Vulnerability Proof of Concept Report

1. Cover Page

- Report title

- Author(s) or team responsible

- Date of report

- Classification (Confidential / Internal Use)

- Client or area to which it is addressed

2. Executive Summary

- Brief description of the main findings

- Scope of the proof of concept

- Overall risk level detected

- Key high-level recommendations

3. Objectives

- What was sought to be demonstrated

- Limited scope

4. Methodology

- Reference framework used

- Phases executed

- Tools used

5. Vulnerability Details

1. Identifier

2. Description

3. Classification

4. Severity / Risk

5. Potential impact

6. Proof of concept (PoC)

- Test environment and conditions

- Detailed steps to reproduce

- Payloads or commands (sanitized)

- Evidence

7. Limitations

6. Evidence

- Screenshots

- Logs or tool outputs

- Comparative results

7. Risk Analysis

- Technical and business impact

- Probability of exploitation

- Consequences

8. Recommendations

- Immediate measures

- Permanent solutions

- Best practices

9. Conclusions

- Summary of security status

- Relevance of addressing vulnerabilities

- Reminder about the scope of the PoC

10. Appendices (Optional)

- Glossary of terms

- References

- Payloads or complete scripts (if applicable)