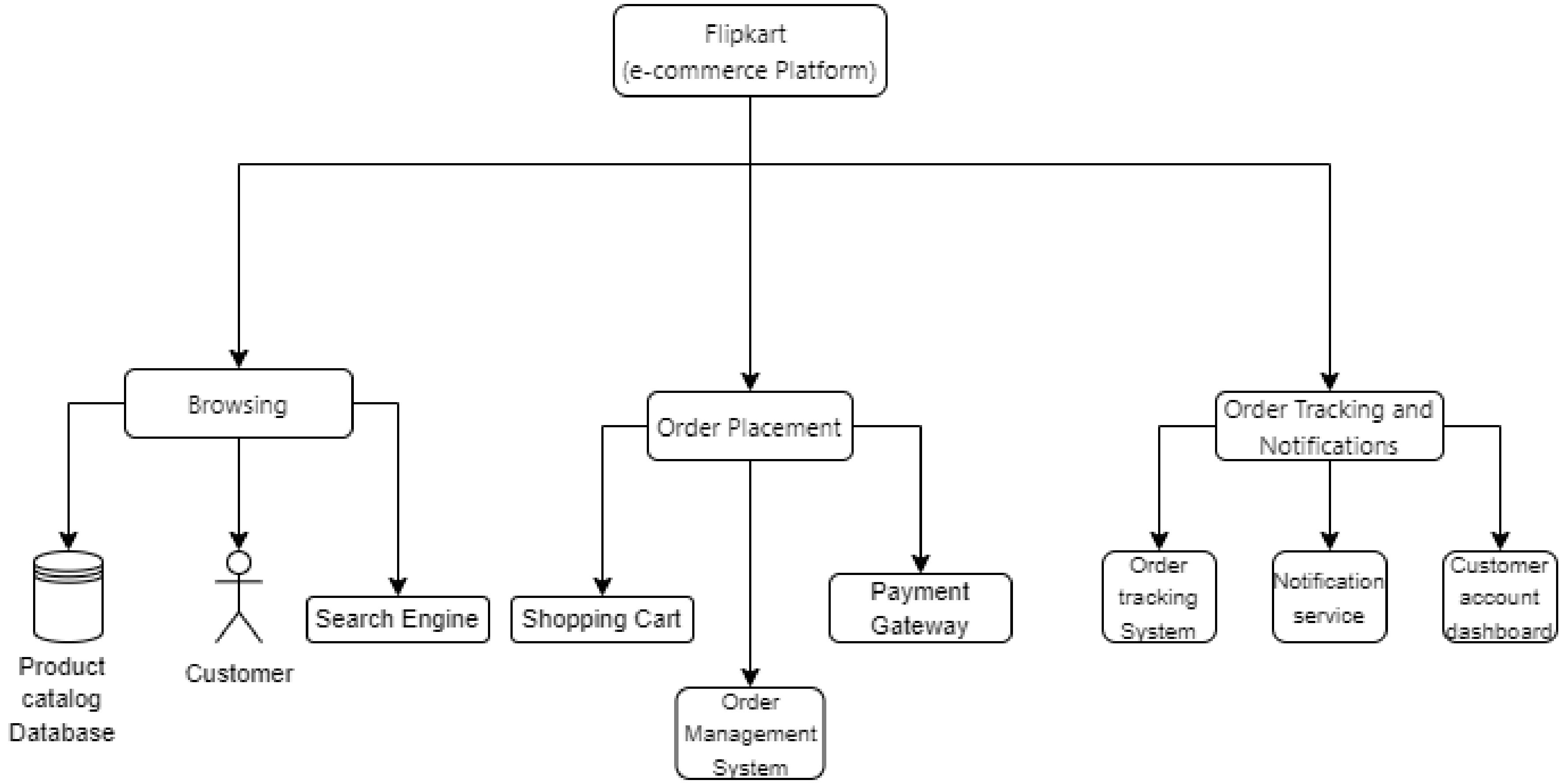
Risk Analysis Report for Flipkart (e-commerce organization)

