Lab: Review X-Force Exchange Threat Reports

Estimated time: 5 minutes

Introduction

IBM X-Force Exchange is a threat intelligence sharing platform. It provides insights into global security threats. It also provides users access to trends, methods used by threat actors, and a vast repository of threat intelligence data.

Purpose of IBM X-Force Exchange

The site provides detailed reports on vulnerabilities, malware, and other cyberthreats that can be used for understanding and mitigating security threats.

Learning objectives

After completing this lab, you will be able to:

- Explore the IBM X-Force Exchange site to understand its purpose
- Amalyze the type of information available, how to use this information, and the concept of CVE numbers

---

Exploring the IBM X-Force Exchange site

1. Navigating the homepage

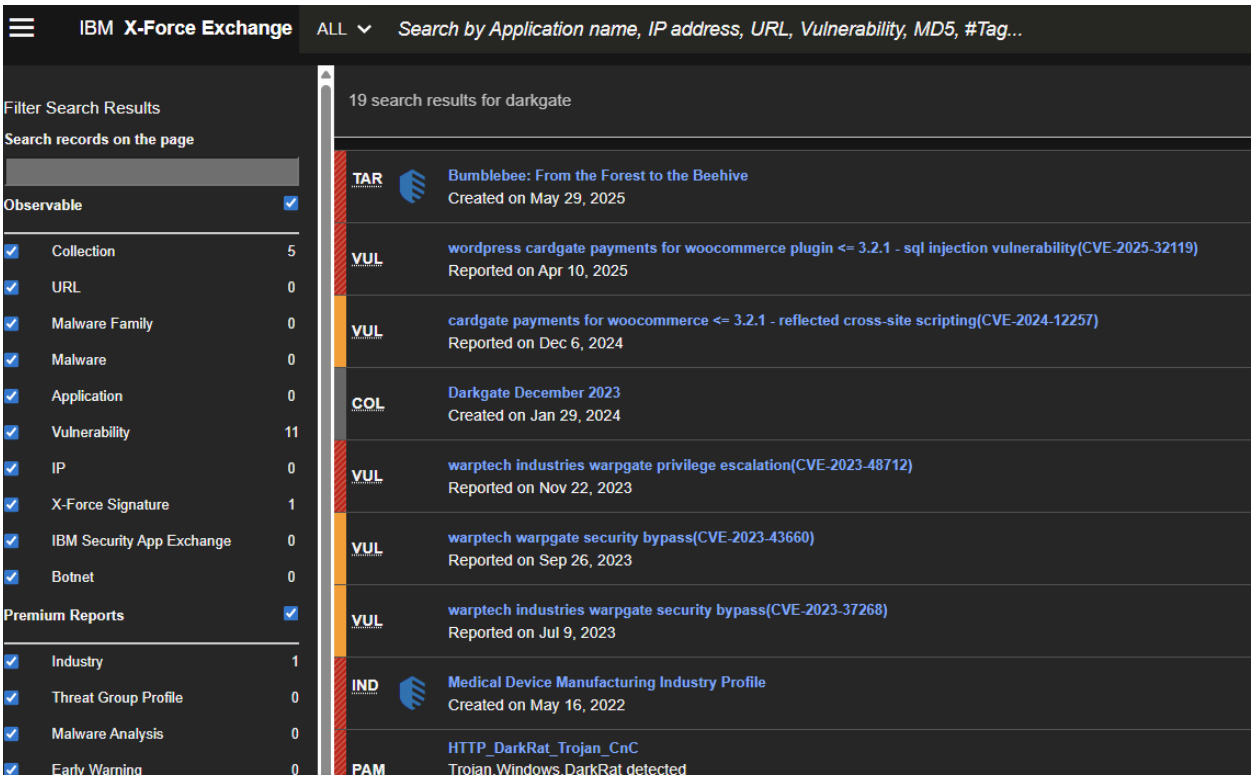
- Visit the IBM X-Force Exchange site.
- You can take a few moments to explore the homepage. You will notice different sections such as **Threat Intelligence Index**, **Industry Reports**, and **Collections.**

