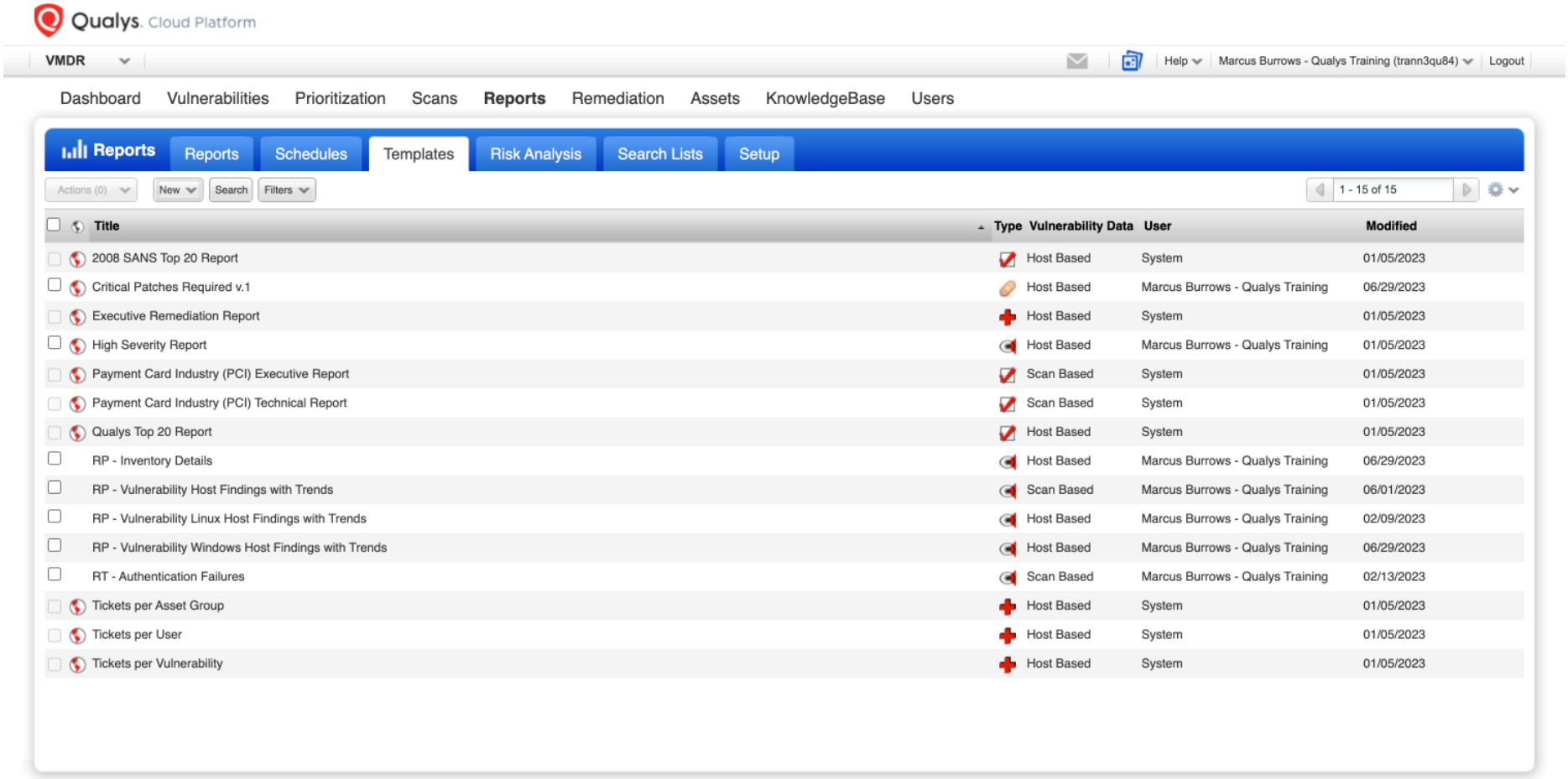
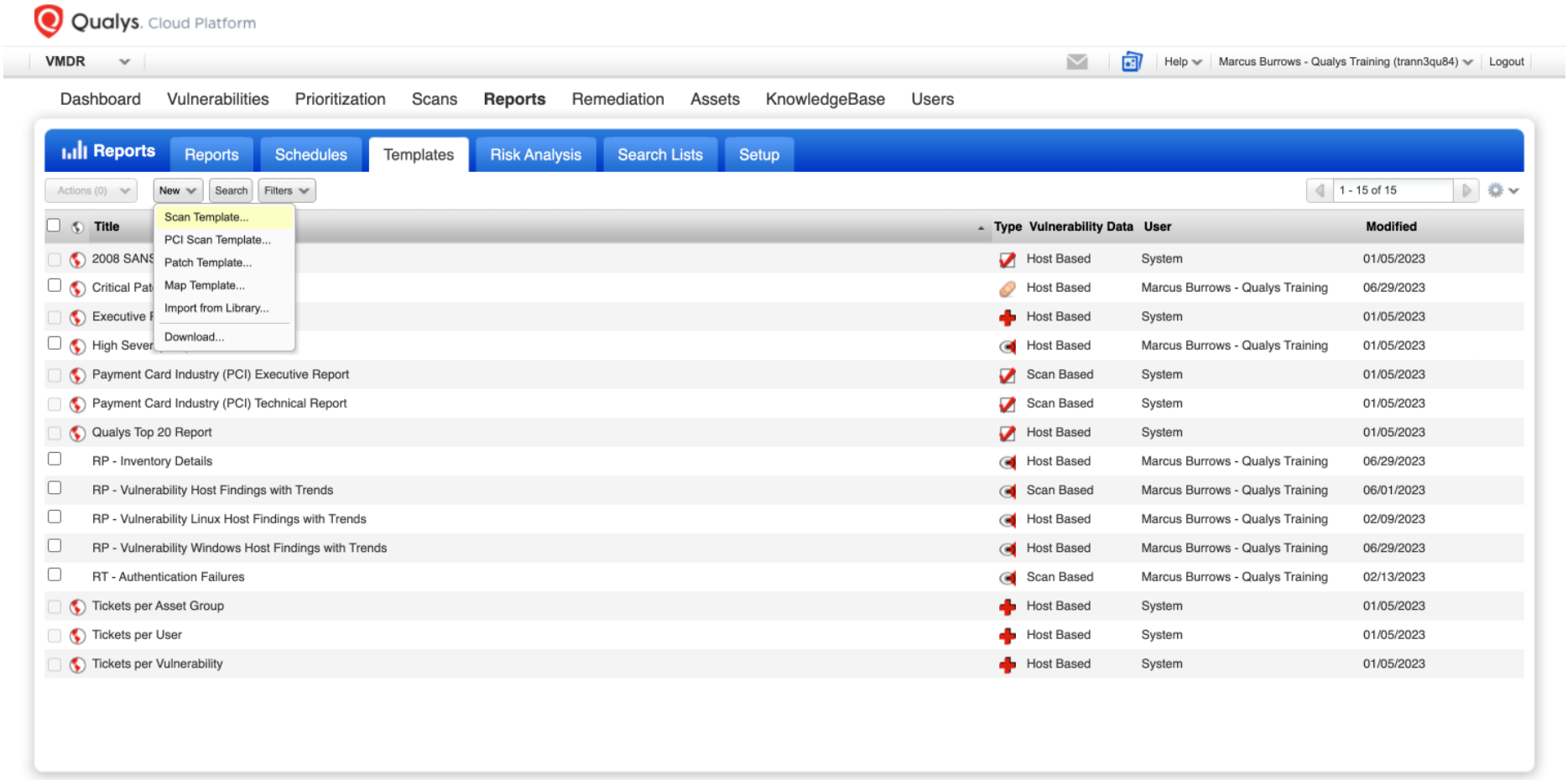
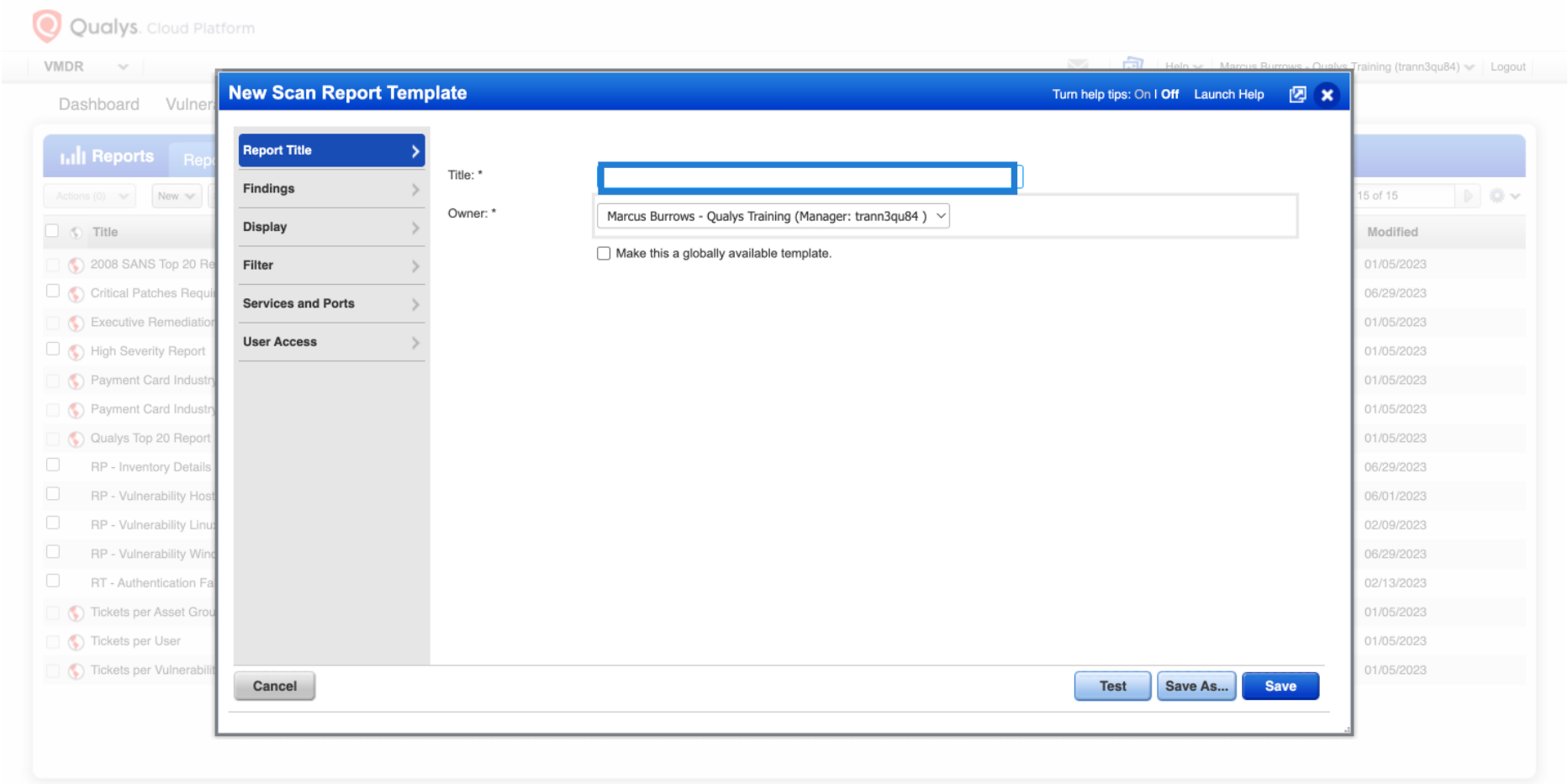
In this lab you will create a report template which focusses on Microsoft Patch Tuesday vulnerabilities which have been discovered on Windows Server assets. Click on the New button to begin.



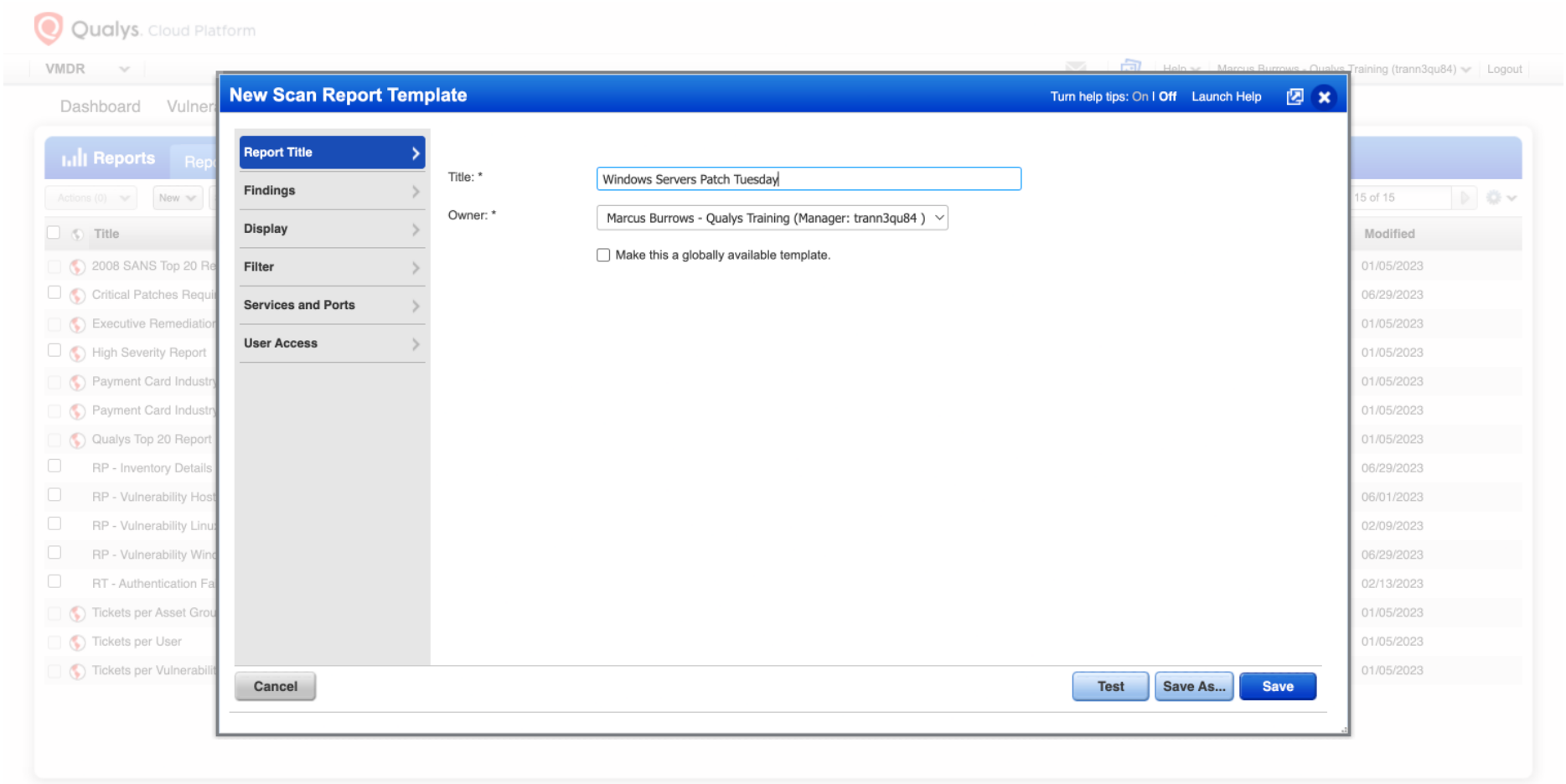
Click Scan Template...



