Hacktales

CYBERSECURITY FOUNDATION PROGRAM

Authors:
Chikodili Udeh & Jide Adebayo

Contents

Hacktales

01
Vulnerability Management (VM)

- Introduction to Vulnerability Management
- Common Vulnerability Management Mistakes

02
VM Lifecycle

- Asset Inventory & Prioritization
- Vulnerability Assessment
- Reporting, Remediation & Verification

03
Vulnerability Management

- Vulnerability Database (VDB)
- Vulnerability Scanners
- Patch Management
- Vulnerability Assessment Workshop

01
Vulnerability Management

Objectives

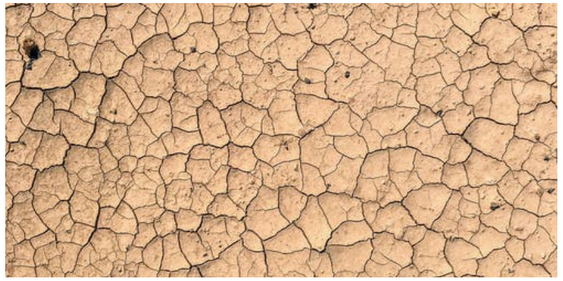
Hacktales

01

At the end of this section, students will understand the importance of vulnerability management within an organization.

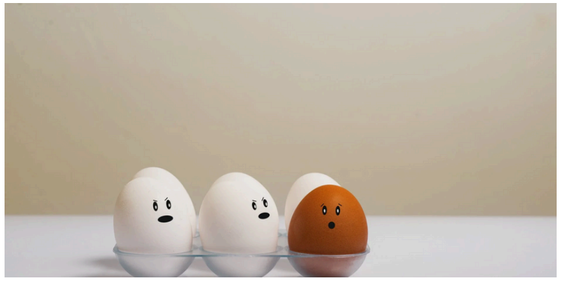
02

Students will learn the attributes of an ineffective vulnerability management program.



03

Students will understand the difference between effective and ineffective vulnerability management.



The bad guys can’t get in if they don’t have a way.

Hacktales

Vulnerability Management

A security practice designed to proactively prevent the exploitation of IT vulnerabilities that exist within an organization.

Module 3: Vulnerability Management
Cybersecurity Foundation Program

Date:
May 10, 2025

Hacktales

Common Mistakes

1. Lack of asset inventory
2. Adhoc VM process
3. Failure to prioritize by risk
4. Overreliance on controls
5. Lack of defined policies

02
Vulnerability Management Lifecycle

Objectives

Hacktales

01

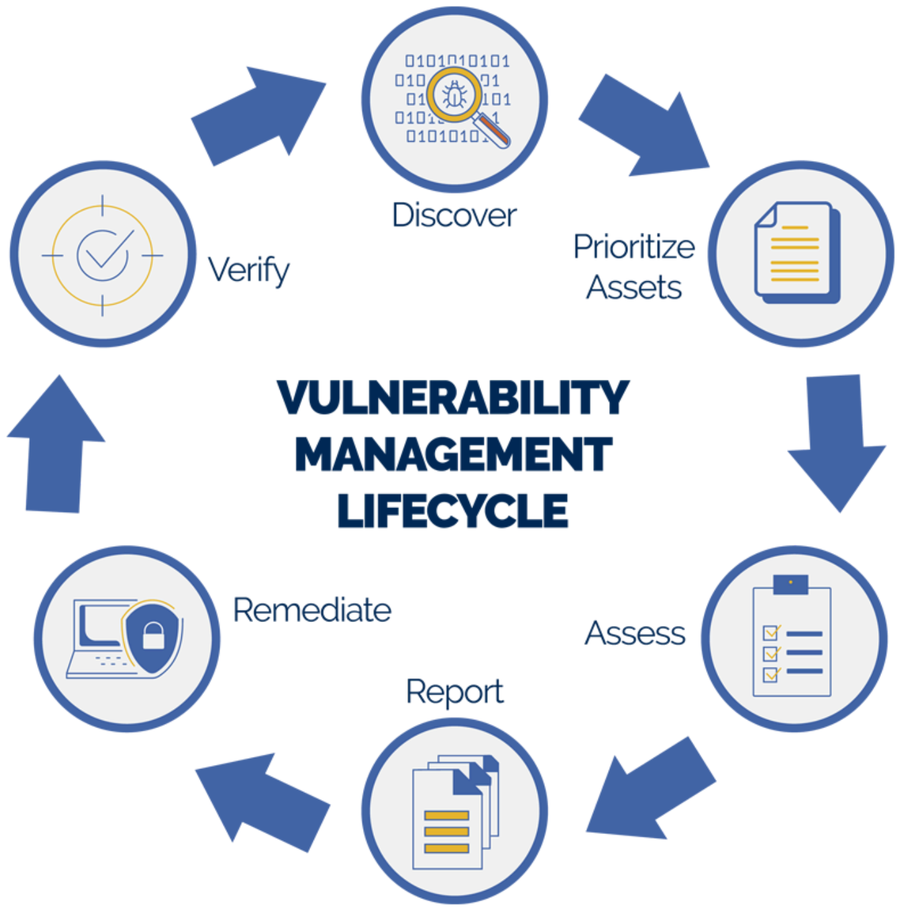
At the end of this section, students will understand the six phases of a vulnerability management lifecycle.

