UI Design | Dashboard | Cybersecurity

# Overview

RiskPrism is a cybersecurity platform that unifies multiple security tools into one intelligent system.

It helps organizations identify, assess, and prioritize vulnerabilities through AI-driven analytics, dashboards, and risk scoring for better visibility and decision-making.

| Project: | Category: | year: |
|---|---|---|
| RiskPrism | Cybersecurity | 2025 |

# Typography & Color

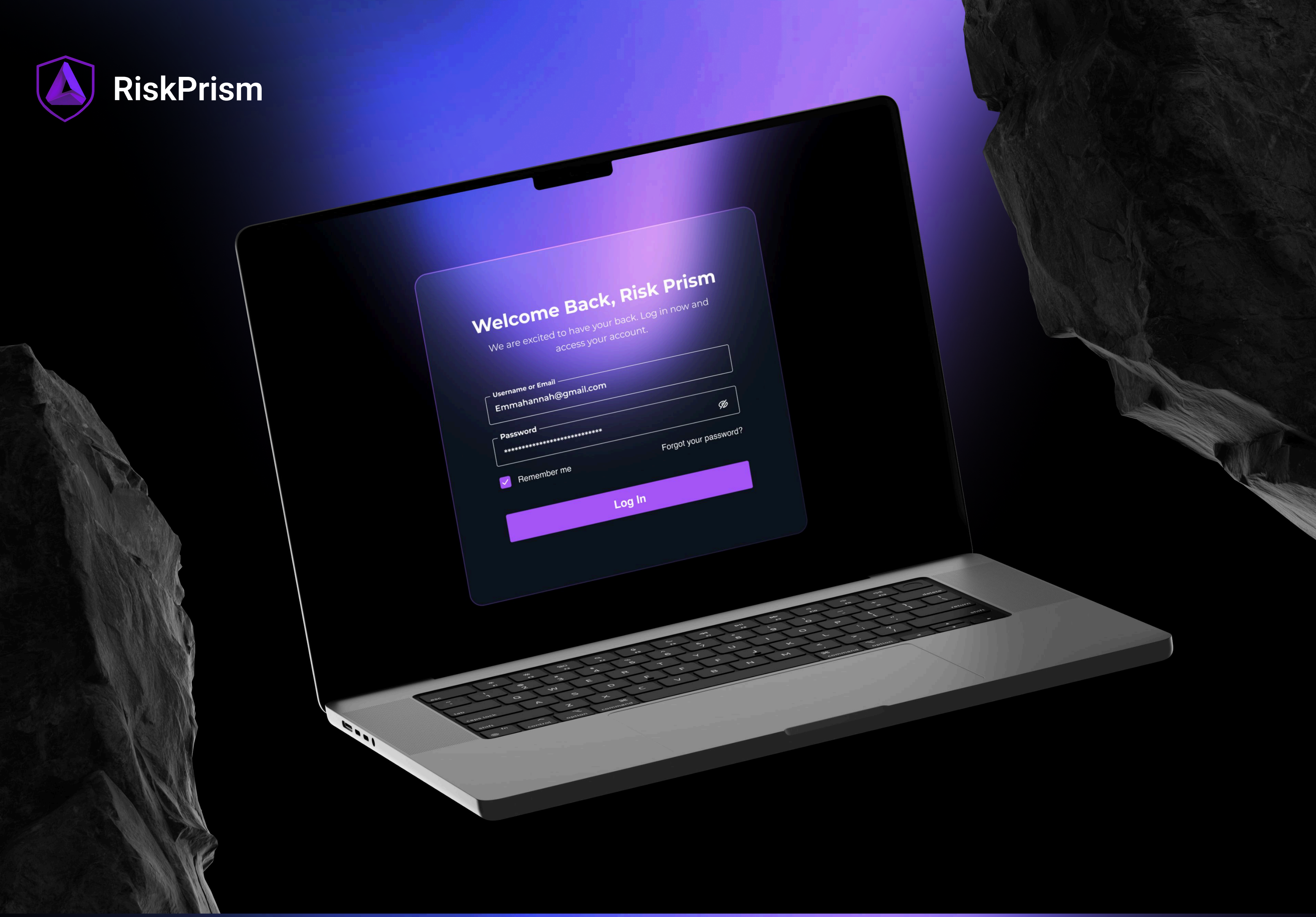
## Montserrat

ABCDEFGHIJKLMN
OPQRSTUVWXYZ -
0123456789

| Heading 1 | 30px | Sub heading | 20px | Body | 14px |
|---|---|---|---|---|---|

| Helitrope | Black | Off White | White |
|---|---|---|---|
| #9847EB | #000000 | #FAFAFA | #FFFFFF |

**RiskPrism**


Welcome Back, Risk Prism
We are excited to have your back. Log in now and access your account.
Log In

