ALI OWJIFARD

Shiraz – IRAN | ali.owjifard.1999@gmail.com | https://linkedin/in/owjifard

🛠 Core Skills

- Static Code Analysis (Semgrep, CodeQL)
- Python RCE Vulnerability Detection
- Batch Scripting & Command Injection Research
- Secure Coding & Exploit Mitigation
- YAML Rule Configuration & Debugging
- Linux File Handling & Shell Safety
- Article Writing & Cybersecurity Communication

Detail-oriented cybersecurity researcher with a strong focus on static code analysis, vulnerability detection, and secure scripting practices. Proficient in Semgrep rule-writing, CodeQL queries, and batch scripting for system-level analysis and automation. Passionate about detecting RCE flaws, server-side vulnerabilities, and making complex security concepts accessible through technical writing.

🧪 Projects & Research Highlights

📌 Semgrep Rule Library – Taint Tracking & Pattern Composition

- Developed modular, maintainable Semgrep rules with a focus on RCE flaws and access control issues
- Integrated pattern-inside/either configurations to boost rule precision
- Created README documentation with use-case demos and insights

📌 CodeQL Query Suite – Python Injection & Access Control

- Built custom CodeQL queries to detect insecure Python functions and misuse patterns
- Employed taint tracking logic to model data flow for exploit potential
- Wrote a comparative blog post analyzing false positives and reduction techniques

📌 Batch Script Auditing – Escalation & Exploitation Analysis

- Analyzed Windows batch scripts for privilege escalation paths and command injection vectors
- Designed scripts to simulate real-world exploitation scenarios
- Drafted internal technical write-ups for educational and security use

Self-Study Tracks:

- Advanced Semgrep rule authoring
- CodeQL for open-source security
- Batch scripting & Windows internals