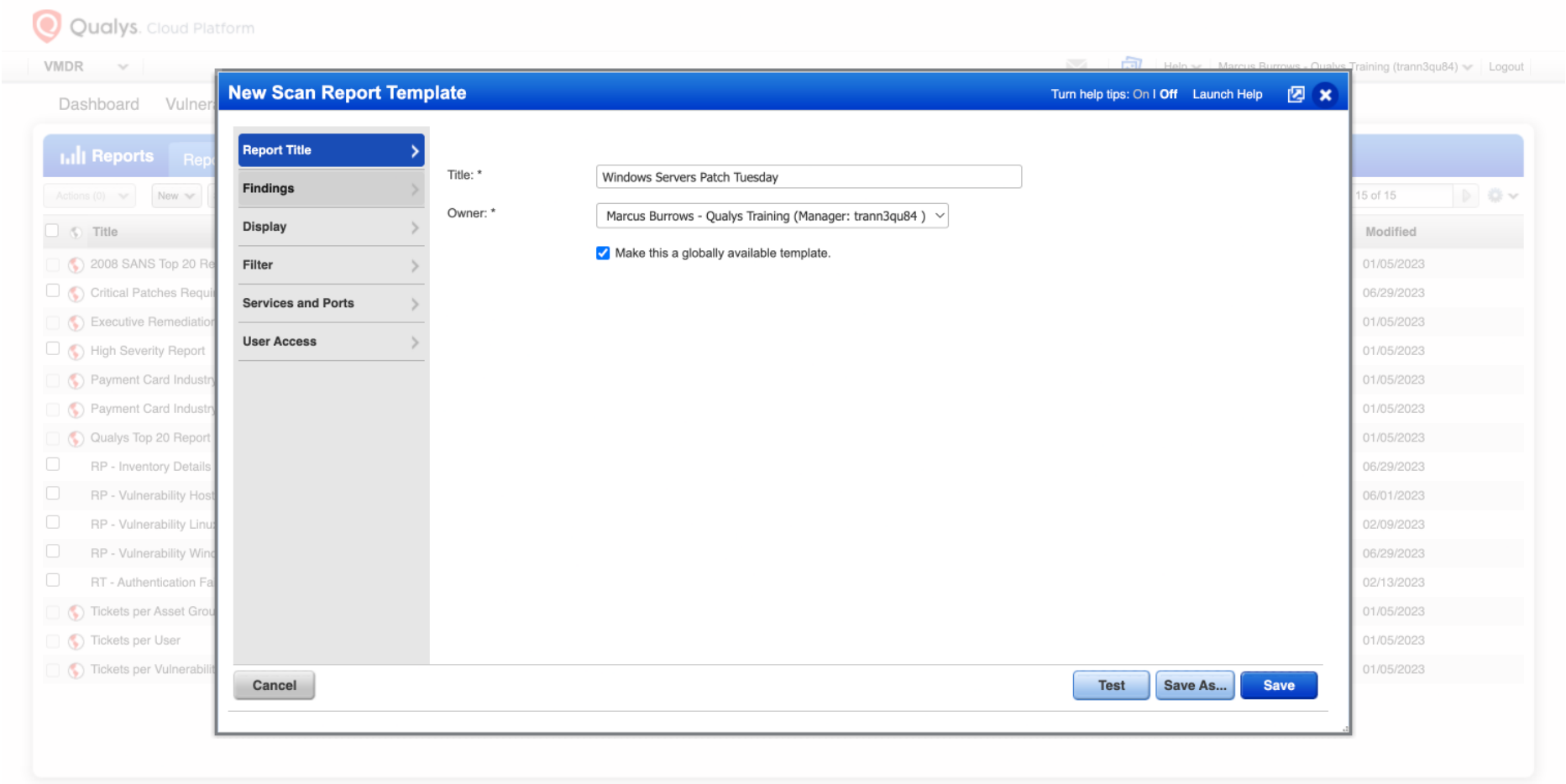
As the name for the Report Template, type Windows Servers Patch Tuesday and press Enter



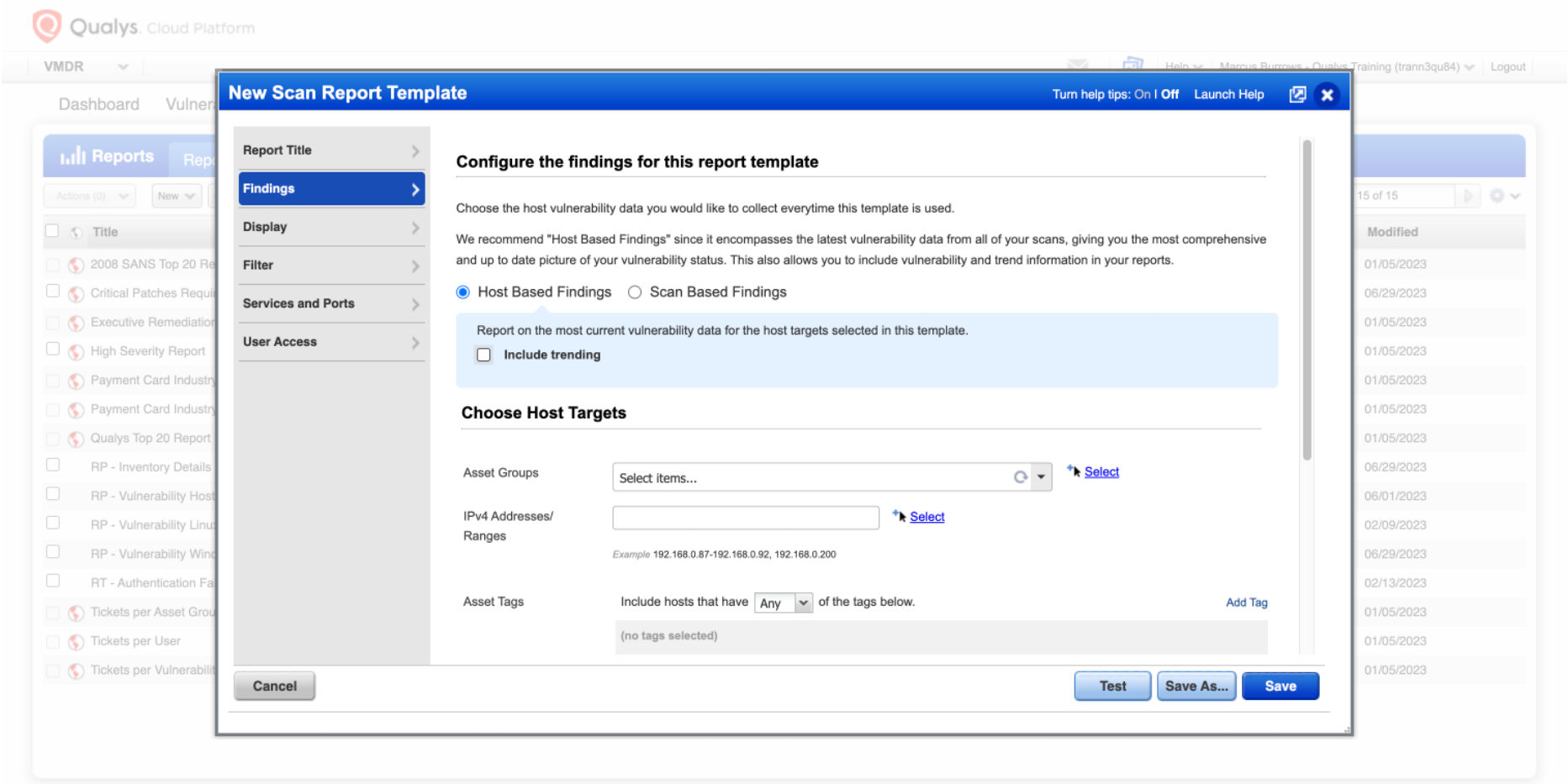
Click on the check box next to "Make this a globally available template". This will allow other users to use this Report Template.



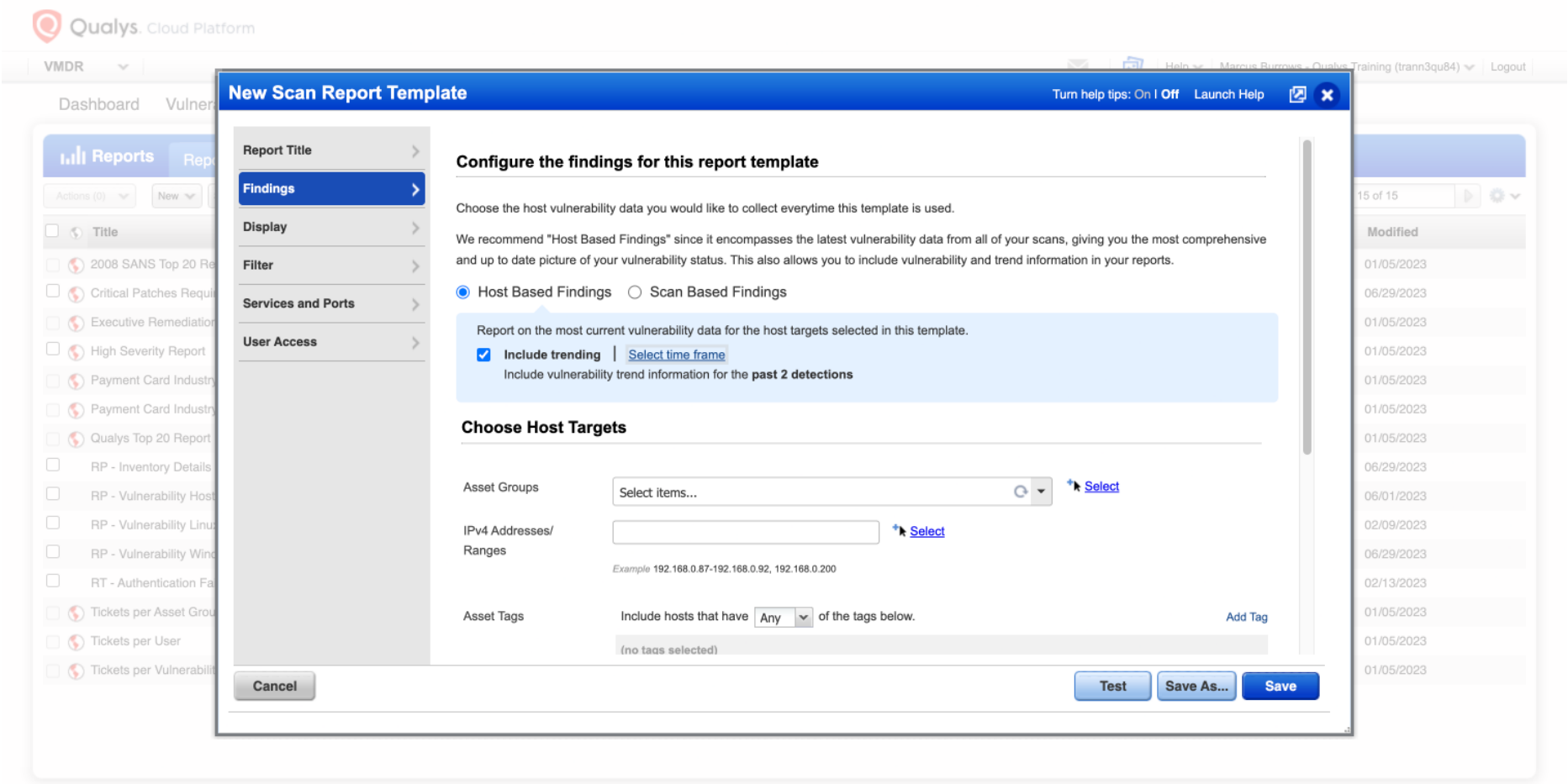
Click on the Findings Tab



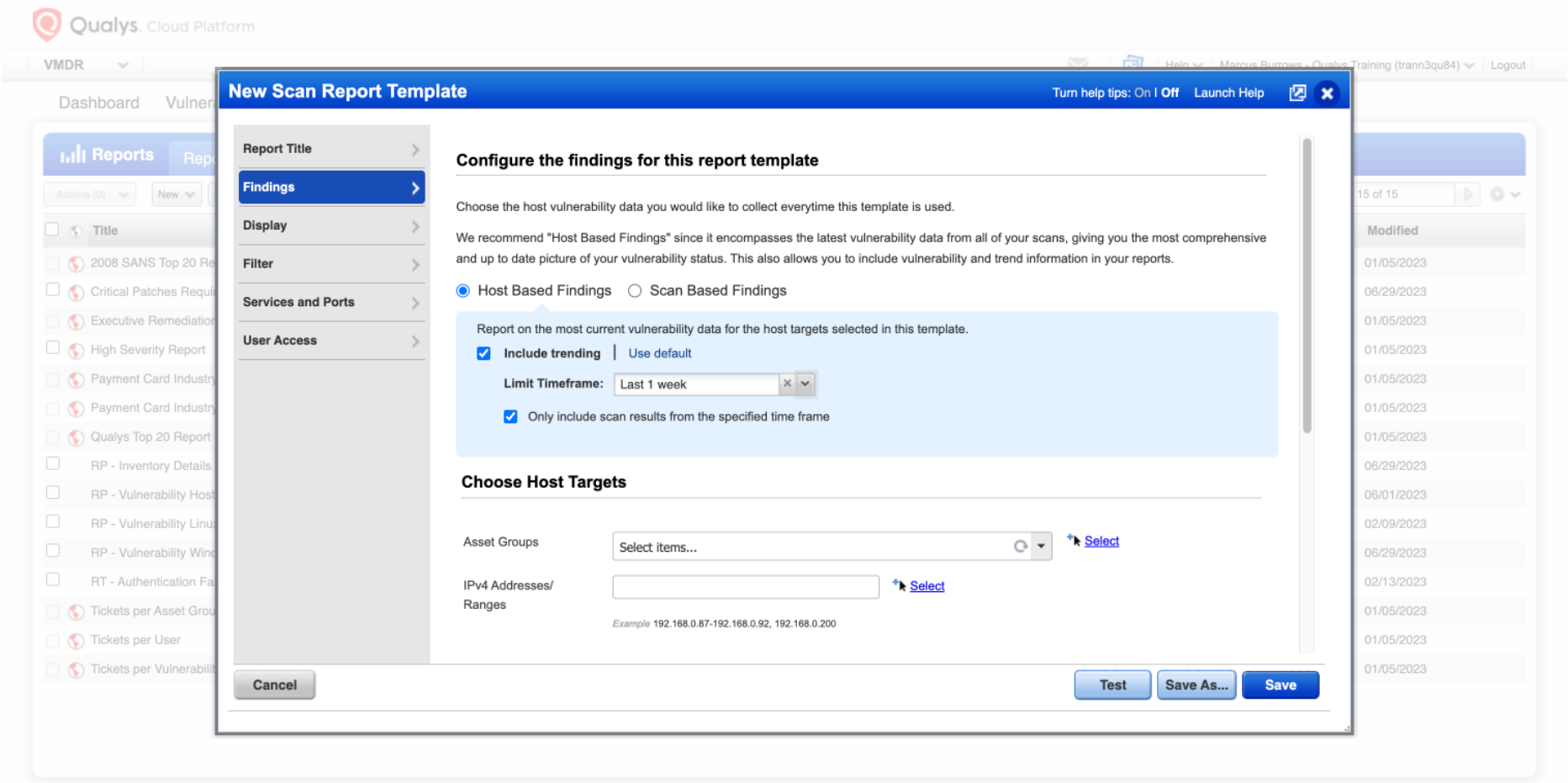
Host Based Findings is selected by default. Click on the check box next to "Include Trending".



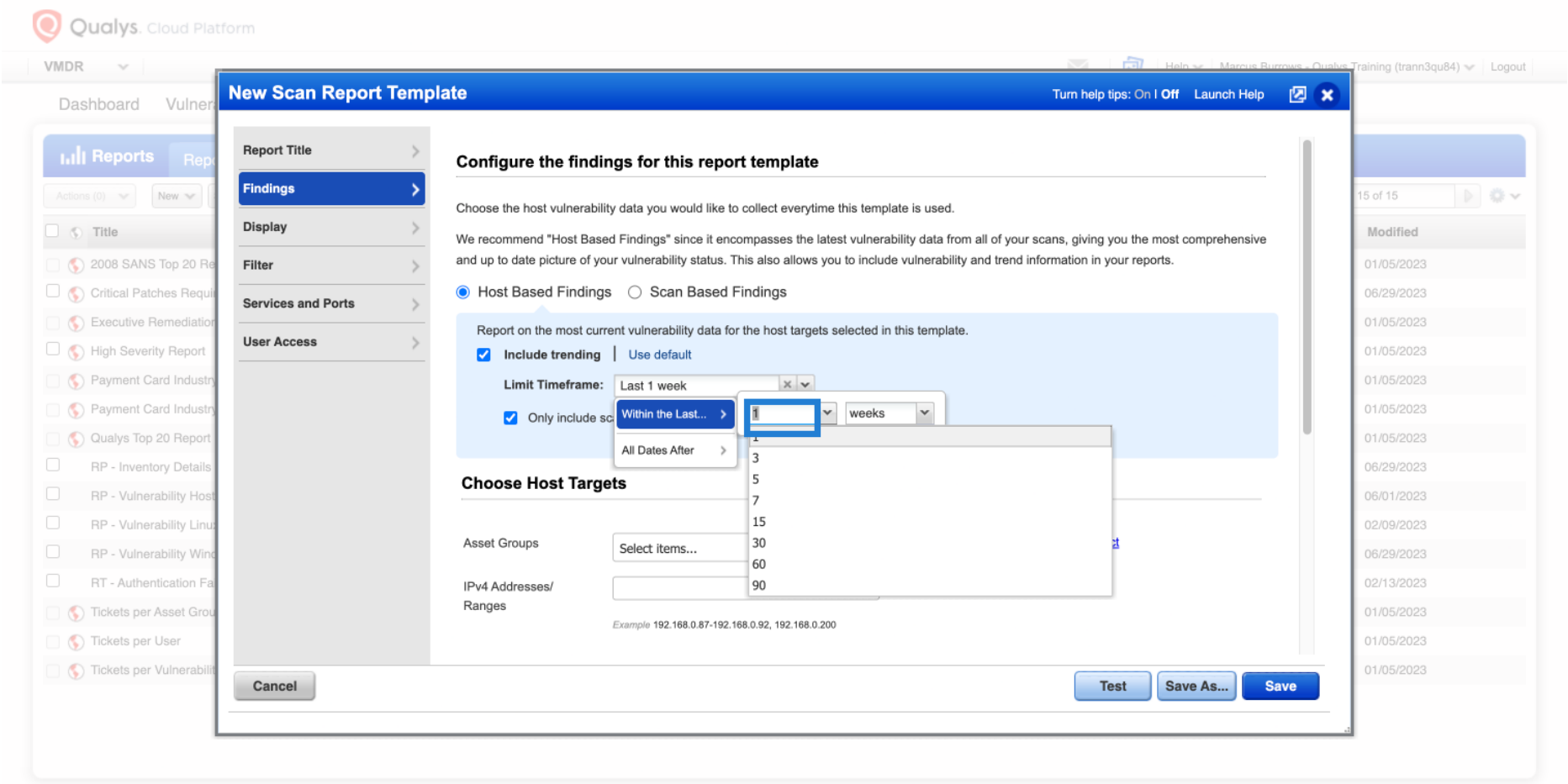
Click Select time frame



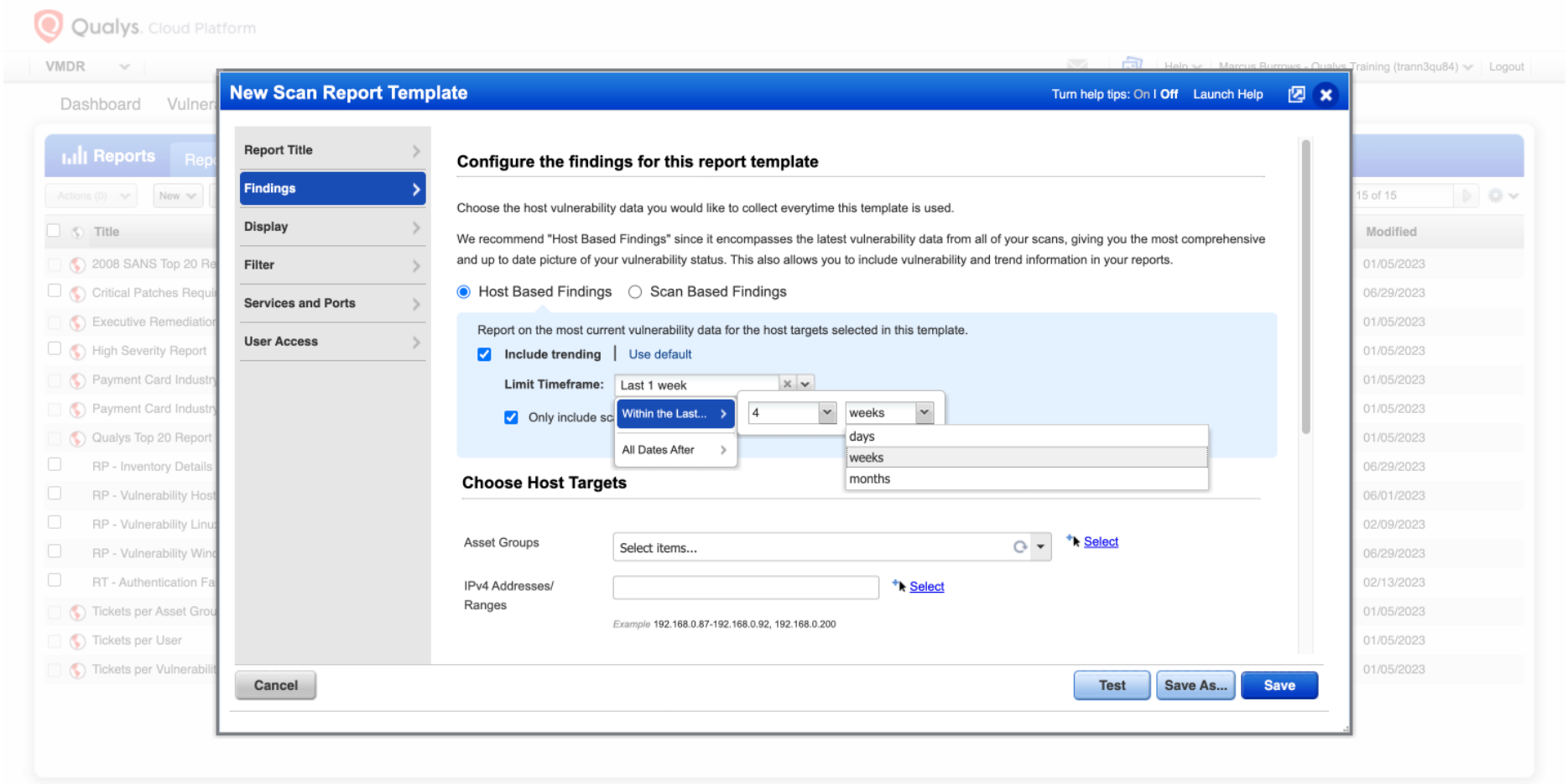
Click on the drop down to limit the timeframe.



