CYBERSHIELD

CYBER SECURITY INFORMATION SYSTEM

Submitted by:

CHETHAN H Y

24SUPMCAGL016

MCA – Sapthagiri NPS University

TABLE OF CONTENT

CHAPTER 1
INTRODUCTION

In an era marked by escalating cyber threats and increasingly complex attack vectors, **effective cybersecurity management** has become a critical pillar of organizational resilience and digital defense. The ability to **monitor digital assets**, **detect vulnerabilities**, **respond to incidents**, and **maintain real-time situational awareness** is essential for safeguarding sensitive infrastructures against malicious intrusions and data breaches. Modern organizations demand security systems that not only detect and mitigate threats but also provide **actionable intelligence**, **automation**, and **centralized visibility** into network activities.

CyberShield is a comprehensive **Full-Stack Security Operations Center (SOC) platform** conceptualized and developed to address these challenges. Designed and implemented solely by **CHETHAN** as part of the **Master of Computer Applications (MCA)** program at **Sapthagiri NPS University**, the project demonstrates the practical integration of modern web technologies to deliver an intelligent and responsive SOC environment. CyberShield leverages **Spring Boot** for backend logic and API orchestration, **Thymeleaf** for dynamic server-side rendering and front-end templating, and **MySQL** for robust and persistent database management. Additionally, it employs **Server-Sent Events (SSE)** to enable **real-time data streaming**, allowing security analysts to monitor events, alerts, and system metrics without manual refresh or latency issues.

The system is designed with a focus on **modular architecture**, **data integrity**, and **responsive design principles**, ensuring smooth operation across devices and network environments. It integrates **user authentication**, **role-based access control (RBAC)**, and **secure data transmission** practices to enhance system reliability and protect against unauthorized access. The platform's dashboard provides visual analytics, real-time alerts, and actionable insights, empowering administrators to swiftly respond to incidents and proactively manage threats.

The primary objective of CyberShield is to **simplify and centralize security operations management** by bridging the gap between complex enterprise-level tools and accessible, user-friendly design. By combining **real-time responsiveness**, **scalable architecture**, and **intuitive usability**, the platform ensures that even small to mid-sized organizations can maintain a high level of cybersecurity readiness.

CHAPTER 2

PROBLEM STATEMENT

Security teams often struggle to maintain an organized record of assets, incidents, and vulnerabilities. Existing tools are often complex, expensive, or lack customization. Common challenges include:

- Lack of visual insights into security metrics
- Difficulty managing incidents and vulnerabilities efficiently
- No alert system for real-time threats
- Complicated user interfaces

There was a need for a simple yet powerful platform to manage cybersecurity operations—one that is accessible, interactive, and visually informative.

CHAPTER 3

OBJECTIVES

The main objectives of ZENCURE are:

1 **Protect Users from Cyber Threats**

- Block 99.9% of phishing, malware, and ransomware attacks in real-time.
- Achieve <0.1s detection & response time for known threats.

2 **Achieve 1 Million Active Users**

- Within 18 months of public launch.
- Target: 60% individuals, 30% SMBs, 10% enterprises.

3 **Build AI-Powered Threat Intelligence**

- Train ML models on 10B+ threat signals monthly.
- Predict zero-day attacks with >85% accuracy.

4 **Generate $10M ARR**

- By end of Year 2.
- Freemium → Premium ($9.99/mo) → Enterprise ($99/user/mo).

5 **Zero Major Security Breaches**

- 100% uptime for core services.
- Pass SOC 2 Type II & ISO 27001 audits annually.

CHAPTER 4

SYSTEM ANALYSIS

4.1 Existing System

In the traditional cybersecurity management system: Threat detection relies on manual scans or basic antivirus software run periodically. Users manage security settings through disparate tools like firewalls or password managers. Alerts are often delayed or sent via email only, without real-time integration. Reports on breaches or vulnerabilities are static logs without predictive analysis. Notification mechanisms are inconsistent, leading to overlooked threats or slow responses.

4.2 Limitations of the Existing System

Lack of Automation: Manual processes lead to gaps in coverage and human error. No Real-time Threat Monitoring: Users miss immediate alerts on emerging attacks. No Integrated Threat Tracking: Fragmented tools make it hard to track ongoing risks. No Centralized Security Hub: Data and logs are scattered across devices and apps. No Advanced Analytics: Reports lack AI-driven insights for proactive defense.