Submitted by: Priya Patel

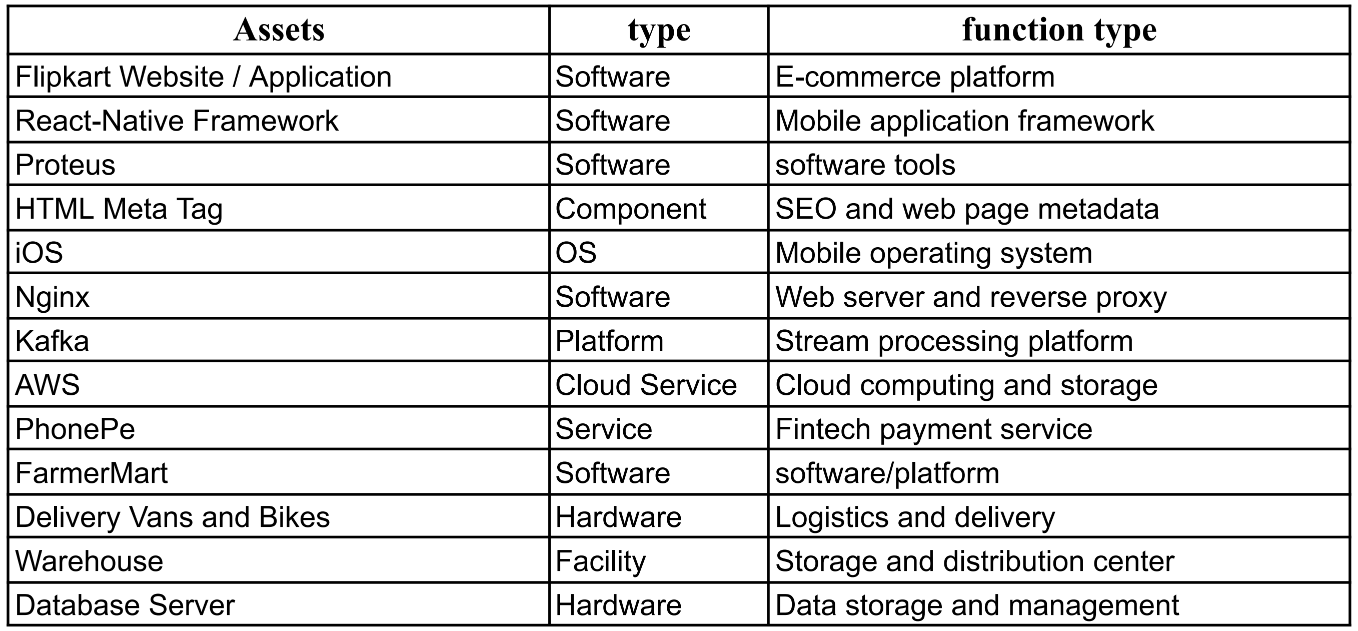
Phase 0. Scope and Delimitations: The scope of this risk analysis focuses on identifying and assessing potential threats and vulnerabilities within Flipkart's e-commerce platform. Delimitations include the time frame, resources, and specific areas of focus outlined in subsequent phases.

Phase 1. Business Analysis: Modelling Flipkart's business processes using Unified Modeling Language (UML).