# DESIGN PROCESS

1 Sprint → **Research** Discovery

2 Sprint → **Wireframes** Define

3 Sprint → **Analysis** Discovery

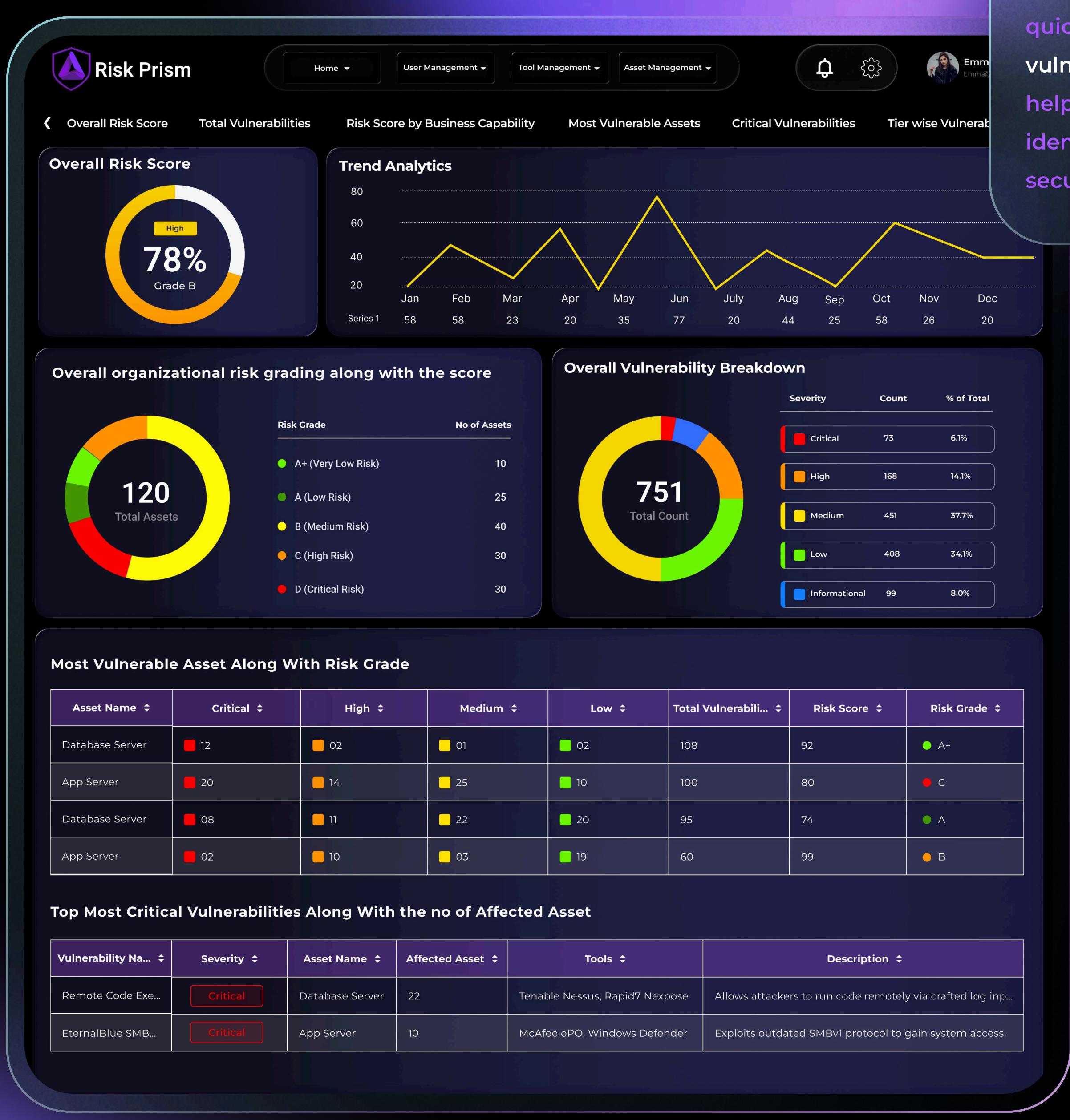
4 Sprint → **UI Design** Develop

## Scope Of Work

From initial research to final design, we've guided the process step by step—empowering the user to confidently test and shape the finished product.

# Dashboard

The RiskPrism dashboard gives a quick view of overall risk, vulnerabilities, and asset grading. It helps teams monitor trends, identify critical issues, and prioritize security actions efficiently.



| | Jan | Feb | Mar | Apr | May | Jun | July | Aug | Sep | Oct | Nov | Dec |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Series 1 | 58 | 58 | 23 | 20 | 35 | 77 | 20 | 44 | 25 | 58 | 26 | 20 |

| Risk Grade | No of Assets |
|---|---|
| A+ (Very Low Risk) | 10 |
| A (Low Risk) | 25 |
| B (Medium Risk) | 40 |
| C (High Risk) | 30 |
| D (Critical Risk) | 30 |