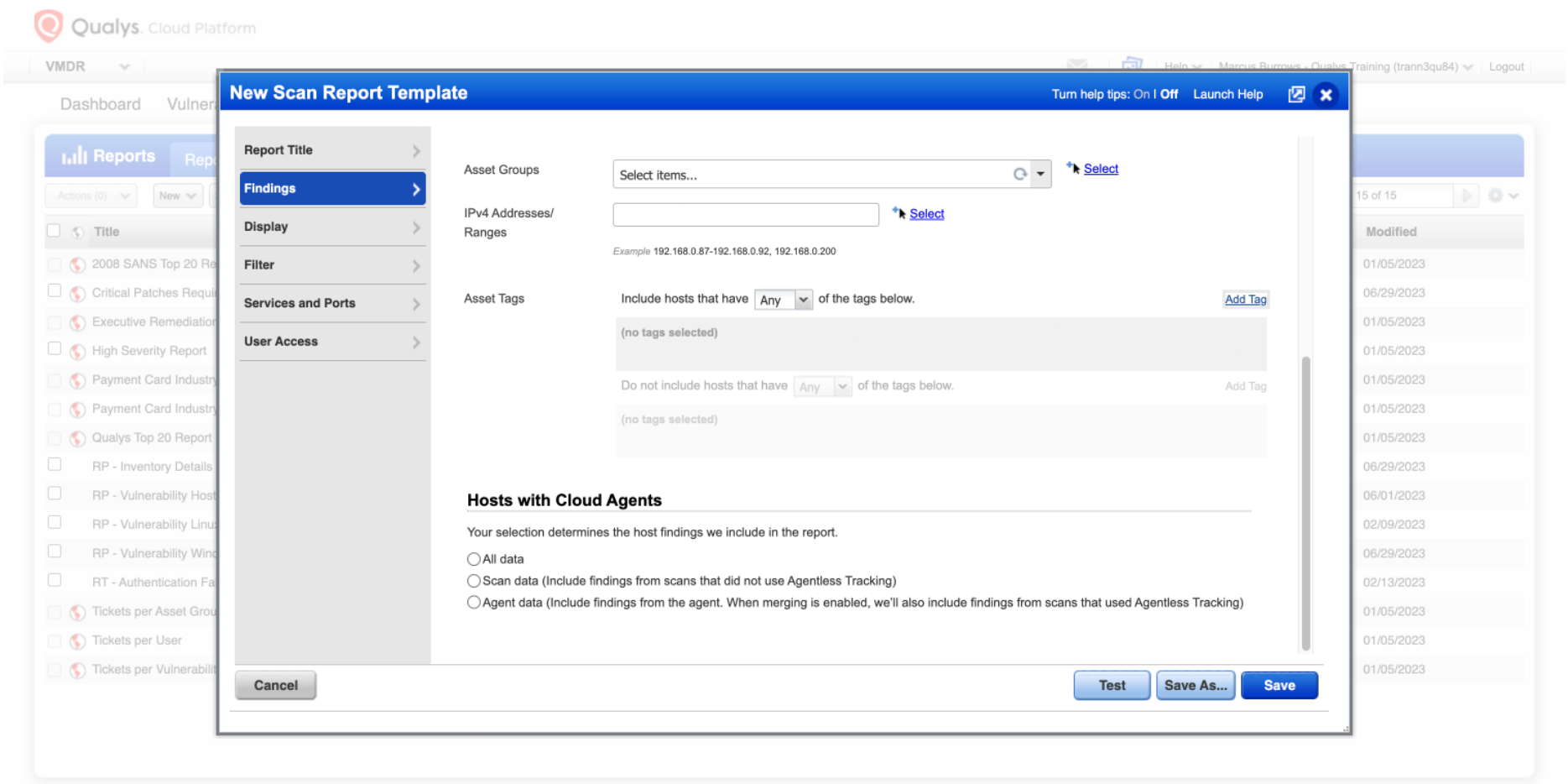
In the number field, type 4 and press Enter.



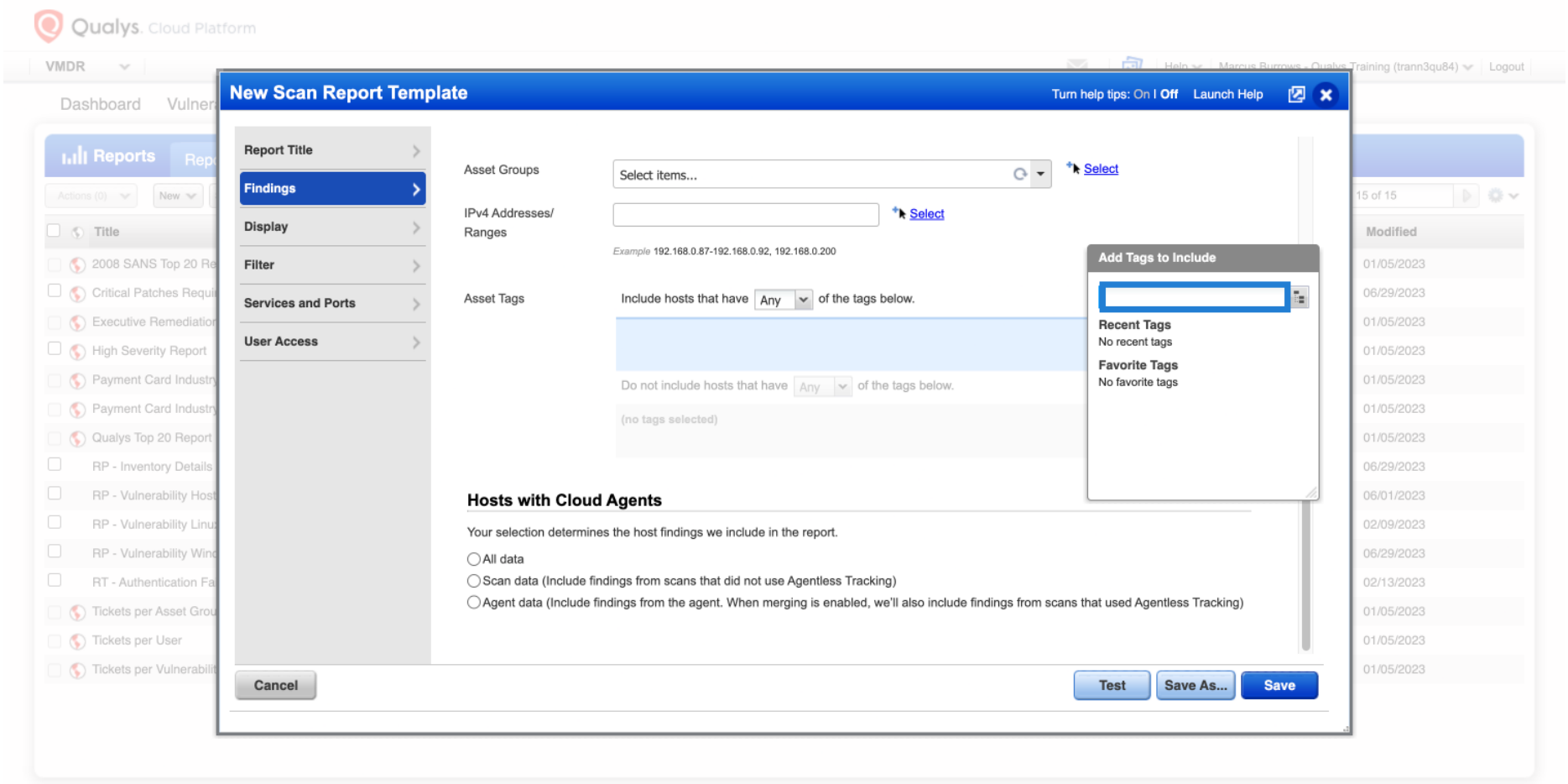
Click the scroll bar on the right of the dialog to scroll down.



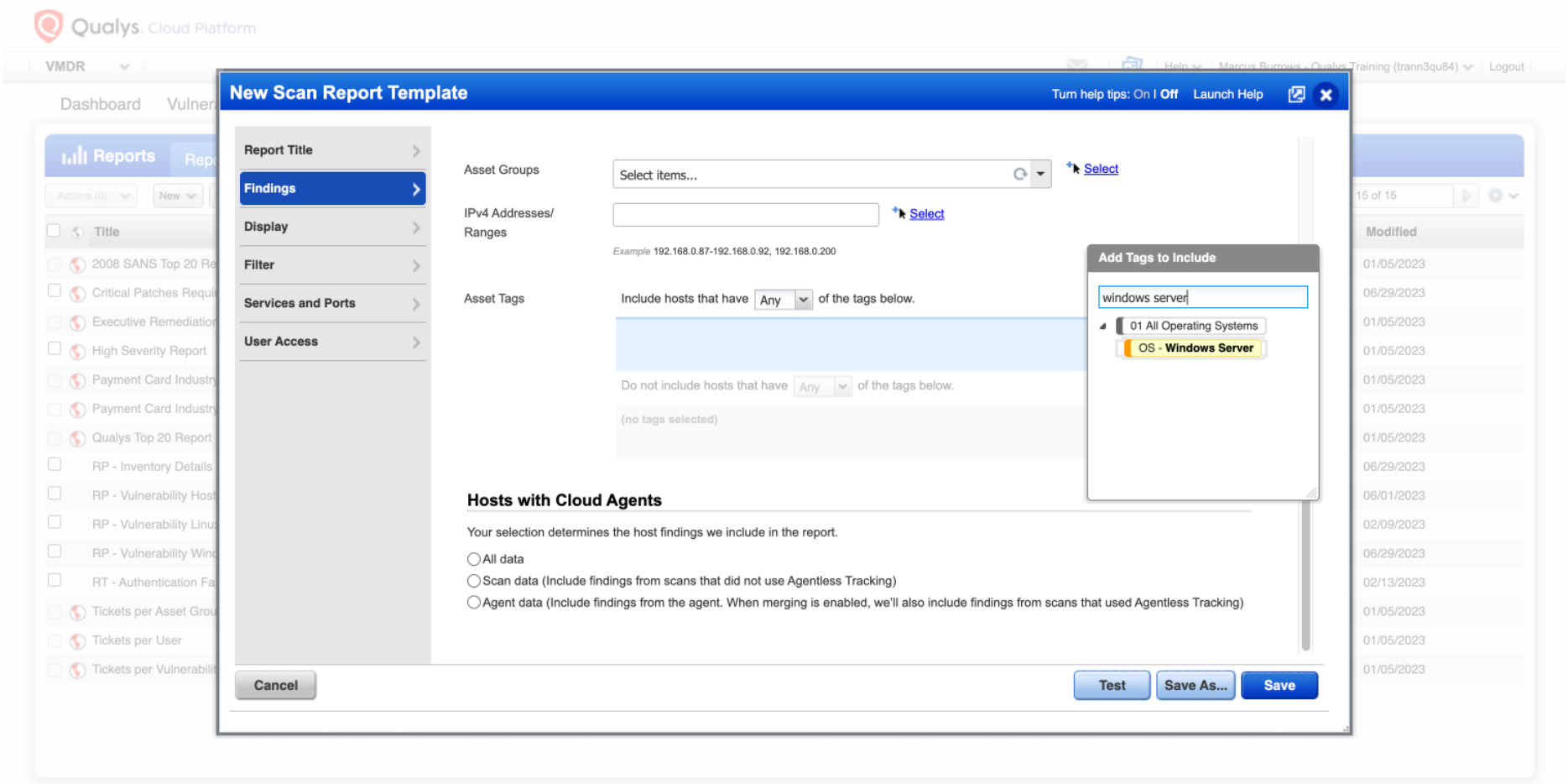
You will now select which Assets to report on. Click on the Add Tag link.



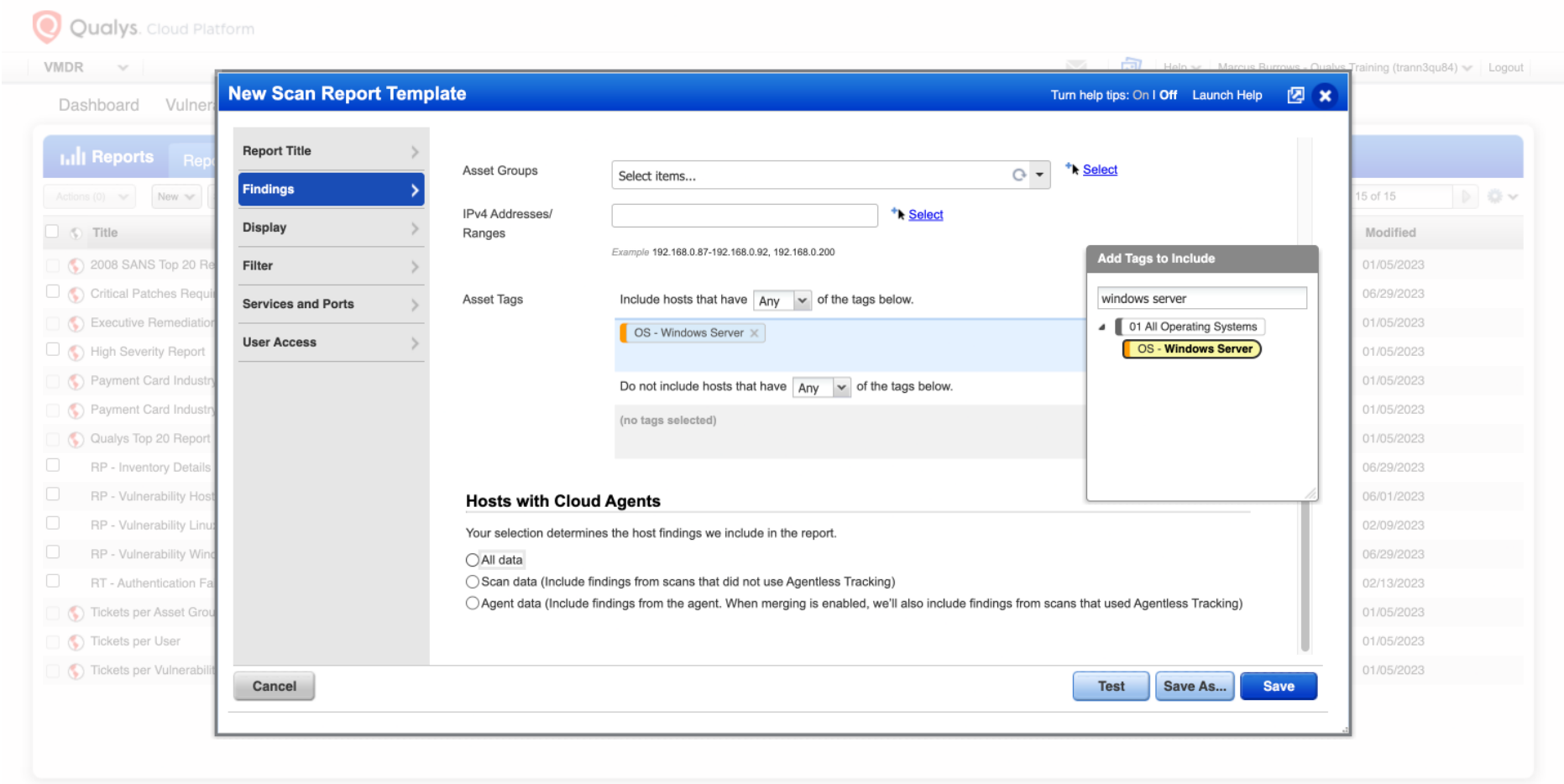
In the search field, type windows server and press Enter



