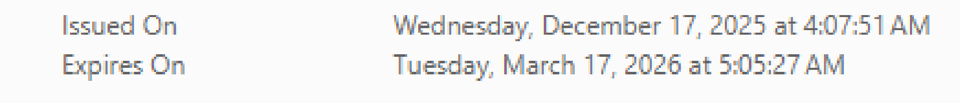
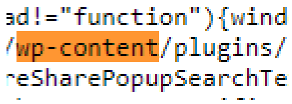
Headline: Cyber Risk Data Collection & Verification Methodology Target Entity: Cavite State University (Public Sector)

1. OBJECTIVE To demonstrate the "Passive Reconnaissance" methodology used for collecting, verifying, and assessing cyber risk indicators as part of an automated Threat Intelligence workflow. This case study focuses on verifying Encryption Standards (SSL), Content Management Systems (CMS), and Network Visibility.

2. DATA COLLECTION & VERIFICATION LOG

Risk Indicator	**Raw Data Findings**	**Verification Method**	**Analyst Assessment**
SSL / TLS Certificate	**Issuer:** Google Trust Services **Expires:** March 17, 2026	**Browser Handshake Analysis:** Verified via Chrome Security Module. Confirmed certificate chain of trust is valid for >1 year.	**LOW RISK** The entity maintains a robust encryption standard with automatic renewal protocols via Google Trust Services.
	 Issued On Expires On	Wednesday, December 17, 2025 at 4:07:51 AM Tuesday, March 17, 2026 at 5:05:27 AM	

Web Technology (CMS)	**Detected:** WordPress	**Source Code Inspection:**
		 `ad!="function"){wind`
		`/wp-content/plugins/`
		`reSharePopupSearchTe`
		Identified /wp-content/ directory and super-socializer plugin script in HTML source code (Line 17).
			MEDIUM RISK
			WordPress requires strict patch management. The presence of third-party plugins increases the potential attack surface if not updated.

Risk Indicator	**Raw Data Findings**	**Verification Method**	**Analyst Assessment**
Network Visibility	**Status:** ICMP Request Timed Out	**Command Line (Ping):** Attempted standard echo request to cvsu.edu.ph. No response received.	**LOW RISK** The server appears to be behind a firewall or security group that blocks ICMP packets, reducing visibility to potential scanners.

3. METHODOLOGY & PROTOCOL

Collection: Data was gathered using non-intrusive, passive scanning techniques to comply with ethical OSINT standards.

Verification: All automated findings were cross-referenced manually.

SSL Verification: Cross-referenced against the browser's trusted root store.

CMS Verification: Confirmed by locating specific directory paths in the DOM (Document Object Model).

Root Cause Analysis: The inability to resolve the server IP via Ping was analyzed not as a failure, but as a security configuration (Firewall/ICMP Blocking), indicating an active defensive posture.

4. TOOLS USED

Browser DevTools: For DOM/Source Code inspection.

Network Terminals: For connectivity testing.

Python (In Development): Automating this specific verification logic for high-volume analysis.