Shariful Islam

ID: 2111252

21 Sep 2024

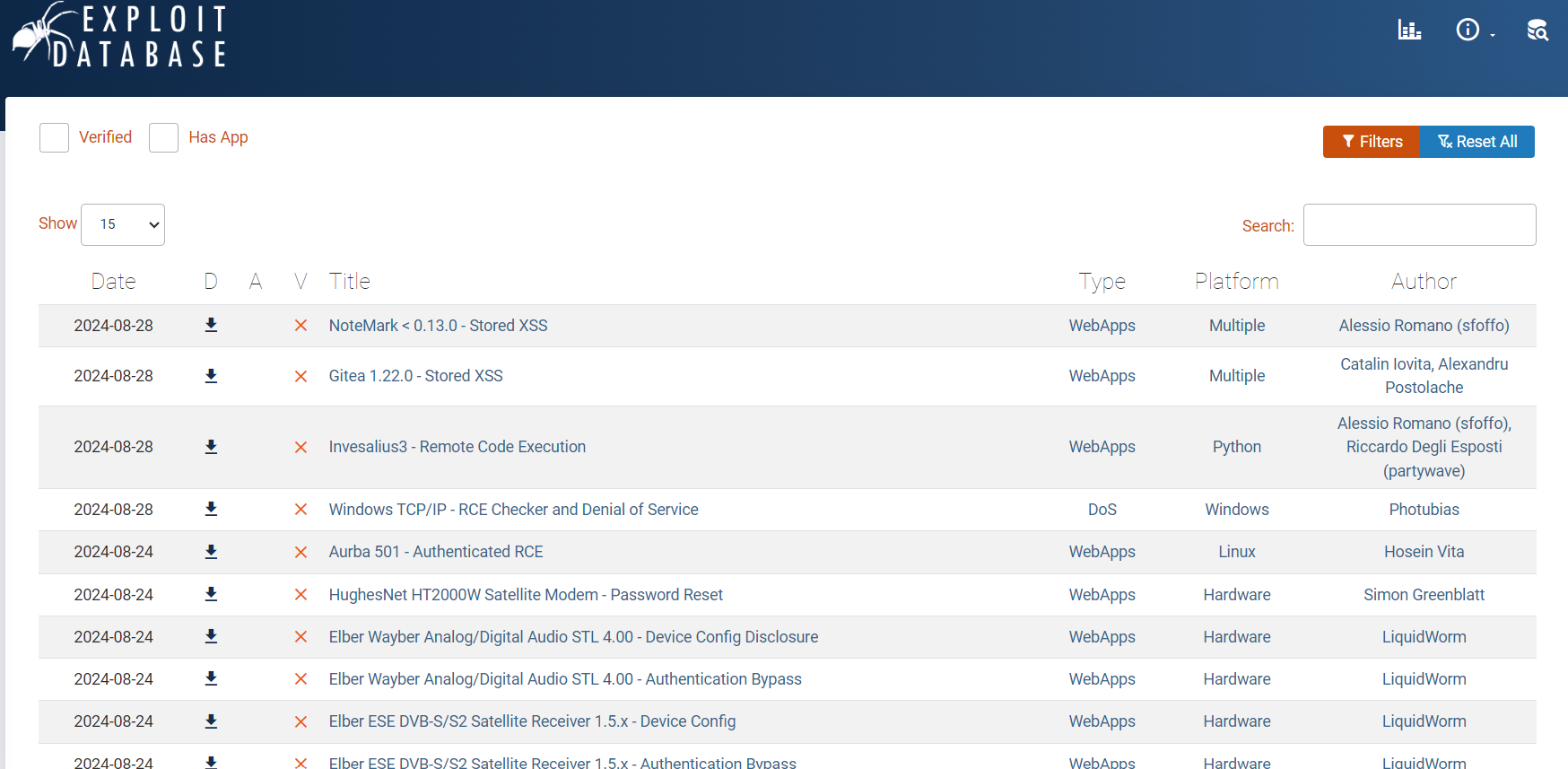
Assignment no 2: **OSINT Framework**

**Three (3) Topic about Threat Intelligence:**

1. **Threat Intelligence 🡪 TTPs 🡪 Malware Exploit TTP Database:**

The TTP (Tactics, Techniques, and Procedures) Database refers to a structured way to understand and classify the behavior of cyber adversaries. TTPs help cybersecurity teams to identify and respond to cyberattacks by analyzing the methods and patterns used by threat actors. These frameworks can be used for activities like threat hunting, malware detection, and exploit analysis.

For example, MITRE's ATT&CK Framework is widely recognized for its comprehensive collection of real-world attack techniques used by adversaries.



*Fig: Exploit TTP Database*



*Fig: MITRE’s ATT&CK: Real-world att&ck techniques*

1. **Threat Intelligence 🡪 Malware Information Sharing Platform:**

The Malware Information Sharing Platform (MISP) is an open-source threat intelligence platform that facilitates the sharing, storing, and correlation of indicators of compromise (IOCs) related to malware, cybersecurity threats, and vulnerability information.

**Key Features of MISP:**

* Threat Intelligence Sharing
* Automation and Integration
* Correlation Engine
* Taxonomy and Tagging
* Community-Driven

**Use Case:**

* Reverse Engineering

1. **Threat Intelligence 🡪** **Malware Patrol:**

Malware Patrol is a cybersecurity service provider that specializes in malware intelligence, threat feeds, and cybersecurity solutions to help organizations protect themselves from cyber threats.

**Key Services Offered by Malware Patrol:**

* Threat Data Feeds
* Malware Analysis
* Phishing Detection

**Use Cases:**

* Enterprises
* Researchers

**Malware Patrol’s evaluation portal provides:**

* Anti-Cryptomining
* Bitcoin Block chain Strings
* Bitcoin Transactions
* C2 Addresses
* Domain Names Generated via DGAs
* DNS-over-HTTPS (DoH) Servers
* DNS RPZ Firewall
* Integration Feeds: Fortinet / MISP / PAN-OS
* Intrusion Insights
* Malicious IPs
* Malware & Ransomware URLs
* Malware Hashes
* Malware Samples (Binaries)
* Newly Registered Domains
* Phishing
* Phishing Screenshots and Raw HTML
* Scam Domains