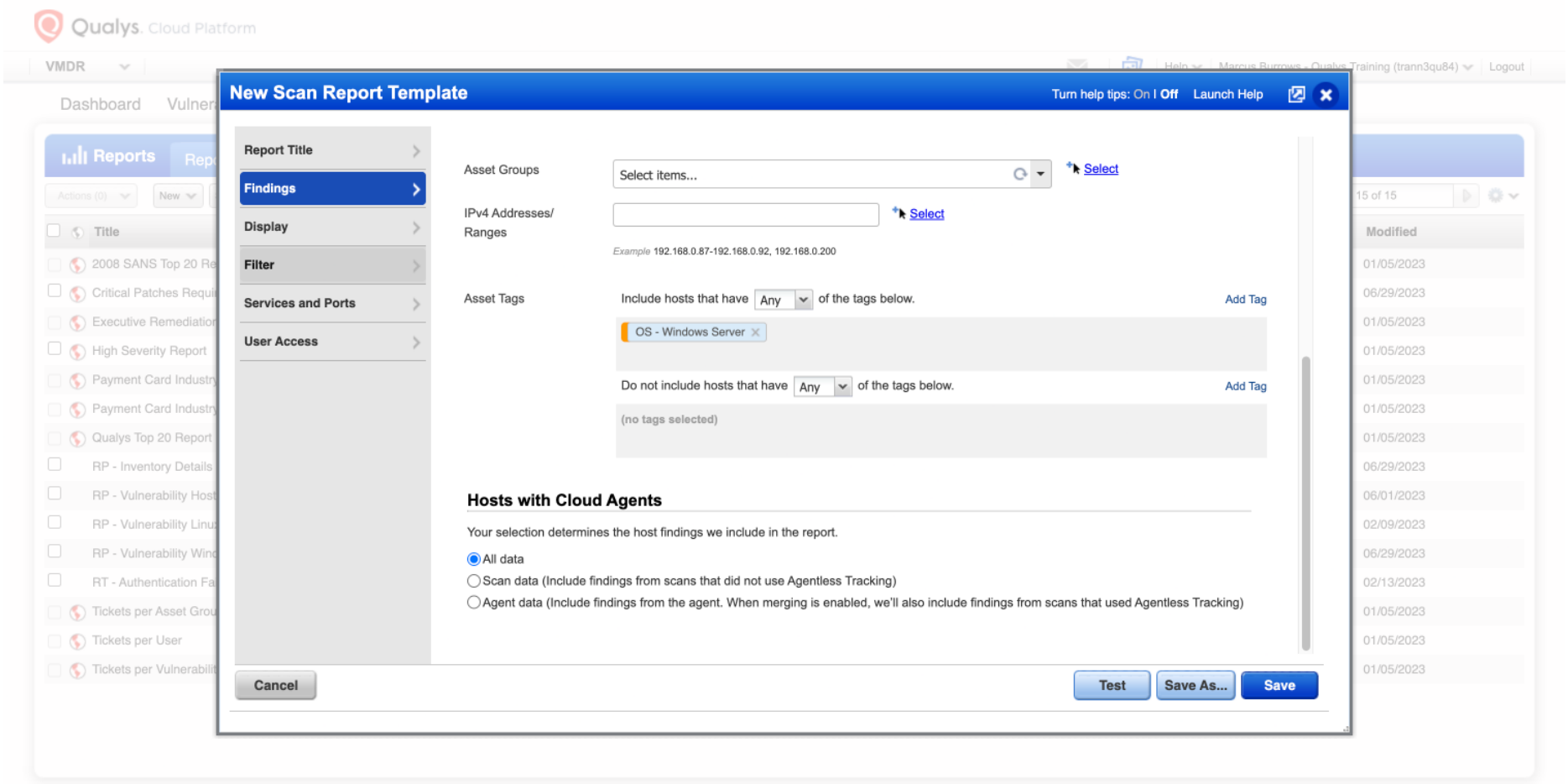
Click on the OS - Windows Server Asset Tag



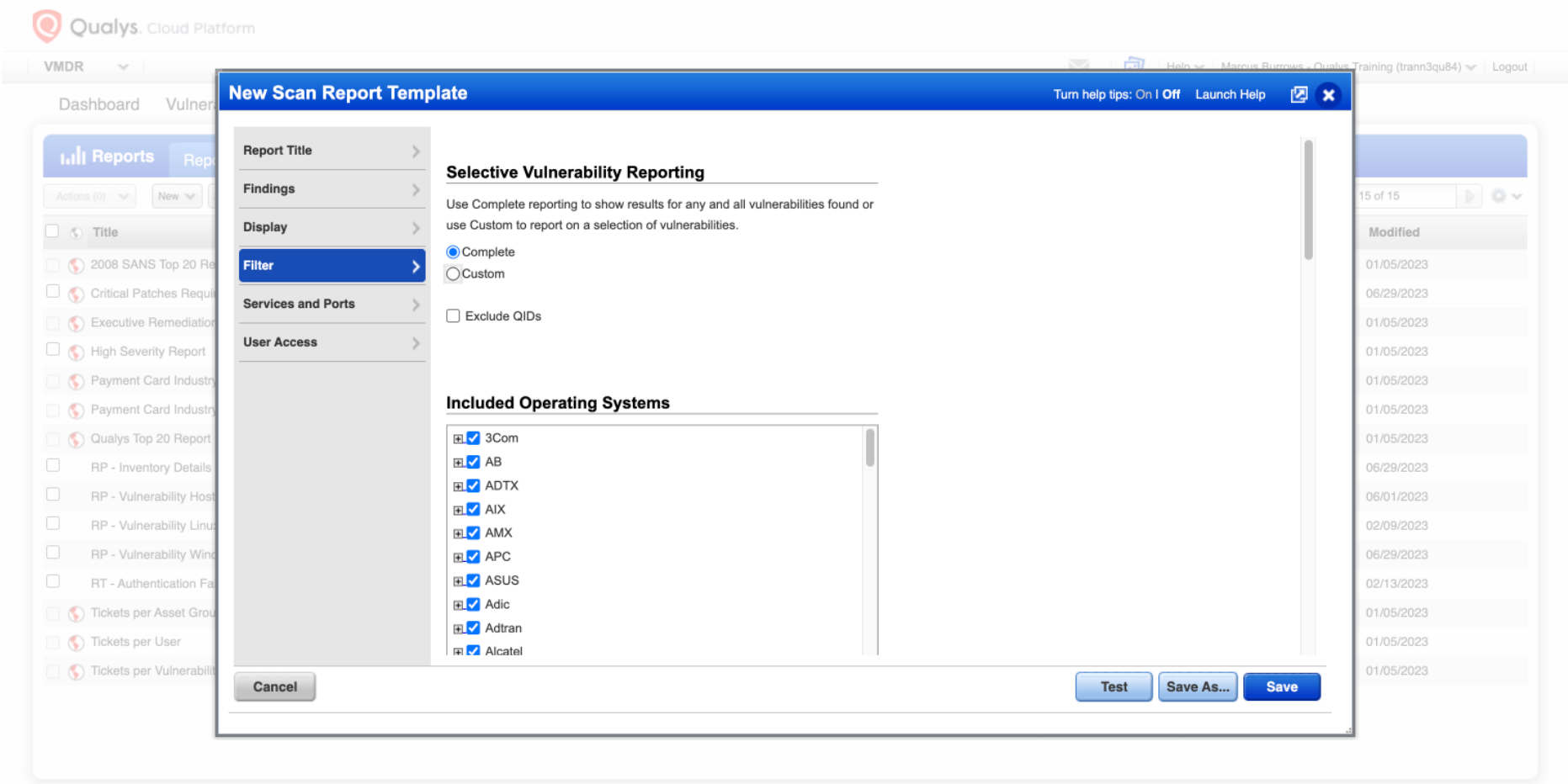
You can include both scan data and Cloud Agent data in this report. Towards the bottom of the dialog, click the radio button next to All data



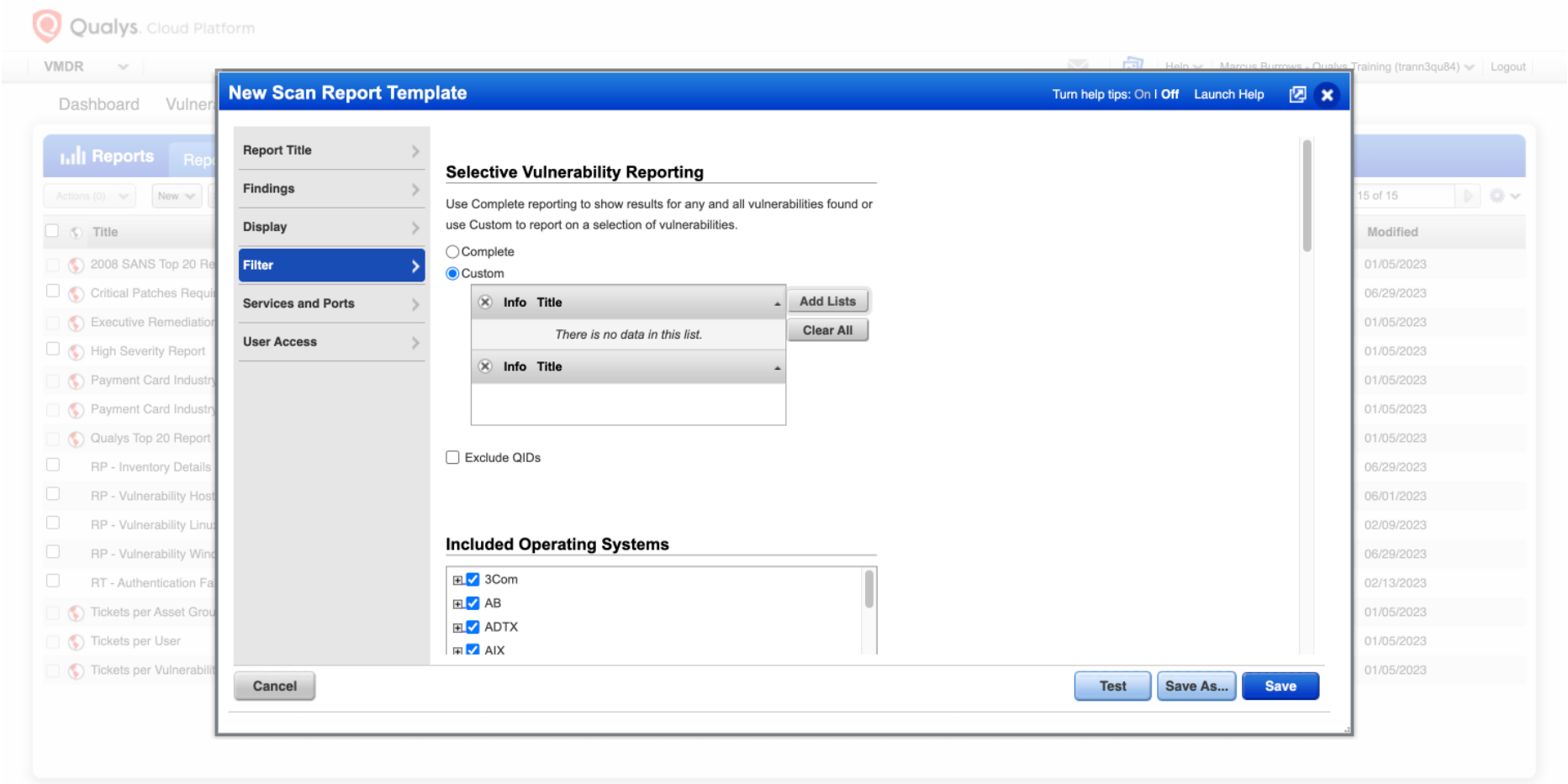
Click on the Filter tab



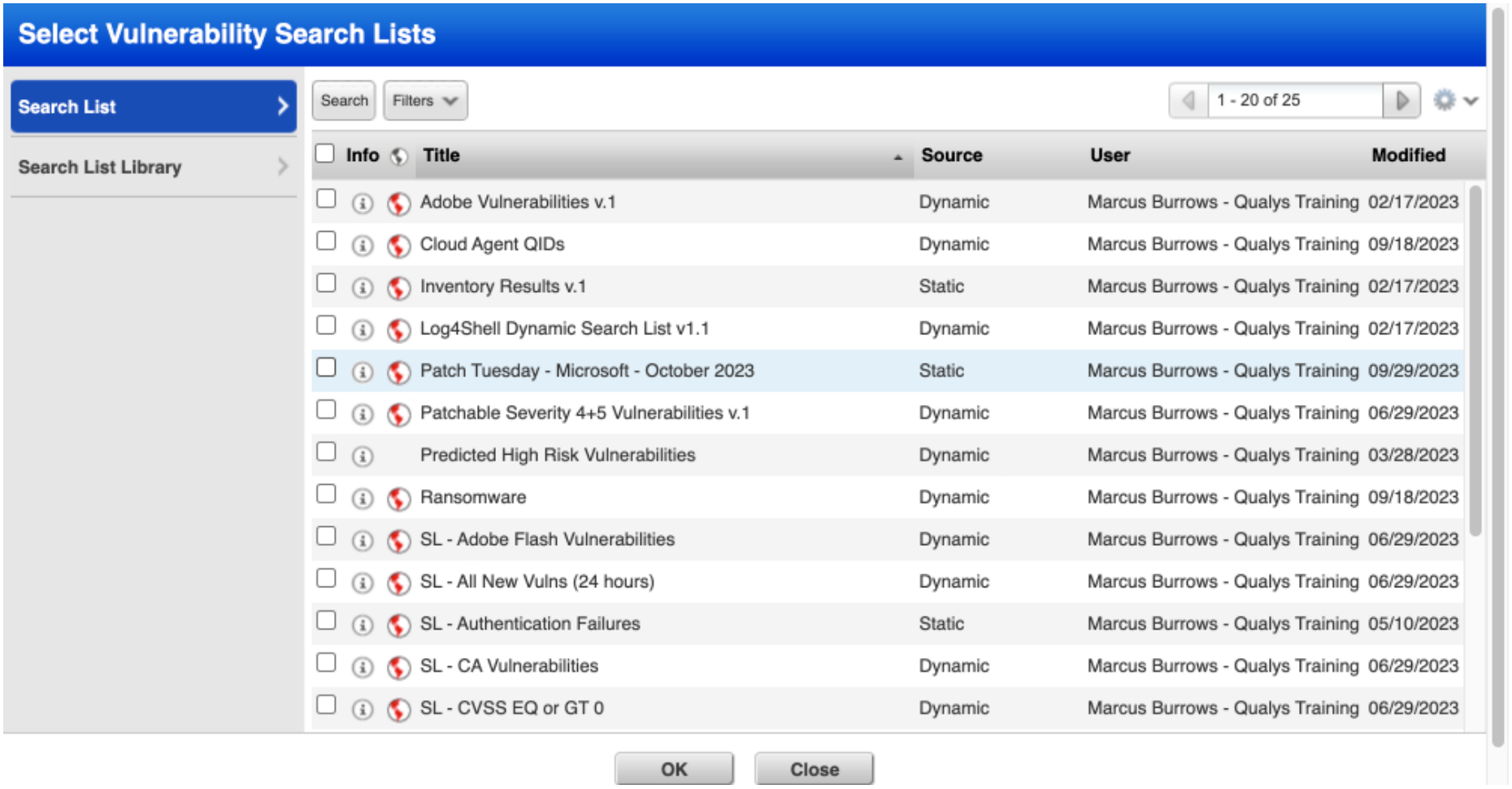
By default, a Report Template will include all vulnerabilities for the target assets. Click on the radio button next to "Custom".



