Cyber Astra - The Cyber Security Framework

A Project Report Submitted by

Sahil Patel– 92100133009

Under the guidance of

Prof. Vishal Akhbari

A Project Submitted to

Marwadi University in Partial Fulfillment of the Requirements for the Bachelor of Technology in Information and Communication Technology

April, 2025

MARWADI UNIVERSITY
Rajkot-Morbi Road, At & Po. Gauridad,
Rajkot- 360003, Gujarat, India.

CERTIFICATE

This is to certify that research/project work embodied in this project This is to confirm that the research/project work contained in this project entitled "**Cyber Astra - The Cyber Security Framework**" was conducted by **Sahil Patel** at Marwadi University as partial fulfillment of the **Bachelor of Technology** in **Information and Communication Technology** awarding by MarwadiUniversity.This research/project work has been conducted under my supervision and guidance and it is to my satisfaction.

Date:
Place: Marwadi University

Prof Vishal Akhbari
Guide

Dr. Arjav Bavarva
Head Of Dept.

Seal of Institute

COMPLIANCE CERTIFICATE

This is to certify that the research/project work embodied in this project titled **Cyber Astra - The Cyber Security Framework** was carried out by **Sahil Patel - 92100133009** at Marwadi University for partial fulfillment of a Bachelor's in Information and Communication Technology at Marwadi University. he has complied with the comments given during Review I, Review II by the Reviewer to my satisfaction.

Date:

Place: Marwadi University

Sahil Patel

(92100133009)

Prof. Vishal Akhbari

Guide

PROJECT APPROVAL CERTIFICATE

This is to certify that the research/project work embodied in this project titled **"CyberAstra- Cyber Security Framework"** was carried out by **Sahil Patel(92100133009)** at Marwadi University is approved for the B.Tech in Information and Communication Technology by Marwadi University.

Date:

Place: Marwadi University

Examiner's Sign and Name:

( ) ( )

DECLARATION

We certify that we are the sole authors of this project/project work and that neither any part nor the whole of the project has been submitted for a degree to any other University or Institution.

We certify that, to the best of our knowledge, the current project/project work does not infringe upon anyone's copyright nor violate any proprietary rights and that any ideas, techniques, quotations or any other material from the work of other people included in our project/project work, published or otherwise, are fully acknowledged in accordance with the standard referencing practices.

Furthermore, to the extent that we have included copyrighted material that surpasses the boundary of fair dealing within the meaning of the Indian Copyright (Amendment) Act 2012, we certify that we have obtained written permission from the copyright owner(s) to include such material(s) in the current project and have included copies of such copyright clearances to our appendix.

We declare that this is a true copy of project/project work, including any final revisions, as approved by project/project work review committee.

We have checked the write-up of the present project/project work using the anti-plagiarism database and it is within the allowable limit. Even though later on in case of any complaint pertaining of plagiarism, we are solely responsible for the same and we understand that as per UGC norms, the University can even revoke the Degree name conferred to the student submitting this project.

Date:

Place: Rajkot, Gujarat

Sahil Patel **Prof. Vishal Akhbari**

(92100133009) Guide

ACKNOWLEDGMENT

I would like to sincerely thank **Mr. Naresh Makwana**, our external guide, for his unwavering guidance throughout the organization and his patient responses to all of my questions.

Additionally, I want to thank **Prof. Vishal Akhbari**, my internal guide, for supporting us during our internship by providing us with the required guidance and recommendations in addition to their invaluable coordination in getting this internship done.

I also want to thank my Head of dept **Dr. Arjav Bavarva** for guiding us to our final year project.

I also want to express my gratitude to our parents, friends, and entire family for their invaluable encouragement and support in helping us finish our task.

Finally, I would like to thank all the open-source communities and contributors whose libraries and tools were crucial in the development of Cyber Astra - The Cyber Security Framework.

Thank you,

Sahil Patel (92100133009)

Table of Contents

List of Tables

List of Figures

Abstract

The experience and training I had while working on the Cyber Astra project while pursuing my B.Tech at Marwadi University is chronicled in this report. Cyber Astra is a digital forensics and cybersecurity framework that was created within a capstone project to replicate actual cyber investigation scenarios. This project combines numerous cybersecurity tools and methods to help with digital evidence analysis, threat investigation, and automated reporting. The idea came from contemporary security operation workflows and learning platforms that balance interactivity with technical sophistication. Through the development of Cyber Astra, I had first-hand experience in front-end development with React.js and back-end scripting with Node.js and Python. I also had the task of integrating such tools as PCAP Viewer, Log Analyzer, Disk Imager, and OSINT modules into a responsive web- based interface. The application also incorporates dynamic visualizations and 3D effects to make it more user-friendly, particularly in simulating security situationss.

1. Introduction

1.1 Project Purpose

The Purpose Of The Cyber Astra Project Is To Devlop A Comprehensive And Interactive Cyber Security Framework That Aids All Cyber Security Concepts.

The main goal of this system is to give users a hands-on environment to experiment, analyze, and simulate actual cyber incidents using combined tools like PCAP Viewer, Log Analyzer, Disk Imager, and OSINT modules.

In addition, Cyber Astra promotes awareness of cybersecurity through the presentation of legal context, reporting functionality, and scenario-based simulations and real-world implementation in the practice of cyber forensics.

1.2 Product Scope

The scope of this project covers cyber security concepts,tools useful in investigations and learning perspective.

It includes features such as a dedicated manual tool section, youtube links,documentations,links for the tools at one place, search optimization.

The system supports a wide variety of cyber security tools—both internally developed and externally linked—including PCAP file analyzers, log analyzers, disk imaging tools.

1.3 Intended Audience

The primary audience for this system includes students and learners persuing courses, security analyst, forensic investigators,legal professionals and law enforcement specialist.

1.4 Technology and Literature Survey

Cyber Astra Is Built Using a modern technology stack that emphasizes modularity,scalablity, and interactivity.The Frontend is devloped using React.js offering a dynamic interface.During the devlopment research was comducted on existing tools such as Autopsy,Wireshark.These Tools served as reference for integrating core functionalities.

A literature review includes chain-of-custody protocols,incident-responses,research on Forensic methodologies and exploring different frameworks helped me design the idea of Cyber Astra.

1.5 Proposed Solution

Cyber Astra seeks to provide an end-to-end solution to close the gap between theoretical cybersecurity education and real-world investigation workflows. The platform addresses significant functional needs Such as:

PCAP file, disk image, system log, and suspicious activity tool-based analysis.
Real-time scenario simulation with only the chosen tools exposed during run-time.
Dynamic 3D visual effects .

Besides, non-functional objectives like system responsiveness, scalability, modularity, security, and cross-platform compatibility are also taken into account. The design of Cyber Astra enables smooth integration of further tools, updates in the future, and deployment in institutional environments or cloud platforms.

1.6 Technology Stack:

Frontend: React.js, Tailwind CSS

Backend: Python,Node,js

Tool Integration: Python Scripts

Visualization: 3D Rendering Using Css

2. Project Management

2.1 Project Planning and Scheduling

Here the project planning is been divided into four major phases which are:

Phase 1: Research and Analysis

- Carried out an in-depth analysis of current cybersecurity frameworks and forensics tools like Autopsy, Wireshark, Volatility, and Shodan to determine how similar tools work.
- Recognized typical investigation issues and needs in digital forensics and cybercrime investigation.
- Explored the integration and automation features of tools like PCAP parsers, log analyzers, OSINT scanners, and disk imagers.
- Collected functional and non-functional requirements for Cyber Astra with emphasis on educational usability, visual simulation, and modular integration.
- Defined a high-level design and a list of internal tools (to be developed) and external tools (to be integrated).

Phase 2: System Design and Architecture

- Implemented a modular web-based design with React.js for front-end, Node.js for API backends, and Python for tool core functionality.
- Implemented 3D visualization effects for dynamic activation of tools for greater realism and user interaction.Incorporate security measures such as role- based access control, data validation, and encryption to protect sensitive asset and user data.
- Focused on security, responsiveness, and cross-platform compatibility during the architectural planning

Phase 3: Development

- Evolved core functionality of Cyber Astra, which are:Scenario-based tool launcher interface,PCAP Viewer, Log Analyzer, Disk Imager, and OSINT Tool integration.
- Created interactive dashboards with smooth transitions and animations.
- Attached external OSINT tools and placed links to research-friendly tools with instant access for enhanced researchability.

Phase 4: Deployment

- All tools load dynamically upon selection of a scenario
- 3D animation and transition effects render properly
- Manual tools and external links are working
- Chatbot areas are fully functional
- The production environment is set up with all required dependencies (Node.js, Python, etc.) installed via package managers.
- The system is released to target users with instructions for usage. A feedback form is embedded to gather input from users for improvements and error reports.
- There are no performance issues or broken components

3. System Requirements Study

The system's functional and quality requirements are described in this section. It gives a thorough rundown of the system's attributes.

3.1 User Requirement

The inputs and outputs of the system are thoroughly explained. It also contains a description of the software communication interfaces and some primitive prototypes of user interfaces.

3.2 Hardware and Software Requirement Specification

This includes the very minimum requirements required to maintain this system's correct operation. The project can only proceed if the following minimal requirements are fulfilled:

3.2.1 Server-side Hardware Requirement:

User	Particulars	Client System	Server System
Admin /Cyber Security- Analyst (AnyPlatform)	Operating System	Windows,Linux,mac -os	Windows Server
	Processor	Dual Core (Minimum)	Intel Xeon
	Hard disk	10GB (Minimum)	50 GB SSD
	RAM	512MB (Minimum)	8 GB Or Higher

Table 3.2.1 Server-side Requirement

3.2.2 Software Requirements:

For Which	Software
Operating System	Windows,Linux, Mac OS
Tools	Visual Studio Code,React.js,Node.js.Python

Table 3.2.2 Software Requirements

3.2.3 Client-side Requirements:

For Which	Requirement
Browser	Any Compatible Browser Device

Table 3.2.3 Client-side

4. System Analysis

4.1 Features of New System

- Cyber Astra incorporates in-house-developed tools for PCAP analysis, disk imaging, log analysis, and OSINT, loading the tools specific to a chosen scenario.
- Scenarios create a hands-on setting with responsive layout, tool visibility control, and visual effects (such as 3D animations) on tool execution.
- Fully responsive UI with support for various devices, built to scale with additional tools, users, and lab scenarios.
- Implements encryption, secure uploads, access control, and aligns with industry standards like NIST, ITIL, and ISO 27001.
- Designed to accommodate more tools, users, and data inputs, and to facilitate ease of performance as the platform expands.
- The user interface is made to be entirely responsive and easy to use on desktops, tablets, and mobiles for wider reach.

