Built a Python-Based Domain Risk Scanner { Multi-Layered Phishing Defense Tool}

I created a command-line Python tool that analyzes domain, URL, or IP risk using a smart, multi-tiered detection architecture:

**Domain Age Check (WHOIS + RDAP):** Determines domain registration age and flags "new" domains (typical phishing start point). It uses RDAP fallback when WHOIS data is unavailable.

**SSL/TLS Inspection:** Establishes HTTPS connection, checks certificate validity and expiry, and extracts issuer details accurately.

**Content Analysis:** Scrapes for phishing indicators like password/login forms, POST forms, and high frequencies of keywords (“login”, “OTP”, “bank”, etc. which are common phishing tactics).

Heuristic Checks: Identifies suspicious behaviors such as rare TLDs, IP-based domains, or deep subdomain patterns often used in scam campaigns.

**Optional Reputation APIs:** Integrates with VirusTotal and Google Safe Browsing Lookup to cross-check domains against known malicious threats for added context.

**Composite Risk Scoring & Verdict:** Aggregates all signal layers into a final risk score and categorizes targets as LOW, MEDIUM, or HIGH RISK.

**Why It Matters:**

Phishing is a dominant factor in today’s cyber landscape, causing 36% of data breaches and accounting for roughly 80–95% of attack chains. Human error plays a critical role too with over 95% of security incidents involving some form of social engineering or misjudgment.

This tool empowers cybersecurity professionals to detect threats proactively through layered analysis, blending domain metadata, SSL validation, content scrutiny, and global reputation feeds to identify phishing infrastructure before it causes damage.