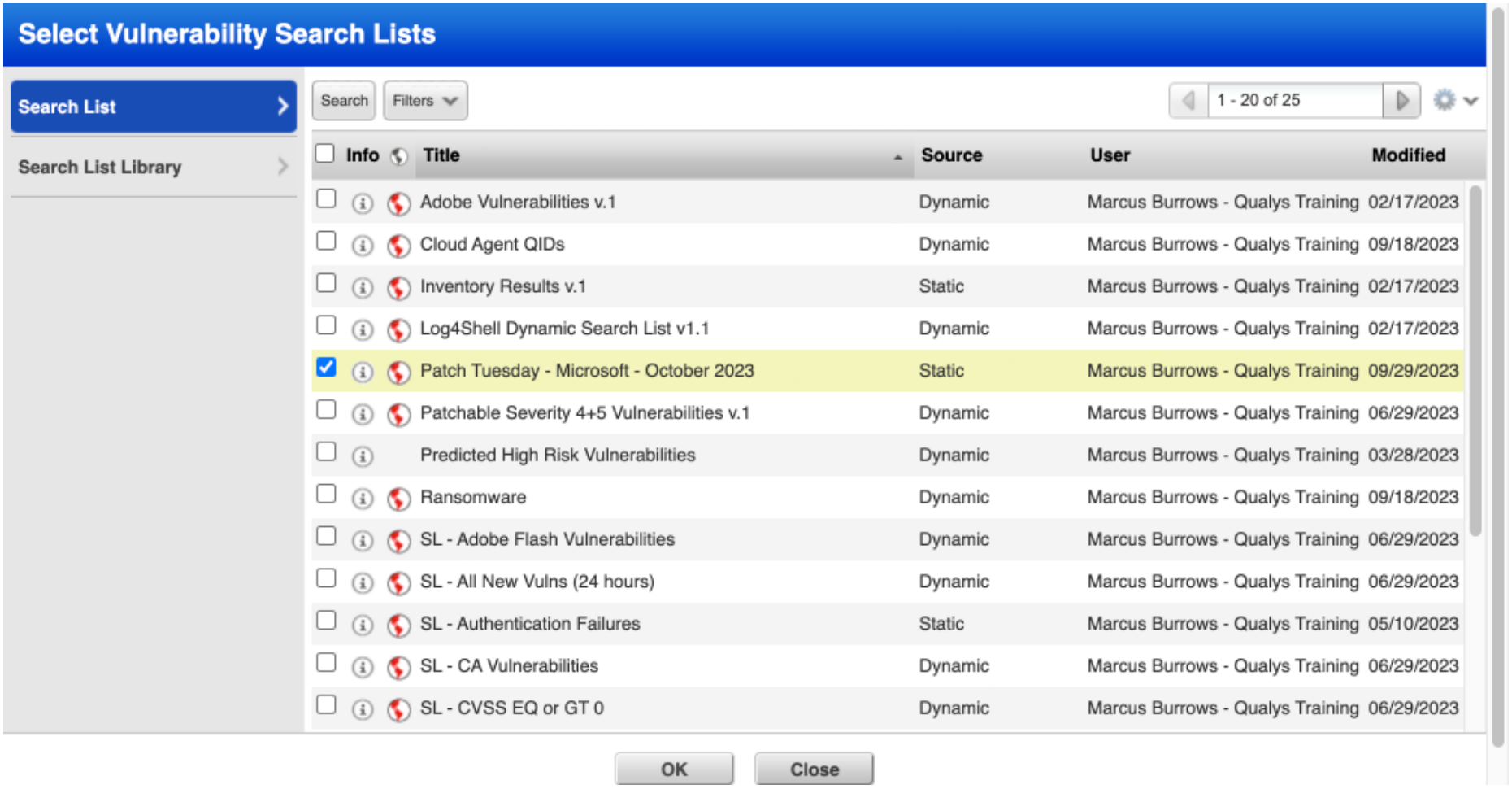
Click Add Lists



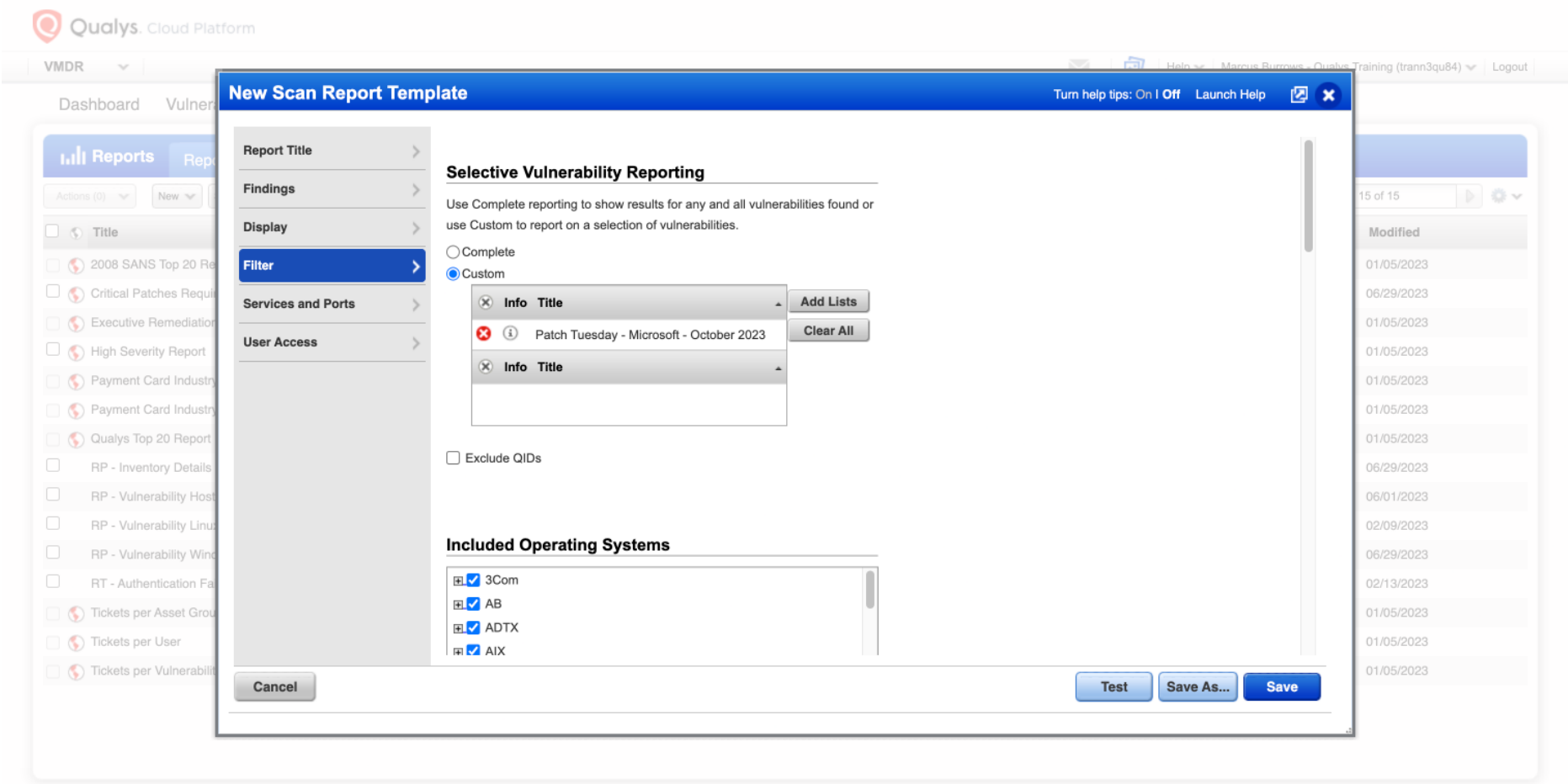
Click on the check box next to "Patch Tuesday - Microsoft - October 2023".



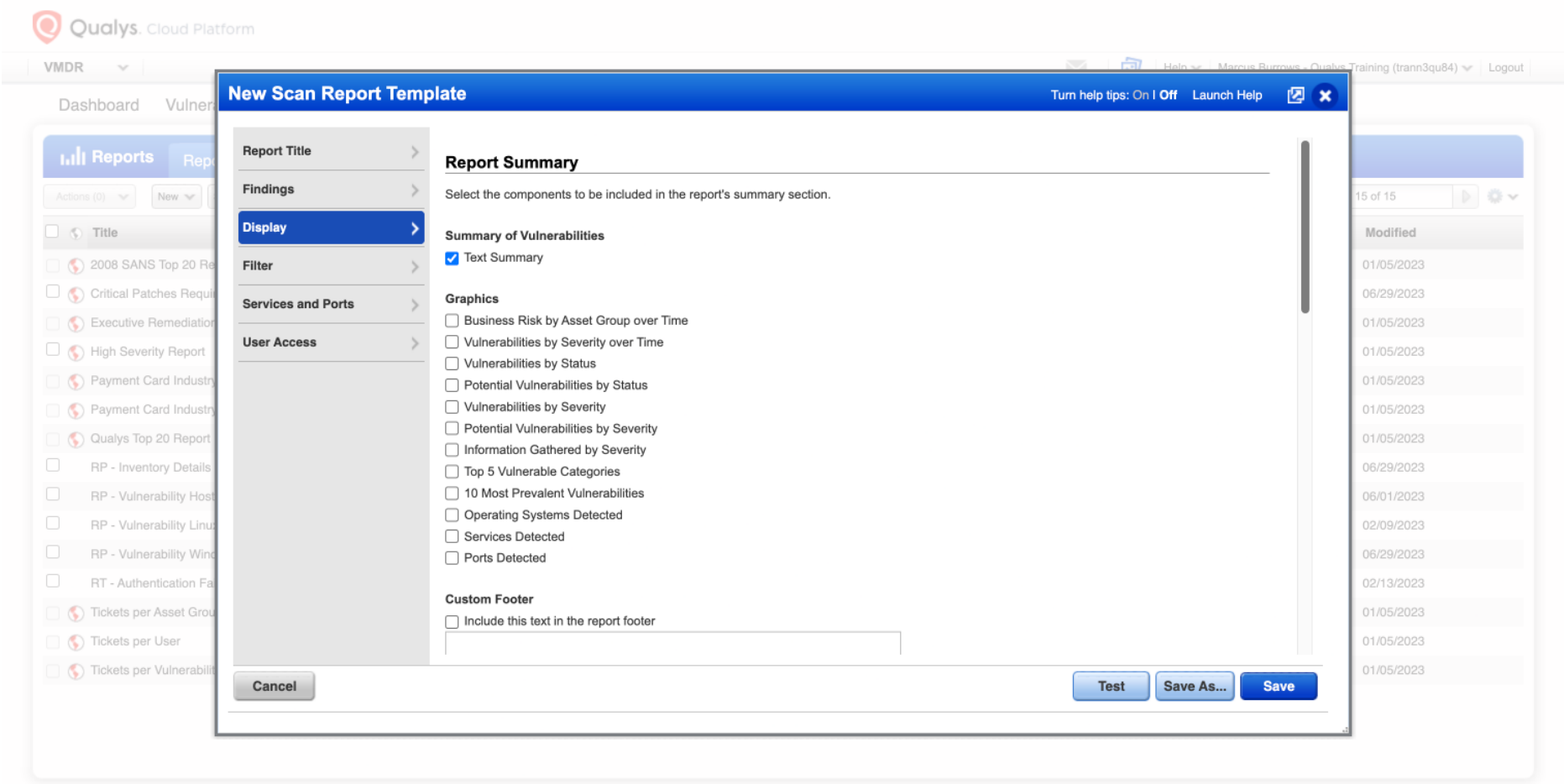
Click OK


Select Vulnerability Search Lists
Search List
Search List Library
Search
Filters
1 - 20 of 25
Info
Title
Source
User
Modified
Adobe Vulnerabilities v.1 Dynamic Marcus Burrows - Qualys Training 02/17/2023
Cloud Agent QIDs Dynamic Marcus Burrows - Qualys Training 09/18/2023
Inventory Results v.1 Static Marcus Burrows - Qualys Training 02/17/2023
Log4Shell Dynamic Search List v1.1 Dynamic Marcus Burrows - Qualys Training 02/17/2023
Patch Tuesday - Microsoft - October 2023 Static Marcus Burrows - Qualys Training 09/29/2023
Patchable Severity 4+5 Vulnerabilities v.1 Dynamic Marcus Burrows - Qualys Training 06/29/2023
Predicted High Risk Vulnerabilities Dynamic Marcus Burrows - Qualys Training 03/28/2023
Ransomware Dynamic Marcus Burrows - Qualys Training 09/18/2023
SL - Adobe Flash Vulnerabilities Dynamic Marcus Burrows - Qualys Training 06/29/2023
SL - All New Vulns (24 hours) Dynamic Marcus Burrows - Qualys Training 06/29/2023
SL - Authentication Failures Static Marcus Burrows - Qualys Training 05/10/2023
SL - CA Vulnerabilities Dynamic Marcus Burrows - Qualys Training 06/29/2023
SL - CVSS EQ or GT 0 Dynamic Marcus Burrows - Qualys Training 06/29/2023
OK
Close

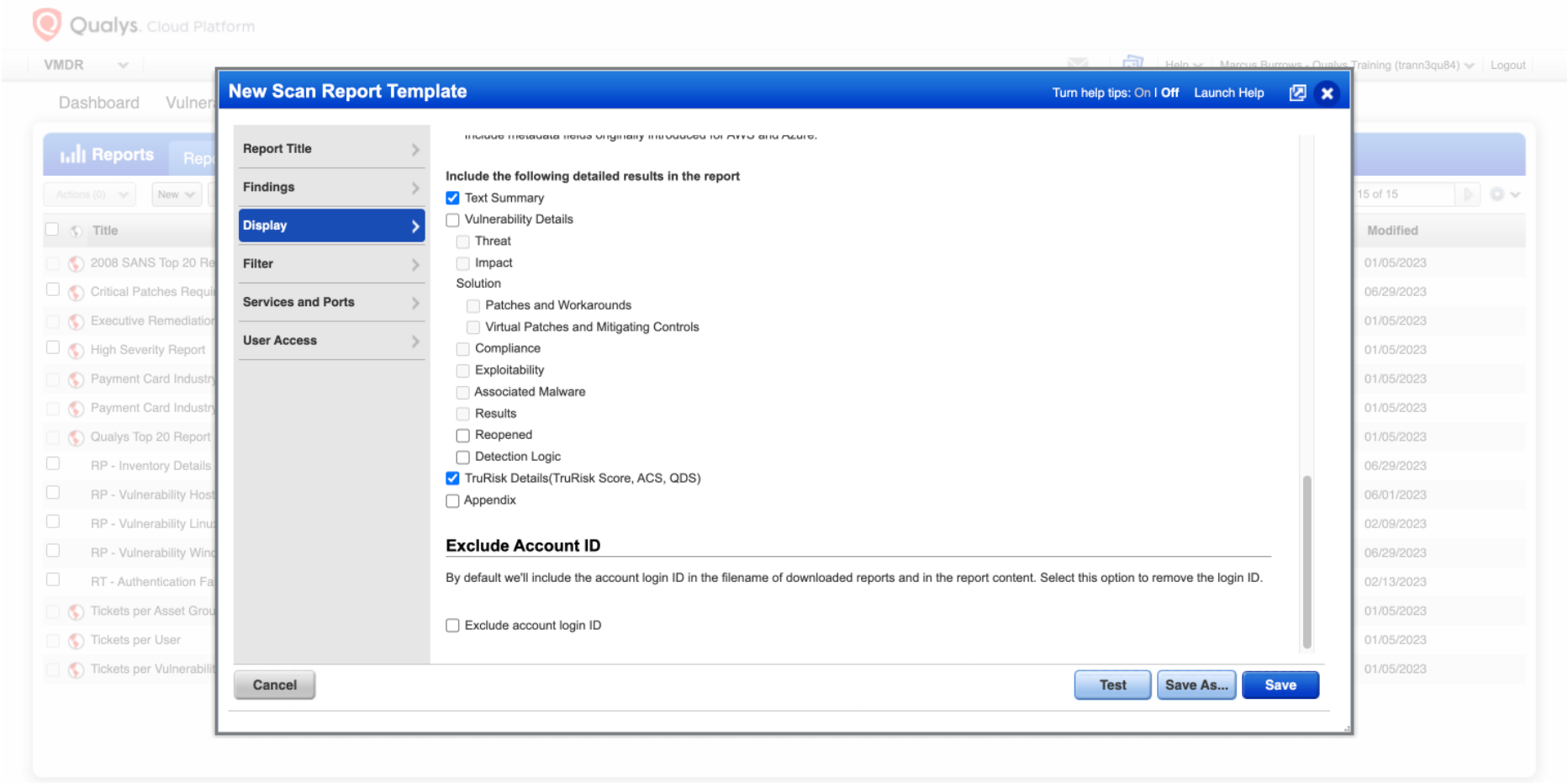
The report will now contain only information about discovered vulnerabilities which are included in this particular Search List. Click on the Display tab to continue.



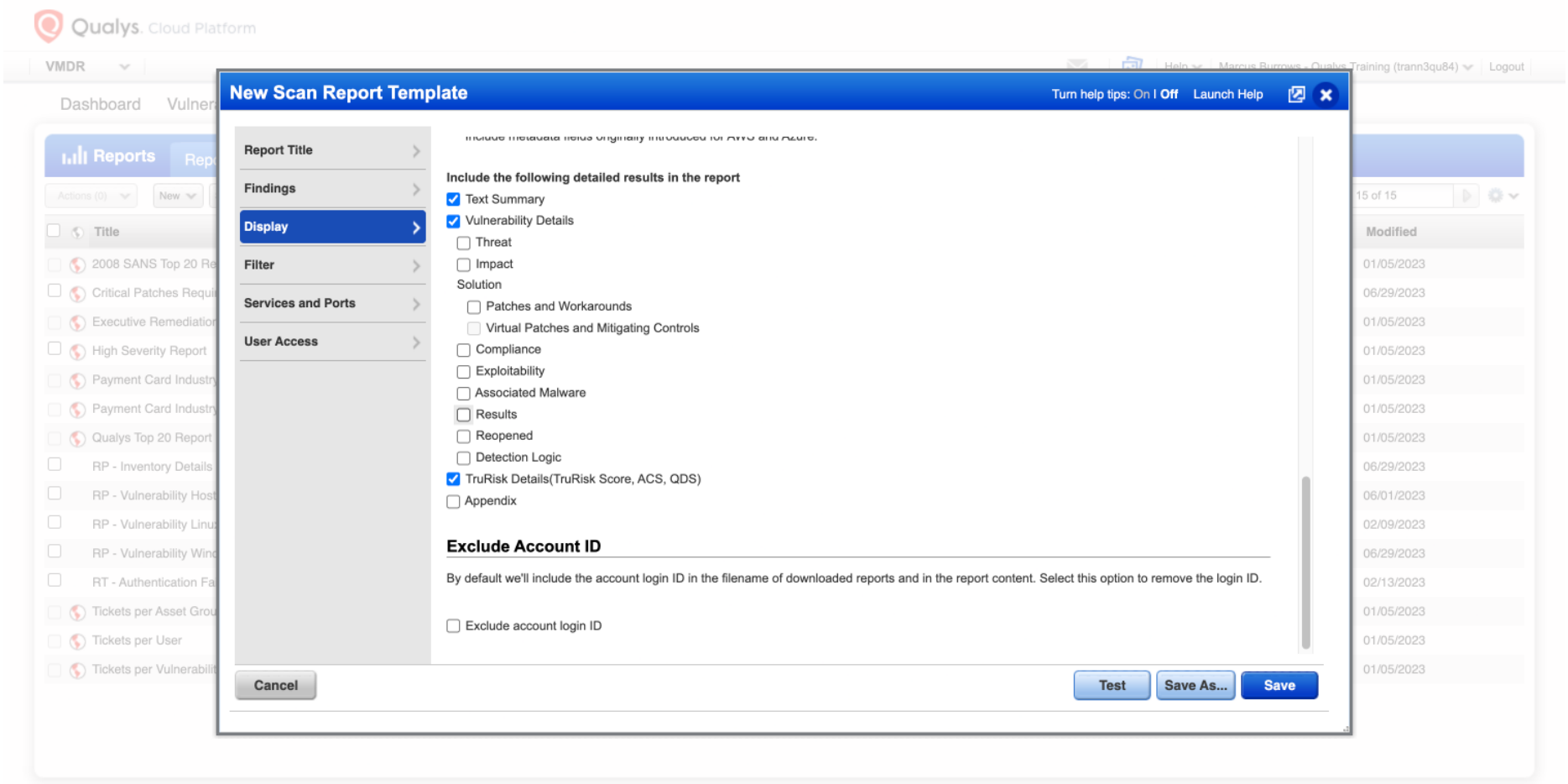
There are different display options to choose from, depending on who the report is for, and what the report is intended to convey. Click on the scroll bar on the right of the dialog to scroll down.



