License Choice

I chose the MIT License for this project. It offers maximum flexibility with minimal obligations only requiring preservation of the license text and a copyright notice. This is ideal for an internal tool or teaching resource where simplicity and broad reuse are priorities. Since there are no patent clauses or copyleft requirements, the license poses little legal risk even if the tool is modified or adapted.

Initial Vulnerability Report Template

Contact

- Preferred email or secure contact form (PGP if applicable)

Product / Version / Environment

- Product name and version
- Operating system or environment

Reproducible Summary

- A concise, step by step summary of how the issue can be observed
- No exploit steps or sensitive data
- Include error messages, logs, or indicators if relevant

Impact Assessment

- Type of impact (privilege escalation, data exposure, denial of service)
- Severity

Mitigation / Workaround (if available)

- Any steps that reduce risk before a full patch is available
- Optional or partial mitigations can be noted

Proposed Coordination Timeline

- Preferred disclosure timeline (90 days)
- Willingness to adjust based on vendor response

Justification

This template aligns with principles outlined in the CISA Vulnerability Disclosure Policy (VDP) guidance and ISO/IEC 29147. It avoids providing active exploit steps and focuses on secure, good-faith communication. By following coordinated disclosure timelines and safe harbor principles, the process promotes long-term security improvements without exposing users to unnecessary risk. The structure also mirrors the CERT CVD Guide's best practices for researcher-vendor collaboration.

Evidence Links

- Case Brief PDF
- Weekly Reflection PDF
- Code Repository or Diagrams (if any)

Reflection

If I were to refine this further, I would integrate automated validation into the reporting form to ensure clarity and completeness. I'd also research how to securely receive encrypted vulnerability reports (via GPG or secure submission portals). These refinements would support both security researchers and vendors by improving usability and minimizing friction during disclosure. Stakeholders impacted include developers, users, and system administrators, all of whom benefit from a safe and responsible process.