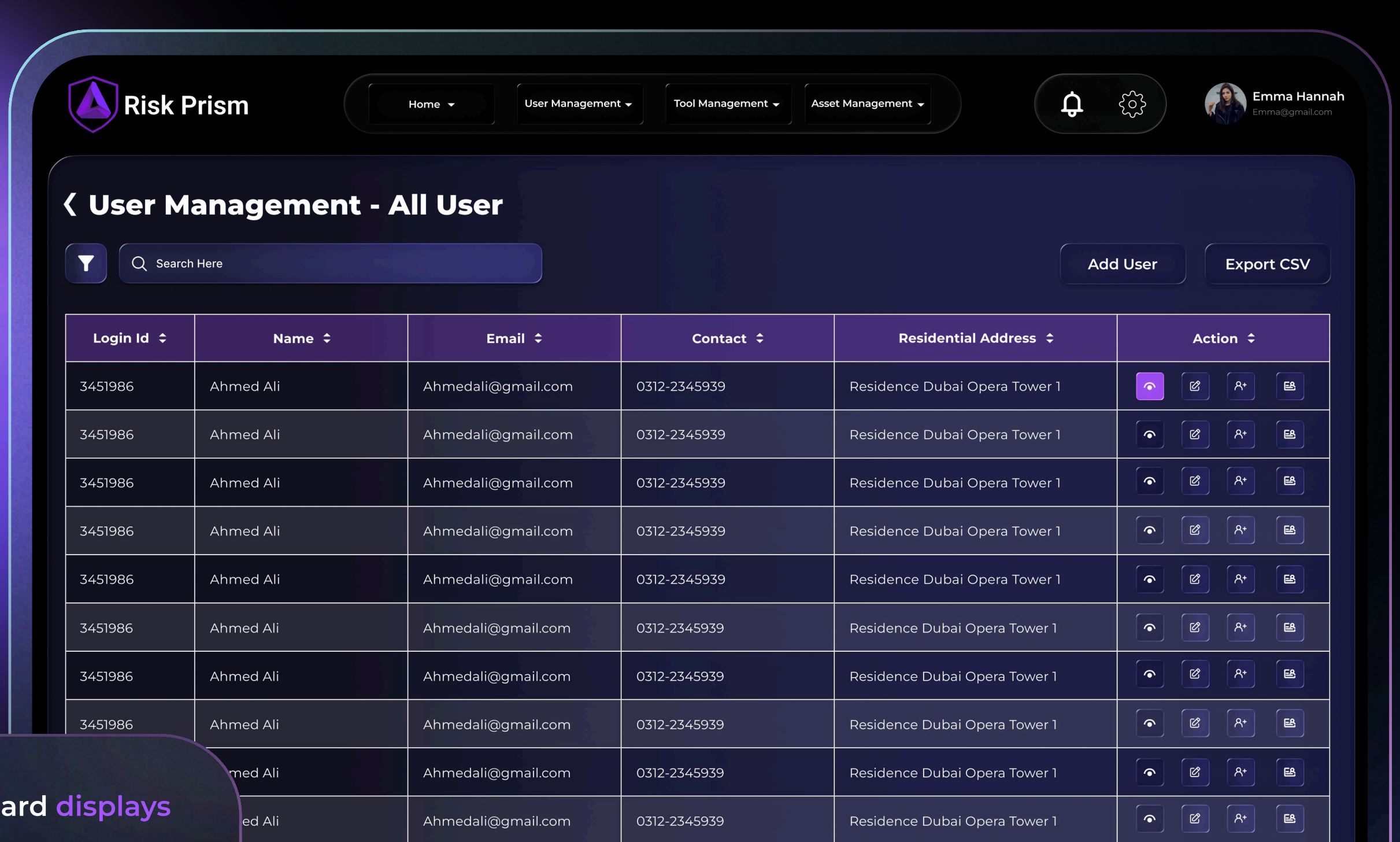
| Severity | Count | % of Total |
|---|---|---|
| Critical | 73 | 6.1% |
| High | 168 | 14.1% |
| Medium | 451 | 37.7% |
| Low | 408 | 34.1% |
| Informational | 99 | 8.0% |

Most Vulnerable Asset Along With Risk Grade

| Asset Name | Critical | High | Medium | Low | Total Vulnerabili... | Risk Score | Risk Grade |
|---|---|---|---|---|---|---|---|
| Database Server | 12 | 02 | 01 | 02 | 108 | 92 | A+ |
| App Server | 20 | 14 | 25 | 10 | 100 | 80 | C |
| Database Server | 08 | 11 | 22 | 20 | 95 | 74 | A |
| App Server | 02 | 10 | 03 | 19 | 60 | 99 | B |