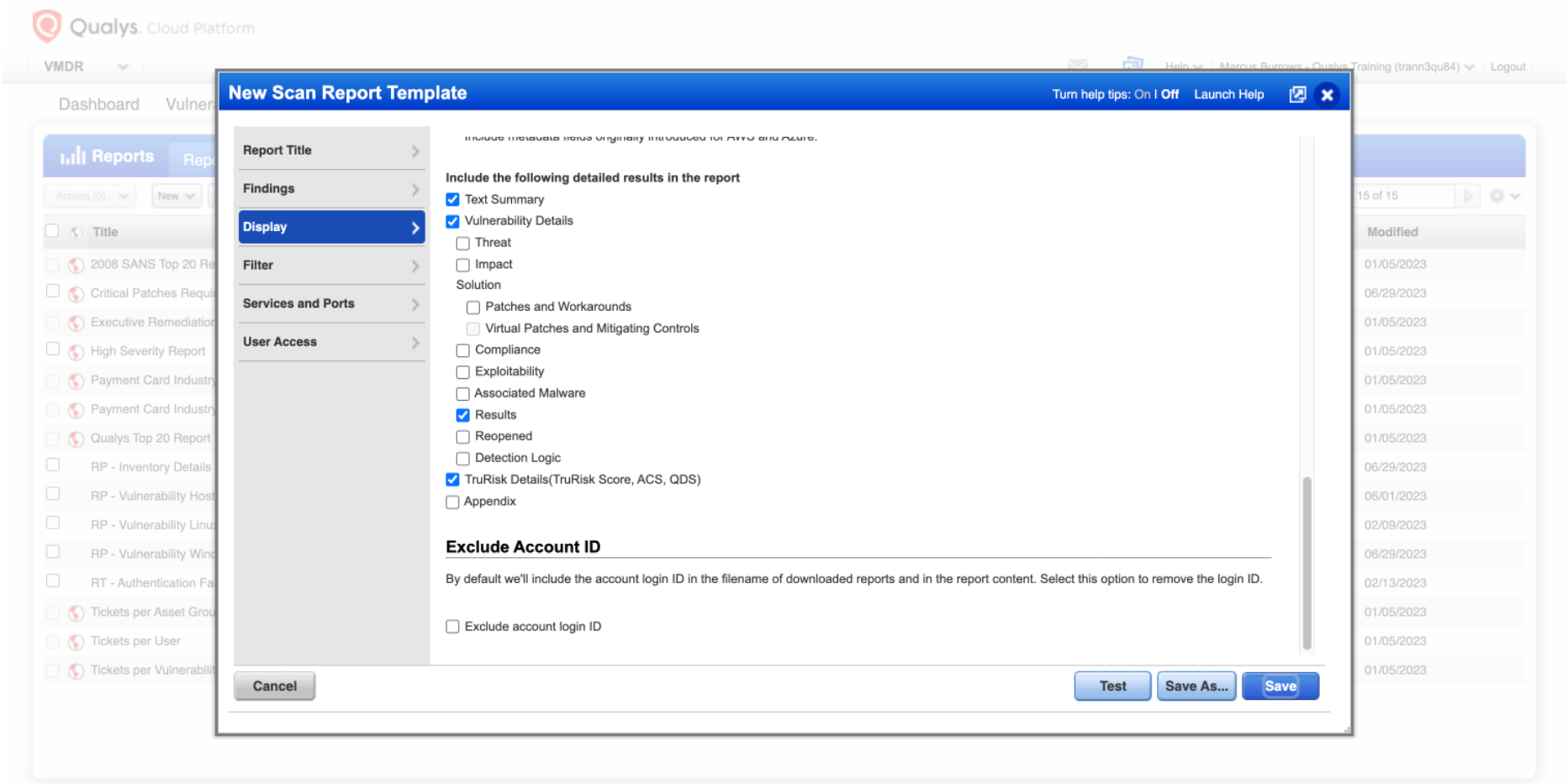
Click the check box next to Vulnerability Details



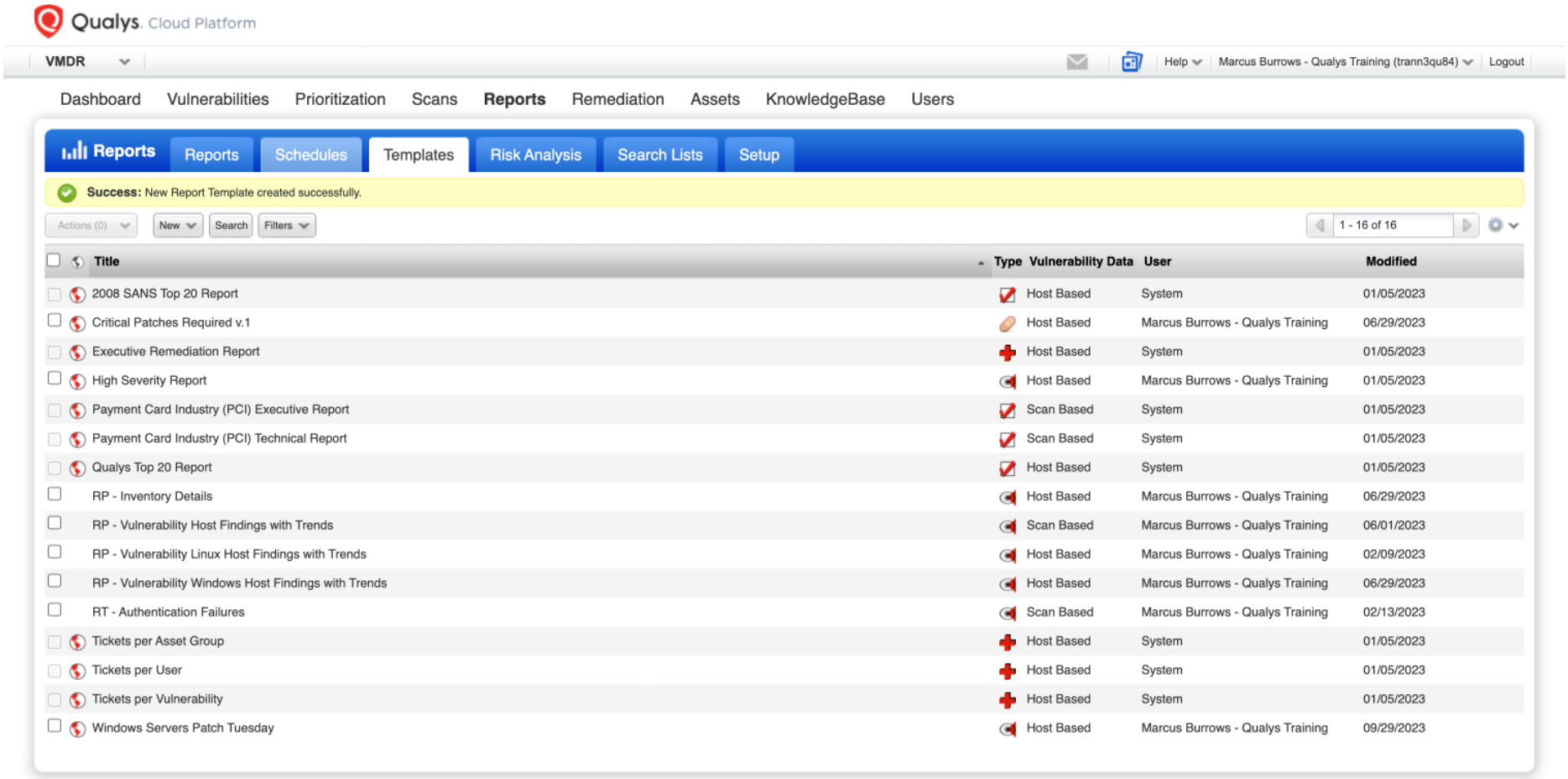
Click the check box next to Results



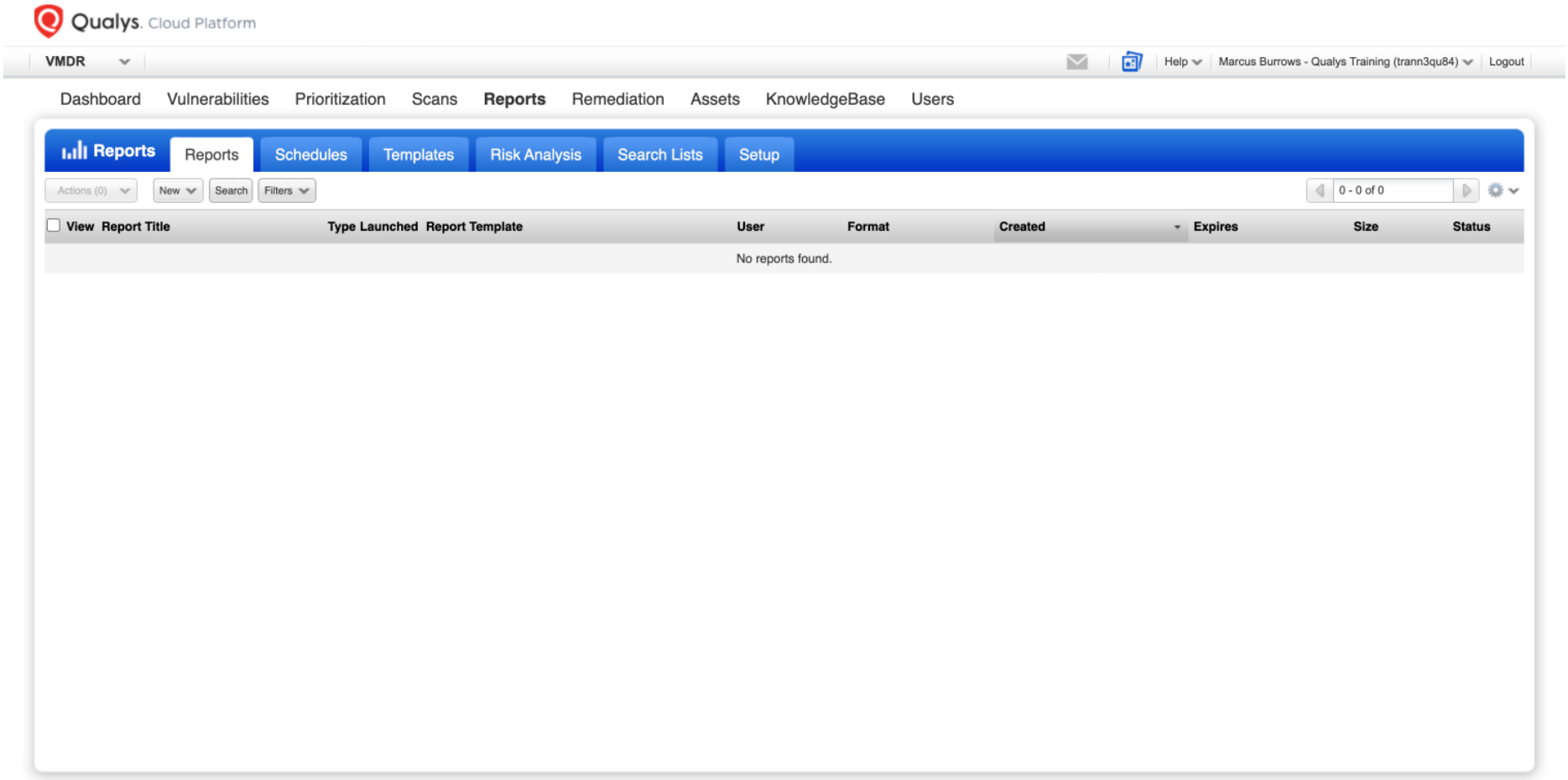
Click Save


New Scan Report Template
Turn help tips: On I Off
Launch Help
Report Title
Findings
Display
Filter
Services and Ports
User Access
Include the following detailed results in the report
Text Summary
Vulnerability Details
Threat
Impact
Solution
Patches and Workarounds
Virtual Patches and Mitigating Controls
Compliance
Exploitability
Associated Malware
Results
Reopened
Detection Logic
TruRisk Details(TruRisk Score, ACS, QDS)
Appendix
Exclude Account ID
By default we'll include the account login ID in the filename of downloaded reports and in the report content. Select this option to remove the login ID.
Exclude account login ID
Cancel
Test
Save As...
Save

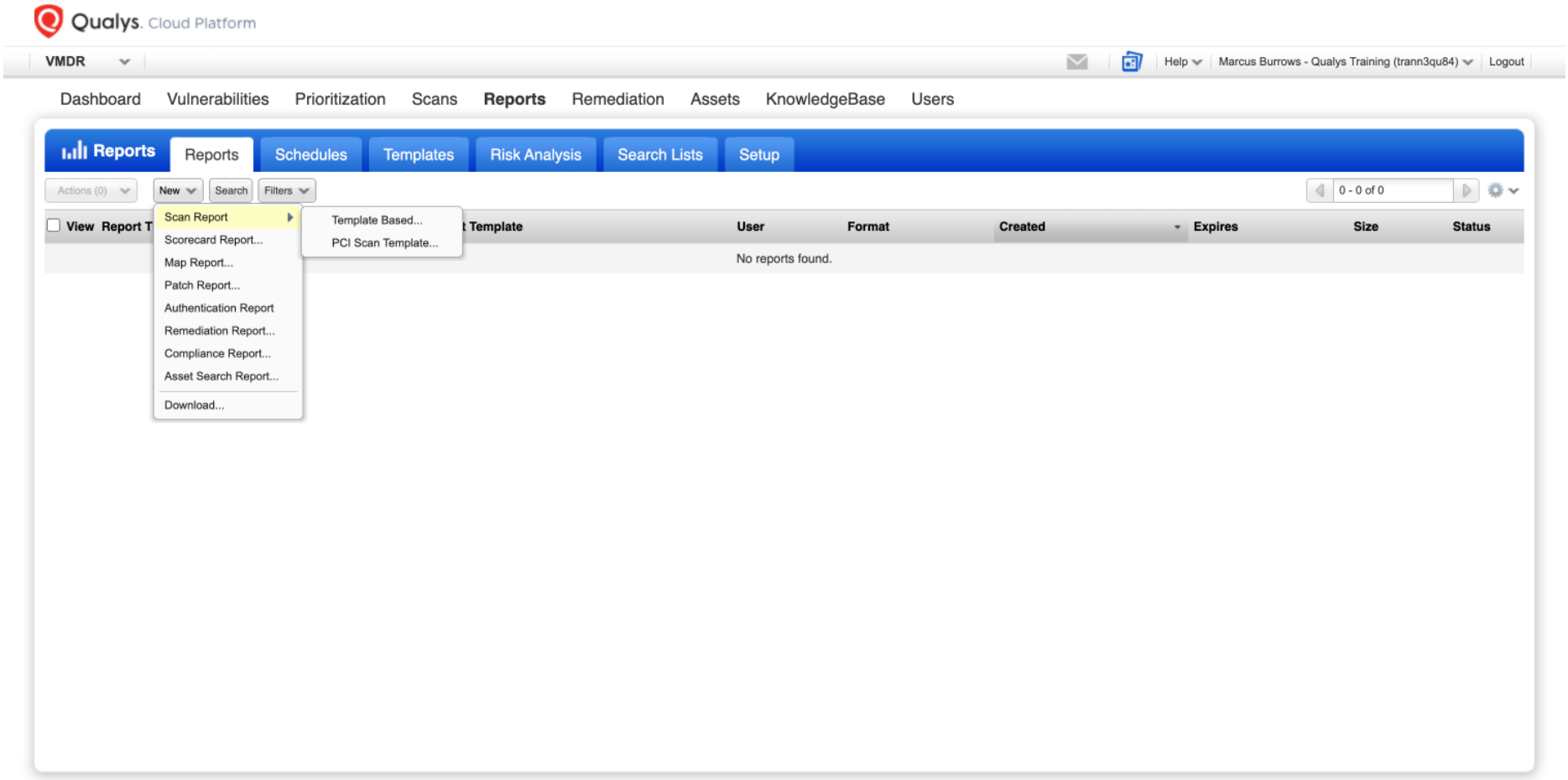
The Report Template has been successfully created. Next, click on the Reports tab.