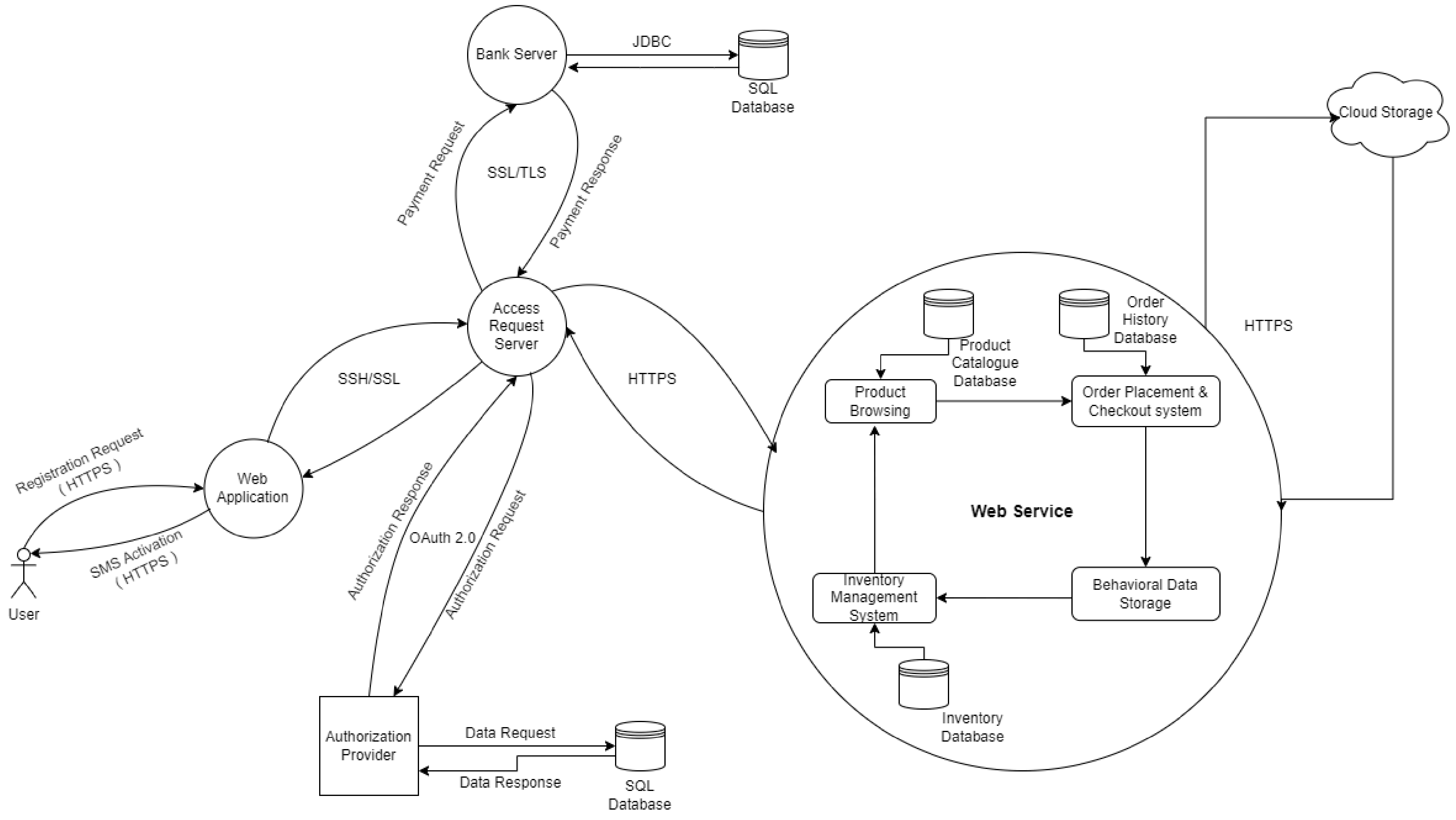
Phase 2. System Definition and Decomposition: To define Flipkart's system components and their relationships.

- Prepared assets excel sheet:



Assets	type	function type
Flipkart Website / Application	Software	E-commerce platform
React-Native Framework	Software	Mobile application framework
Proteus	Software	software tools
HTML Meta Tag	Component	SEO and web page metadata
iOS	OS	Mobile operating system
Nginx	Software	Web server and reverse proxy
Kafka	Platform	Stream processing platform
AWS	Cloud Service	Cloud computing and storage
PhonePe	Service	Fintech payment service
FarmerMart	Software	software/platform
Delivery Vans and Bikes	Hardware	Logistics and delivery
Warehouse	Facility	Storage and distribution center
Database Server	Hardware	Data storage and management

- **Data flow diagram** illustrating information flow across the system:



Phase 3. Threat Analysis: To identify potential threats and adversaries targeting Flipkart.

- **Attacker profiles** based on known threat actors.

Attacker Profile	Script Kiddie	Hacktivist	Organized Crime Targeting Ransomware
Risk Tolerance	High	Mid to High	High
Concern for Collateral Damage	Low	Mid	Low
Skill (Quality, Domain)	Low	Mid	High
Resources (Time, Headcount, Tools)	Low	Mid	High
Sponsorship	Low	Mid	High
Derived Threat Capability	17%	50%	90%

- **Abuse cases** outlining potential attack scenarios.