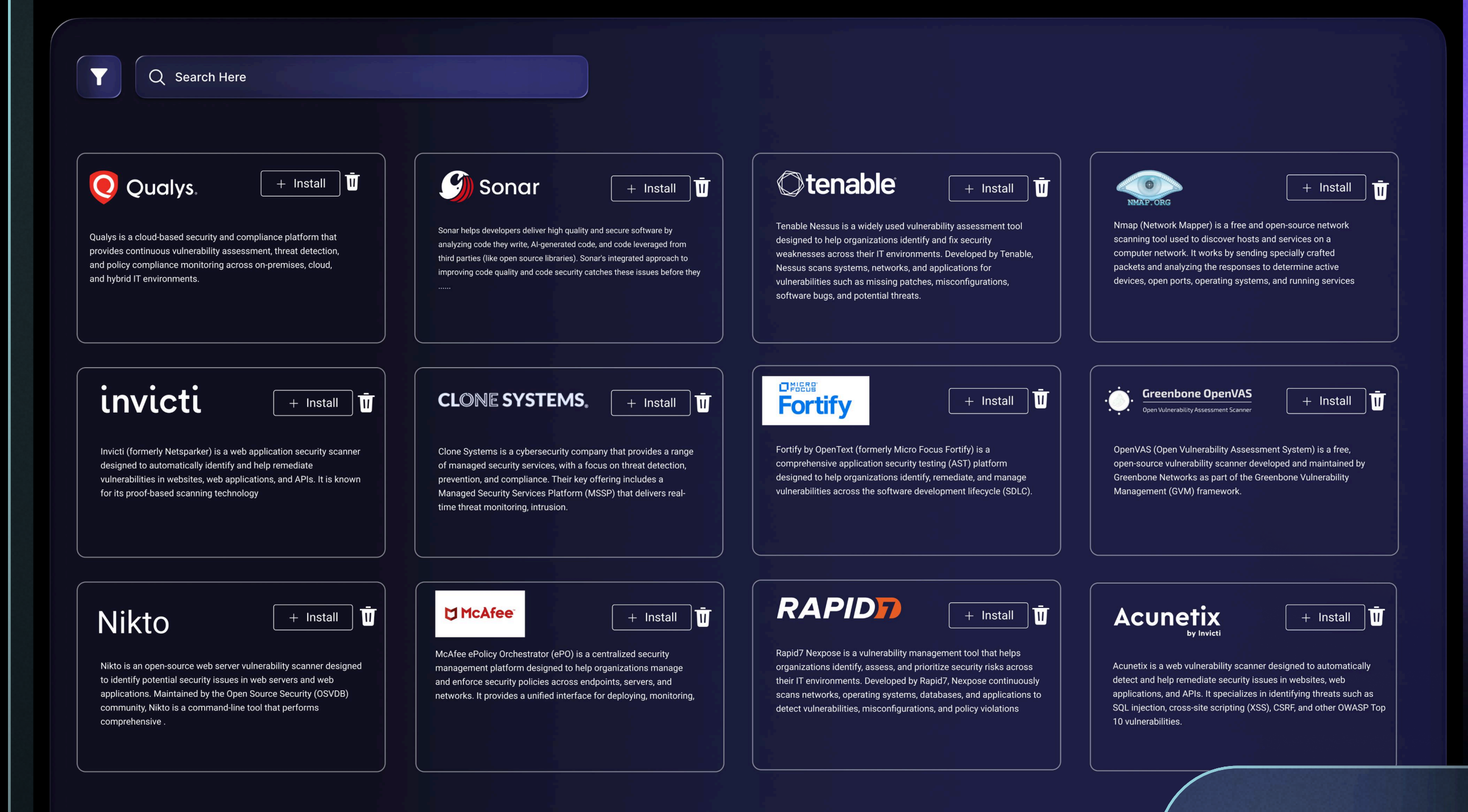
Top Most Critical Vulnerabilities Along With the no of Affected Asset

| Vulnerability Na... | Severity | Asset Name | Affected Asset | Tools | Description |
|---|---|---|---|---|---|
| Remote Code Exe... | Critical | Database Server | 22 | Tenable Nessus, Rapid7 Nexpose | Allows attackers to run code remotely via crafted log inp... |
| EternalBlue SMB... | Critical | App Server | 10 | McAfee ePO, Windows Defender | Exploits outdated SMBv1 protocol to gain system access. |



| Login Id | Name | Email | Contact | Residential Address | Action |
|---|---|---|---|---|---|
| 3451986 | Ahmed Ali | Ahmedali@gmail.com | 0312-2345939 | Residence Dubai Opera Tower 1 | |
| 3451986 | Ahmed Ali | Ahmedali@gmail.com | 0312-2345939 | Residence Dubai Opera Tower 1 | |
| 3451986 | Ahmed Ali | Ahmedali@gmail.com | 0312-2345939 | Residence Dubai Opera Tower 1 | |
| 3451986 | Ahmed Ali | Ahmedali@gmail.com | 0312-2345939 | Residence Dubai Opera Tower 1 | |
| 3451986 | Ahmed Ali | Ahmedali@gmail.com | 0312-2345939 | Residence Dubai Opera Tower 1 | |
| 3451986 | Ahmed Ali | Ahmedali@gmail.com | 0312-2345939 | Residence Dubai Opera Tower 1 | |
| 3451986 | Ahmed Ali | Ahmedali@gmail.com | 0312-2345939 | Residence Dubai Opera Tower 1 | |
| 3451986 | Ahmed Ali | Ahmedali@gmail.com | 0312-2345939 | Residence Dubai Opera Tower 1 | |
| | med Ali | Ahmedali@gmail.com | 0312-2345939 | Residence Dubai Opera Tower 1 | |
| | ed Ali | Ahmedali@gmail.com | 0312-2345939 | Residence Dubai Opera Tower 1 | |