4.2 UML Diagrams

4.2.1 Class diagram:

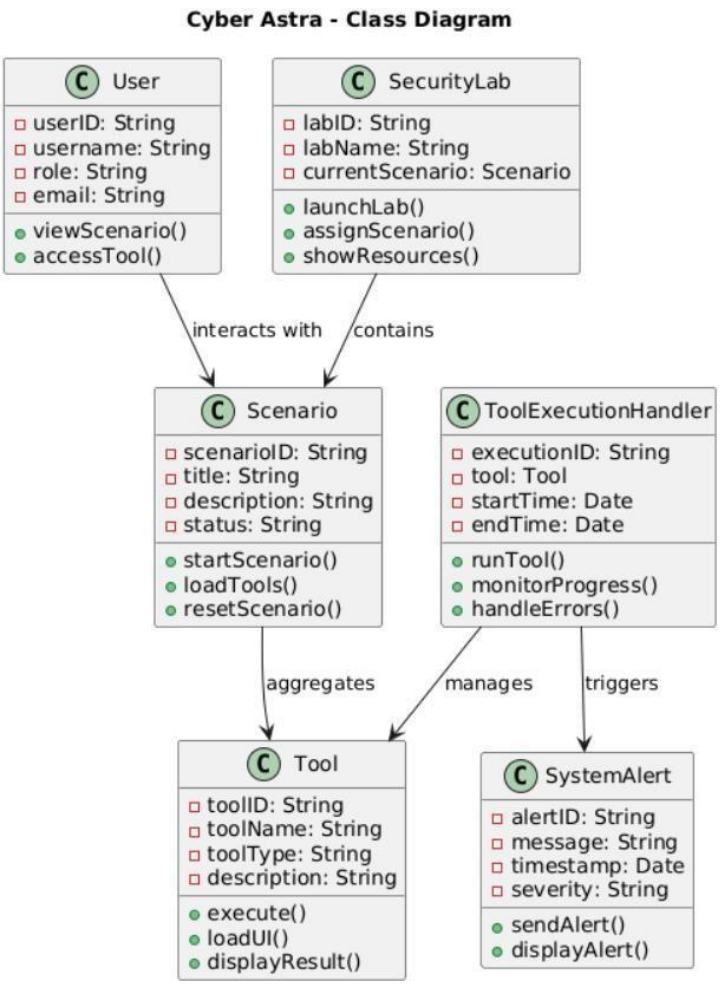


Fig. 4.2.1 Class diagram

4.2.2 Use Case Diagram:

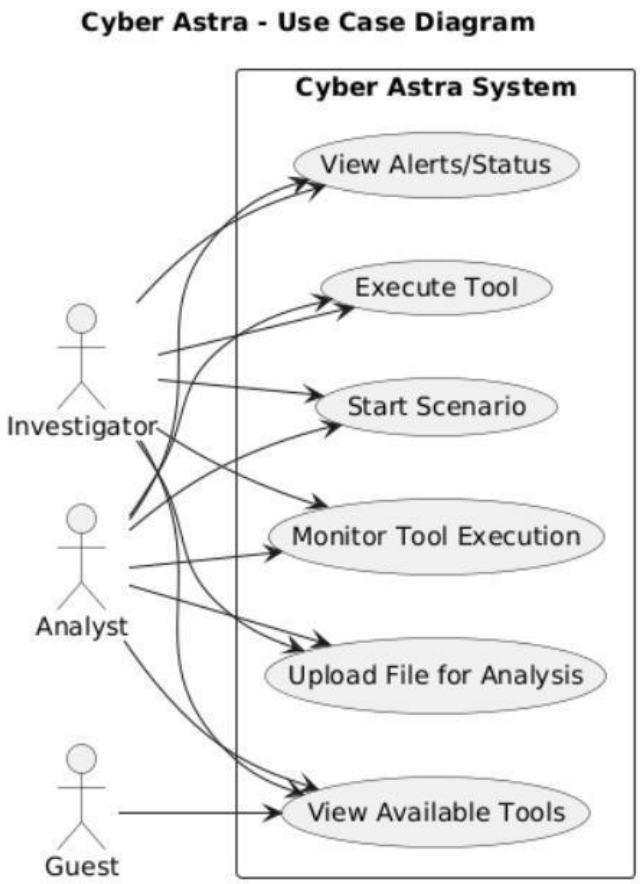


Fig. 4.2.2 Use Case Diagram

4.2.3 DFD Diagram

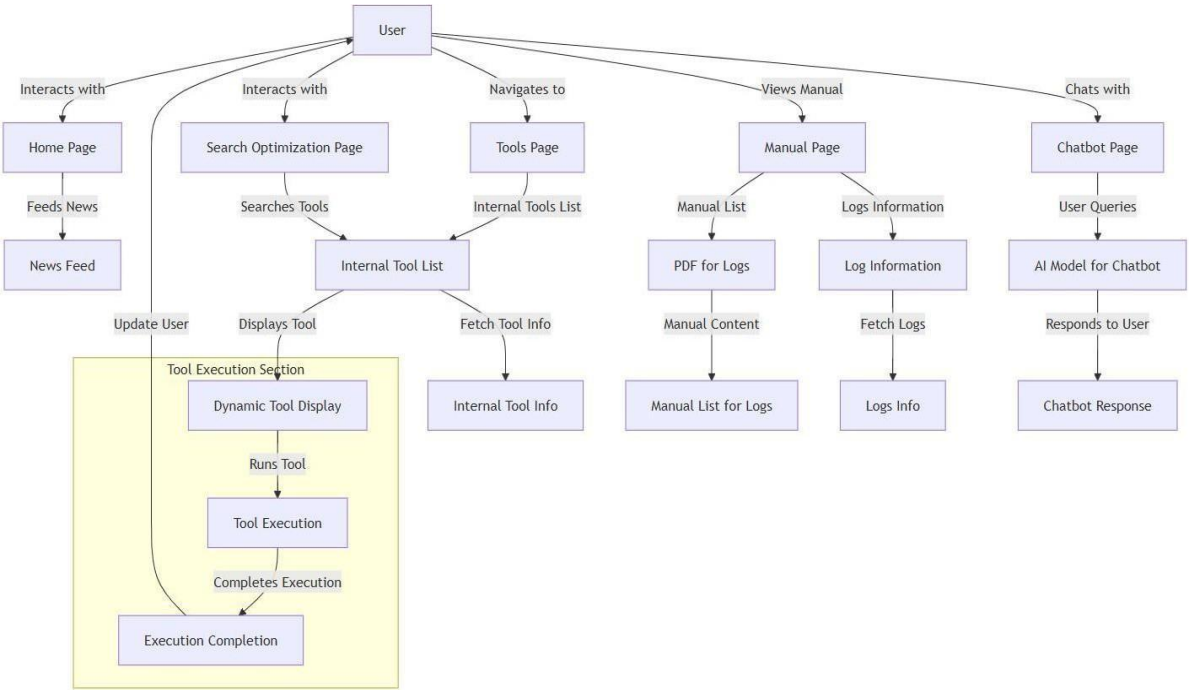


Fig. 4.2.3 DFD Diagram

4.2.4 Sequence Diagram

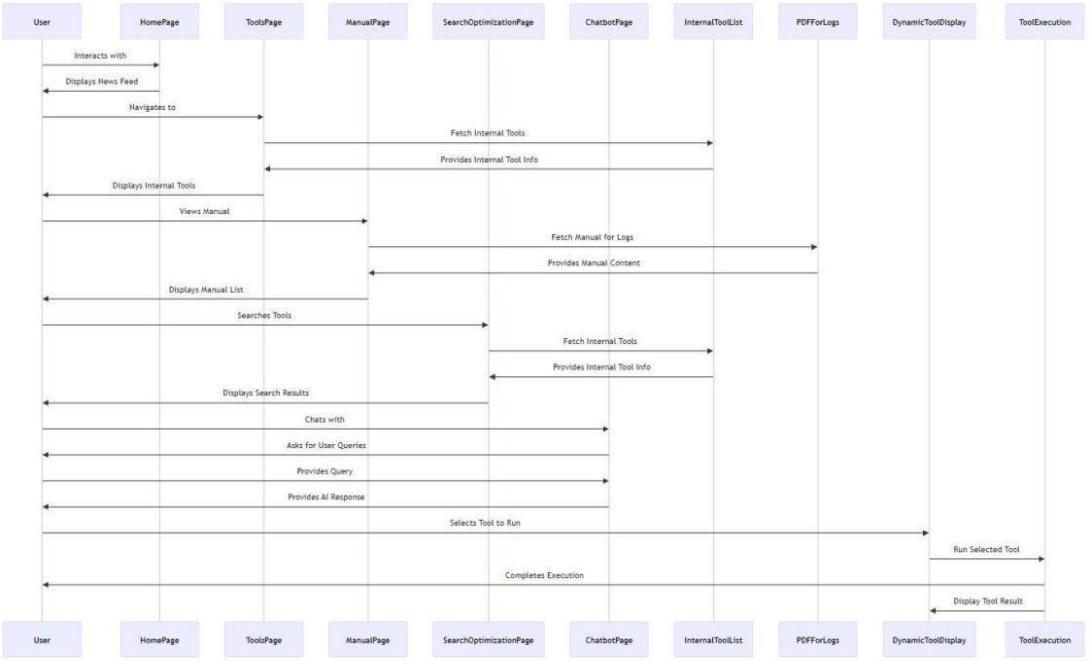


Fig. 4.2.4 Sequence Diagram

4.2.5 Activity Diagram

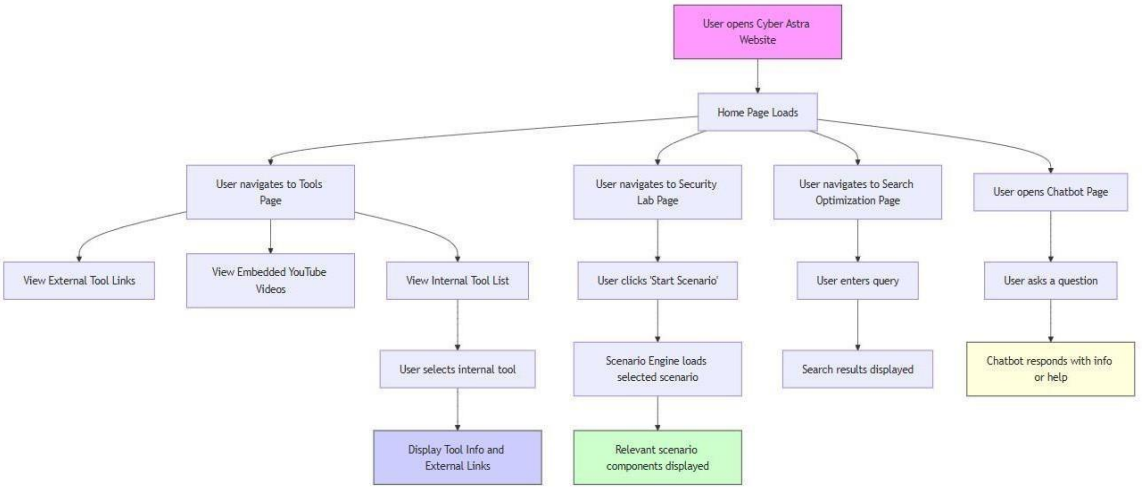


Fig. 4.2.5 Activity Diagram

4.2.6 ER Diagram

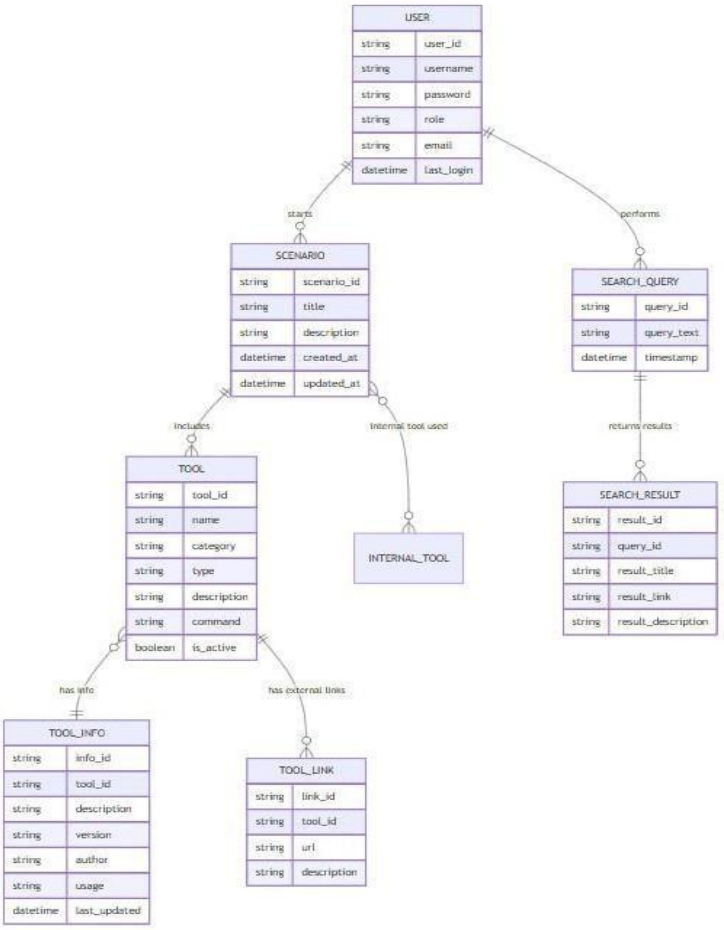


Fig. 4.2.6 ER Diagram

5. Implementation Planning and Details

5.1. User Documentation:

Purpose: Cyber Astra user documentation will take the users through the process of registering and give them step-by-step instructions on how to work on and access the most important features of the site. This documentation will help the users make efficient use of the Cyber Astra toolset and comprehend the functionalities available.