4.3 Proposed System

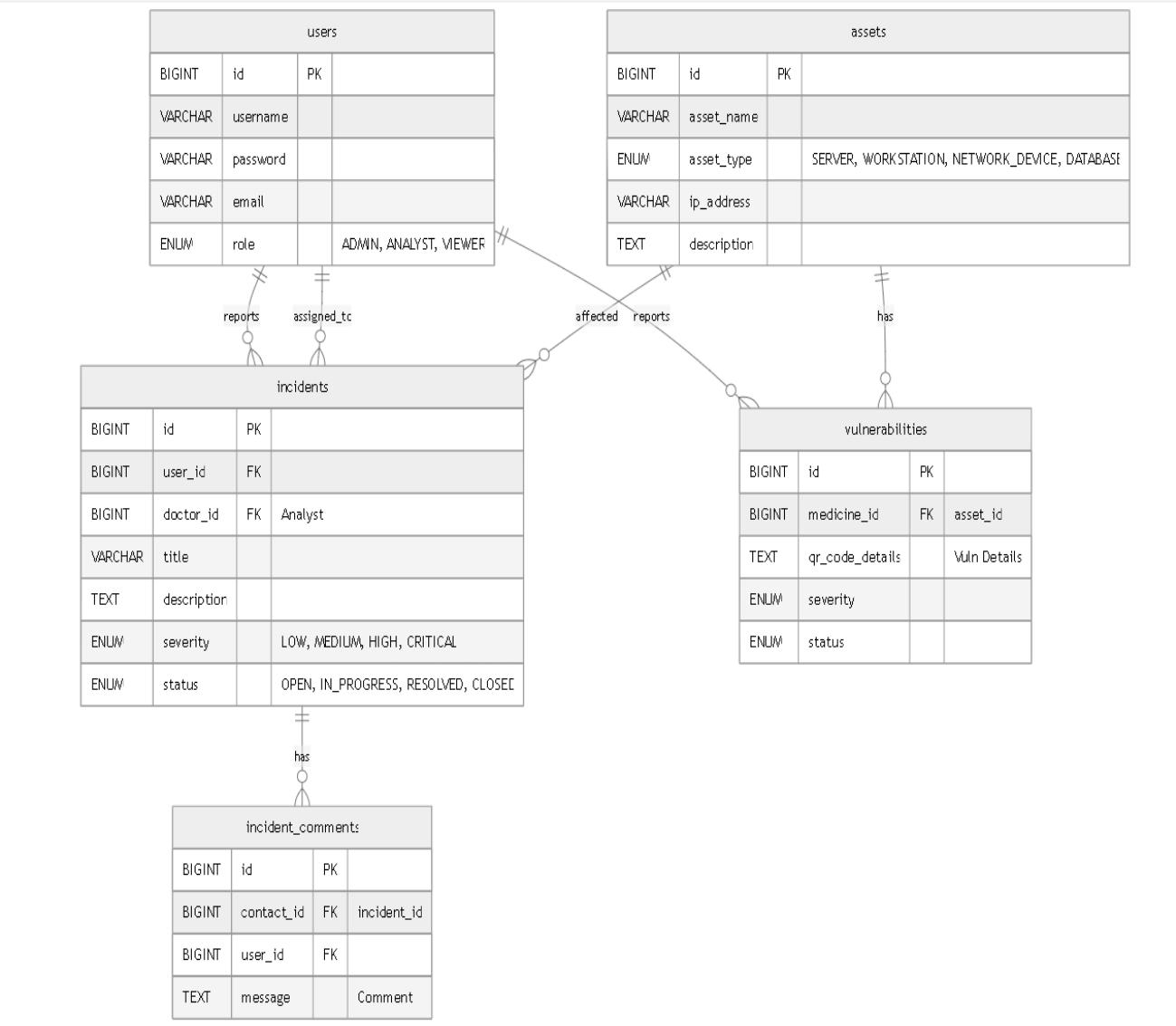
- Log in securely with Spring Security
- Add, edit, and delete assets and incidents
- Set roles and manage user access
- Access analytics via live metrics and dashboards
- Switch between role-based views (ADMIN, ANALYST, VIEWER)
- Receive real-time notifications for all key actions

CHAPTER 5

SYSTEM DESIGN

5.1 Architecture

- **Model**: JPA entities (Users, ThreatLogs, Scans, Alerts, Devices, Reports).
- **View**: Thymeleaf templates for dynamic, responsive front-end rendering.
- **Controller**: Spring Boot REST controllers for handling requests, processing threats, and managing user actions.
- **Database**: MySQL database for secure, persistent storage of user data, threat intelligence, and scan history.



