expires in **309d 17h 26m** by **Jun 22, 2026 12:59 AM**

Issued by **Sectigo RSA Domain Validation Secure ...**

Valid

Renew

Issued to

Name:	demo.testfire.net
Organization:	-

Issued by

Name:	Sectigo RSA Domain Validation Secure Server CA
Organization:	Sectigo Limited
Country:	GB

Fingerprints

Fingerprint:	B0EAC225501DB594A9639F9E718BC0367 59B9F492C7C729A60C8473568393382
Parent Fingerprint:	7FA4FF68EC04A99D7528D5085F94907F4 D1DD1C5381BACDC832ED5C960214676

Revocation Information

OCSP:	http://ocsp.sectigo.com
CRL:	-
Status:	Scan Pending

Certificate Details:

Serial Number:	0850b6e8f99775
Certificate Type:	Leaf
Key:	RSA 2048 bits
Signature Algorithm:	SHA256withRSA
First Found:	Aug 16, 2025
Last Found:	Aug 16, 2025

Subject Alternative Names:

DNS Name:	demo.testfire.net

Key Usage:

Key Usage:	Digital signature Key encipherment

Validity:

Valid From:	May 21, 2025
Valid To:	Jun 22, 2026

Same Host Instance

Qualys. Enterprise TruRisk™ Platform

← Certificate Details: **demo.testfire.net**

- Information
- **Hosts**
- Certificate Path
- Raw
- Activity Log

Host Instances

Host Instances Breakdown

Hosts	Instances
1	1

Search for Hosts...

1 - 1 of 1

ASSET NAME	SOURCES	PORT	PROTOCOL	SERVICE	LAST FOUND	GRADE
altoro.testfire.net 65.61.137.117		443	TLSv1,TLSv1.2,TLSv1.1	https	Aug 16, 2025	B Grade Summary

← Certificate Details: demo.testfire.net

Information
Hosts
Certificate Path
Raw
Activity Log

Certificate Path

USERTrust RSA Certification Authority
Valid
Valid from Feb 01, 2010 to **Jan 19, 2038**
Issued by USERTrust RSA Certification Authority

Sectigo RSA Domain Validation Secure Server CA
Valid
Valid from Nov 02, 2018 to **Jan 01, 2031**
Issued by USERTrust RSA Certification Authority

demo.testfire.net
Valid
Valid from May 21, 2025 to **Jun 22, 2026**
Issued by Sectigo RSA Domain Validation Secure Server CA
First found: Aug 16, 2025
Last found: Aug 16, 2025

← Asset Details: **altoro.testfire.net**

INVENTORY
- Asset Summary
- System Information
- Network Information
- Open Ports
- Installed Software

SECURITY
- Vulnerabilities
- Certificates

SOURCES
- Summary
- CAPS
- Agent Summary

Certificate Instances

Search for certificates...

CERTIFICATE NAME	SOURCES	PORT	PROTOCOL	SERVICE	GRADE
Sectigo RSA Domain Validation Secure ...		443	TLSv1,TLSv1.2,TLSv1.1	https	B Grade Summary
demo.testfire.net		443	TLSv1,TLSv1.2,TLSv1.1	https	B Grade Summary

Grade Summary for Host Instance

Sectigo RSA Domain Validation Secure Server CA

Windows Vista / Windows 2008 / Windows 7 / Windows 2012

Sectigo Limited

Assessed on
Sat, 16 Aug 2025 07:03:00

Protocol
TLSv1,TLSv1.2,TLSv1.1

Port
443

FQDN
-

Service
https

Network
-

Certificate Details

B

This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B.

TLS 1.0 Supported. Grade capped to B.

TLS 1.1 Supported. Grade capped to B.

Continuation…

TLS 1.3 is not supported.

This server does not support HSTS or sent an invalid HSTS policy.

SSLv3 is not Supported.

RC4 is not supported.