5.2 Front-End Side

5.2.1 Home Page : Includes News Api For Fetching Real Time News

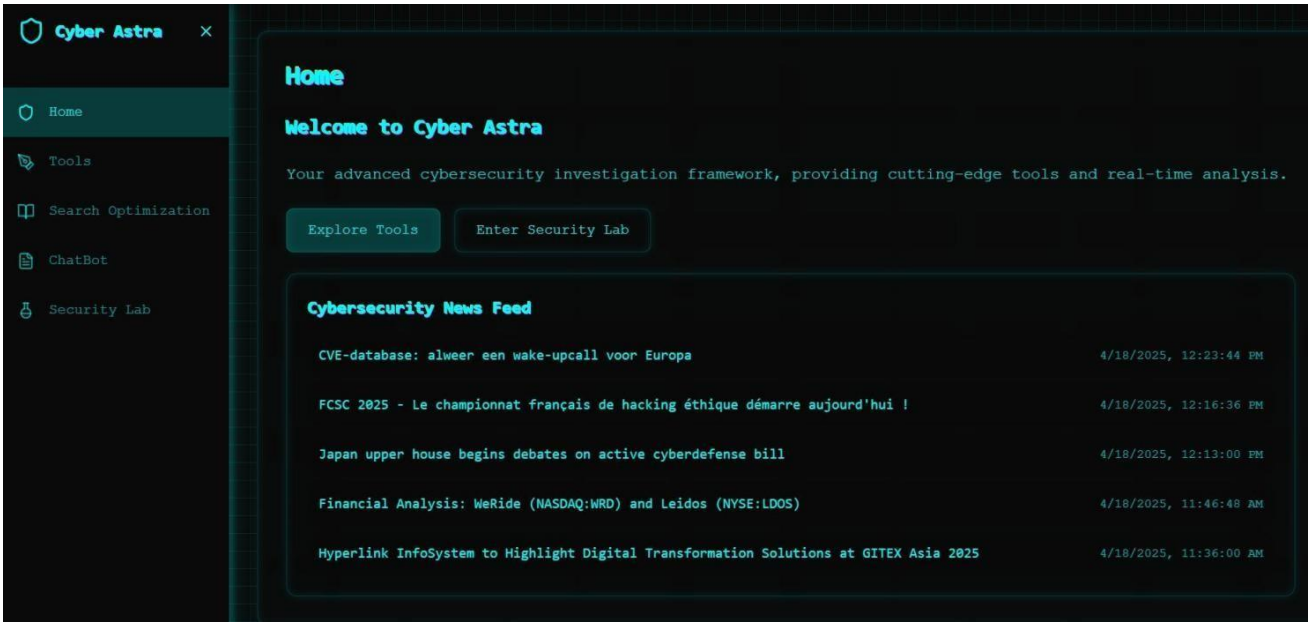


Fig 5.2.1 Home Page - CyberSecurity News, Main Page

5.2.2 News Information : One of link is clicked and it takes to the specified news page

Fig 5.2.2 News Information - After Clicking Link It Is Displayed

5.2.3 Search Optimization : Can Search If In Doubt While Investigation.

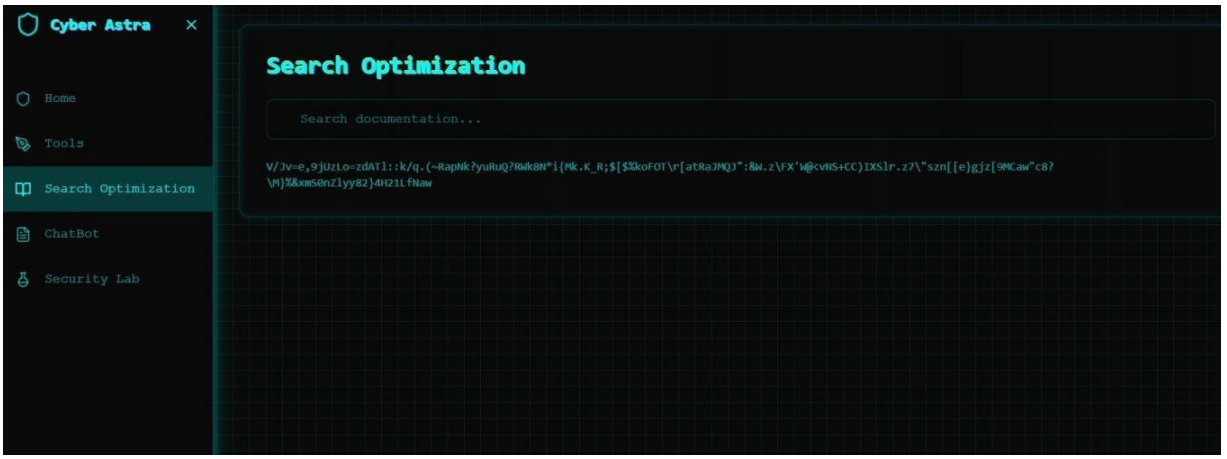


Fig 5.2.3 Search Optimization - All Data Can Be Searched

5.2.4 Searched Query :

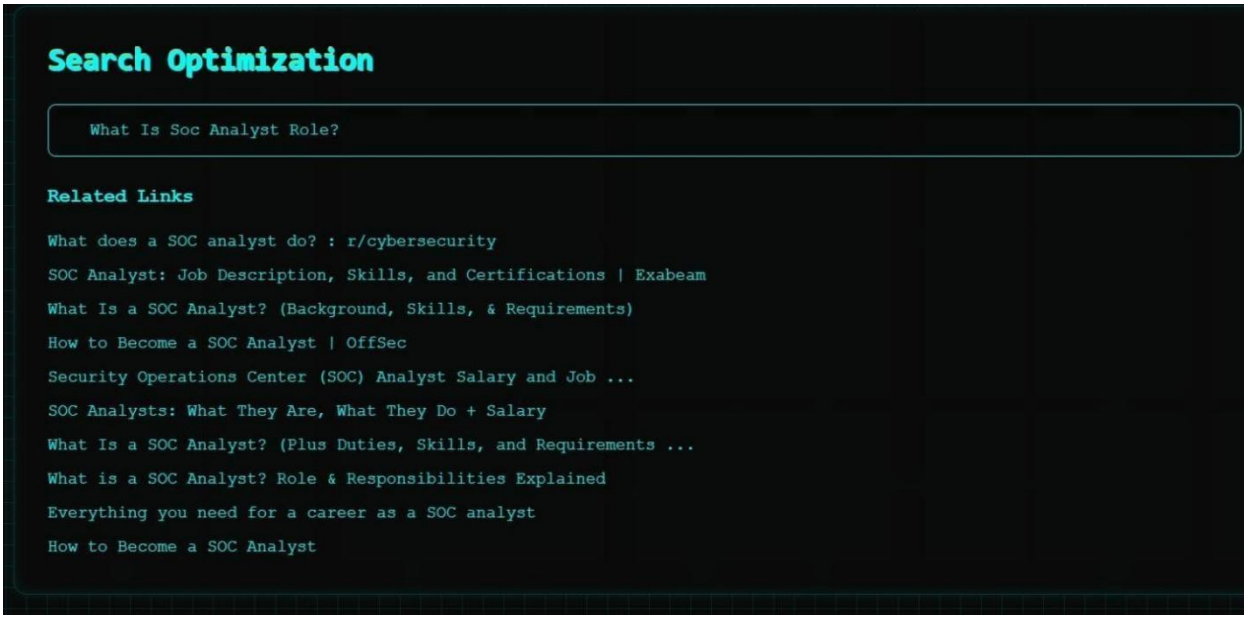


Fig 5.2.4 Searched Query- Demonstration

5.2.5 Searched Query Results : Result Obatined/Link Obtained

Fig 5.2.5 Searched Query Results - Results After Search

5.2.6 Chatbot : For User Queries