Abuse case (threat action or attack goal)	Credential stuffing attack	Data manipulation	Order manipulation	Fraudulent returns	Unauthorized Access, phishing, malware	Organized retail crime (ORC)	Supply chain disruptions, delayed Deliveries, Stockout	Mismanagement
Number of abuse case	1	2	3	4	5	6	7	8
Target asset	User Accounts	product catalog	Financial transactions	Refund Processing system	Customer data, User credentials, End-user devices	inventory items, supply chain logistics	Inventory management system, supplier relationships	Financial records, Operational processes

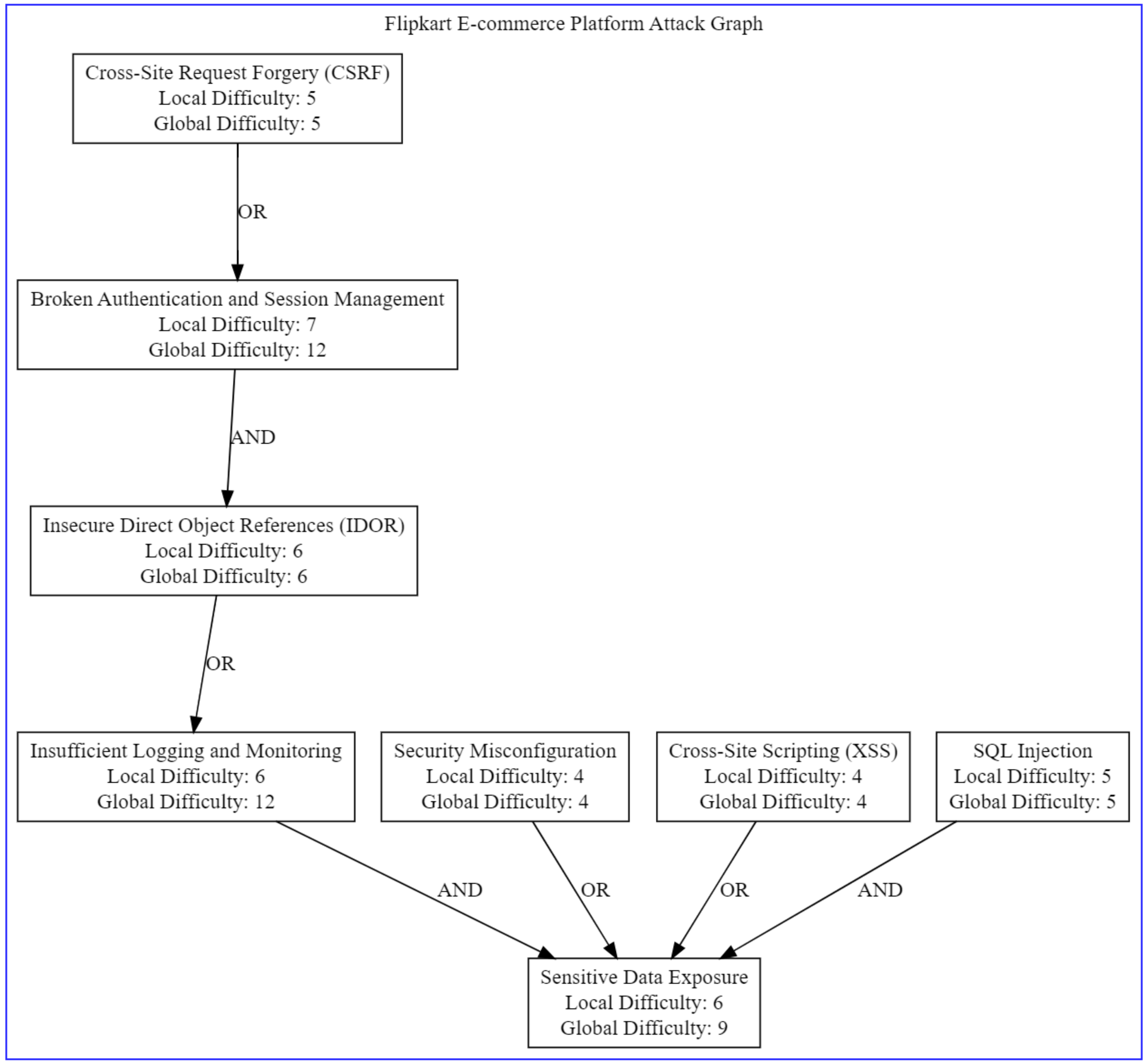
attack surface	web, mobile app	product catalog database, inventory management system	order management systems, payment gateway	Payment gateways, Customer portals	Access management system, Email communication channel, Network communication channel	Warehouses, Delivery routes	Inventory Tracking system, supply chain communication channels	Internal system, Employee access controls
Accessibility to Attack Surface	High	Mid	Mid	Mid to High	High	Mid to High	Low to Mid	Low to Mid
Window of Opportunity	High	Mid	Mid	High	High	Mid to High	Low to Mid	Low
Probability of Contact (PoC)	100%	50%	50%	100%	90%	50%	25%	90%
Concern for Collateral Damage	Low	Mid	Low	Low	High	High	High	High
Risk Tolerance (Attacker)	High	Mid	Mid	Mid to High	High	High	Mid to High	Low
Ability to Repudiate	Low	Mid	Mid	Mid	Low	Low	Mid to High	High
Perceived Deterrence	Low	Mid	Mid	Low	Low to Mid	Low to Mid	Mid	Mid
Perceived Ease of Attack	High	Mid	Mid	High	High	Mid	Low to Mid	Low
Probability of Action (PoA) (%)	75%	50%	45%	70%	80%	75%	60%	30%
Threat Event Probability (TEP)	56.25%	25%	22.50%	56%	64%	56.25%	36%	9%

