

# **Cyber Suraksha**

Purple Team Exercise

## **Incident Response Report**

**(IRREP)**

**Version 1.0**

**Date:**

**Time:**

**Incident ID:**

## 1. Incident Overview

Description:

Severity Level:

Impact:

Affected Systems:

---

## 2. Incident Details

Detection Method:

Initial Detection Time:

Attack Vector:

Attackers:

---

## 3. Response Actions Taken

Containment:

Eradication:

Recovery:

Lessons Learned:

---

## 4. Technical Analysis

Evidence:

Indicators of Compromise (IOCs):

Tactics, Techniques, and Procedures (TTPs):

Mitigation Recommendations:

---

## 5. Communication

Internal Notification:

External Notification:

Updates:

---

## 6. Follow-Up Actions

Incident Review:

Documentation:

Training:

---

## 7. POC (Screenshots)