The User Management dashboard displays all registered users with details like login ID, name, email, contact, and address. It allows admins to add new users, edit details, export data, and manage user access efficiently.



**Qualys** — Qualys is a cloud-based security and compliance platform that provides continuous vulnerability assessment, threat detection, and policy compliance monitoring across on-premises, cloud, and hybrid IT environments.

**Sonar** — Sonar helps developers deliver high quality and secure software by analyzing code they write, AI-generated code, and code leveraged from third parties (like open source libraries). Sonar's integrated approach to improving code quality and code security catches these issues before they ......

**tenable** — Tenable Nessus is a widely used vulnerability assessment tool designed to help organizations identify and fix security weaknesses across their IT environments. Developed by Tenable, Nessus scans systems, networks, and applications for vulnerabilities such as missing patches, misconfigurations, software bugs, and potential threats.

**NMAP.ORG** — Nmap (Network Mapper) is a free and open-source network scanning tool used to discover hosts and services on a computer network. It works by sending specially crafted packets and analyzing the responses to determine active devices, open ports, operating systems, and running services

**invicti** — Invicti (formerly Netsparker) is a web application security scanner designed to automatically identify and help remediate vulnerabilities in websites, web applications, and APIs. It is known for its proof-based scanning technology

**CLONE SYSTEMS** — Clone Systems is a cybersecurity company that provides a range of managed security services, with a focus on threat detection, prevention, and compliance. Their key offering includes a Managed Security Services Platform (MSSP) that delivers real-time threat monitoring, intrusion.

**MICRO FOCUS Fortify** — Fortify by OpenText (formerly Micro Focus Fortify) is a comprehensive application security testing (AST) platform designed to help organizations identify, remediate, and manage vulnerabilities across the software development lifecycle (SDLC).

**Greenbone OpenVAS** (Open Vulnerability Assessment Scanner) — OpenVAS (Open Vulnerability Assessment System) is a free, open-source vulnerability scanner developed and maintained by Greenbone Networks as part of the Greenbone Vulnerability Management (GVM) framework.

**Nikto** — Nikto is an open-source web server vulnerability scanner designed to identify potential security issues in web servers and web applications. Maintained by the Open Source Security (OSVDB) community, Nikto is a command-line tool that performs comprehensive .

**McAfee** — McAfee ePolicy Orchestrator (ePO) is a centralized security management platform designed to help organizations manage and enforce security policies across endpoints, servers, and networks. It provides a unified interface for deploying, monitoring,

**RAPID7** — Rapid7 Nexpose is a vulnerability management tool that helps organizations identify, assess, and prioritize security risks across their IT environments. Developed by Rapid7, Nexpose continuously scans networks, operating systems, databases, and applications to detect vulnerabilities, misconfigurations, and policy violations

**Acunetix** by Invicti — Acunetix is a web vulnerability scanner designed to automatically detect and help remediate security issues in websites, web applications, and APIs. It specializes in identifying threats such as SQL injection, cross-site scripting (XSS), CSRF, and other OWASP Top 10 vulnerabilities.

The Tool Integration screen lets admins connect and manage security tools like Qualys, Nessus, and SonarQube, showing each tool's status, sync time, and data flow for centralized control.

**RiskPrism**

# Thanks For Scrolling