02

Students will learn the importance of both hardware and software vulnerability assessment.

03

Students will understand how to apply the vulnerability management lifecycle to achieve maximum results.



Vulnerability management is not a one-time task you get done and then forget.

It is a process that takes time and effort in order to be successful.

Hacktales

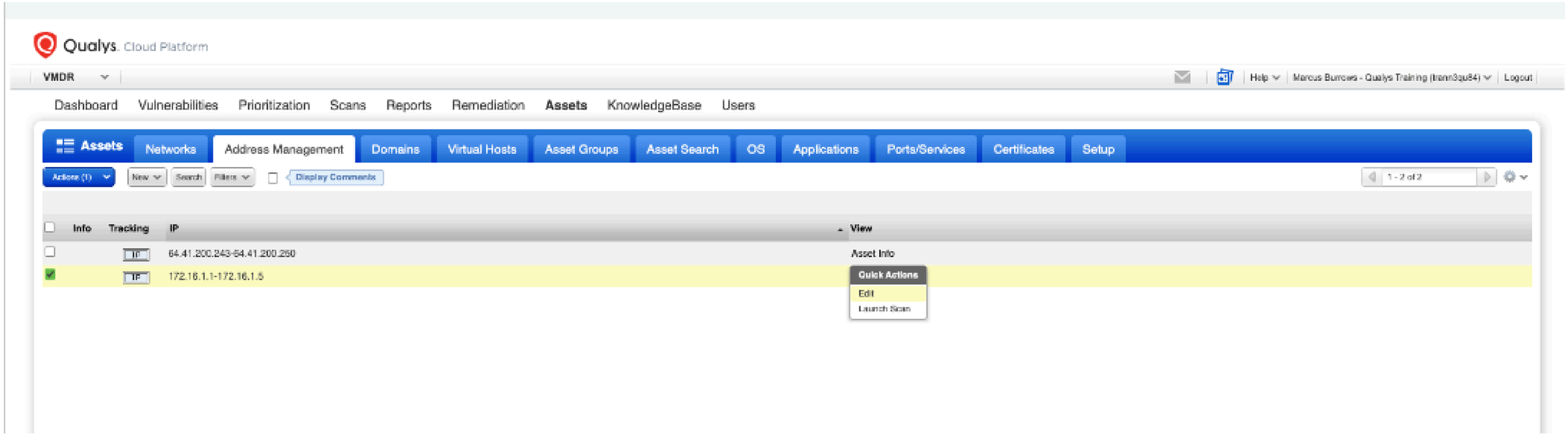
STEP 1: DISCOVER

Develop a network baseline.

Create an inventory of all assets across the network and identify host details including operating system and open services to identify vulnerabilities.

Discover

Hacktales

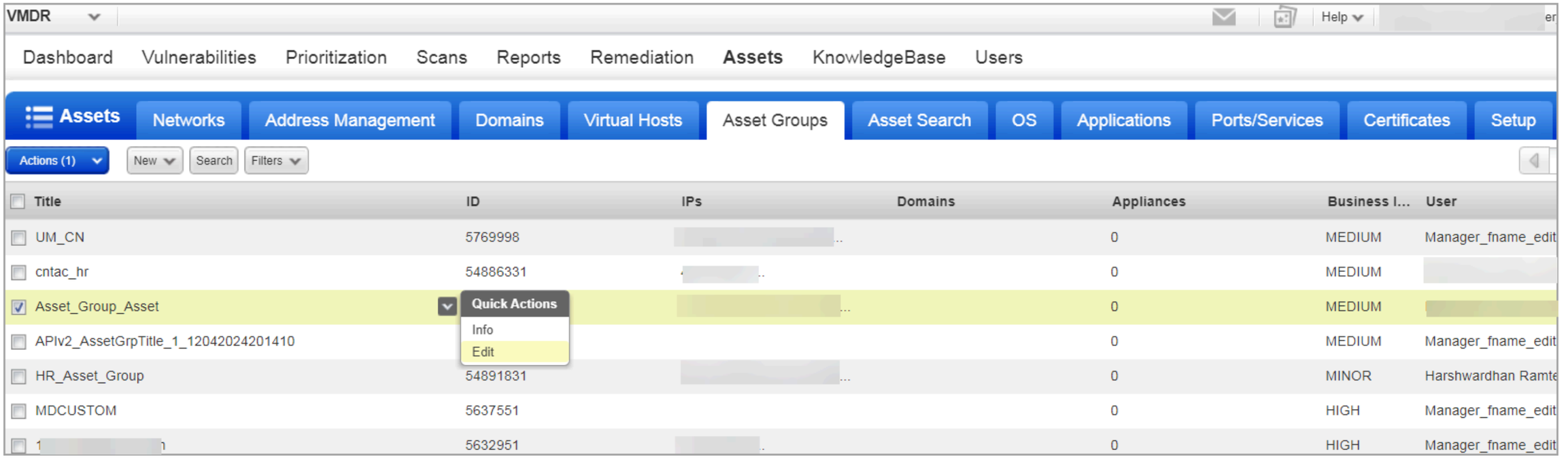


Hacktales

STEP 2: PRIORITIZE

Categorize identified assets.