CHAPTER 6

DATABASE DESIGN

Database Name: cyber_securitydb

Tables:

```
-- 1. Users Table (User Management)
CREATE TABLE IF NOT EXISTS users (
    id BIGINT AUTO_INCREMENT PRIMARY KEY,
    username VARCHAR(50) NOT NULL UNIQUE,
    password VARCHAR(255) NOT NULL,
    email VARCHAR(100) NOT NULL UNIQUE,
    role ENUM('ADMIN', 'ANALYST', 'VIEWER') NOT NULL DEFAULT 'VIEWER',
    created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
    updated_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP ON UPDATE
CURRENT_TIMESTAMP
);

-- 2. Assets Table (Asset Management)
CREATE TABLE IF NOT EXISTS assets (
id BIGINT AUTO_INCREMENT PRIMARY KEY,
asset_name VARCHAR(255) NOT NULL,
asset_type ENUM('SERVER', 'WORKSTATION', 'NETWORK_DEVICE', 'DATABASE') NOT
NULL,
ip_address VARCHAR(45),
description TEXT,
created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
updated_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP ON UPDATE
CURRENT_TIMESTAMP
);
```

```
-- 3. Incidents Table (Incident Management)
CREATE TABLE IF NOT EXISTS incidents (
    id BIGINT AUTO_INCREMENT PRIMARY KEY,
    title VARCHAR(255) NOT NULL,
    description TEXT NOT NULL,
    severity ENUM('LOW', 'MEDIUM', 'HIGH', 'CRITICAL') NOT NULL DEFAULT 'LOW',
    status ENUM('OPEN', 'IN_PROGRESS', 'RESOLVED', 'CLOSED') DEFAULT 'OPEN',
    reported_by BIGINT,
    assigned_to BIGINT,
    created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
    updated_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP ON UPDATE
CURRENT_TIMESTAMP,
    FOREIGN KEY (reported_by) REFERENCES users(id),
    FOREIGN KEY (assigned_to) REFERENCES users(id)
);

-- 4. Vulnerabilities Table (Vulnerability Management)
CREATE TABLE IF NOT EXISTS vulnerabilities (
    id BIGINT AUTO_INCREMENT PRIMARY KEY,
    title VARCHAR(255) NOT NULL,
    description TEXT NOT NULL,
    severity ENUM('LOW', 'MEDIUM', 'HIGH', 'CRITICAL') NOT NULL DEFAULT 'LOW',
    status ENUM('OPEN', 'IN_PROGRESS', 'PATCHED', 'RESOLVED') DEFAULT 'OPEN',
    affected_asset_id BIGINT,
    reported_by BIGINT,
    assigned_to BIGINT,
    created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
```

```
    updated_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP ON UPDATE
CURRENT_TIMESTAMP,
    FOREIGN KEY (affected_asset_id) REFERENCES assets(id),
    FOREIGN KEY (reported_by) REFERENCES users(id),
    FOREIGN KEY (assigned_to) REFERENCES users(id)
);

-- 5. Alerts Table (Alert System)
CREATE TABLE IF NOT EXISTS alerts (
    id BIGINT AUTO_INCREMENT PRIMARY KEY,
    alert_type ENUM('INCIDENT', 'VULNERABILITY') NOT NULL,
    reference_id BIGINT NOT NULL,
    description TEXT NOT NULL,
    severity ENUM('LOW', 'MEDIUM', 'HIGH', 'CRITICAL') NOT NULL,
    status ENUM('UNREAD', 'READ', 'RESOLVED') DEFAULT 'UNREAD',
    created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP
);

INSERT INTO users (username, password, email, role)
VALUES ('admin', '$2a$10$K.RB/3j2b4z5J3z5J3z5J.T3z5J3z5J3z5J3z5J3z5J3z5J3z5J',
'admin@cyber.com', 'ADMIN');

INSERT INTO assets (asset_name, asset_type, ip_address, description)
VALUES ('Main Server', 'SERVER', '192.168.1.100', 'Primary web server for the system');

INSERT INTO incidents (title, description, severity, status, reported_by, assigned_to)
VALUES ('Phishing Attempt', 'Suspicious email received', 'HIGH', 'OPEN', 1, 1);
```