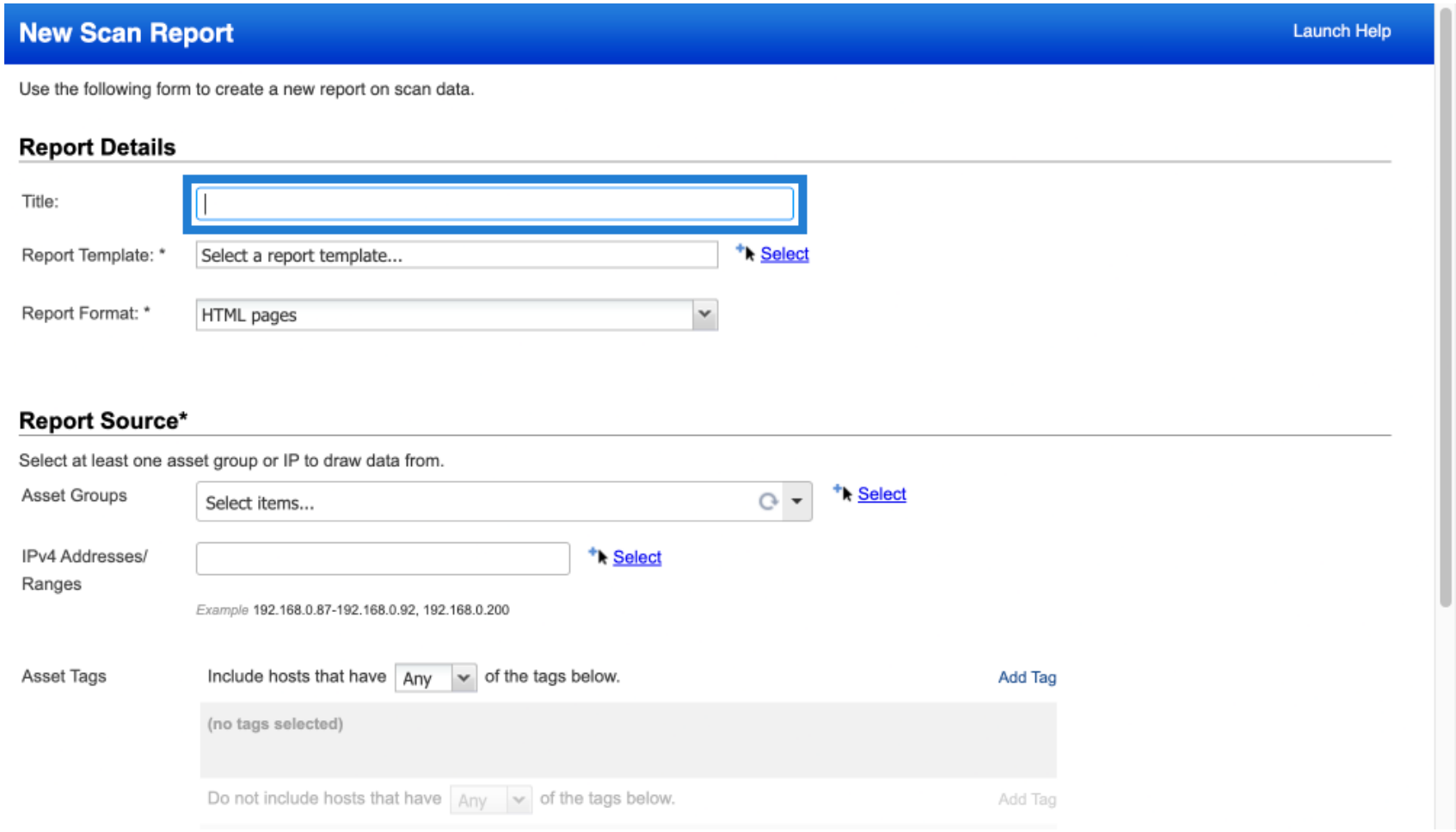
Click on the New button



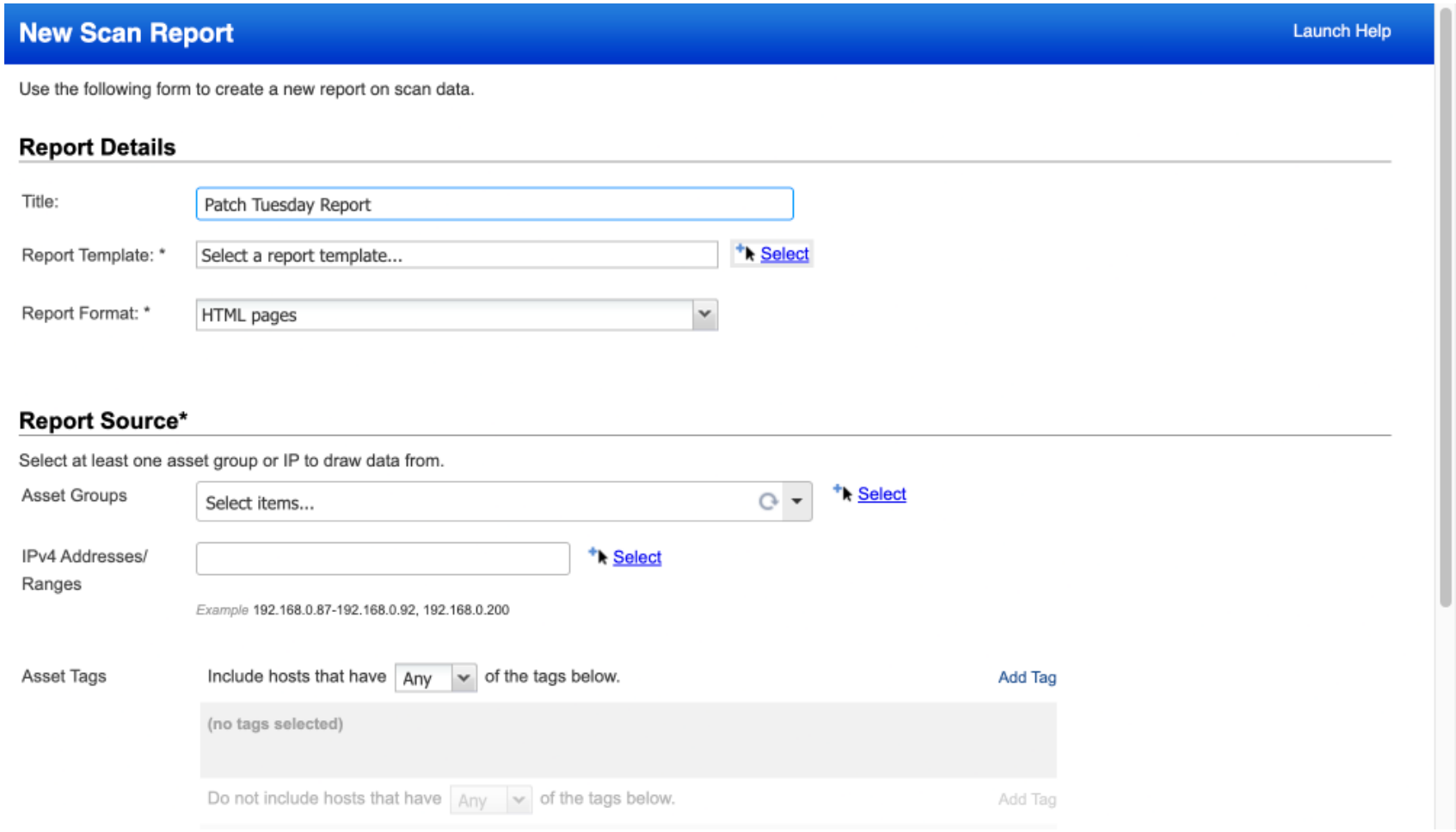
Click on "Template Based ..."



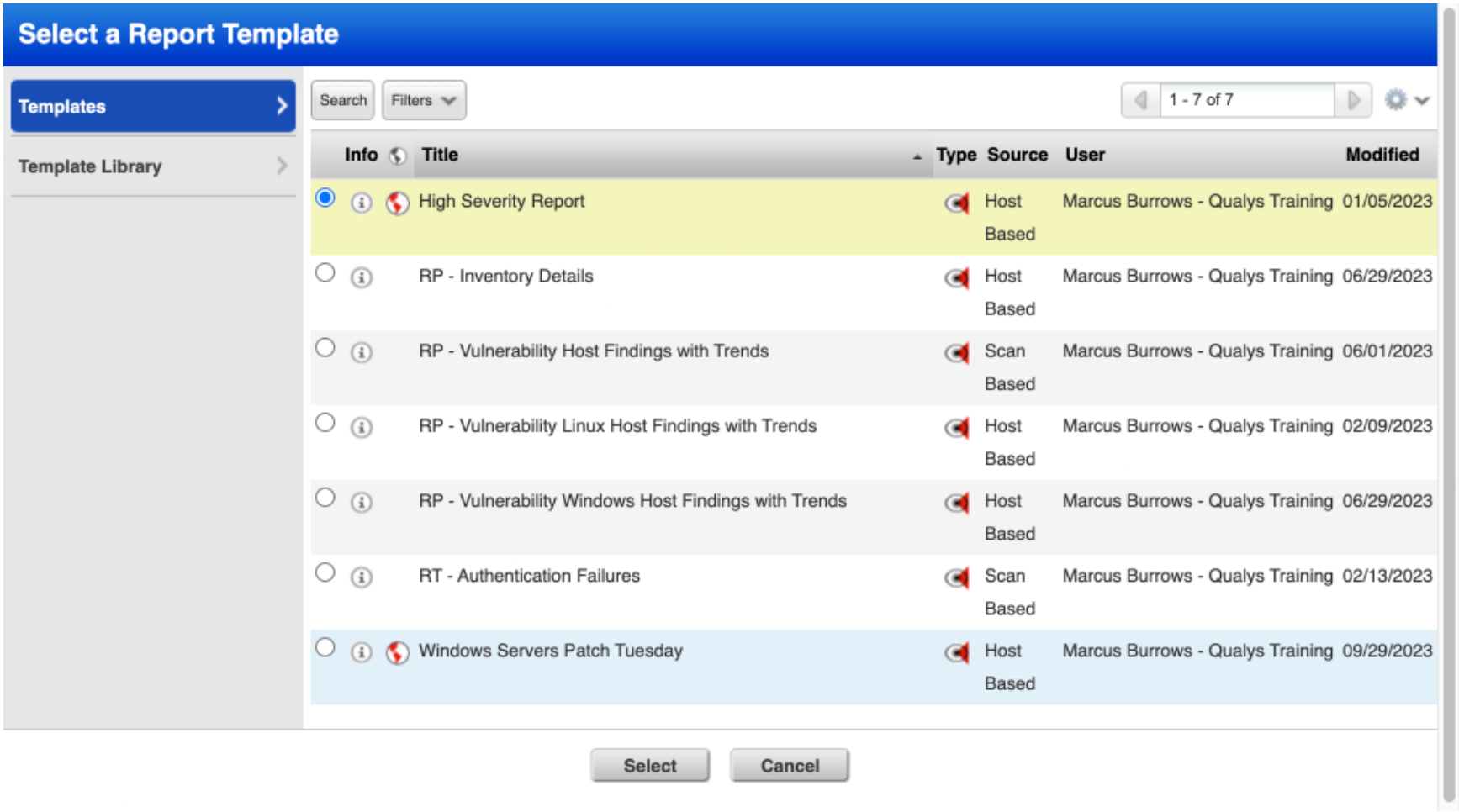
As the name for this report, type Patch Tuesday Report and press Enter



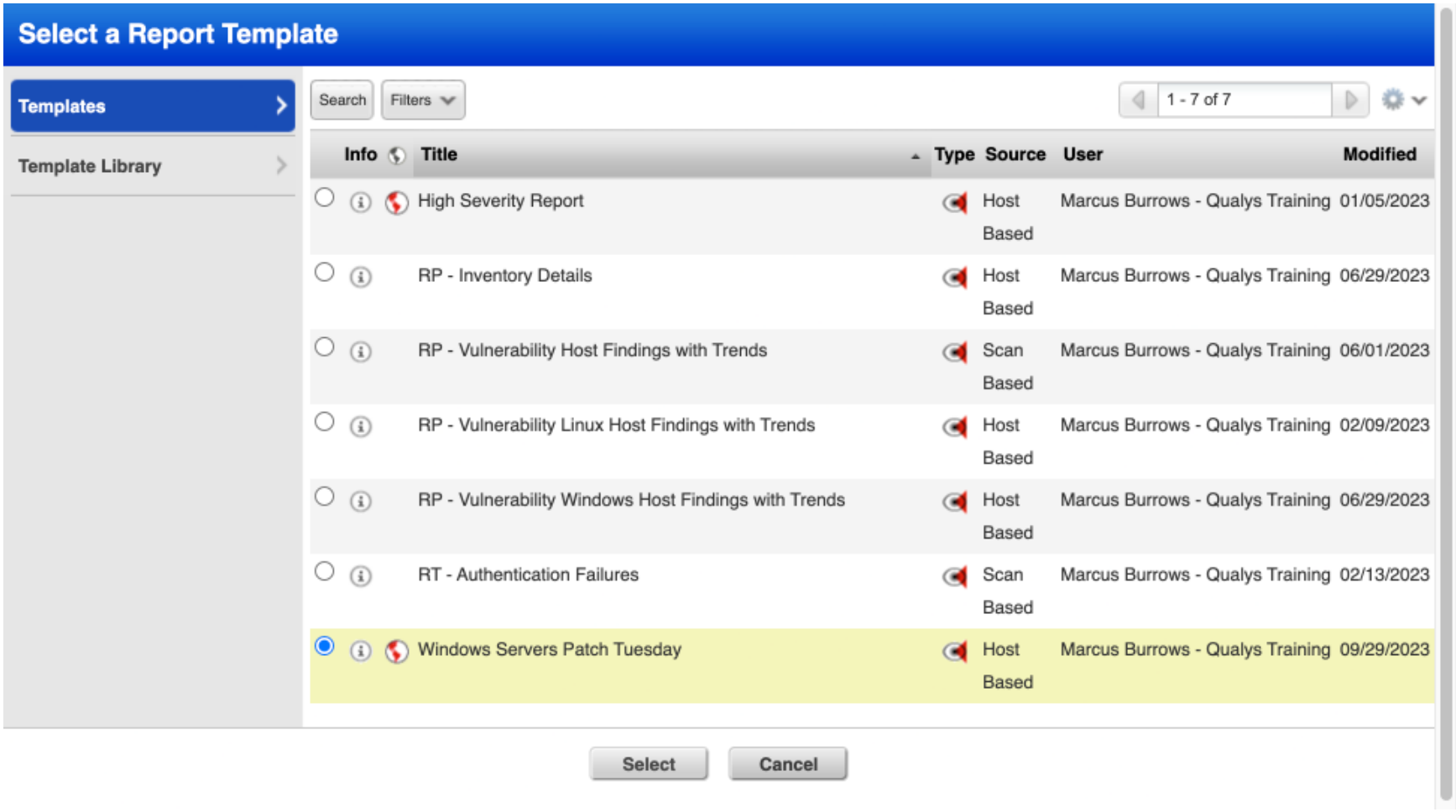
You now need to select the Template which you created earlier. Click on the Select hyperlink.



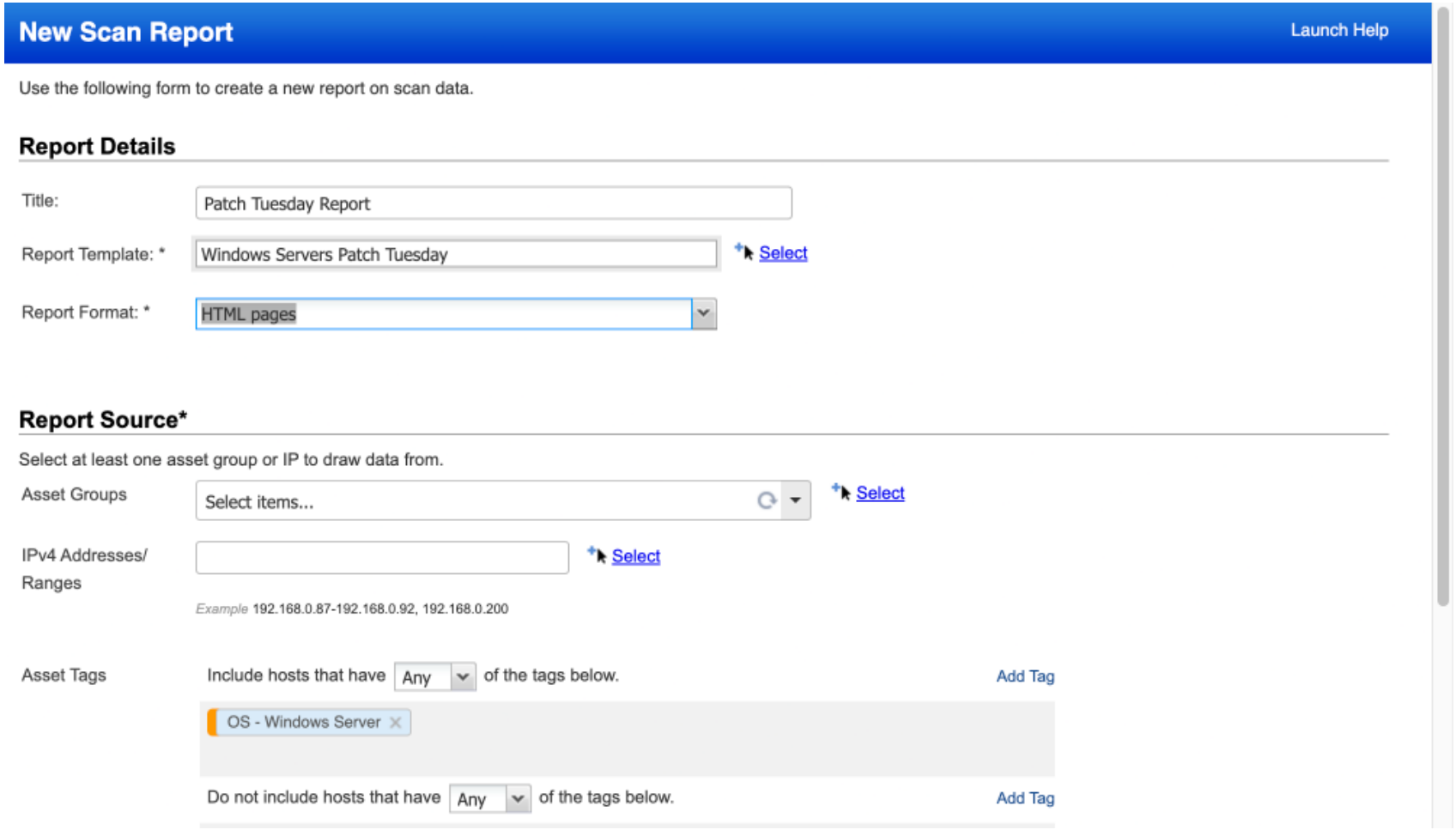
Click on the radio button next to "Windows Servers Patch Tuesday".