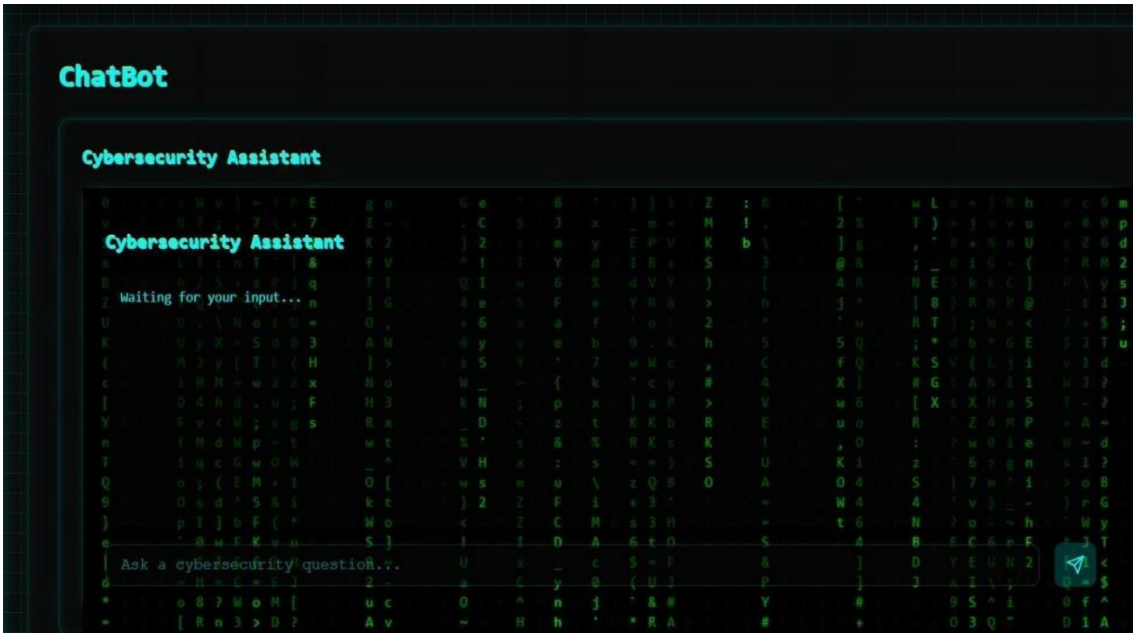


Fig 5.2.6 Chatbot - For Queries

5.2.7 Chatbot - Search Queries And Results:

Fig 5.2.7-1 Chatbot - Search queries Answered With Google Support

Fig 5.2.7-2 Chatbot - Search Queries And Results

5.2.8 Tools Page : Different Tools Used In Investigation

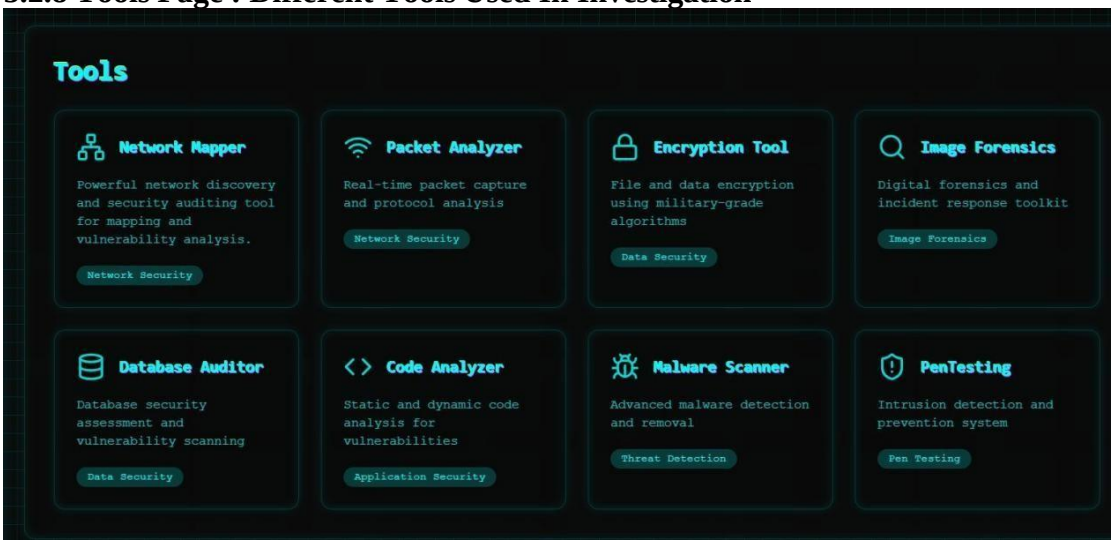


Fig 5.2.8 Tools Page

5.2.8.1 Network Mapper:

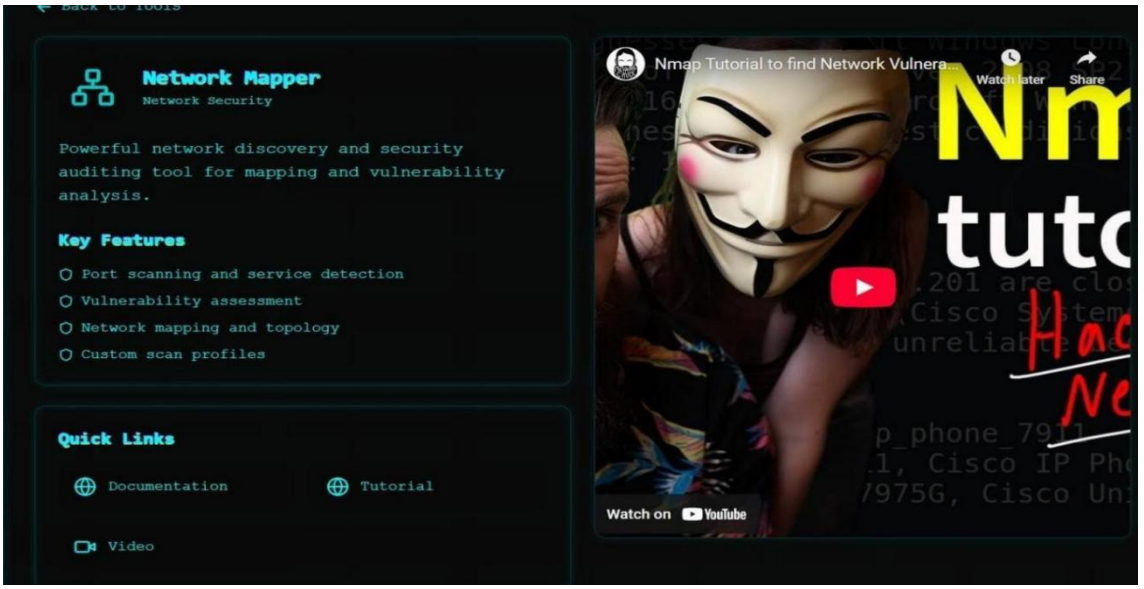


Fig 5.2.8.1-1 Network Mapper - Page With Youtube Links, Tutorial Links

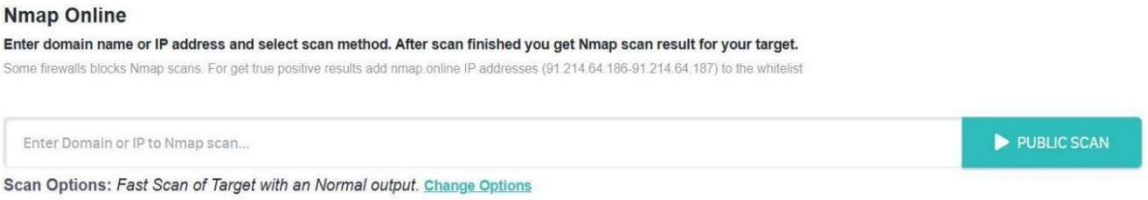


Fig 5.2.8.1-2 Network Mapper - Nmap Online Tool For Investigators

5.2.8.2 Packet Analyzer:

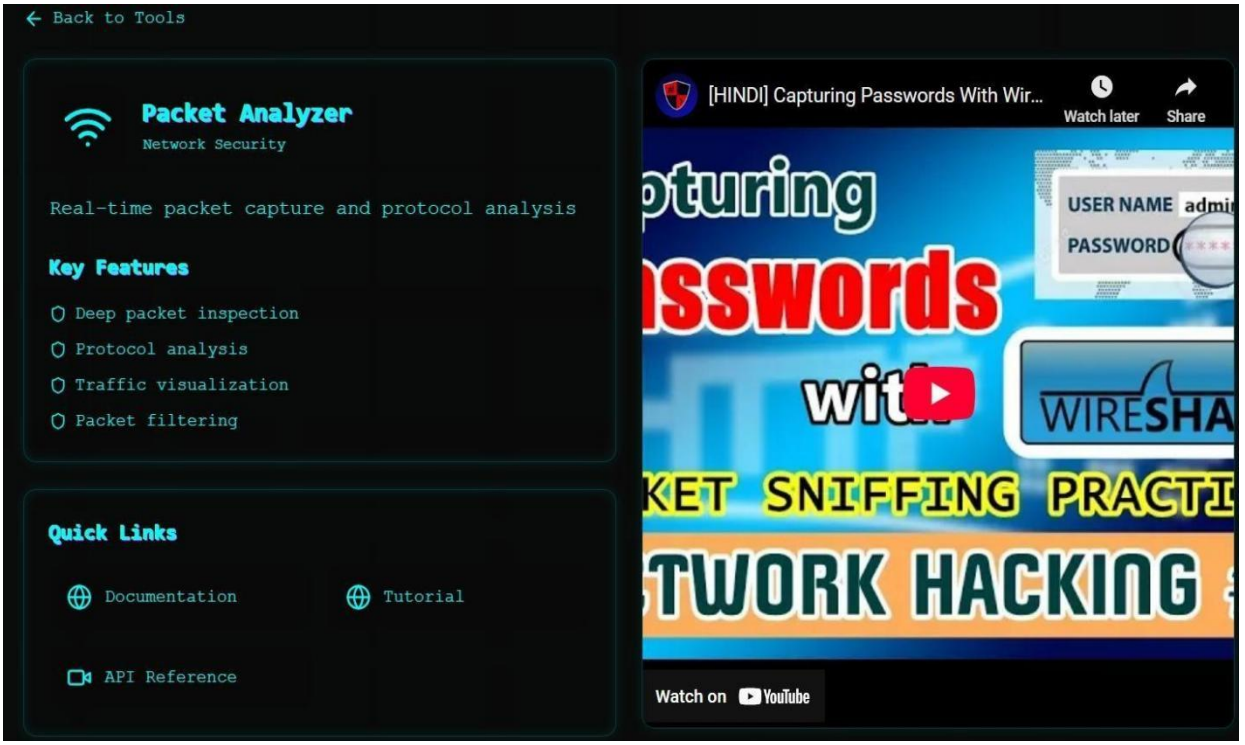


Fig 5.2.8.2-1 Packet Analyzer - Page With Youtube Links, Tutorial Links

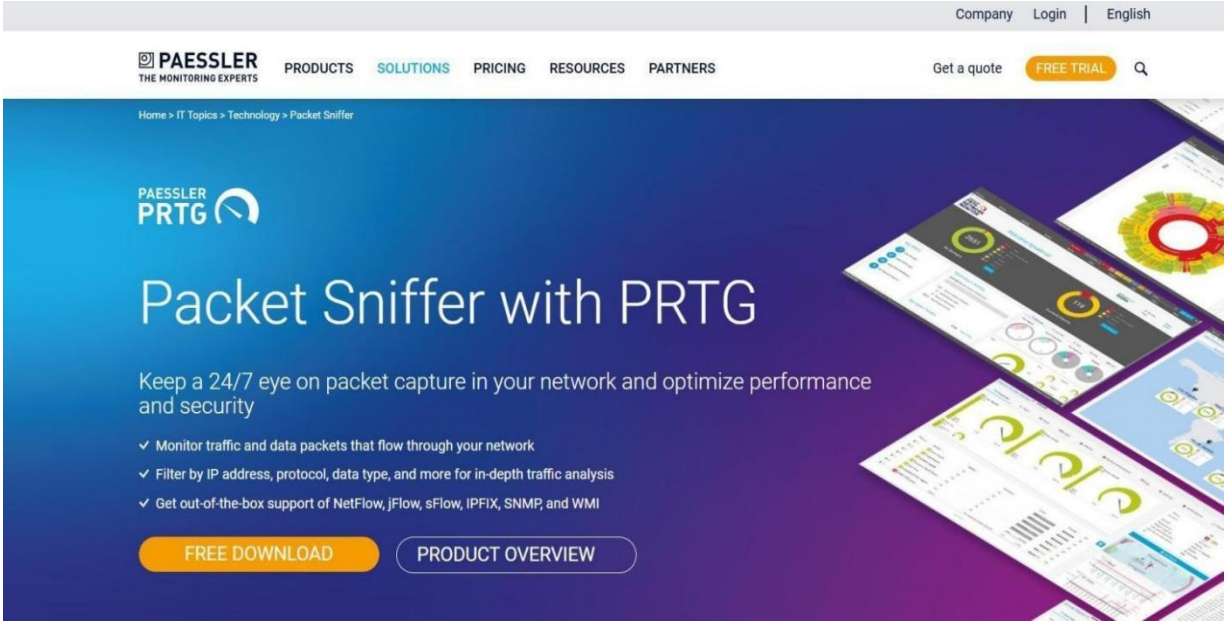