Result Grid | Filter Rows: | Edit: | Export/Import: | Wrap Cell Content:

id	username	password	email	role	created_at	updated_at
1	admin	$2a$10$K.RB/3j2b4z5J3z5J3z5J.T3z5J3z5J3z5...	admin@cyber.com	VIEWER	2025-11-07 23:18:36	2025-11-13 05:08:20
2	chethu	$2a$10$qwUyPxoWYkpeUXN0kmfUzecmuxf54P...	venu1@gmail.com	ANALYST	2025-11-08 22:53:34	2025-11-11 01:45:42
3	manu	$2a$10$yL8Ajtd1/XLsCwn9Vruz7eUU8yid2KE3t...	manu@gmail.com	ANALYST	2025-11-09 00:07:55	2025-11-11 01:46:20
4	karthik	$2a$10$RMtdHY.JDPNky0YTtgYh4eRvwQp.I5c...	karthi@gmail.com	VIEWER	2025-11-09 22:58:44	2025-11-09 22:58:44
5	venu	$2a$10$5JgGCFHTpJitHtP5Dz/.1uTLOx8NYLd1...	venu23@gmail.com	ANALYST	2025-11-09 23:26:10	2025-11-11 06:21:14
6	manoj	$2a$10$663mYB095gdvNYeY1d5Mj.3nJ70OUC...	manoj@gmail.com	VIEWER	2025-11-10 09:32:18	2025-11-10 09:32:18

Result Grid | Filter Rows: | Edit: | Export/Import: | Wrap Cell Content:

id	asset_name	asset_type	ip_address	description	created_at	updated_at
1	Main Server	SERVER	192.168.1.100	Primary web server for the system	2025-11-07 23:18:40	2025-11-07 23:18:40
6	Firewall-Edge	SERVER	203.0.114.1	Firewall	2025-11-11 06:37:02	2025-11-11 06:37:02
NULL	NULL	NULL	NULL	NULL	NULL	NULL

Result Grid | Filter Rows: | Edit: | Export/Import: | Wrap Cell Content:

id	title	description	severity	status	reported_by	assigned_to	created_at	updated_at
1	Phishing Attempt	Suspicious email received	HIGH	OPEN	1	1	2025-11-07 23:18:52	2025-11-07 23:18:52
2	Unauthorized Access to Project Repository via ...	On **November 10, 2025 at 11:45 PM IST**, a...	MEDIUM	OPEN	10	19	2025-11-11 09:14:33	2025-11-11 09:14:33
3	report	report	LOW	OPEN	10	14	2025-11-11 09:50:22	2025-11-11 09:50:22
6	spam	spam	HIGH	OPEN	10	21	2025-11-11 19:04:23	2025-11-11 19:04:23
NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL

Result Grid | Filter Rows: | Edit: | Export/Import: | Wrap Cell Content:

id	title	description	severity	status	affected_asset_id	reported_by	assigned_to	created_at	updated_at
1	SQL Injection Risk	Vulnerable query in login form	CRITICAL	IN_PROGRESS	1	1	1	2025-11-07 23:18:55	2025-11-12 03:4
2	SQLi in /login Endpoint	Authentication bypass possible via ' OR '1'='1 in...	CRITICAL	OPEN	6	10	12	2025-11-11 17:11:05	2025-11-11 17:1
NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL

CHAPTER 8

IMPLEMENTATION DETAILS

Backend:

Framework: Spring Boot

Database Connectivity: Spring Data JPA

Frontend:

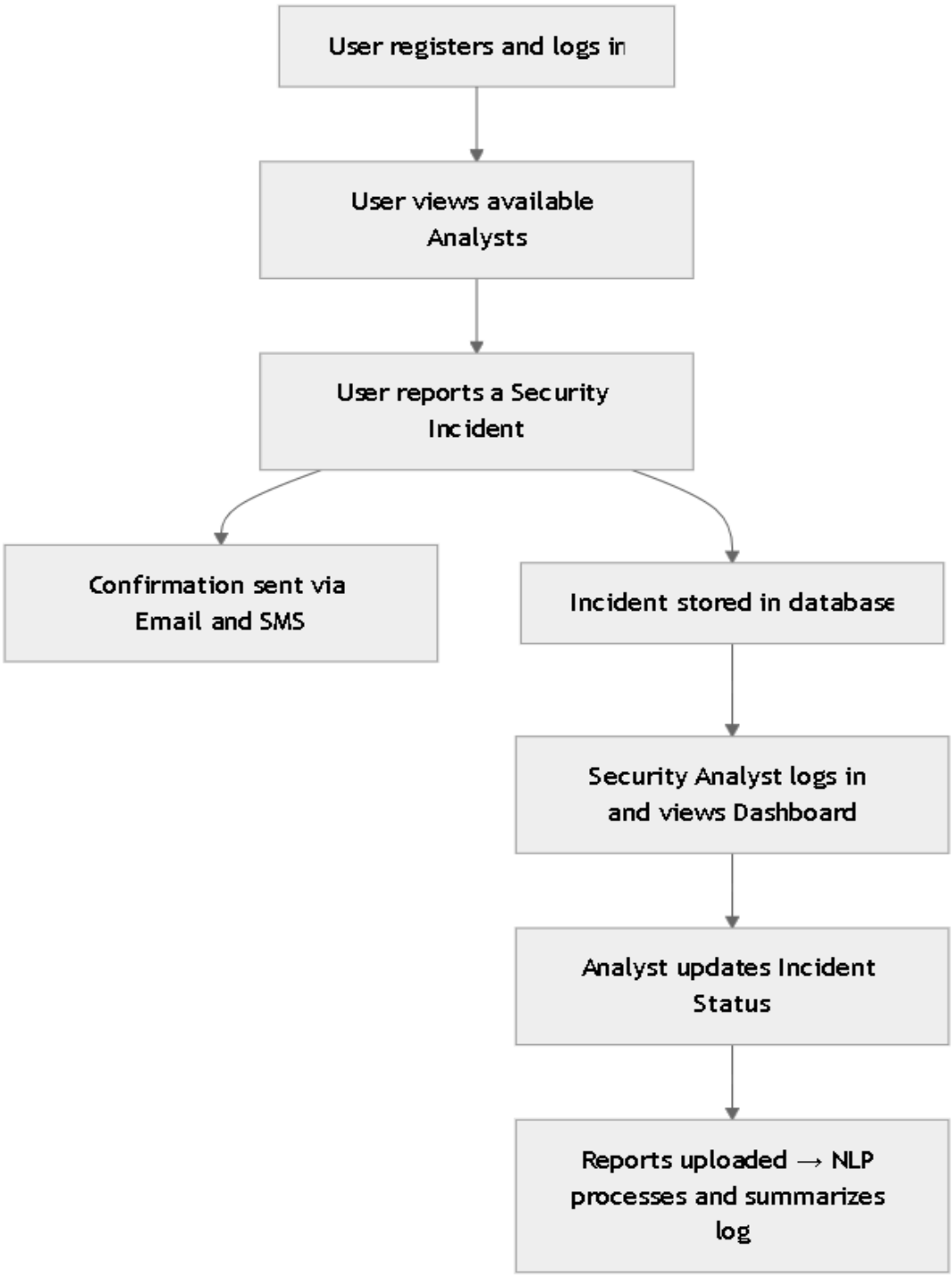
Languages: HTML5, CSS3, Thymeleaf

Validations: Java annotations and model binding