Group assets into groups or business units, and assign a business value to asset groups based on their criticality to your business operation.

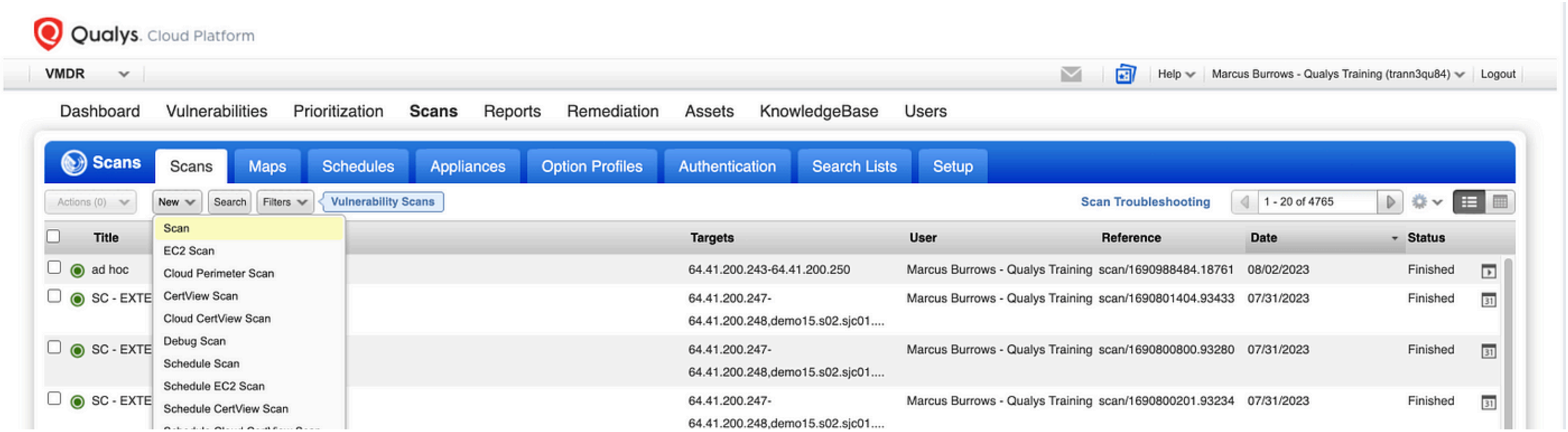

VMDR
Help
Dashboard
Vulnerabilities
Prioritization
Scans
Reports
Remediation
Assets
KnowledgeBase
Users
Assets
Networks
Address Management
Domains
Virtual Hosts
Asset Groups
Asset Search
OS
Applications
Ports/Services
Certificates
Setup
Actions (1)
New
Search
Filters
Title
ID
IPs
Domains
Appliances
Business I...
User
UM_CN
5769998
0
MEDIUM
Manager_fname_edit
cntac_hr
54886331
0
MEDIUM
Asset_Group_Asset
Quick Actions
Info
Edit
0
MEDIUM
APIv2_AssetGrpTitle_1_12042024201410
0
MEDIUM
Manager_fname_edit
HR_Asset_Group
54891831
0
MINOR
Harshwardhan Ramte
MDCUSTOM
5637551
0
HIGH
Manager_fname_edit
5632951
0
HIGH
Manager_fname_edit

Hacktales

STEP 3: ASSESS

Conduct vulnerability assessment.

Determine a baseline risk profile so you can eliminate risks based on asset criticality, vulnerability threat, and asset classification.