Phase 4. Attack and Resilience Analysis: To assess vulnerabilities and resilience capabilities of Flipkart's systems.

- **Vulnerabilities** detailing identified weaknesses:

Vulnerabilities	Severity (CVSS Score)	Asset	Defense Mechanism
SQL Injection (CWE-89)	9.8 (Critical)	Database Server	Input validation, parameterized queries, WAF
Cross-Site Scripting (XSS) (CWE-79)	6.1 (Medium)	Flipkart Website / Application, React-Native Framework, HTML Meta Tag	Content Security Policy, input validation
Cross-Site Request Forgery (CSRF) (CWE-352)	6.5 (Medium)	Flipkart Website / Application, React-Native Framework	Anti-CSRF tokens, SameSite cookie attribute
Broken Authentication and Session Management (CWE-287)	8 (high)	Flipkart Website / Application, React-Native Framework	Multi-factor authentication, secure session handling
Sensitive Data Exposure (CWE-200)	7.5 (high)	AWS, PhonePe, Database Server	Encryption, access controls
Security Misconfiguration (CWE-933)	7 (high)	Nginx, Kafka, AWS	Regular security audits, automated configuration tools
Insecure Direct Object References (CWE-706)	7.5 (high)	Flipkart Website / Application, Database Server	Access control checks, secure coding practices
Insufficient Logging and Monitoring (CWE-778)	6.4 (medium)	AWS, Database Server	SIEM, continuous monitoring
Unvalidated Redirects and Forwards (CWE-601)	6.3 (medium)	Flipkart Website / Application, React-Native Framework	URL validation, user education
Using Components with Known Vulnerabilities (CWE-937)	7.2 (high)	React-Native Framework, HTML Meta Tag, Nginx	Regular updates, vulnerability scanning
Weak Password Policies (CWE-521)	5 (Medium)	Flipkart Website / Application, Database Server	Strong password policies, password strength checks
Improper Access Control (CWE-284)	7.8 (high)	Flipkart Website / Application, AWS	Role-based access control, regular audits
Improper Error Handling (CWE-209)	5.5 (medium)	Flipkart Website / Application, Nginx	Proper error handling, logging
Failure to Restrict URL Access (CWE-425)	7.2 (high)	Flipkart Website / Application, React-Native Framework	Access controls, secure coding practices
Server-Side Request Forgery (SSRF) (CWE-918)	8 (high)	AWS, Nginx, Kafka	Input validation, network segmentation

- **Attack graph** to visualize potential attack paths:



Phase 5. Risk Assessment and Recommendations: To quantify risks and propose mitigation strategies for Flipkart.

