KRYPTOTECK

YOUR CRYPTO HUB

# Vulnerability Identification Template

**Project Name:**

*(Name of the smart contract project)*

**Audit Date:**

*(Date when the vulnerability was identified)*

**Auditor Name(s):**

*(Names of auditors documenting the vulnerability)*

---

### 1. Vulnerability ID

- *(Unique identifier for each vulnerability, e.g., VULN-001)*

### 2. Vulnerability Title

- *(Short, descriptive title of the vulnerability, e.g., “Reentrancy Attack in Function X”)*

### 3. Vulnerability Description

- *(Detailed description of the vulnerability, including how it could be exploited and what assets or data could be at risk.)*

### 4. Location in Code

- *(Specify where the vulnerability is located, e.g., line numbers, function names, or files.)*

### 5. Risk Level

- *(Assign a risk level based on the potential impact, e.g., “Low,” “Medium,” “High,” or “Critical.”)*

### 6. Potential Impact

- *(Explain the possible consequences if the vulnerability is exploited, e.g., financial loss, data exposure, or system failure.)*

**7. Mitigation Steps**

- *(List recommended steps to resolve or reduce the risk of this vulnerability, such as code modifications, security patches, or specific best practices to follow.)*

**8. Verification Status**

- *(Indicate if the vulnerability has been mitigated or if further action is required. Options might include "Pending," "Mitigated," "In Progress," or "Re-Audit Needed.")*

**9. Testing Results**

- *(Include results from any testing done to verify the mitigation's effectiveness, such as successful or failed tests, and the methods used to test.)*

**10. Date of Resolution**

- *(Date when the vulnerability was fully resolved.)*