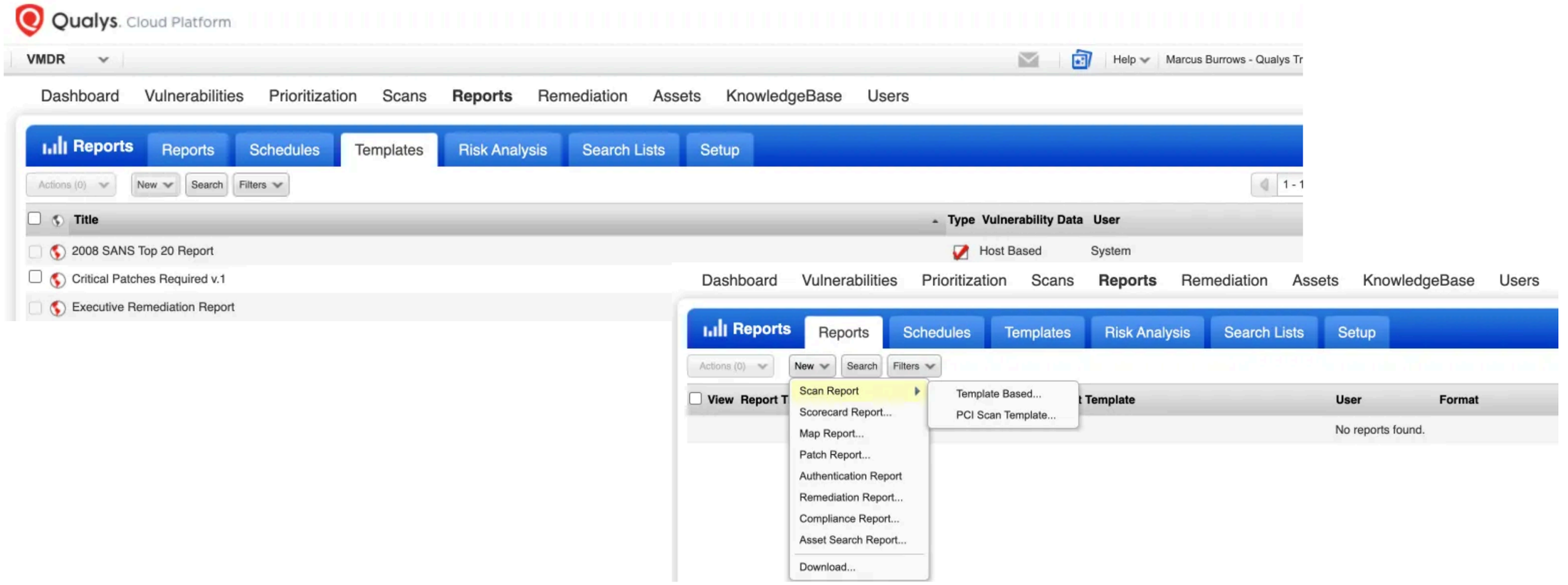

Qualys. Cloud Platform
VMDR
Help
Marcus Burrows - Qualys Training (trann3qu84)
Logout
Dashboard
Vulnerabilities
Prioritization
Scans
Reports
Remediation
Assets
KnowledgeBase
Users
Scans
Scans
Maps
Schedules
Appliances
Option Profiles
Authentication
Search Lists
Setup
Actions (0)
New
Search
Filters
Vulnerability Scans
Scan Troubleshooting
1 - 20 of 4765
Scan
EC2 Scan
Cloud Perimeter Scan
CertView Scan
Cloud CertView Scan
Debug Scan
Schedule Scan
Schedule EC2 Scan
Schedule CertView Scan
Title
Targets
User
Reference
Date
Status
ad hoc
64.41.200.243-64.41.200.250
Marcus Burrows - Qualys Training
scan/1690988484.18761
08/02/2023
Finished
SC - EXTE
64.41.200.247-
64.41.200.248,demo15.s02.sjc01....
Marcus Burrows - Qualys Training
scan/1690801404.93433
07/31/2023
Finished
SC - EXTE
64.41.200.247-
64.41.200.248,demo15.s02.sjc01....
Marcus Burrows - Qualys Training
scan/1690800800.93280
07/31/2023
Finished
SC - EXTE
64.41.200.247-
64.41.200.248,demo15.s02.sjc01....
Marcus Burrows - Qualys Training
scan/1690800201.93234
07/31/2023
Finished

Hacktales

STEP 4: REPORT

Generate threat landscape report.

Get a summary of the level of business risk associated with your assets.