Fig 5.2.8.2-2 Packet Analyzer : Tool For Testing

5.2.8.3 Encryption Tool:

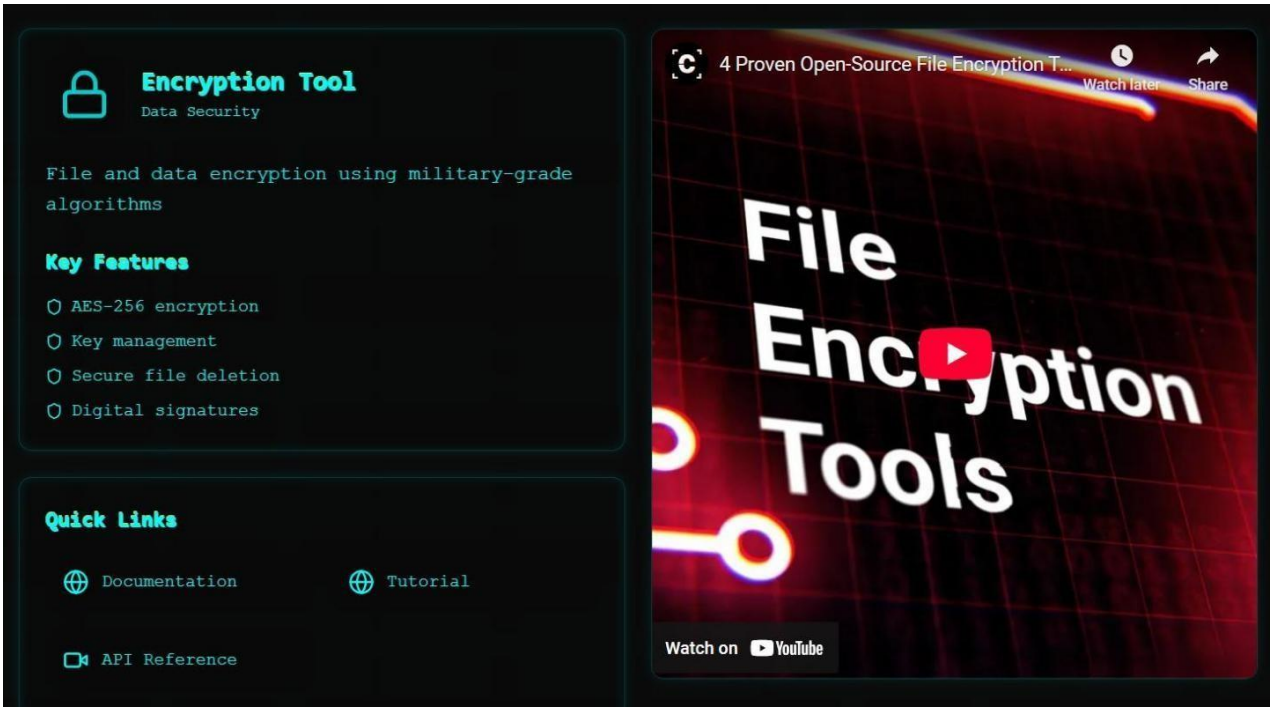


Fig 5.2.8.3-1 Encryption Tool : Youtube Links, Tutorial Links

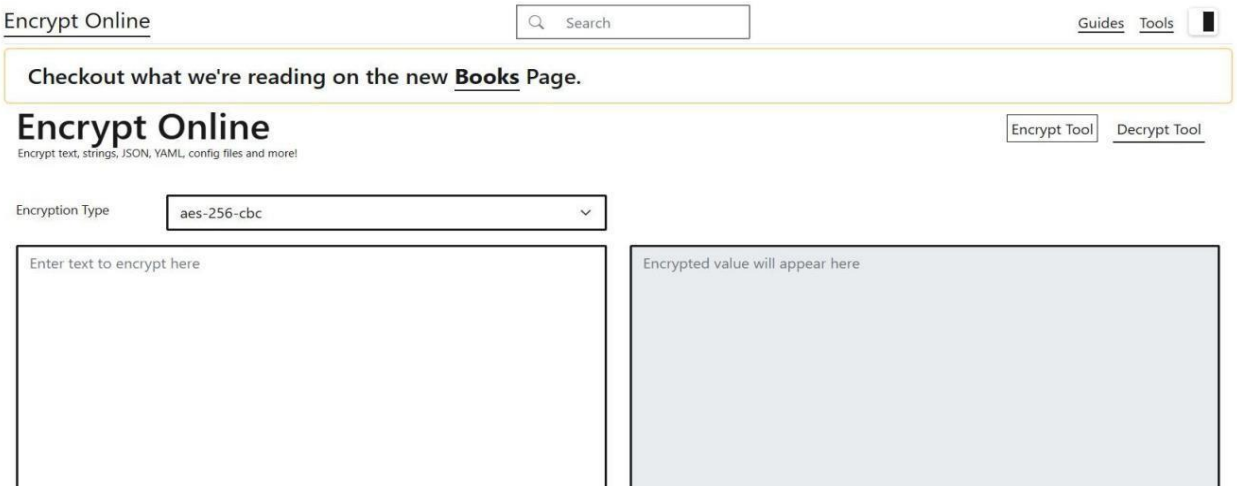


Fig 5.2.8.3-2 Encryption Tool : Tool For Investigation

5.2.8.4 Image Forensics:

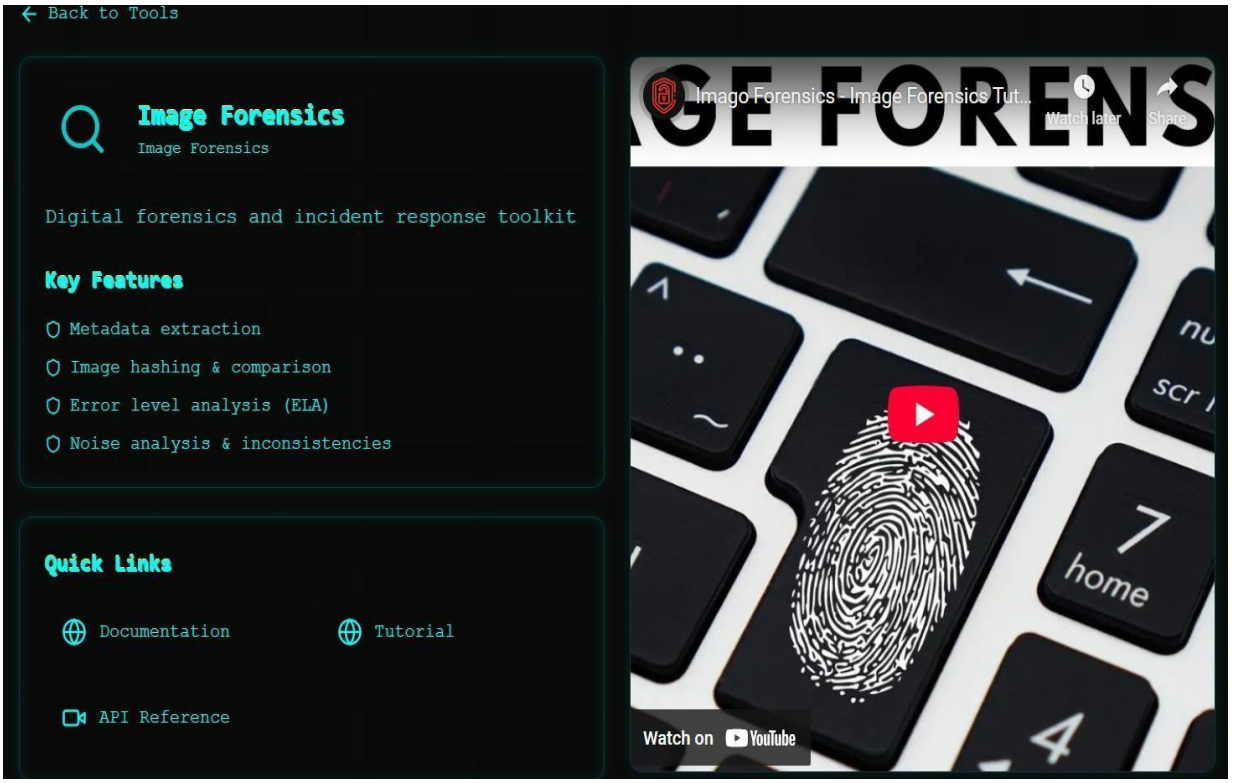


Fig 5.2.8.4-1 Image Forensics : Youtube Links, Tutorial Links

Fig 5.2.8.4-2 Image Forensics : Tools For Investigation

5.2.8.5 Databse Auditor:

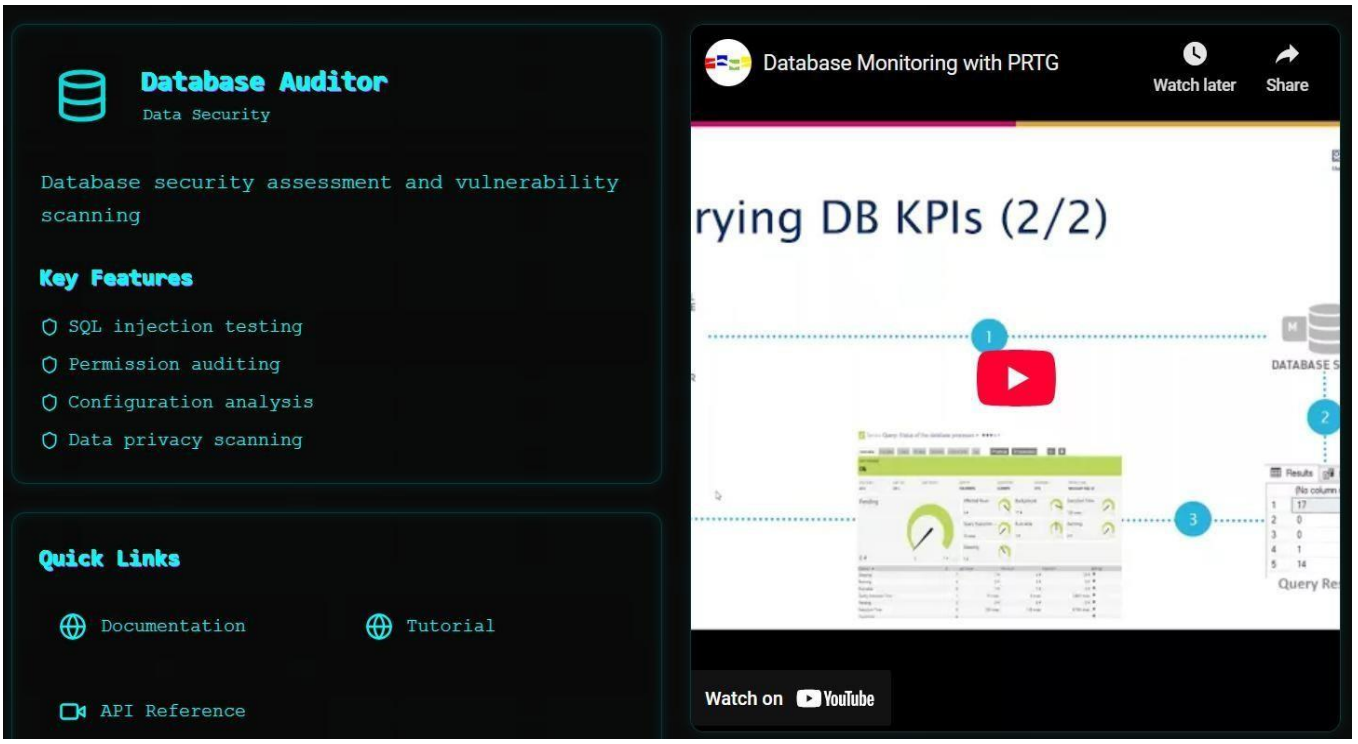


Fig 5.2.8.5-1 Database Auditor - Youtube Links

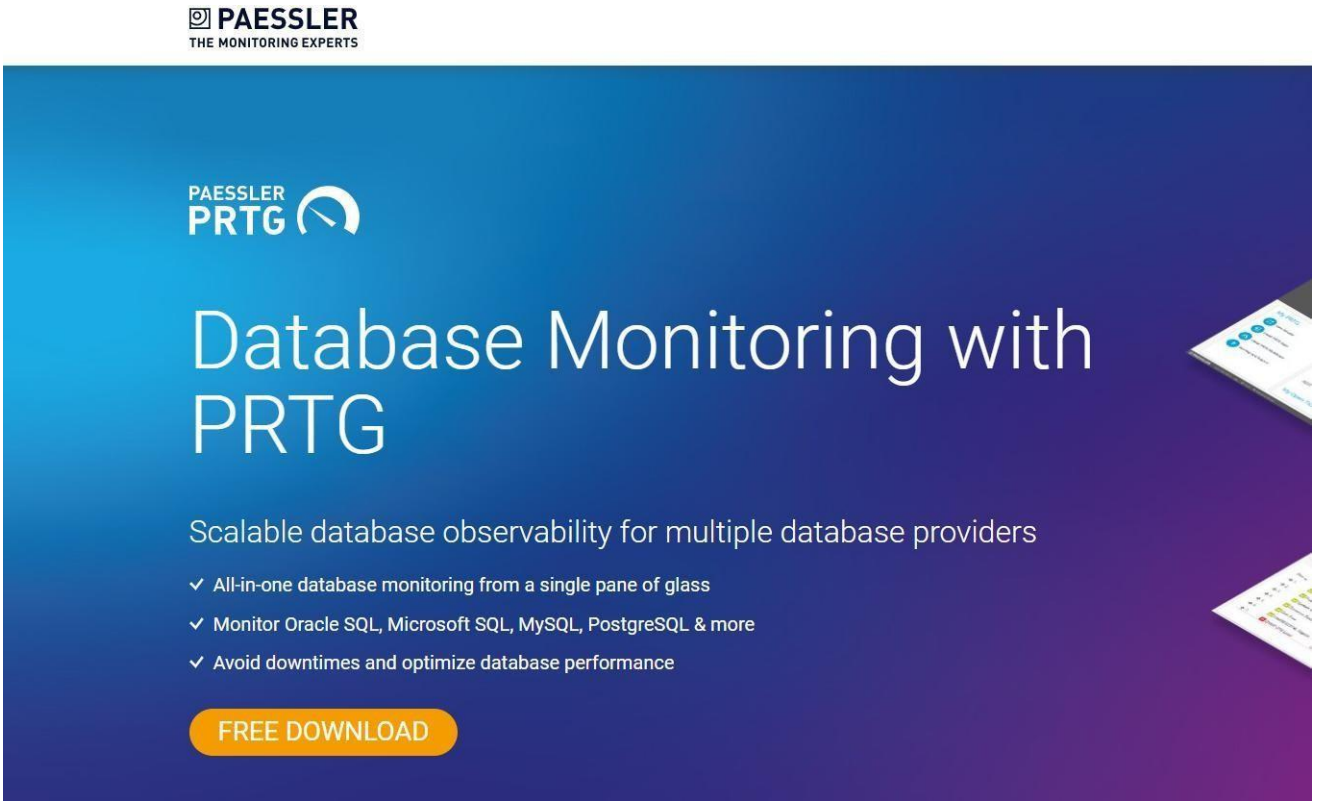


Fig 5.2.8.5-2 Databse Auditor : Tool

5.2.8.6 Code Analyzer:

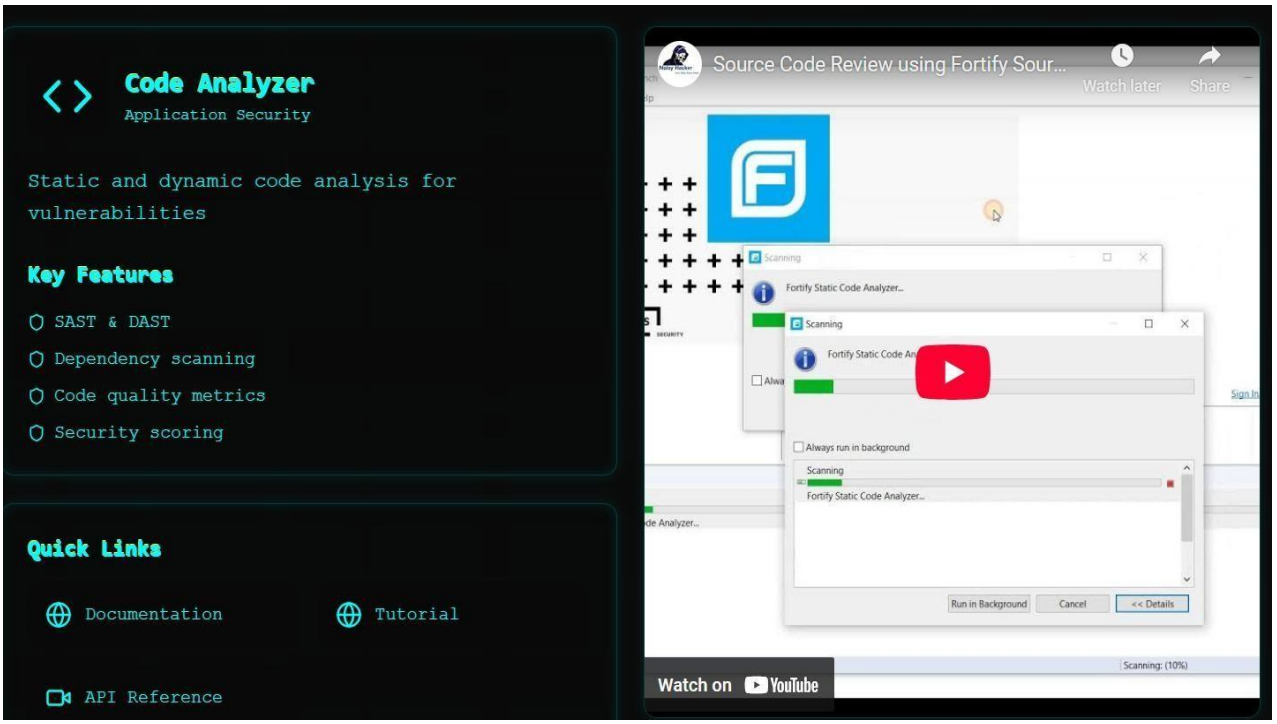


Fig 5.2.8.6-1 Code Analyzer : Tutorial Links