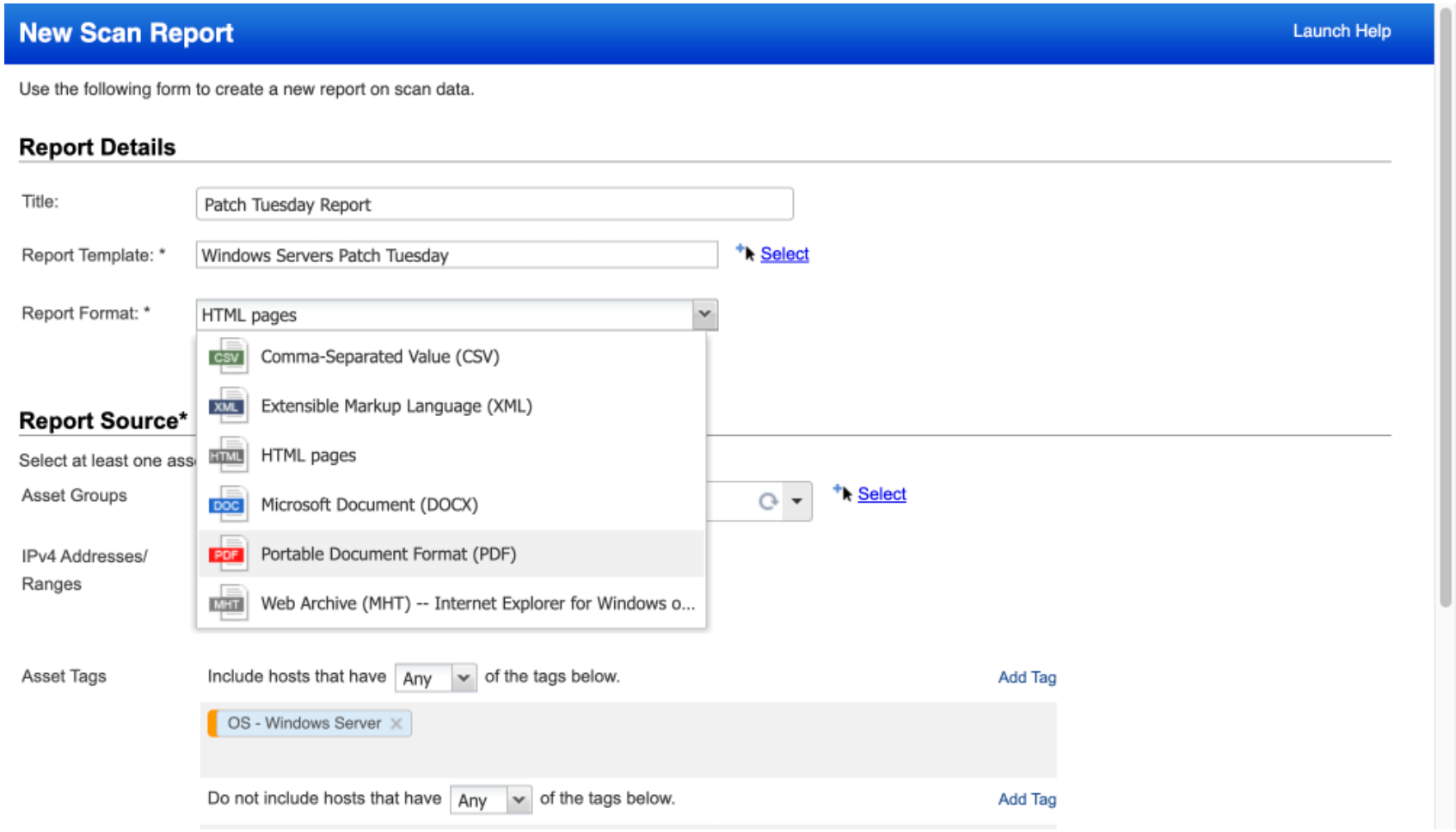
Click Select



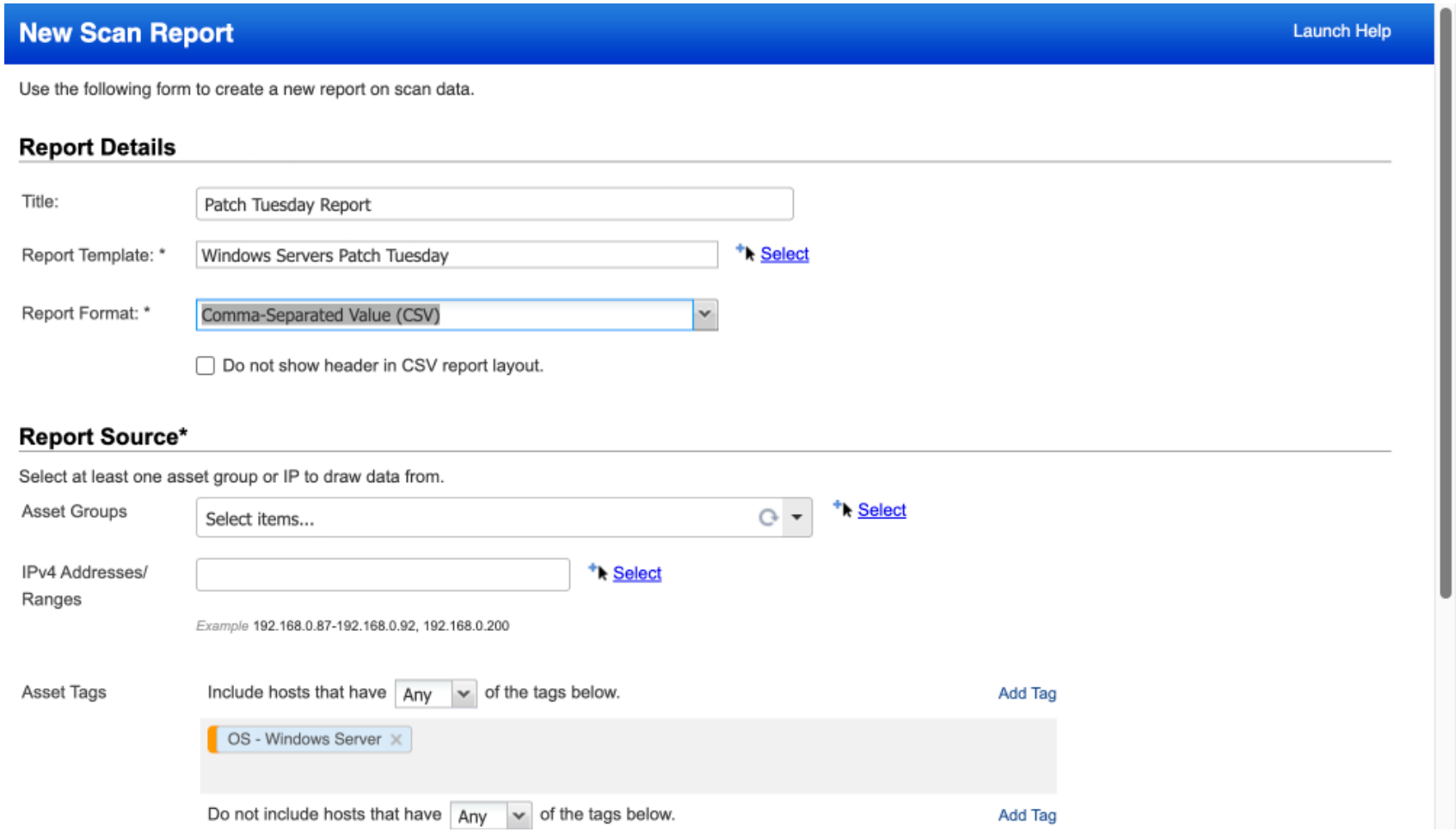
There are different report formats to choose from. Again, the choice will depend on who the report is for, and how the recipient intends to use the information. Click on the drop down next to "Report Format".


New Scan Report
Launch Help
Use the following form to create a new report on scan data.
Report Details
Title:
Patch Tuesday Report
Report Template: *
Windows Servers Patch Tuesday
Select
Report Format: *
HTML pages
Report Source*
Select at least one asset group or IP to draw data from.
Asset Groups
Select items...
Select
IPv4 Addresses/ Ranges
Select
Example 192.168.0.87-192.168.0.92, 192.168.0.200
Asset Tags
Include hosts that have
Any
of the tags below.
Add Tag
OS - Windows Server
Do not include hosts that have
Any
of the tags below.
Add Tag

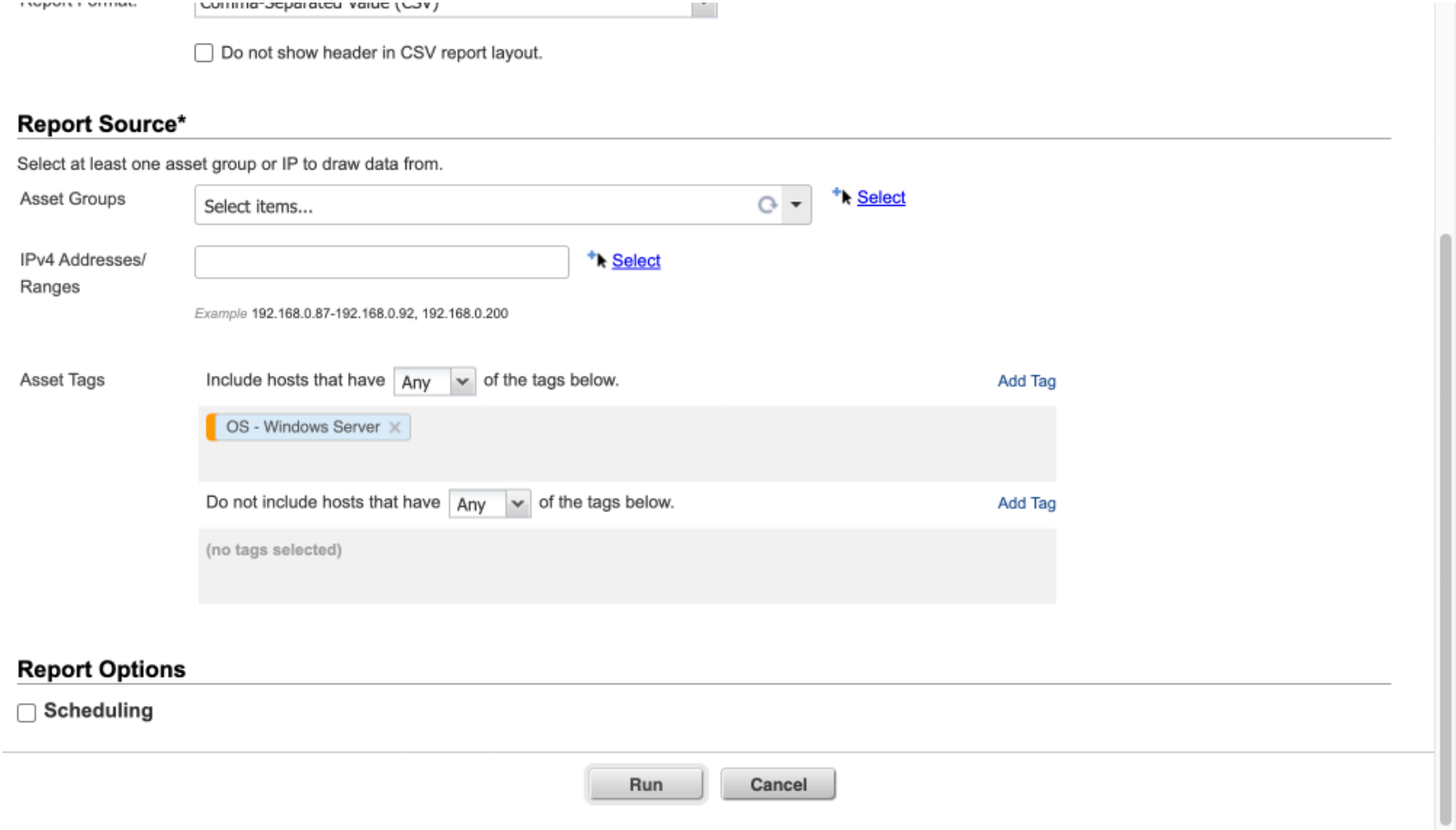
Click Comma-Separated Value (CSV)



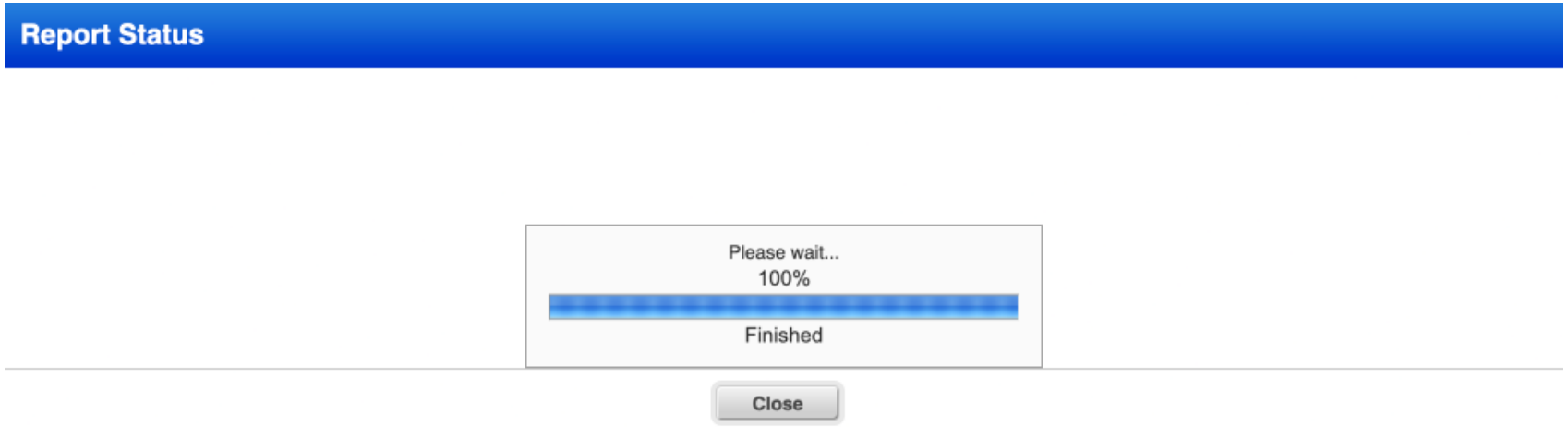
Click on the scroll bar on the right of the dialog box to scroll down.



Notice that the target assets setting has been inherited from the template, but could be changed if required. Click on Run.

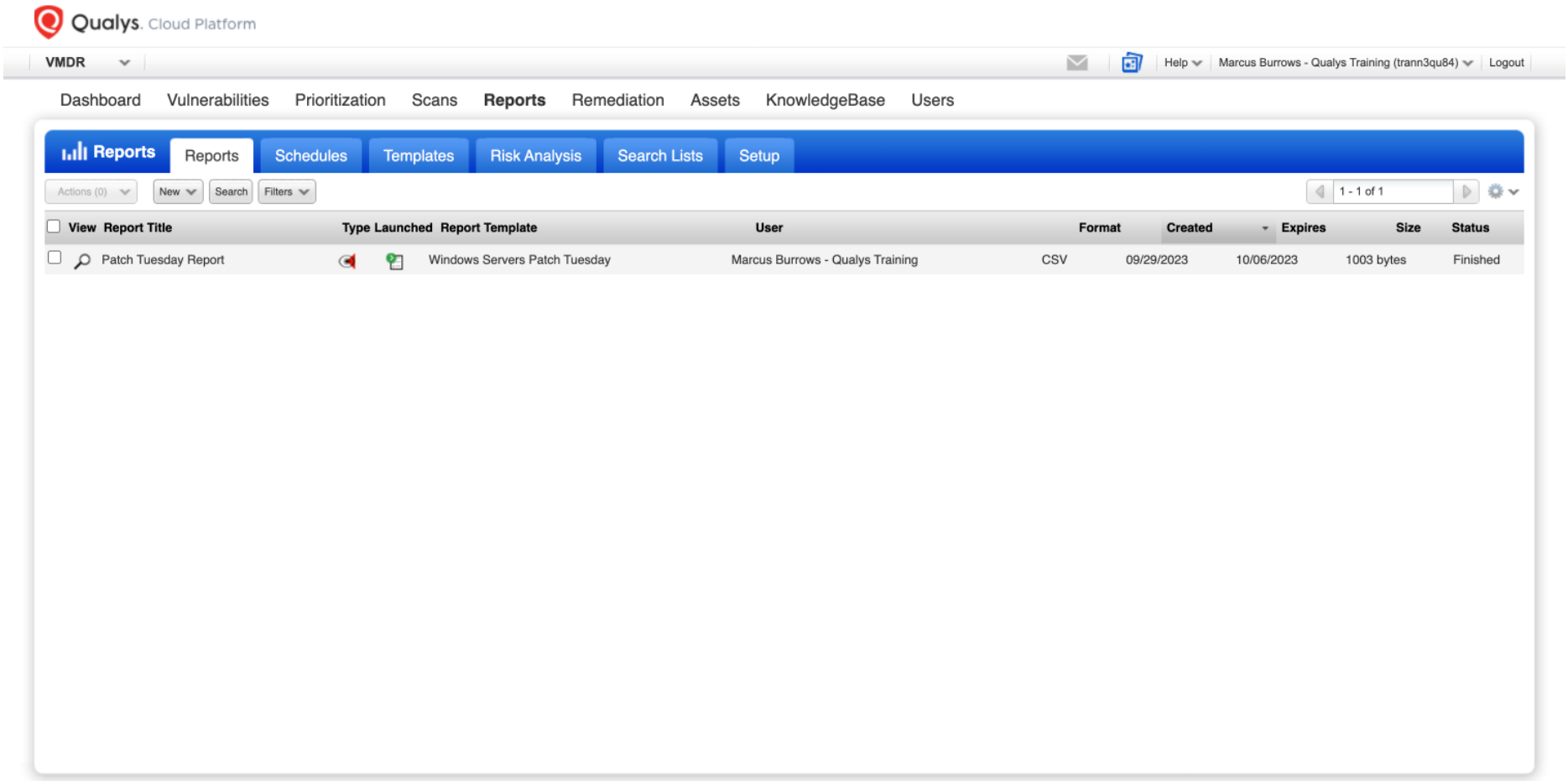


The report runs immediately. When the report has completed running, the user is prompted to download the CSV file to the local computer. Click Close



In this lab, you have created a Report Template and run a report based on that template. When required, the template could be changed to include a different Search List with the latest Patch Tuesday vulnerabilities. That's it. You're done.

Creating a custom report



Scan to go to the interactive player