Valid

Sectigo RSA Domain Validation Secure Server CA

Valid from: Nov 02, 2018 to **Jan 01, 2031**

Issued by: USERTrust RSA Certification Authority

First found: Aug 16, 2025

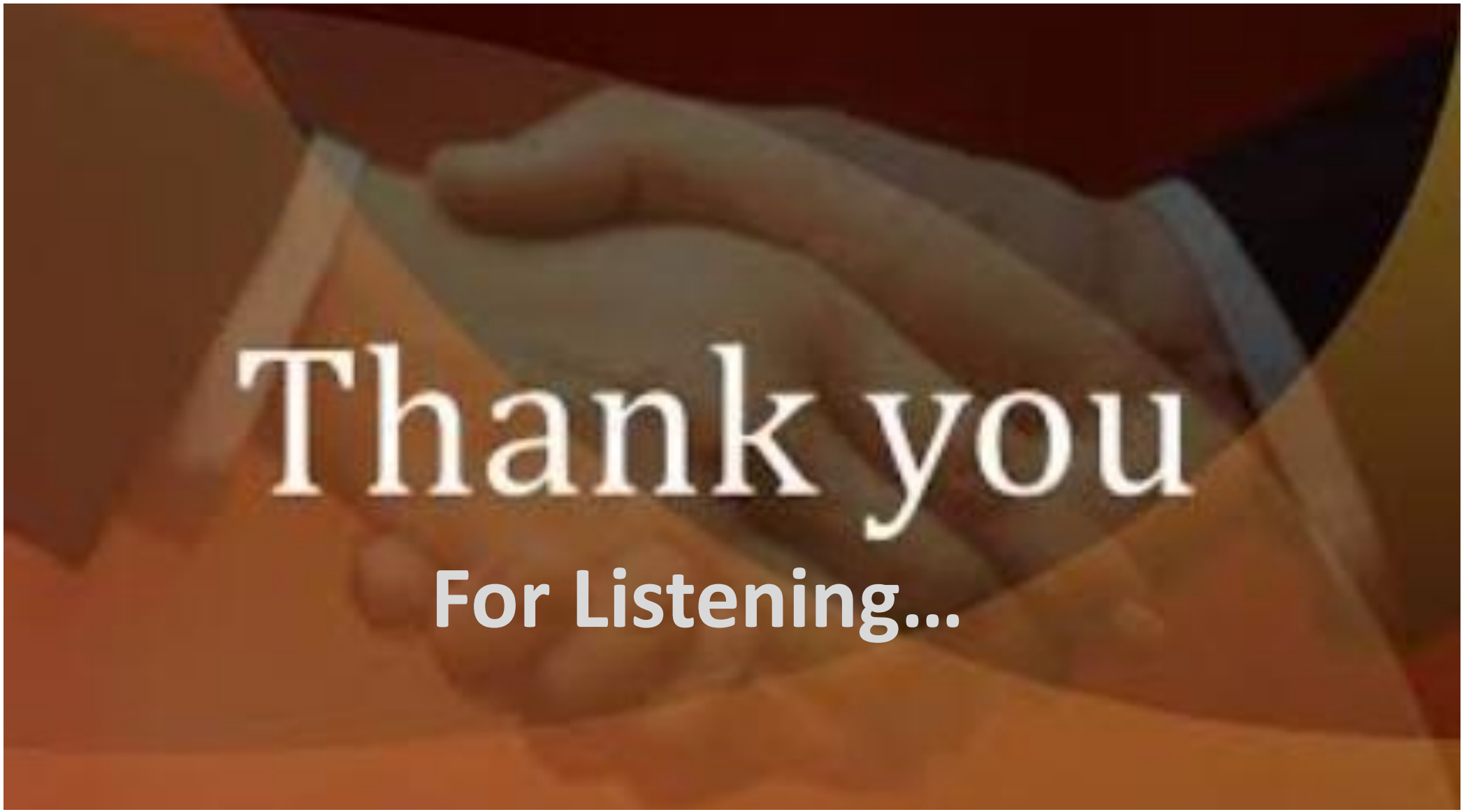
Last found: Aug 16, 2025

Configuration Details

Protocol Support

Score: **24**

SSLv2 :	No
SSLv3 :	No
TLSv1 :	Yes
TLSv1.1 :	Yes
TLSv1.3 :	No
TLSv1.2 :	Yes


Thank you
For Listening…