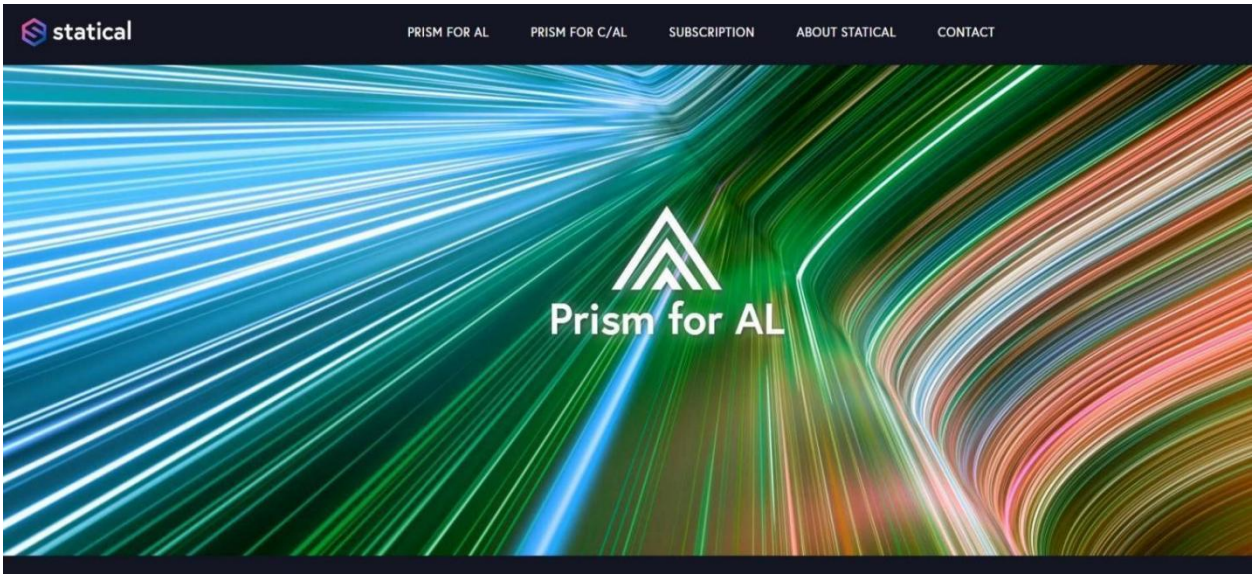


Fig 5.2.8.6-2 Code Analyzer : Tool

5.2.8.7 Malware Scanner:

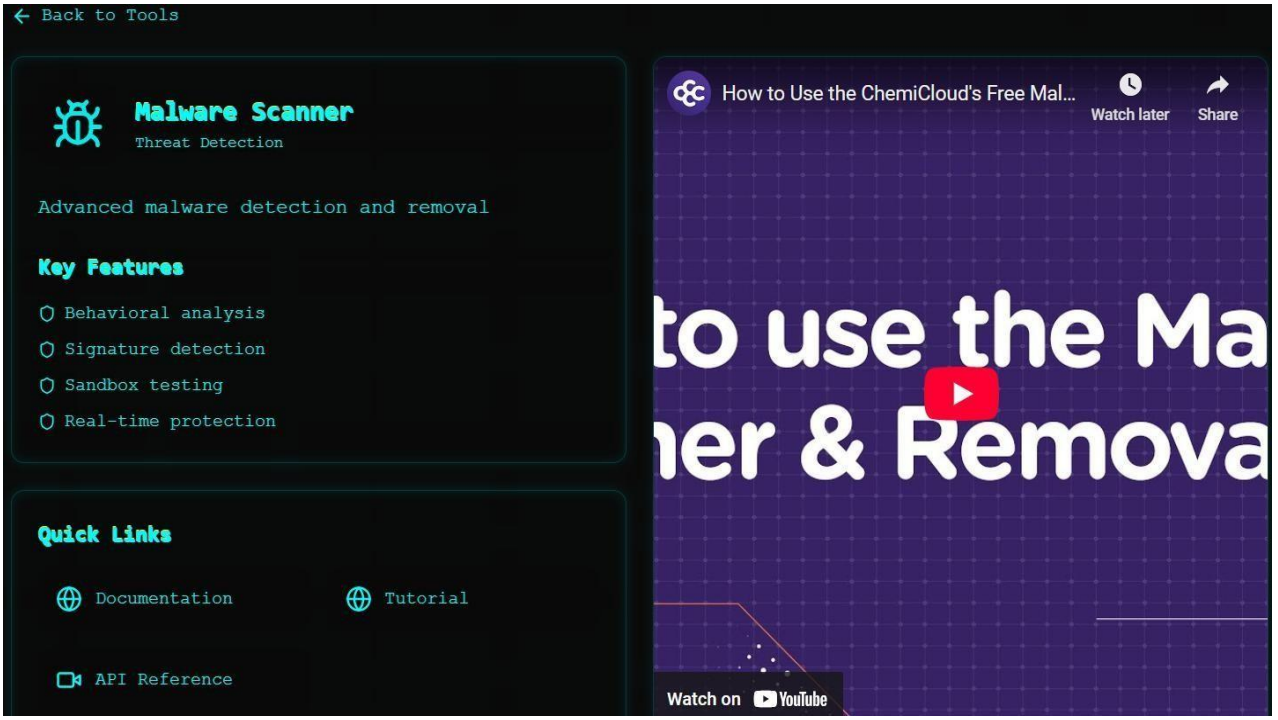


Fig 5.2.8.7-1 Malware Scanner : Youtube Links, Tutorial Links

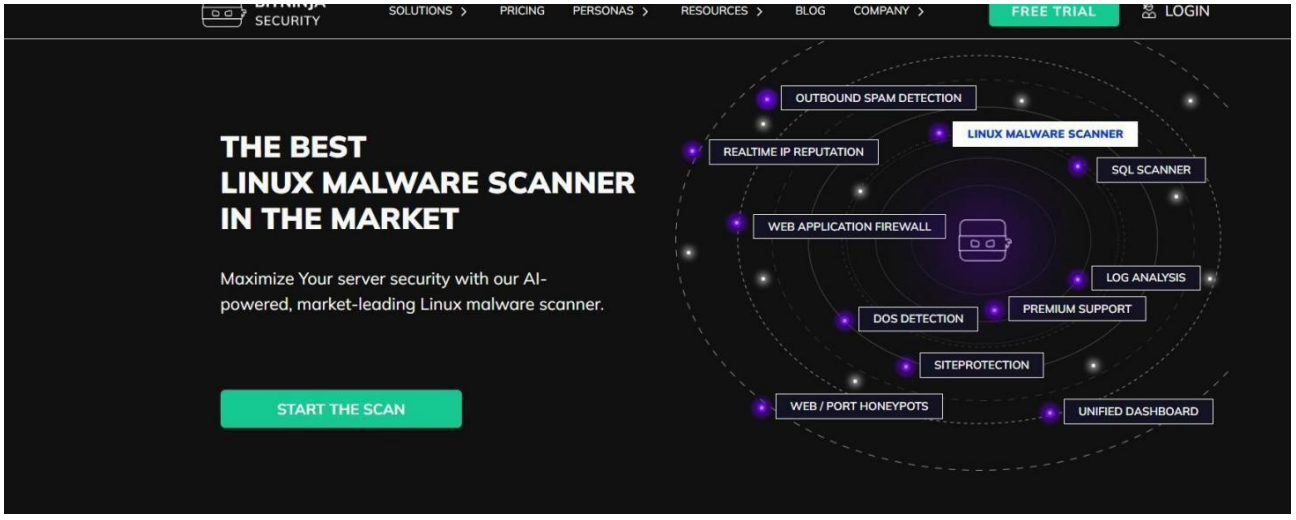


Fig 5.2.8.7-2 Malware Scanner : Tool

5.2.8.8 Pen-testing:

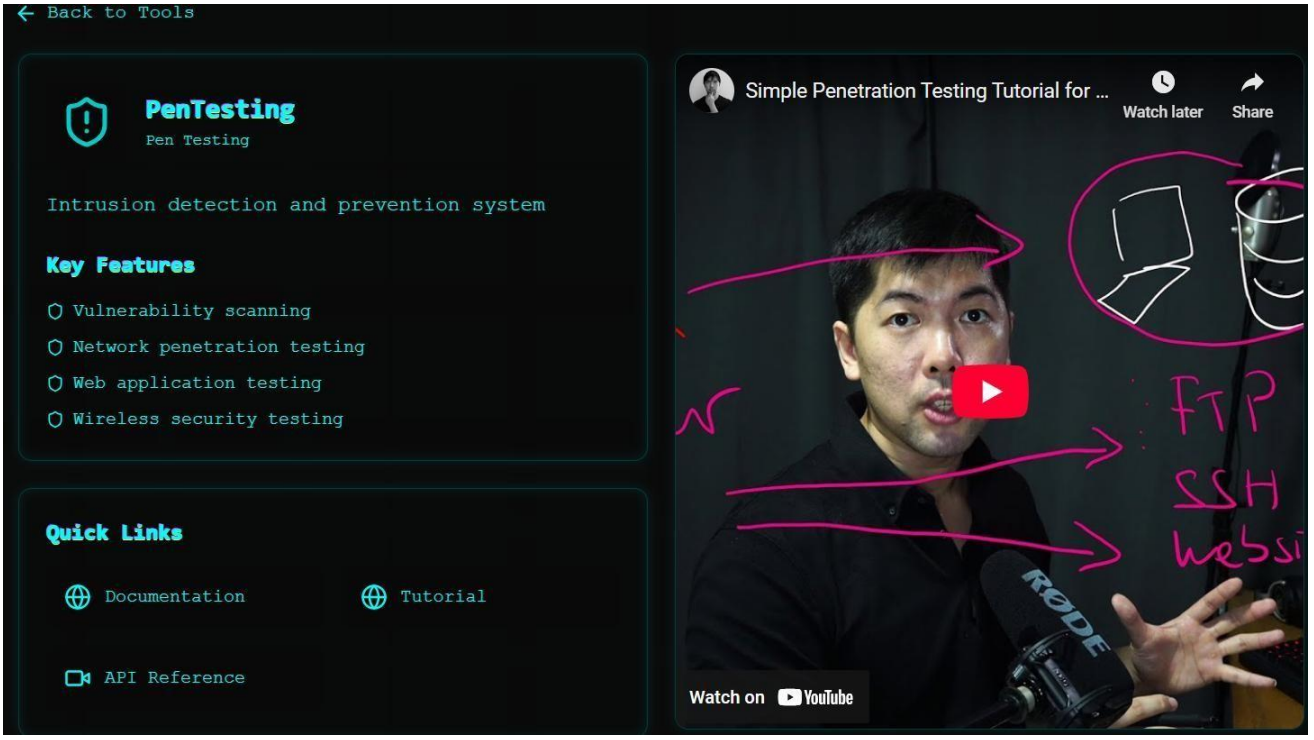


Fig 5.2.8.8-1 Pen Testing : Yotube Links, Tutorial Links

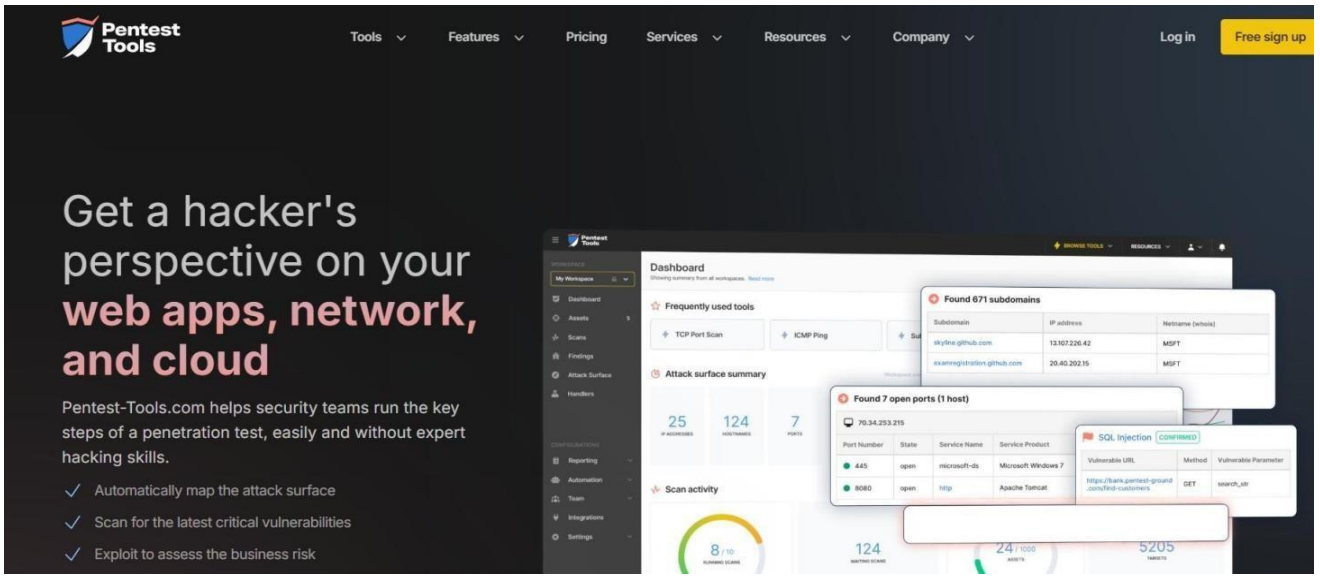


Fig 5.2.8.8-2 Pen-testing: Tool

5.2.9 Security Lab : Various Tools Manually Implemented :

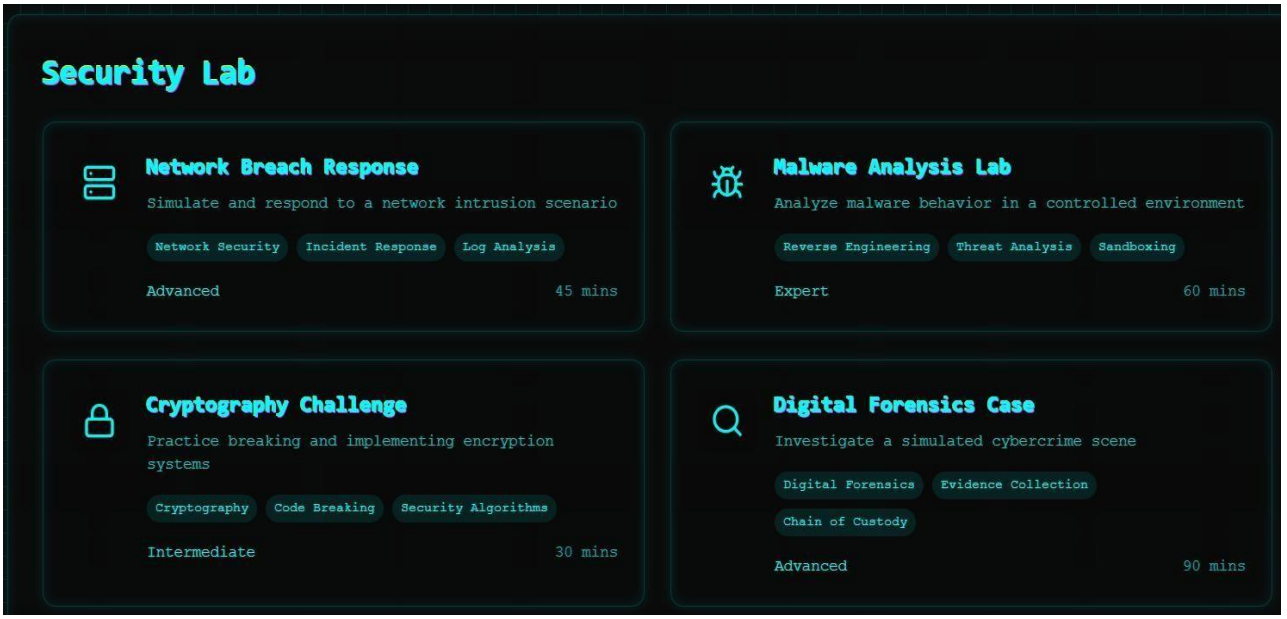


Fig 5.2.9 Security Lab

5.2.9.1 Network Breach Response : PCAP Viewer And Log Analyzer

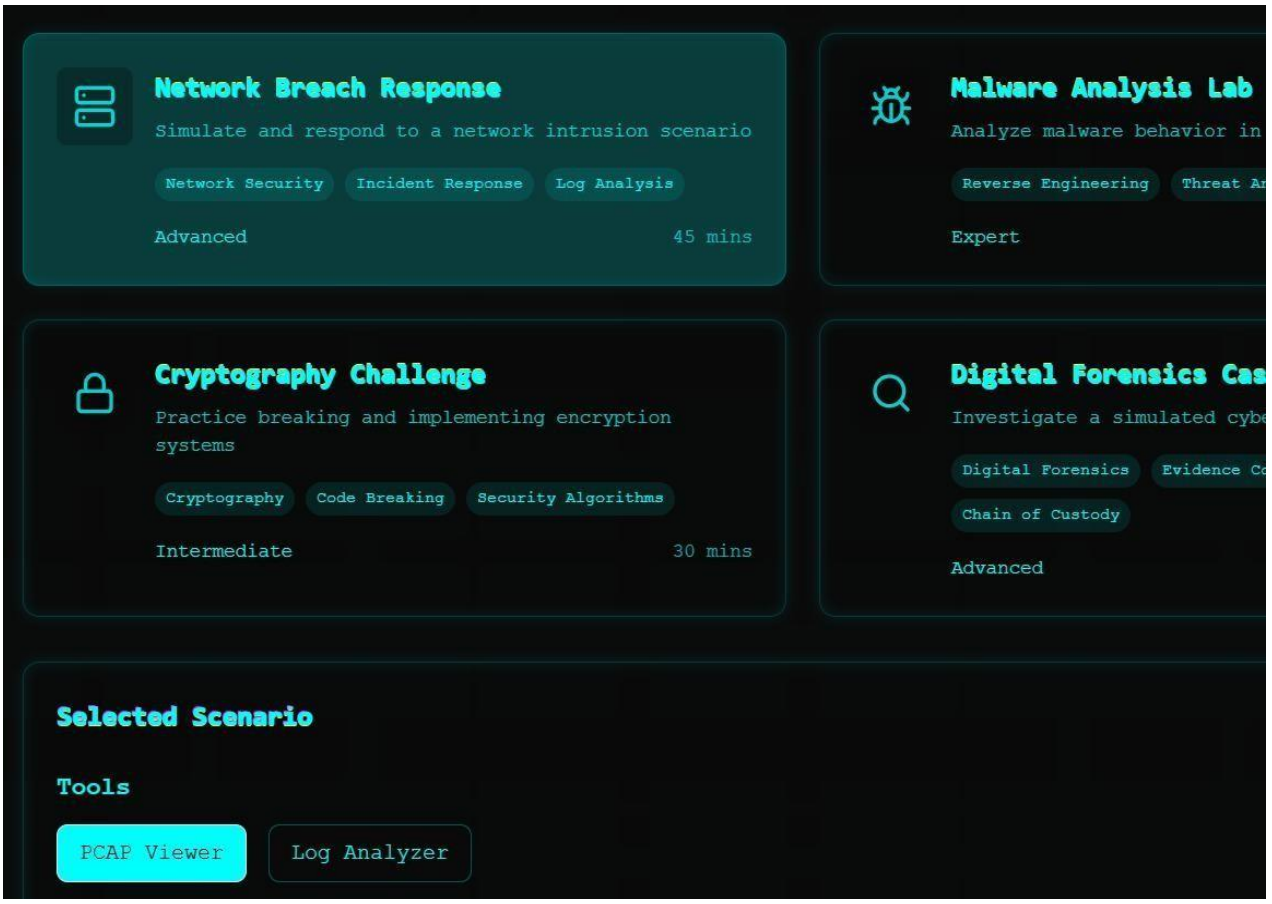


Fig 5.2.9.1 Network Breach Response

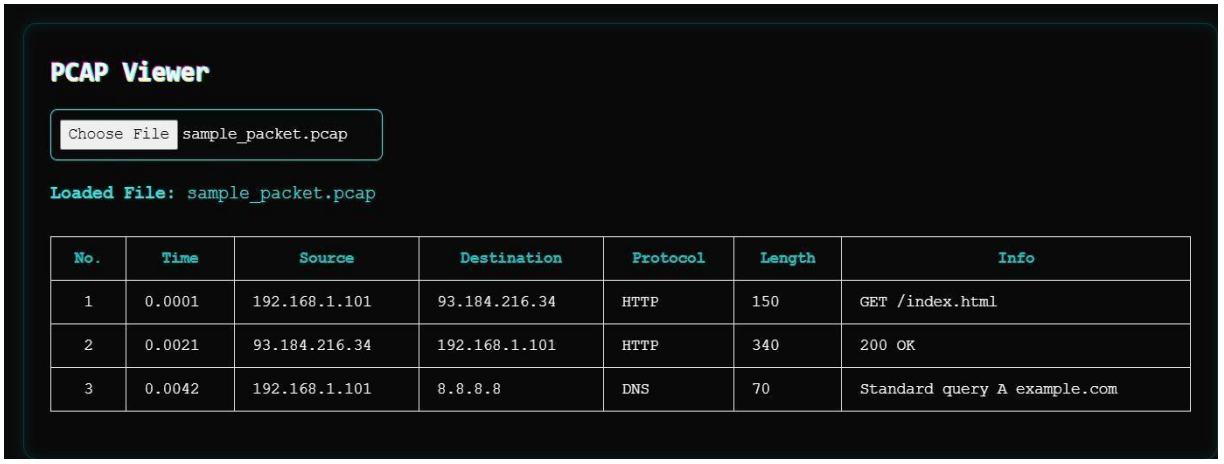