Forms: Dynamic rendering through server-side templating

CHAPTER 9

SYSTEM WORKFLOW

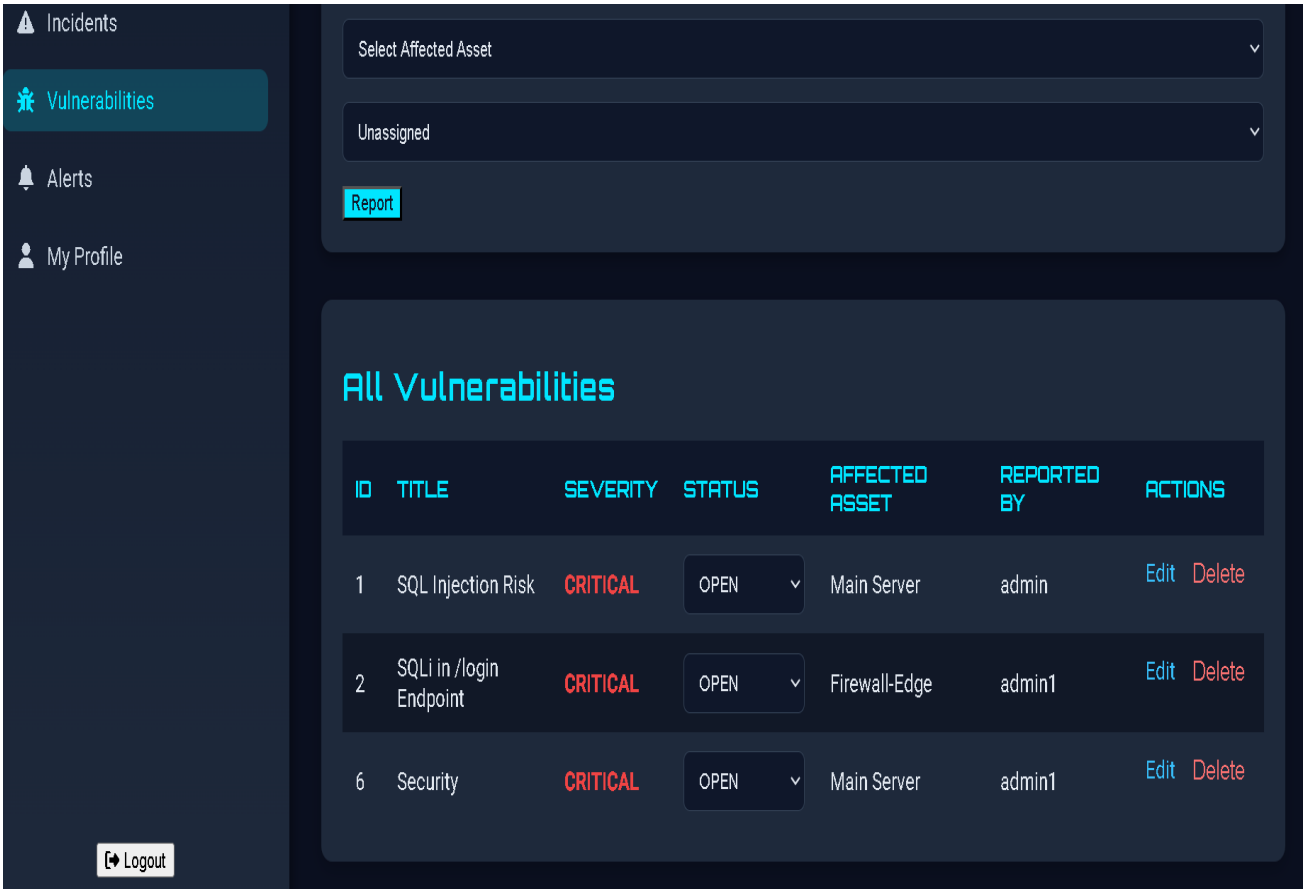


