From Vulnerability Descriptions to ATT&CK Techniques

Complementary Ranking and Multi-Level Evidence Verification

Research Overview

Map vulnerability descriptions to plausible MITRE ATT&CK techniques, then examine selected mappings using progressively more specific evidence.

Goals

- Improve the ranking of primary-impact techniques.
- Assess selected mappings using documentary, artifact, and execution evidence.
- Record technique support, impact role, and attribution limits.

Dataset

- **459** selected CVEs from the CIRCL dataset.
- **546** primary-impact CVE–technique reference pairs.
- Frozen catalogue of **201** parent techniques.
- Prediction input: the original vulnerability description.

Known local demonstration, development, and earlier evaluation CVEs were excluded. This selected cohort is not CIRCL's official test split.

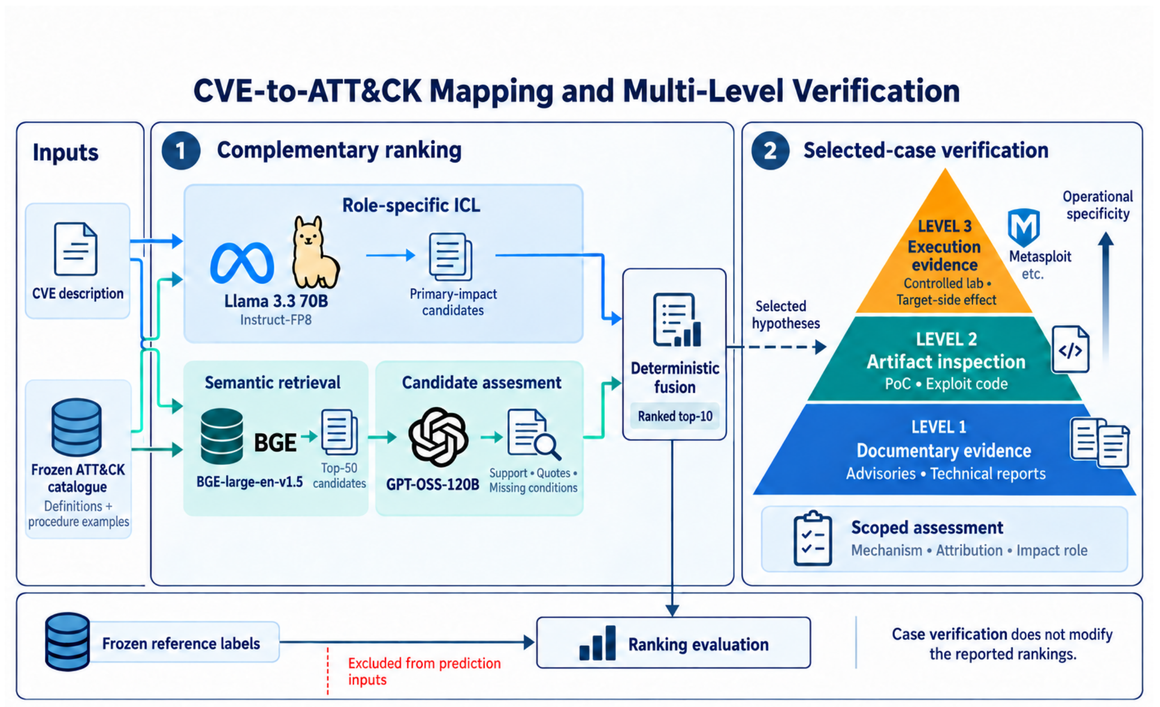
Methods

Complementary prediction: Combine role-specific in-context learning (Llama 3.3 70B) with semantic retrieval (BGE-large-en-v1.5).
Candidate assessment: Use GPT-OSS-120B to assess retrieved candidates against the vulnerability description, recording support, evidence quotes, and missing requirements.
Ranking integration: Interleave the two rankings to produce up to ten candidate techniques.
Multi-level verification: Examine selected hypotheses through documentary evidence, exploit-code inspection, and controlled laboratory observations.

