**Project Report:** Cybersecurity Risk Assessment and Mitigation Strategy Implementation for an E-Commerce Platform

**Introduction**

In today’s digital world, e-commerce platforms are increasingly targeted by sophisticated cyber threats. This report focuses on improving the cybersecurity posture of an e-commerce platform through a comprehensive risk assessment and implementation of best mitigation strategies. The issue like, rapid increase in threats to online retail systems, data breaches, phishing attacks, and unauthorized access to system, has raised concern to e-commerce businesses to protect their sensitive data and digital assets. Our teams aim to identify existing vulnerabilities, evaluate associated risks, and propose actionable solutions for an e-commerce platform to enhance their security posture. The report outlines the complete project plan, scope, Gantt chart with interdependence, risk assessment and change management processes. The report also presents the use of industry standard tools such as GitHub for version control and Jira for team collaboration.

**Project Plan Document: Cybersecurity Risk Assessment and Mitigation Strategy Implementation for an E-Commerce Platform**

1. **Project Scope Statement**

Objective: To conduct a comprehensive cybersecurity risk assessment and mitigate cybersecurity risks in an e-commerce platform by identifying vulnerabilities, prioritizing threats, and implementing effective actionable measures.

**In-Scope Activities**

* Identification of cybersecurity risks through scans and assessment.
* Developing and implementing mitigation control such as MFA, firewalls, and encryption.
* Identifying threats such as malware, phishing, DDoS attacks, and insider threats.
* Use of GitHub for version control
* Use of Jira for team collaboration and project tracking
* Delivering a final report and presentation.

**Out-of-Scope Activities:**

* Physical security audits and controls.
* Applying hardware-based solutions in addition to software setups.
* Redesign of the e-commerce platform infrastructure.
* Ongoing monitoring and maintenance after project completion.

**Deliverables**

* Risk Assessment Report
* Mitigation Strategy Plan
* Gantt Chart with timeline phases including (Planning, Assessment, Mitigation, Monitoring.)
* Screenshots of GitHub and Jira usage.

1. **Gantt Chart with Interdependencies**

The Gantt chart below outlines the project timeline, tasks, duration and interdependencies to ensure timely project delivery and manage interrelated task effectively.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | Phase | Task | Start Date | End Date | Duration | Dependency |
| T1 | Planning | Define scope and objectives | 01/06/2025 | 02/06/2025 | 2 days | - |
| T2 | Planning | Assign roles and responsibilities | 03/06/2025 | 04/06/2025 | 2 days | T1 |
| T3 | Planning | Select tools (GitHub, Jira) | 05/06/2025 | 07/06/2025 | 3 days | T2 |
| T4 | Risk Assessment | Perform vulnerability scanning | 08/06/2025 | 11/06/2025 | 4 days | T3 |
| T5 | Risk Assessment | Conduct threat modelling and analysis | 12/06/2025 | 15/06/2025 | 4 days | T4 |
| T6 | Risk Assessment | Prioritize identified risks | 16/06/2025 | 21/06/2025 | 6 days | T5 |
| T7 | Mitigation | Implement Multi-Factor Authentication (MFA) | 22/06/2025 | 26/06/2025 | 5 days | T6 |
| T8 | Mitigation | Update and configure firewall rules | 27/06/2025 | 01/07/2025 | 5 days | T7 |
| T9 | Mitigation | Conduct cybersecurity training for employees | 02/07/2025 | 05/07/2025 | 4 days | T8 |
| T10 | Monitoring | Set up continuous threat detection tools | 06/07/2025 | 12/07/2025 | 7 days | T9 |
| T11 | Monitoring | Test incident response procedures | 13/07/2025 | 19/07/2025 | 7 days | T10 |

Table-1: Gantt Chart with interdependencies

The following visual representation of the Gantt chart provides a clearer timeline and task flow with visible dependencies and duration.

Figure-1: Visual Gantt chart

# RISK AND MANAGEMENT ISSUE STRATEGY

Proper Risk identification along with the best mitigation techniques is essential to protect the integrity, availability and confidentiality of e-commerce system. This section presents a comprehensive risk and issues management strategy and outlines the key risks to the project with their likelihood and impact. The strategy is aligned with industry standards such as ISO 27001and NIST Cybersecurity Framework.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Risk ID** | **Risk Description** | **Likelihood** | **Impact** | **Risk Level** | **Mitigation Strategy** |
| **R1** | Unpatched software vulnerabilities exploited | High | High | **Extreme** | Regular system updates and patch management. |
| **R2** | Phishing attacks targeting employees | Medium | High | **High** | Conduct awareness on phishing scenarios. |
| **R3** | DDoS attack causing service interruption | Low | High | **Medium** | Use Web Application Firewall (WAF) and DDoS mitigation services |
| **R4** | Insider threat due to improper use of privileges | Medium | Medium | **Medium** | Apply role-based access control (RBAC), monitor logins |
| **R5** | Third-party vendor breach | Low | High | **Medium** | Conduct vendor risk assessments and enforce security SLAs |
| **R6** | Leaking of data due to misconfigured cloud settings | Medium | High | **High** | Implement automated configuration scanning and auditing tools |
| **R7** | Ransomware infection from malicious downloads | Medium | High | **High** | Deploy endpoint detection & response (EDR), regular backups |

Table 2: Risk Assessment and Mitigation Strategy for E-Commerce Cybersecurity Project

# Change Request Management Process

In dynamic projects, like Cyber Security Risk Assessment for e-commerce changes are unavoidable. While addressing changes, it is also necessary to maintain the projects scope, timeline, and quality. The change request management process for the e-commerce cybersecurity project ensures that all suggested changes are systematically evaluated, approved, and implemented without interfering the project’s goals.