Fig 5.2.9.1-1 PCAP Viewer

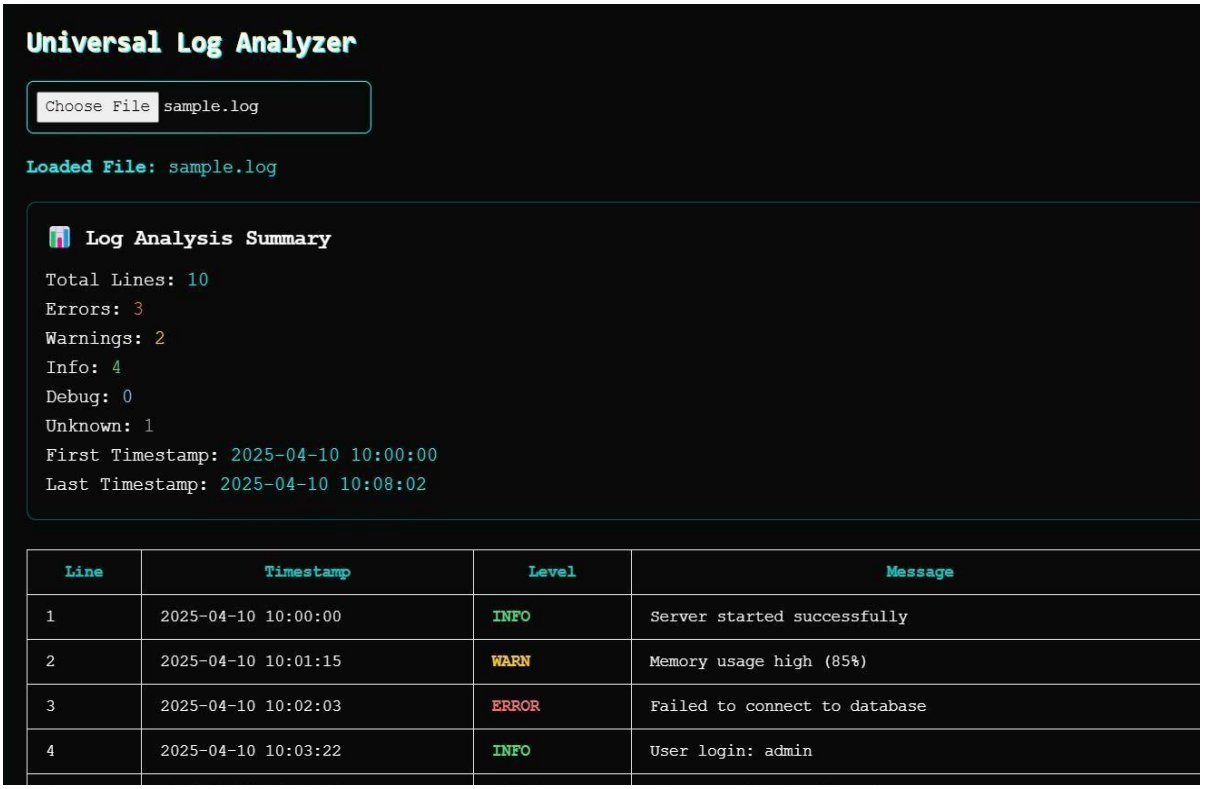


Fig 5.2.9.1-2 Log Analyzer

5.2.9.2 Malware Analysis Lab : Dyamic And Static Analyzer

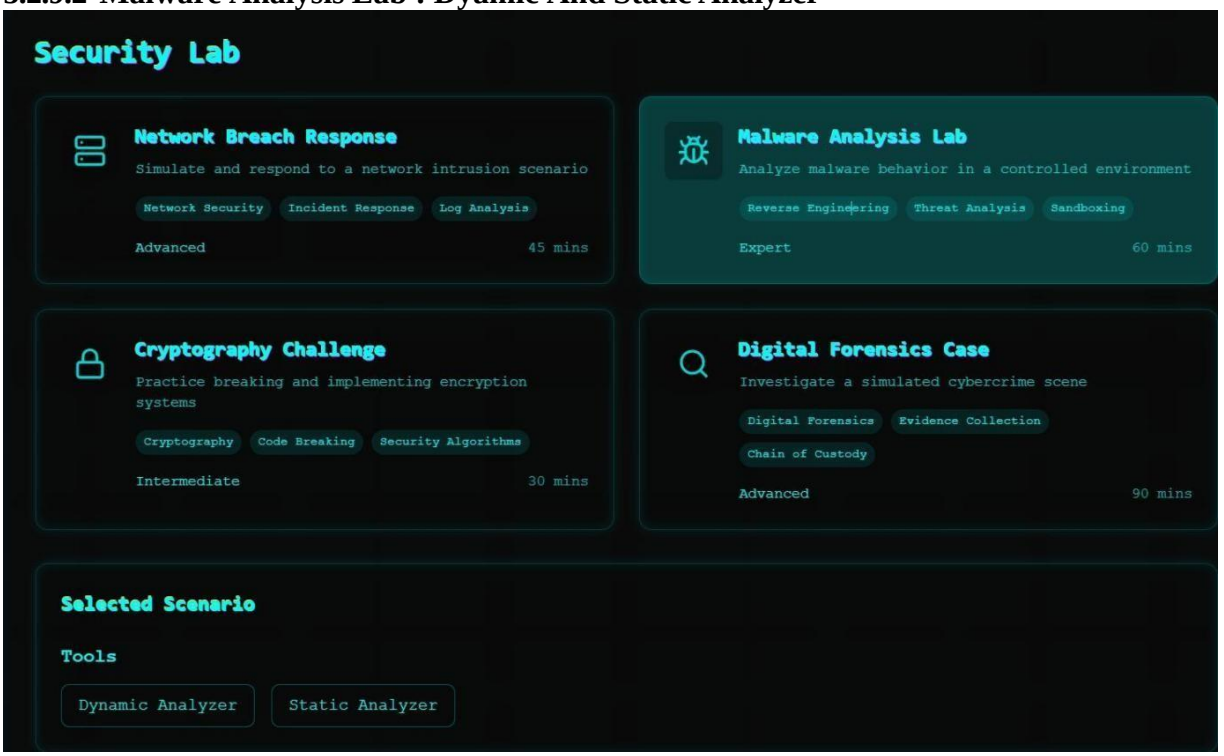
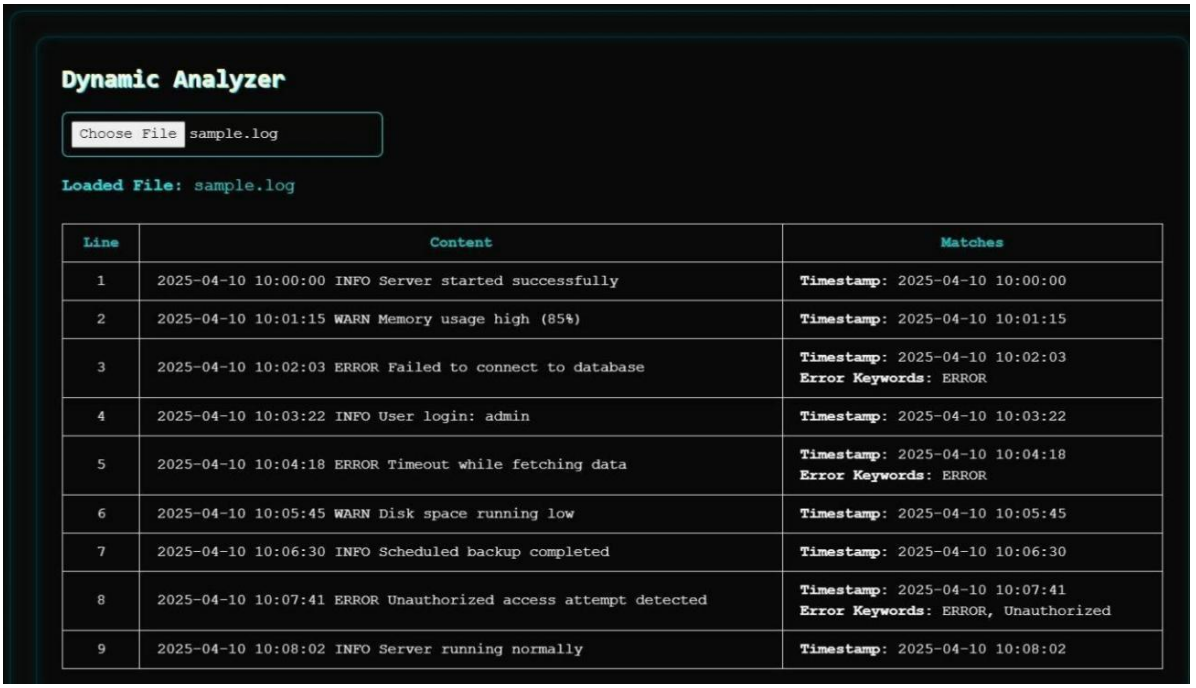


Fig 5.2.9.2 Malware Analysis Lab



Dynamic Analyzer

Choose File sample.log

Loaded File: sample.log

Line	Content	Matches
1	2025-04-10 10:00:00 INFO Server started successfully	**Timestamp:** 2025-04-10 10:00:00
2	2025-04-10 10:01:15 WARN Memory usage high (85%)	**Timestamp:** 2025-04-10 10:01:15
3	2025-04-10 10:02:03 ERROR Failed to connect to database	**Timestamp:** 2025-04-10 10:02:03 **Error Keywords:** ERROR
4	2025-04-10 10:03:22 INFO User login: admin	**Timestamp:** 2025-04-10 10:03:22