Component Analysis

- Direct ICL + retrieval fusion: 36.75% MAP@10.
- ICL + assessed retrieval: 40.92% MAP@10.
- Assessment improved fusion by 4.17 percentage points [95% interval: 3.08–5.32].

This supports the implemented assessment stage.



Ranking Performance

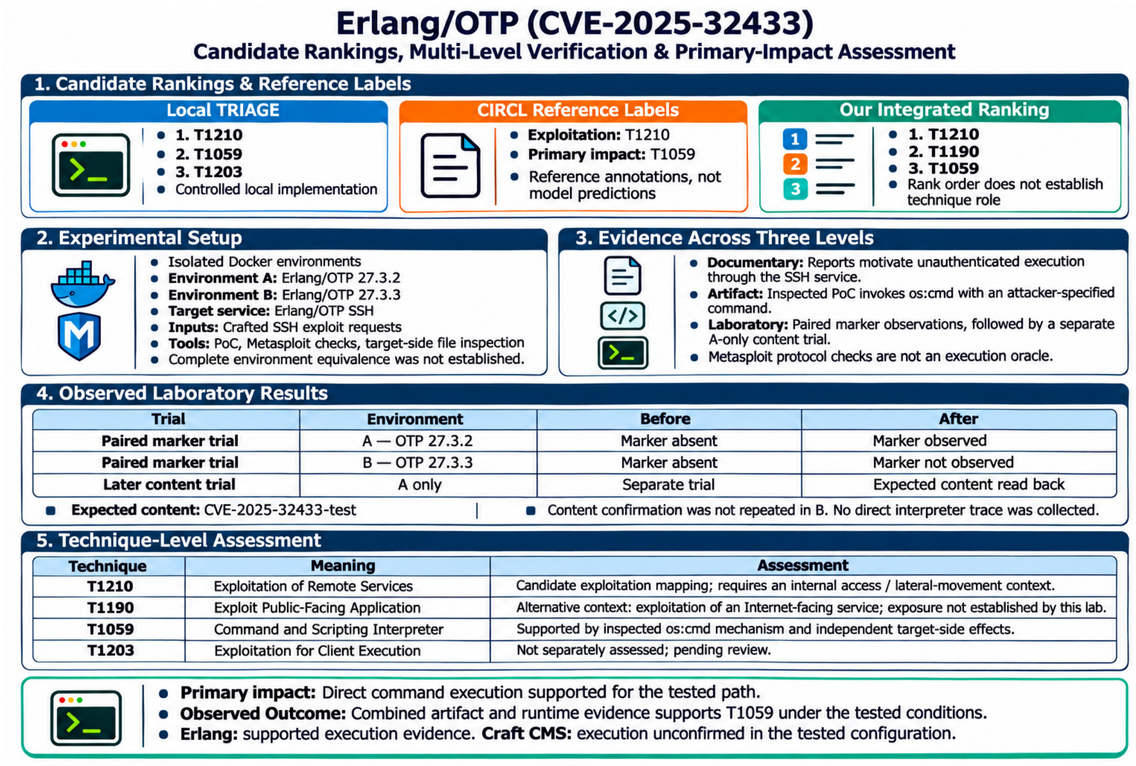
SMET [1] and controlled local **TRIAGE** [2] are comparators; **CIRCL** [3] supplies evaluation data and primary-impact references.

Method	MAP@10	Recall@10
SMET	19.46%	38.64%
Local TRIAGE	38.30%	53.30%
Ours	**40.92%**	**57.88%**

+2.62 pp MAP@10 over local TRIAGE (95% paired interval: 1.36–3.91 pp).