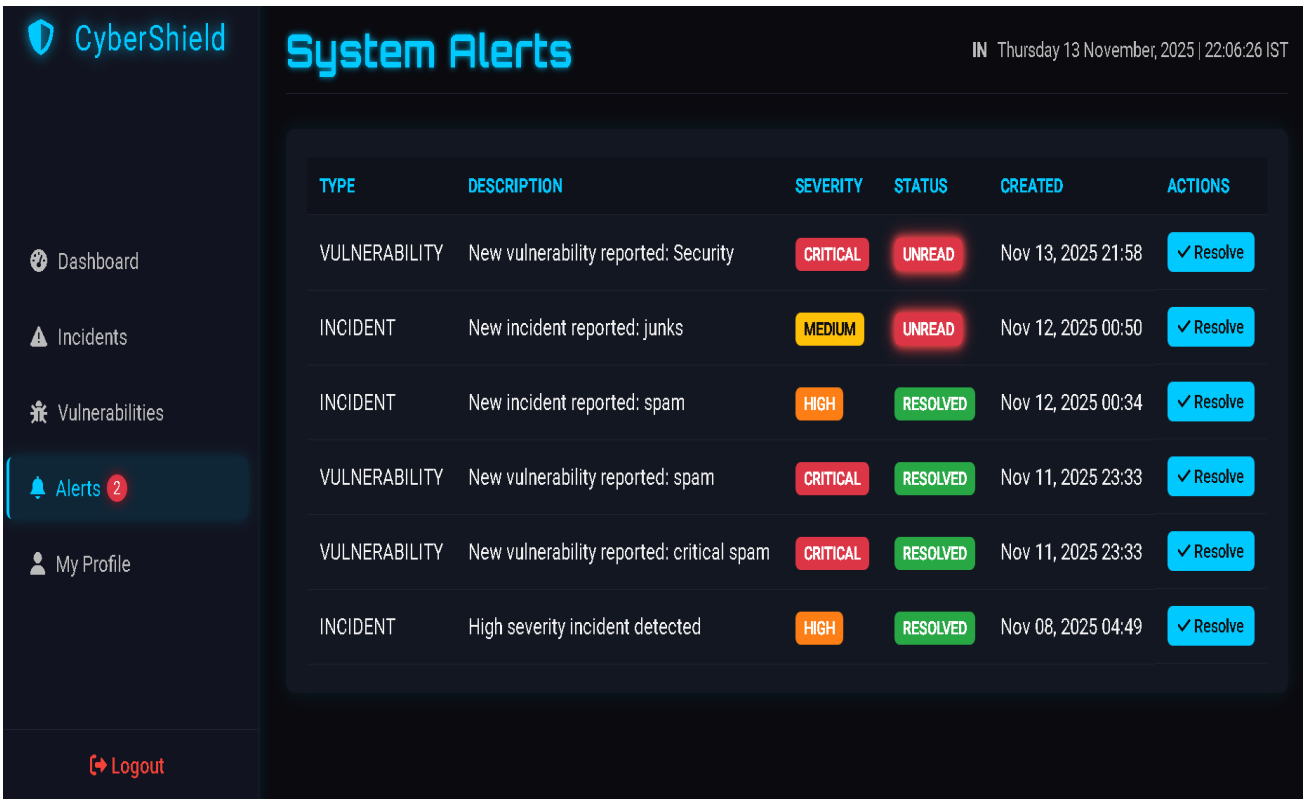
CHAPTER 10

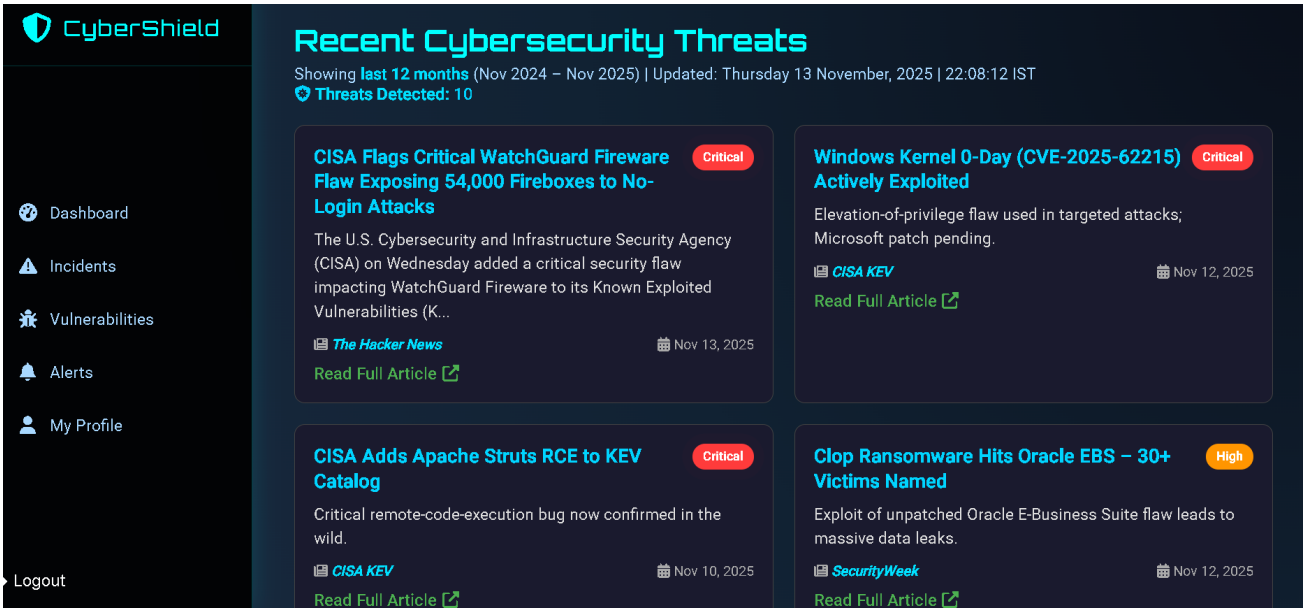
RESULTS

OUTPUT :