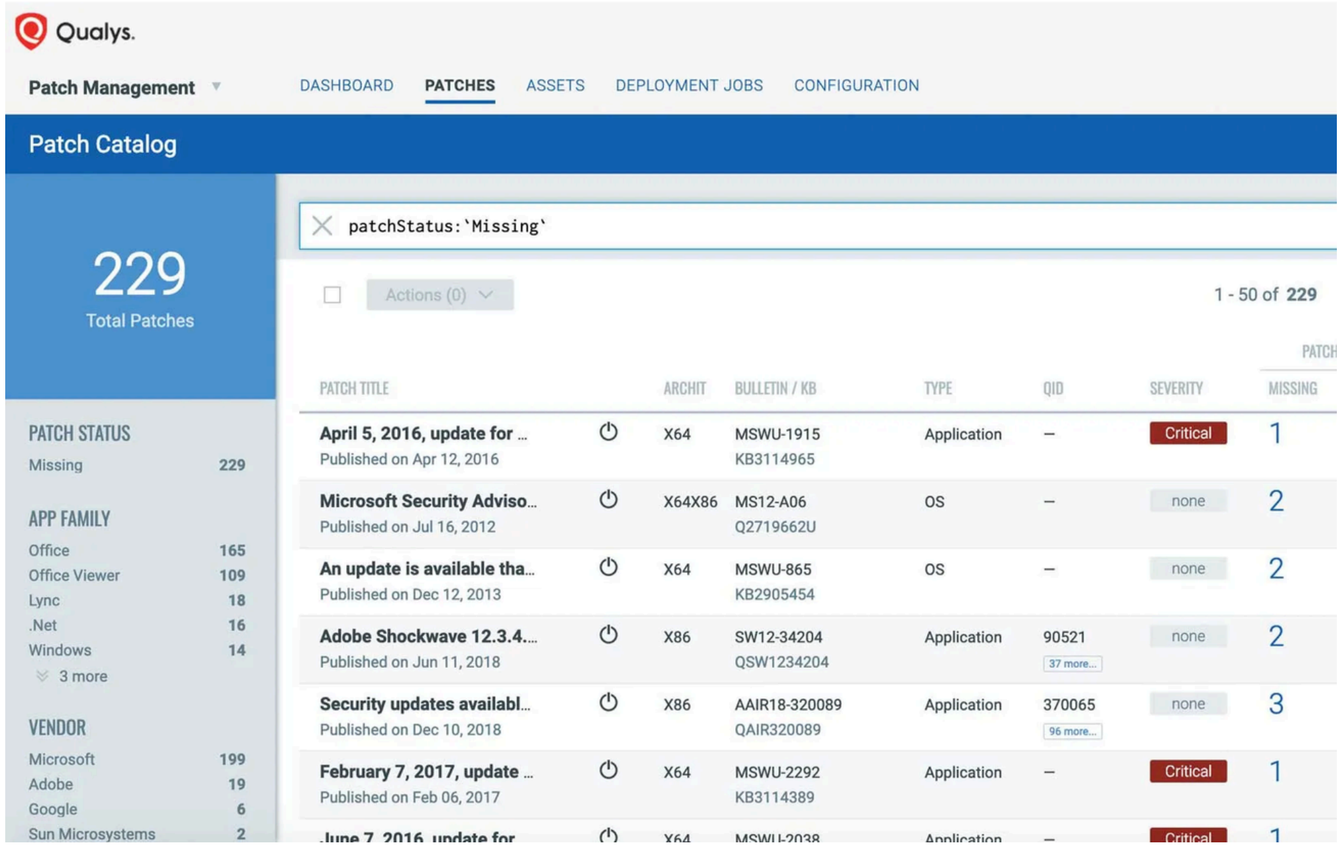

Qualys. Cloud Platform
VMDR
Help
Marcus Burrows - Qualys Tr
Dashboard
Vulnerabilities
Prioritization
Scans
Reports
Remediation
Assets
KnowledgeBase
Users
Reports
Reports
Schedules
Templates
Risk Analysis
Search Lists
Setup
Actions (0)
New
Search
Filters
1 - 1
Title
Type
Vulnerability Data
User
2008 SANS Top 20 Report
Host Based
System
Critical Patches Required v.1
Executive Remediation Report
Dashboard
Vulnerabilities
Prioritization
Scans
Reports
Remediation
Assets
KnowledgeBase
Users
Reports
Reports
Schedules
Templates
Risk Analysis
Search Lists
Setup
Actions (0)
New
Search
Filters
Scan Report
Scorecard Report...
Map Report...
Patch Report...
Authentication Report
Remediation Report...
Compliance Report...
Asset Search Report...
Download...
Template Based...
PCI Scan Template...
View
Report T
Template
User
Format
No reports found.

Hacktales

STEP 5: REMEDIATE

Establish control to fix vulnerabilities.

Prioritize and patch vulnerabilities in order according to business risk.