- Overall **risk assessment** combining threat likelihood and impact:
  Effort Spent (abuseCase) = frequency Effort(Perceived Ease of Attack abuseCase, Perceived Benefit of Success abuseCase)
  Attack Difficulty = frequency (Threat Capability(skill, Resources, sponsorship), Defense Mechanism)
  Probability of Success (%) = Effort Spent / Attack Difficulty

Loss Event	Online fraud, data breaches, and cyberattacks	Online fraud, data breaches, and cyberattacks	Employee errors (order processing, inventory management, pricing)	Customers returning items fraudulently	Online fraud, data breaches, and cyberattacks	Coordinated theft by criminal groups	Interruptions in the supply chain	Employee errors (order processing, inventory management, pricing)
CIA Impact Breach	Confidentiality, Integrity	Integrity, Availability	Integrity	Integrity	Confidentiality, Integrity	Integrity, Availability	Availability	Integrity, Availability
Attacker	Script Kiddie, Hacktivist, Organized Crime targeting ransomware	Hacktivist, Organized Crime targeting ransomware, Insiders	Insiders	Customers	Script Kiddie, Hacktivist, Organized Crime targeting ransomware	Organized Crime targeting ransomware, Criminal groups	Organized Crime targeting ransomware, Insiders, Malicious actors	Insiders

Effort Spent (Cost in INR)	50,000 - 1,00,000	30,000 - 50,000	40,000 - 70,000	60,000 - 1,20,000	70,000 - 1,50,000	60,000 - 1,20,000	50,000 - 1,00,000	20,000 - 40,000
Attack Difficulty (Cost in INR)	1,00,000 - 2,00,000	50,000 - 1,00,000	70,000 - 1,50,000	1,20,000 - 2,50,000	1,50,000 - 3,00,000	1,20,000 - 2,50,000	1,00,000 - 2,00,000	40,000 - 80,000
Probability of Success (%)	80%	75%	80%	85%	85%	80%	75%	80%

- Calculated **Risk using FAIR (Factor Analysis of Information Risk) framework**:

  $\text{Loss Event Magnitude}_{lossEvent} = f_{Mag}(\text{Impact}(\text{lossEvent}))$

  $\text{Loss Event Probability}_{lossEvent} = \text{TEP}_{abuseCase} \times \text{PoS}_{attackEvent}$

  $\text{Risk}_{lossEvent} = \text{LEP}_{lossEvent} \times \text{Magnitude}_{lossEvent}$

Loss event	**Abuse case**	**Attacked Asset**	**Impacted Actor**	**Type (FAIR category)**	**Loss Event Magnitude (in INR)**	**Loss Event Probability**	**RISK (in INR)**
Customers returning items fraudulently	Fraudulent returns	financial transactions	Retailer (Flipkart)	Transaction/Operational loss	50,000 -1,00,000	65.0%	32,000 - 65,000
Online fraud, data breaches, and cyberattacks	Unauthorized Access, phishing, malware	IT infrastructure, Customer data	Customer, Flipkart	Reputation, competitive advantage	5,00,000 -10,00,000	80.0%	80,000 - 4,00,000
Coordinated theft by criminal groups	Organized retail crime (ORC)	Supply chain, financial transactions	Retailer (Flipkart)	Theft/Legal/Compliance Event	2,00,000 -5,00,000	70.0%	1,40,000 - 7,00,000
Interruptions in the supply chain	Supply chain disruptions, delayed Deliveries, Stockout	Logistic system, financial transactions	Customer (external)	Operational loss	1,00,000 -3,00,000	60.0%	30,000 - 1,20,000
Customers returning items without a valid reason	Order manipulation	Inventory, financial transactions	Flipkart	Transaction/Operational Loss	30,000 - 50,000	50.0%	15,000 - 25,000
Employee Errors (order processing, inventory management, or pricing)	mismanagement	Order accuracy, inventory records, financial transactions	Flipkart	Human error event	20,000 - 1,00,000	55.0%	22,000 - 44,000

Conclusion: This report summarizes the risk analysis conducted for Flipkart, highlighting critical findings and recommendations to enhance cybersecurity resilience. By integrating rigorous threat modeling with structured risk calculation frameworks, this analysis aims to support informed decision-making and proactive risk management within Flipkart's operations.