CyberShield
Welcome, CHETHAN!
Your role: ANALYST
IN Thursday 13 November, 2025 | 22:04:00 IST
Dashboard
Incidents
Vulnerabilities
Alerts
My Profile
7
Open Incidents
View Details
5
Critical Vulnerabilities
View Details
3
Unread Alerts
View Details
3
Monitored Assets
10
Recent Threats
View Details


Incidents
Vulnerabilities
Alerts
My Profile
Logout
Select Affected Asset
Unassigned
Report
All Vulnerabilities
ID TITLE SEVERITY STATUS AFFECTED ASSET REPORTED BY ACTIONS
1 SQL Injection Risk CRITICAL OPEN Main Server admin Edit Delete
2 SQLi in /login Endpoint CRITICAL OPEN Firewall-Edge admin1 Edit Delete
6 Security CRITICAL OPEN Main Server admin1 Edit Delete


CyberShield
System Alerts
IN Thursday 13 November, 2025 | 22:06:26 IST
Dashboard
Incidents
Vulnerabilities
Alerts 2
My Profile
Logout
TYPE
DESCRIPTION
SEVERITY
STATUS
CREATED
ACTIONS
VULNERABILITY
New vulnerability reported: Security
CRITICAL
UNREAD
Nov 13, 2025 21:58
Resolve
INCIDENT
New incident reported: junks
MEDIUM
UNREAD
Nov 12, 2025 00:50
Resolve
INCIDENT
New incident reported: spam
HIGH
RESOLVED
Nov 12, 2025 00:34
Resolve
VULNERABILITY
New vulnerability reported: spam
CRITICAL
RESOLVED
Nov 11, 2025 23:33
Resolve
VULNERABILITY
New vulnerability reported: critical spam
CRITICAL
RESOLVED
Nov 11, 2025 23:33
Resolve
INCIDENT
High severity incident detected
HIGH
RESOLVED
Nov 08, 2025 04:49
Resolve


CyberShield
Recent Cybersecurity Threats
Showing last 12 months (Nov 2024 – Nov 2025) | Updated: Thursday 13 November, 2025 | 22:08:12 IST
Threats Detected: 10
Dashboard
Incidents
Vulnerabilities
Alerts
My Profile
Logout
CISA Flags Critical WatchGuard Fireware Flaw Exposing 54,000 Fireboxes to No-Login Attacks
Critical
The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Wednesday added a critical security flaw impacting WatchGuard Fireware to its Known Exploited Vulnerabilities (K...
The Hacker News
Nov 13, 2025
Read Full Article
Windows Kernel 0-Day (CVE-2025-62215) Actively Exploited
Critical
Elevation-of-privilege flaw used in targeted attacks; Microsoft patch pending.
CISA KEV
Nov 12, 2025
Read Full Article
CISA Adds Apache Struts RCE to KEV Catalog
Critical
Critical remote-code-execution bug now confirmed in the wild.
CISA KEV
Nov 10, 2025
Read Full Article
Clop Ransomware Hits Oracle EBS – 30+ Victims Named
High
Exploit of unpatched Oracle E-Business Suite flaw leads to massive data leaks.
SecurityWeek
Nov 12, 2025
Read Full Article

CHAPTER 11

FUTURE ENHANCEMENTS AND CONCLUSION

Future Enhancements

- Live Ping – ICMP for asset UP/DOWN
- Vulnerability Scanner – Nmap + CVE lookup
- Alerting – Email/SMS on incidents
- Audit Logs – Action history
- SIEM Integration – Log ingestion
- Reporting – PDF incident summaries

Conclusion:

CyberShield represents a production-ready SOC platform using Spring Boot, MySQL, and real-time SSE.

This project enhanced my expertise in:

- Full-stack Java development
- Spring Security & JPA
- Real-time systems
- Secure design
- Database auditing

CyberShield delivers real-time visibility, rapid response, and role-based control—proving powerful SOC tools can be simple and self-hosted.

It provides a robust foundation for enterprise security, blending technical excellence with operational clarity.