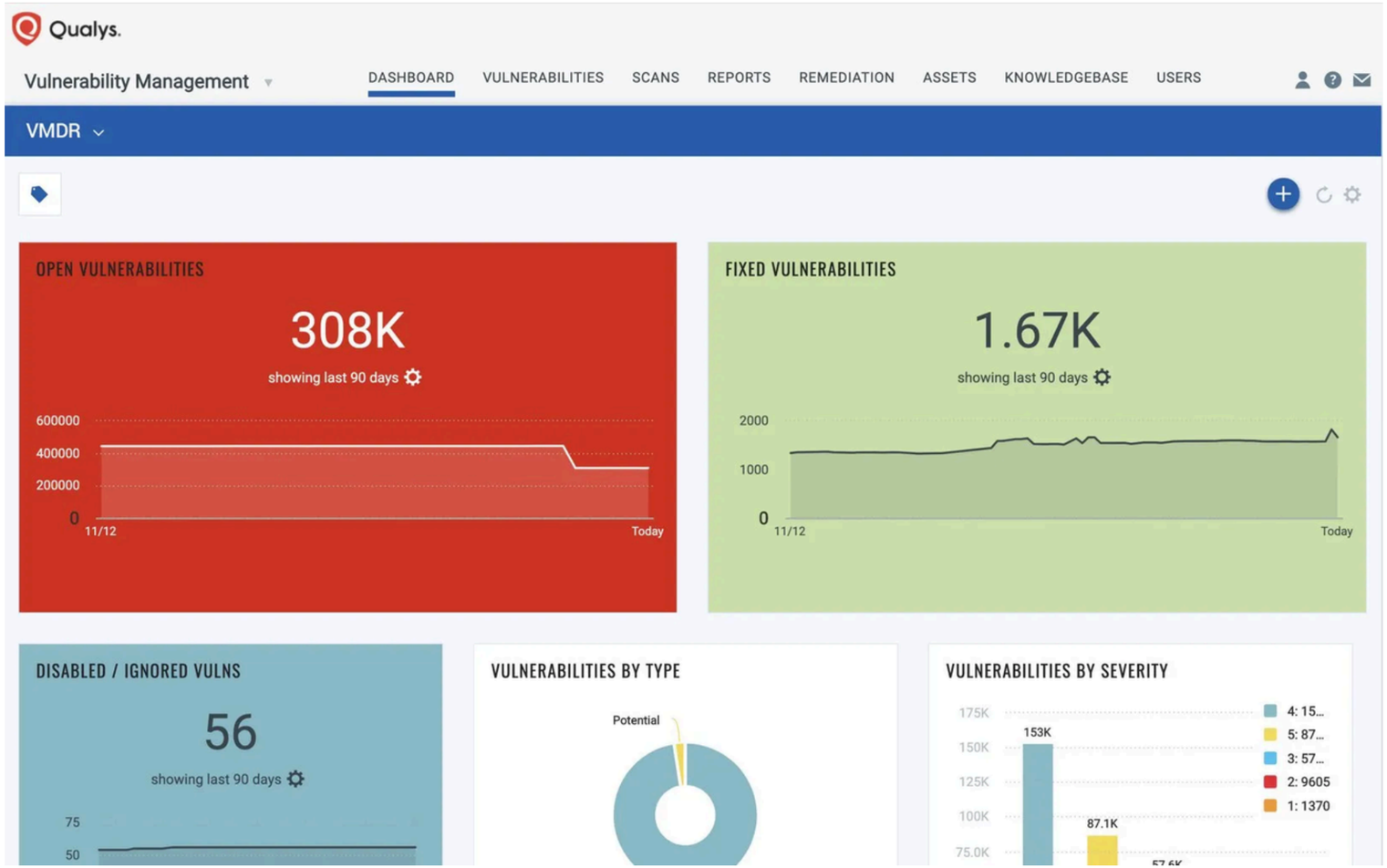

Qualys.
Patch Management
DASHBOARD
PATCHES
ASSETS
DEPLOYMENT JOBS
CONFIGURATION
Patch Catalog
229
Total Patches
PATCH STATUS
Missing 229
APP FAMILY
Office 165
Office Viewer 109
Lync 18
.Net 16
Windows 14
3 more
VENDOR
Microsoft 199
Adobe 19
Google 6
Sun Microsystems 2
patchStatus:`Missing`
Actions (0)
1 - 50 of 229
PATCH TITLE
ARCHIT
BULLETIN / KB
TYPE
QID
SEVERITY
MISSING
April 5, 2016, update for ...
Published on Apr 12, 2016
X64
MSWU-1915
KB3114965
Application
–
Critical
1
Microsoft Security Adviso...
Published on Jul 16, 2012
X64X86
MS12-A06
Q2719662U
OS
–
none
2
An update is available tha...
Published on Dec 12, 2013
X64
MSWU-865
KB2905454
OS
–
none
2
Adobe Shockwave 12.3.4....
Published on Jun 11, 2018
X86
SW12-34204
QSW1234204
Application
90521
37 more...
none
2
Security updates availabl...
Published on Dec 10, 2018
X86
AAIR18-320089
QAIR320089
Application
370065
96 more...
none
3
February 7, 2017, update ...
Published on Feb 06, 2017
X64
MSWU-2292
KB3114389
Application
–
Critical
1

Hacktales

STEP 6: VERIFY

Double-check success of the process.

Check if the previous phases have been successfully implemented.



Hacktales

VMDR Dashboard

Module 3: Vulnerability Management
Cybersecurity Foundation Program

Date:
May 10, 2025

Hacktales

Got Questions?

Module 3: Vulnerability Management
Cybersecurity Foundation Program

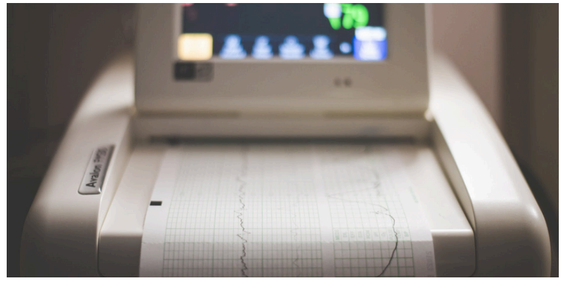
03 Vulnerability Management

Objectives

Hacktales

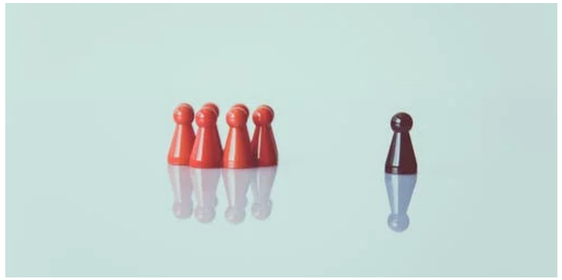
01

At the end of this section, students will learn how vulnerability scanners work.