2. Searching for information

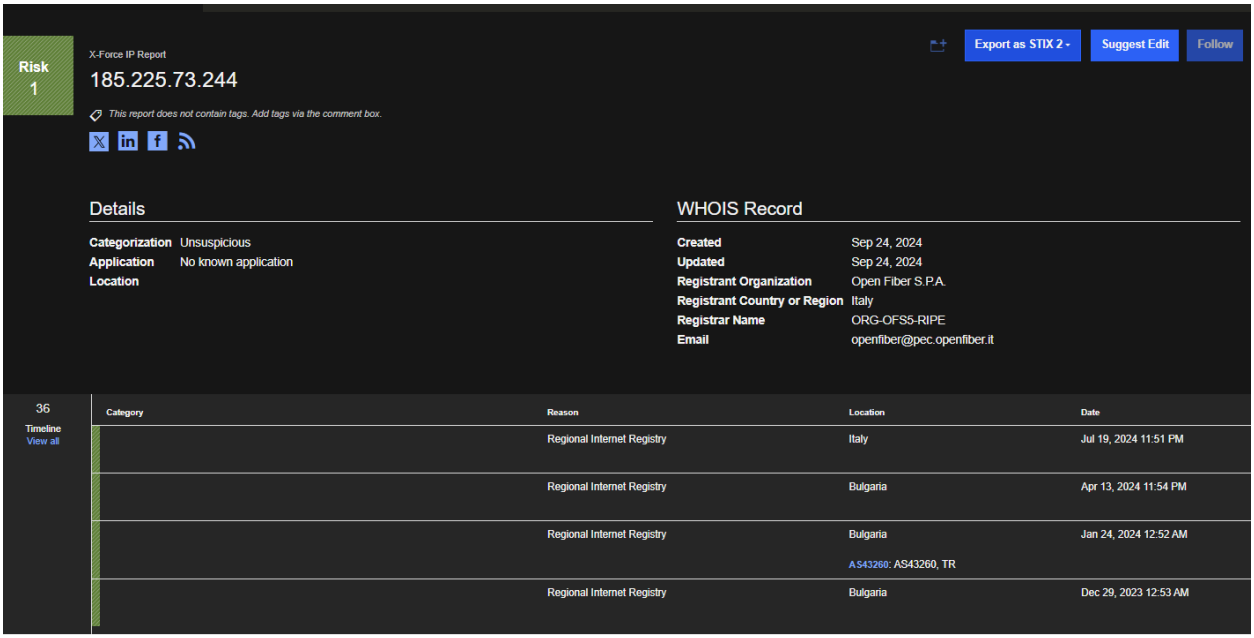
- Use the search bar to look up specific threats, vulnerabilities, or malware.

Example: Search for a recent malware name or a specific IP address to see related reports and collections.

Recent Malware Name: `DarkGate`
DarkGate is a prominent malware variant active in 2024–2025, often distributed through phishing emails and fake software installers. It includes remote access trojan (RAT) capabilities, data exfiltration, and keylogging



Suspicious IP Address Example: `185.225.73.244`
This IP has been reported in threat intelligence sources as being associated with command-and-control infrastructure for malware campaigns (including QakBot variants).



3. Understanding the information

Types of information available:

- **Threat intelligence reports:** Detailed analyses of specific threats, including methods and tools used by attackers

  These provided detailed analysis of specific threats, including attacker tactic tools, and behavior patterns.

- **Vulnerability reports:** Information on known vulnerabilities, including CVE numbers, descriptions, and potential impacts

  These included CVE numbers (e.g., CVE-2025-32119) with descriptions and severity assessments, useful for vulnerability management and patch planning.

- **Malware analysis:** Reports on various malware, including their behavior, indicators of compromise (IOCs), and mitigation strategies.

  These reports described how malware operates, listed indicators of compromise (IOC's) and outlined strategies for mitigation.