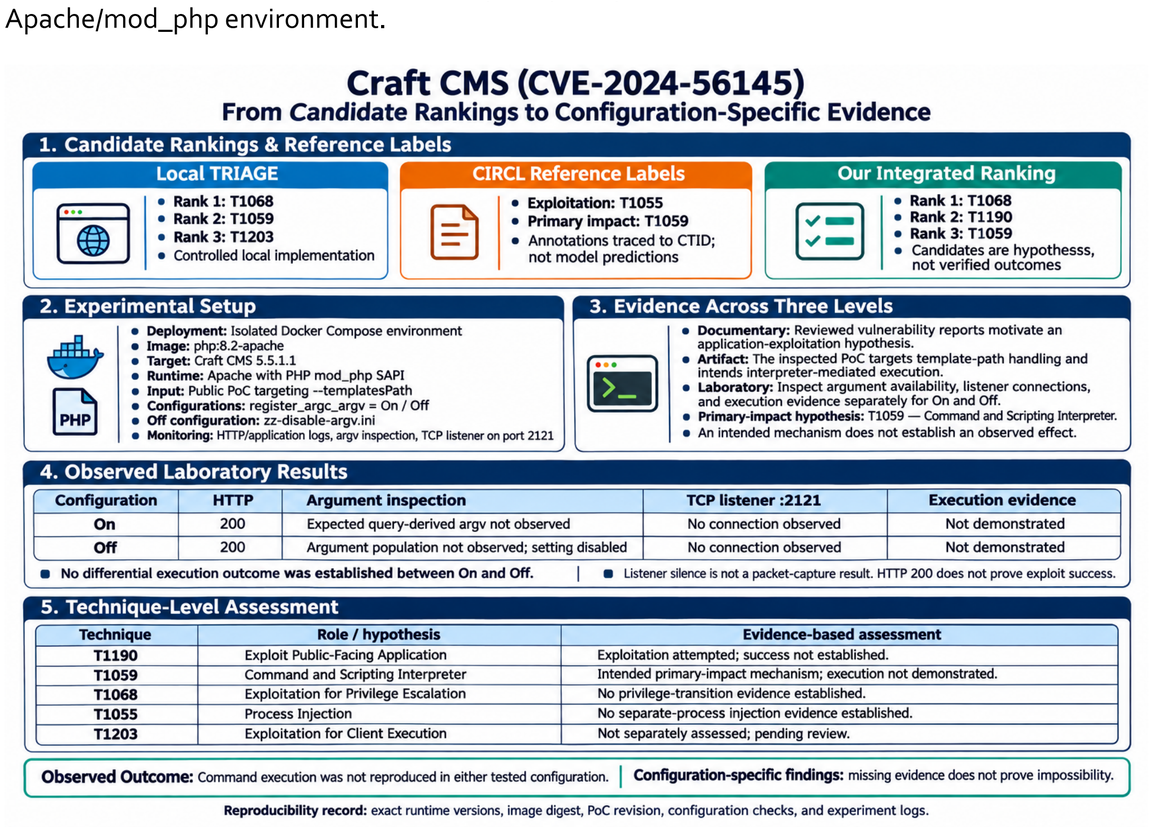
Erlang/OTP: Execution Evidence

CVE-2025-32433
Hypothesis: T1059 — Command and Scripting Interpreter.
We examined whether the tested exploit path supports Command and Scripting Interpreter.



Craft CMS: Configuration-Specific Evidence

CVE-2024-56145
Hypothesis: T1059 — Command and Scripting Interpreter.
We examined whether the intended exploit path produces command execution in the tested Apache/mod_php environment.



This research was sponsored by Slovak Republic under the SRDA grant APVV-23-0292 (DyMAX) and VEGA grant no. 1/0630/25 (eXSec). Noufal Issa was supported by Grant No. UK/1023/2026 from Comenius University Bratislava.

FAKULTA MATEMATIKY, FYZIKY A INFORMATIKY
Univerzita Komenského v Bratislave

MATFYZ CONNECTIONS

Noufal Issa, Damas Gruska
Comenius University in Bratislava, Slovakia

Loubna Ali
Berlin School of Business and Innovation, Berlin, Germany