Here, in this project, the process aligned with the industry-standard project management practices, the procedure uses GitHub for version control and Jira for monitoring change request. The following steps shows the change request management process:

* 1. Request Initiation: Any team member can initiate a change request using Jira ticket.
  2. Review & Evaluation: Project Manager and QA member will evaluate the impact how modification will affect the project scope, objectives, and deliverables.
  3. Approval/ Rejection: After examining the risk of modification, Decision will be made based on risk, time and resources.
  4. Implementation: Approved changes will be implemented by updating relevant task. (Responsible team member updates the Jira ticket to reflect implementation progress)
  5. Documentation: All team members will be notified of approved changes, and all changes recorded in the project change log.

# Configuration Management Tool: GitHub

In this Project, we have used GitHub for Configuration and version control, As a group leader I created repository for our project and upload our files. Here below, are the screenshots demonstrating repository creation, file uploads, collaboration, and version history. Each version reflects our progress, enabling traceability and team collaboration.

A screenshot of a computer

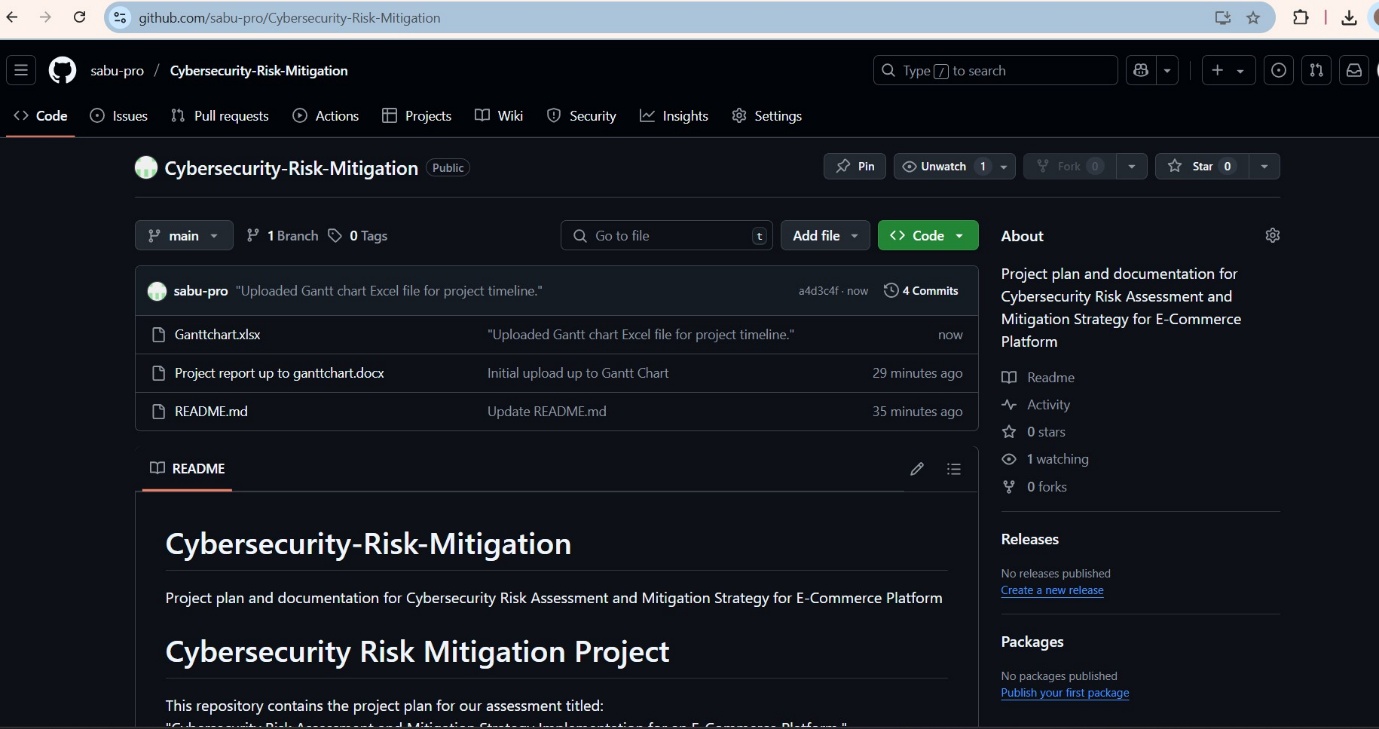
AI-generated content may be incorrect.

(Dashboard after Repository Creation)

A screenshot of a computer

AI-generated content may be incorrect.

(Initial upload of file-after commit changes)



(Updated files with commit history showing version control)

A screenshot of a computer

AI-generated content may be incorrect.

(Edited Readme.md file)