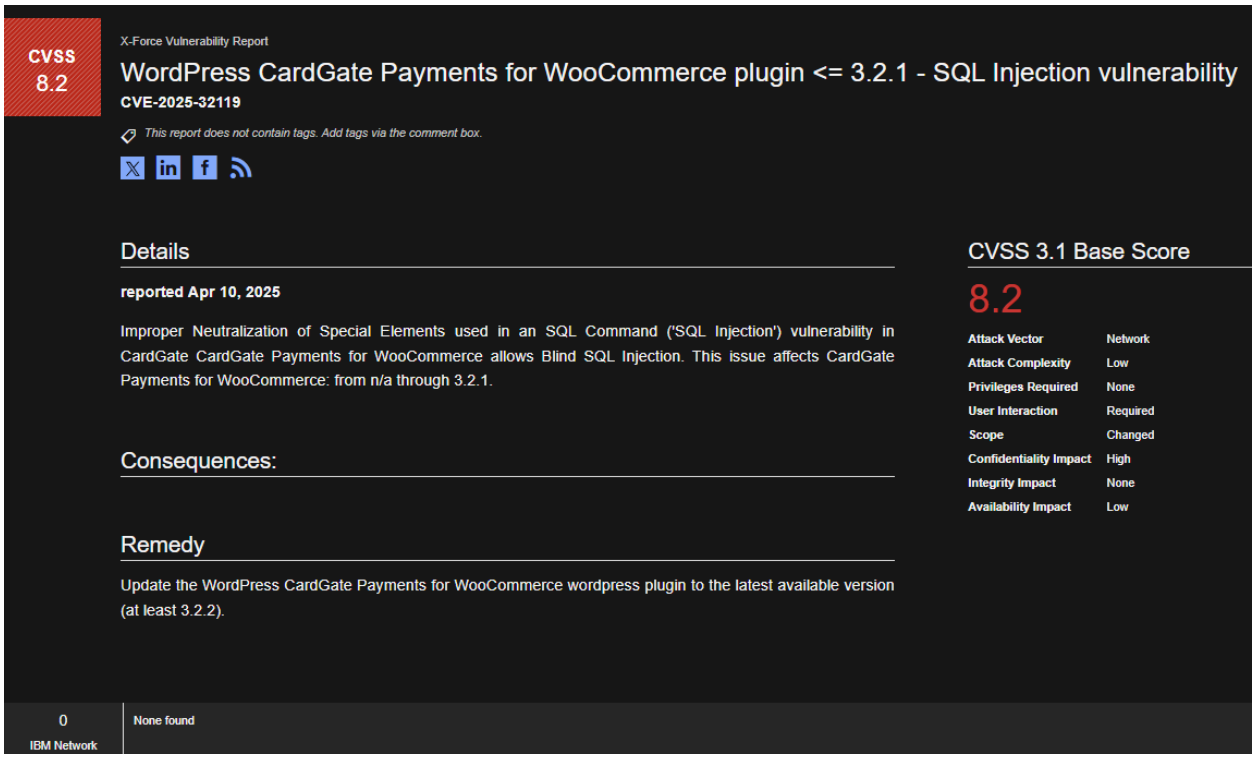
4. Exploring CVE numbers

- **What are CVE numbers?**
  CVE stands for Common Vulnerabilities and Exposures. It is a list of publicly disclosed computer security flaws. Each CVE entry contains a unique identifier (e.g., CVE-2024-12345), a brief description, and references to related vulnerability reports and advisories.

- **Importance of CVE numbers**
  CVE numbers provide a standardized way to reference known vulnerabilities, making it easier for security professionals to share and access information across different platforms and reports.

5. Analyzing a CVE report

- Run a search for "CVE number" in the top search bar and notice the results.



- Analyze a report by selecting a CVE report from your search results.

CVE Report Analysis: CVE-2025-32119

As part of the lab, I searched for and reviewed a vulnerability report using a CVE number. I selected CVE-2025-32119, which details a SQL Injection vulnerability in the WordPress GardGate Payments for WooCommerce plugin (versions ≤ 3.2.1).

- Identify the key components of the report, such as the description of the vulnerability, affected systems, and recommended mitigation steps.

Findings from the report:

- *Vulnerability type: Improper Neutralization of Special Elements used in an SQL Command*
- *Risk score (CVSS 3.1): 8.2 – High Severity*
- *Attack Vector: Network*
- *Attack complexity: Low*
- *Privileges required: None*
- *User interaction: Required*
- *Confidentiality impact: High*
- *Remedy: Update to version 3.2.2 or later.*

- Think about how the information in the CVE report can be used to protect an organization's systems and data.

This report demonstrates how attackers could exploit a common web application vulnerability (SQL injection) to gain unauthorized access or manipulate database content. The standardized CVE format allows teams to quickly access severity and determine patch priorities, helping organizations proactively secure their systems.

Resource: https://www.ibm.com/support/pages/using-ibm-x-force-exchange-xfe-portal-understand-threats-vulnerabilities-or-malware

Summary

In this lab, you performed an activity that provided you with a comprehensive understanding of the IBM X-Force Exchange site, the type of information it offers, and the significance of CVE numbers in cybersecurity.