02

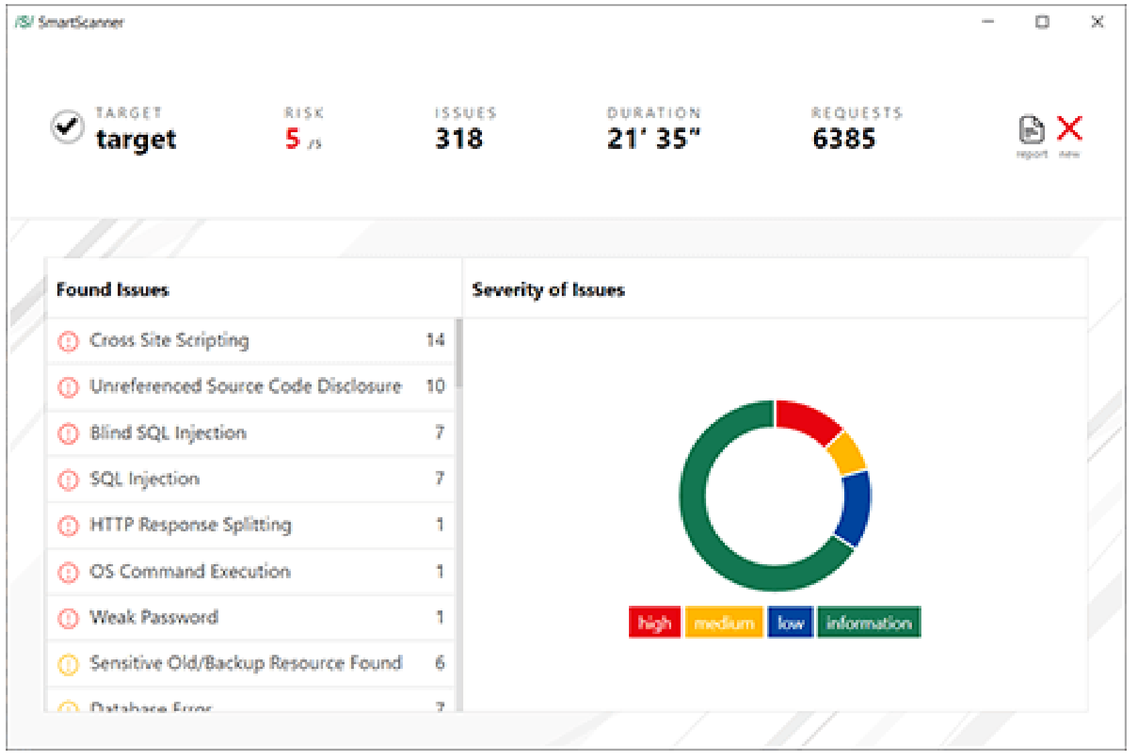
Students will understand the impact of patch management in the vulnerability management lifecycle.



03

Students will review the Qualys cloud platform to learn how to manage vulnerabilities.

Hacktales



Vulnerability Scanner

Scanners sit at the heart of a vulnerability management program.

Module 3: Vulnerability Management
Cybersecurity Foundation Program

Date:
May 10, 2025

Hacktales

Vulnerability Database

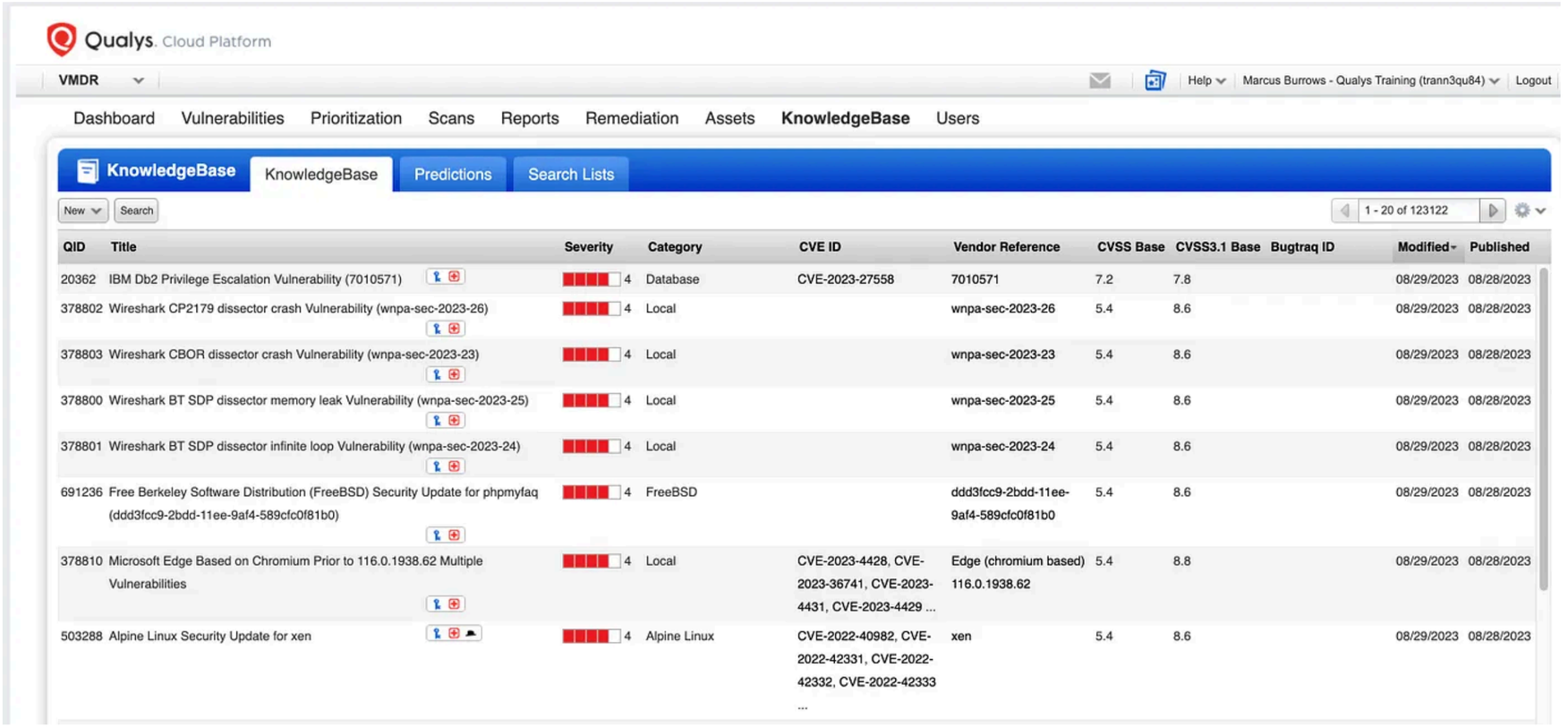
A platform aimed at collecting, maintaining, and disseminating information about discovered computer security vulnerabilities.

Module 3: Vulnerability Management
Cybersecurity Foundation Program

Date:
May 10, 2025

Qualys Knowledgebase

Hacktales



QID	Title	Severity	Category	CVE ID	Vendor Reference	CVSS Base	CVSS3.1 Base	Bugtraq ID	Modified	Published
20362	IBM Db2 Privilege Escalation Vulnerability (7010571)	4	Database	CVE-2023-27558	7010571	7.2	7.8		08/29/2023	08/28/2023
378802	Wireshark CP2179 dissector crash Vulnerability (wnpa-sec-2023-26)	4	Local		wnpa-sec-2023-26	5.4	8.6		08/29/2023	08/28/2023
378803	Wireshark CBOR dissector crash Vulnerability (wnpa-sec-2023-23)	4	Local		wnpa-sec-2023-23	5.4	8.6		08/29/2023	08/28/2023
378800	Wireshark BT SDP dissector memory leak Vulnerability (wnpa-sec-2023-25)	4	Local		wnpa-sec-2023-25	5.4	8.6		08/29/2023	08/28/2023
378801	Wireshark BT SDP dissector infinite loop Vulnerability (wnpa-sec-2023-24)	4	Local		wnpa-sec-2023-24	5.4	8.6		08/29/2023	08/28/2023
691236	Free Berkeley Software Distribution (FreeBSD) Security Update for phpmyfaq (ddd3fcc9-2bdd-11ee-9af4-589cfc0f81b0)	4	FreeBSD		ddd3fcc9-2bdd-11ee-9af4-589cfc0f81b0	5.4	8.6		08/29/2023	08/28/2023
378810	Microsoft Edge Based on Chromium Prior to 116.0.1938.62 Multiple Vulnerabilities	4	Local	CVE-2023-4428, CVE-2023-36741, CVE-2023-4431, CVE-2023-4429 ...	Edge (chromium based) 116.0.1938.62	5.4	8.8		08/29/2023	08/28/2023
503288	Alpine Linux Security Update for xen	4	Alpine Linux	CVE-2022-40982, CVE-2022-42331, CVE-2022-42332, CVE-2022-42333 ...	xen	5.4	8.6		08/29/2023	08/28/2023

Hacktales

Types of Vulnerability Databases

1. MITRE'S CVE
2. NIST's NVD
3. OSVDB

Hacktales

Vulnerability Assessment Workshop

Qualys Cloud Platform

Module 3: Vulnerability Management
Cybersecurity Foundation Program

Hacktales

Security Patch

A security patch is software that corrects errors in computer software code.

Types: Hotfix, Point Release, Service Pack.

Module 3: Vulnerability Management
Cybersecurity Foundation Program

Date:
May 10, 2025

Hacktales

Patch Management Process

EVALUATION
Determine whether a given patch is applicable.

PATCH TESTING
Check if the patch causes problems such as system instability.

APPROVAL
After successful testing, approve a specific patch for application.

Hacktales

Patch Management Process

DEPLOYMENT

Apply the patches on live systems.

VERIFICATION AND TESTING

Test and audit systems after deployment to see if the patches were applied correctly, and that there were no unforeseen side effects.

Hacktales

Got Questions?

Module 3: Vulnerability Management
Cybersecurity Foundation Program