5	2025-04-10 10:04:18 ERROR Timeout while fetching data	**Timestamp:** 2025-04-10 10:04:18 **Error Keywords:** ERROR
6	2025-04-10 10:05:45 WARN Disk space running low	**Timestamp:** 2025-04-10 10:05:45
7	2025-04-10 10:06:30 INFO Scheduled backup completed	**Timestamp:** 2025-04-10 10:06:30
8	2025-04-10 10:07:41 ERROR Unauthorized access attempt detected	**Timestamp:** 2025-04-10 10:07:41 **Error Keywords:** ERROR, Unauthorized
9	2025-04-10 10:08:02 INFO Server running normally	**Timestamp:** 2025-04-10 10:08:02

Fig 5.2.9.2-1 Dynamic Analyzer

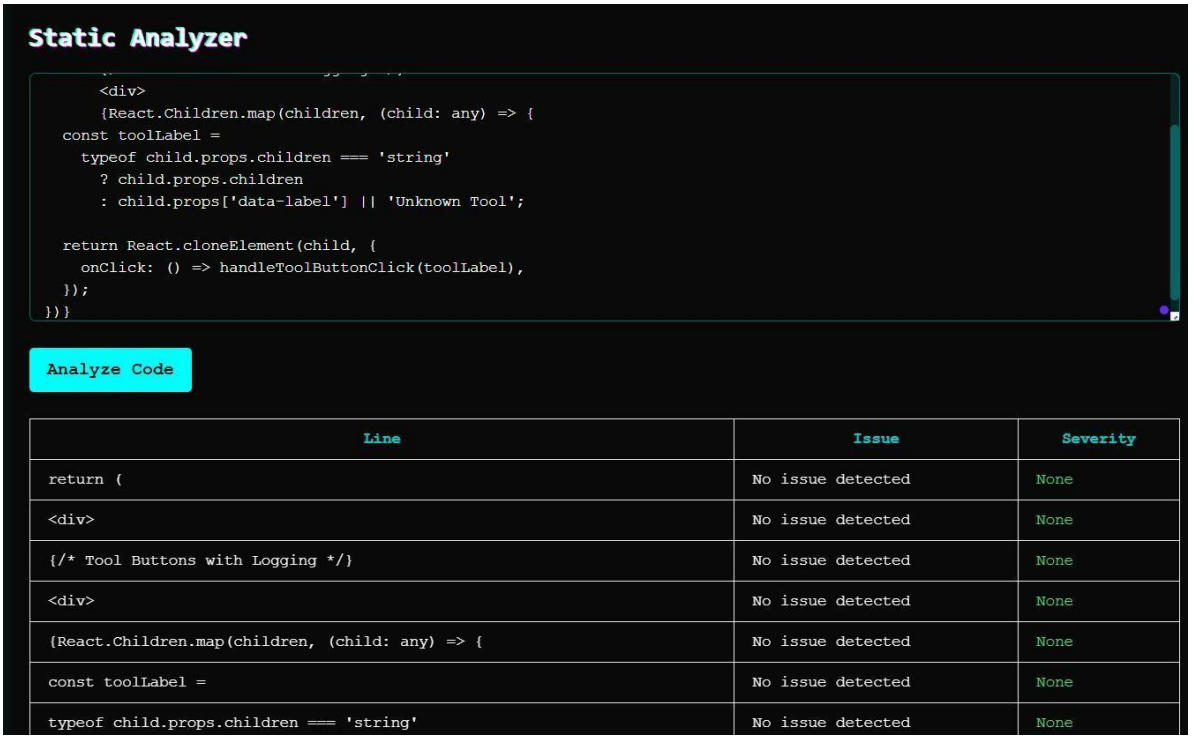


Fig 5.2.9.2-2 Static Analyzer

5.2.9.3 Crytography Challenge : Key Analyzer And Encryptor Tool

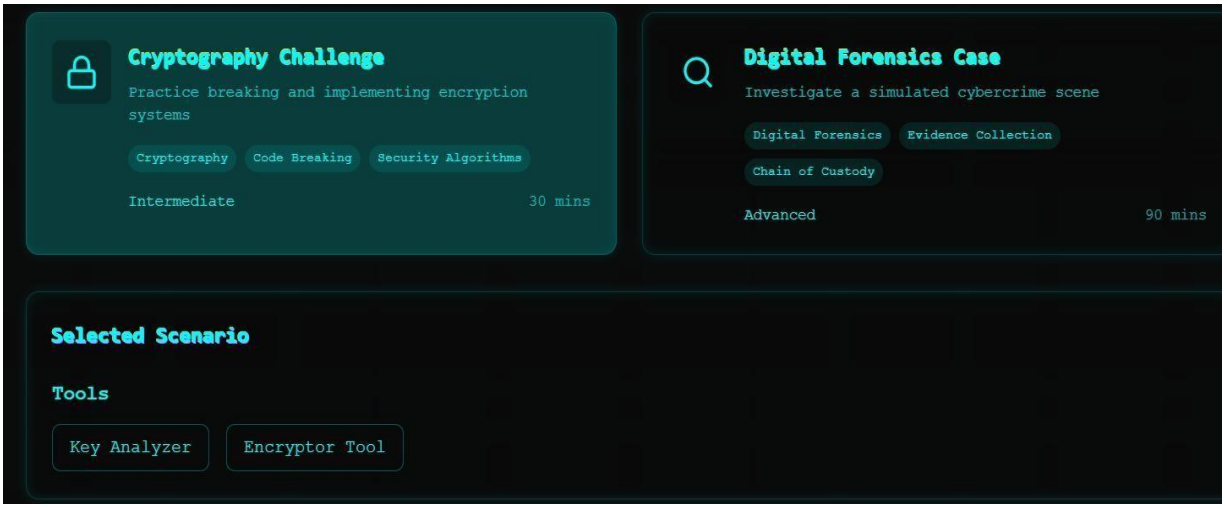


Fig 5.2.9.3 Crytography Challenge

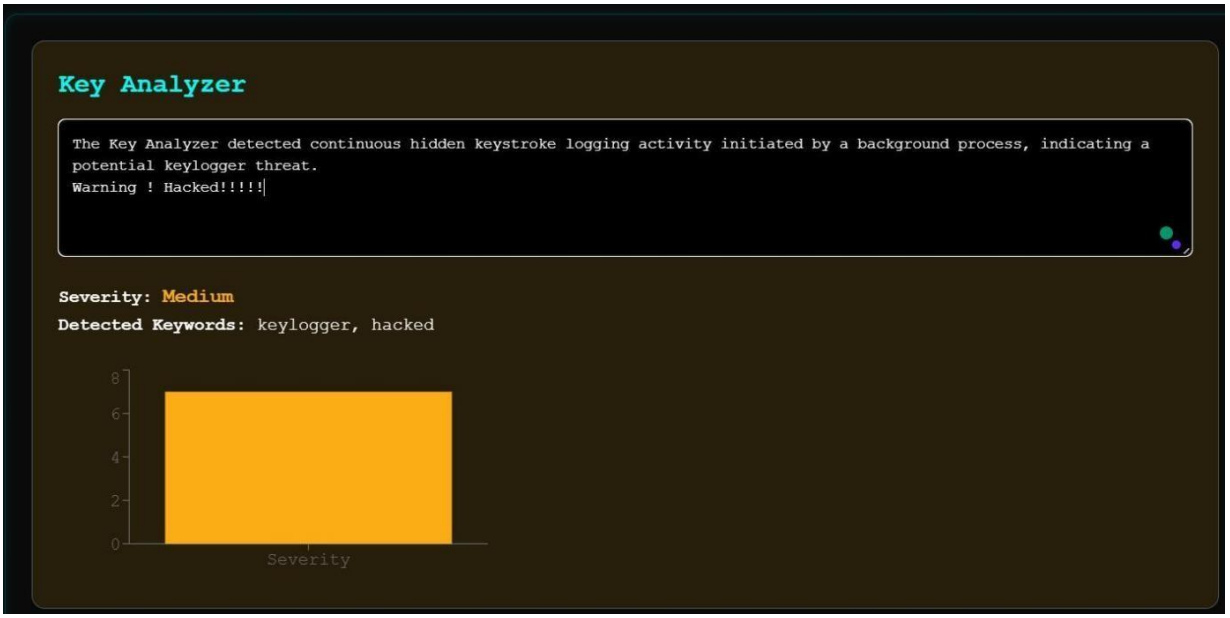


Fig 5.2.9.3-1 Key Analyzer

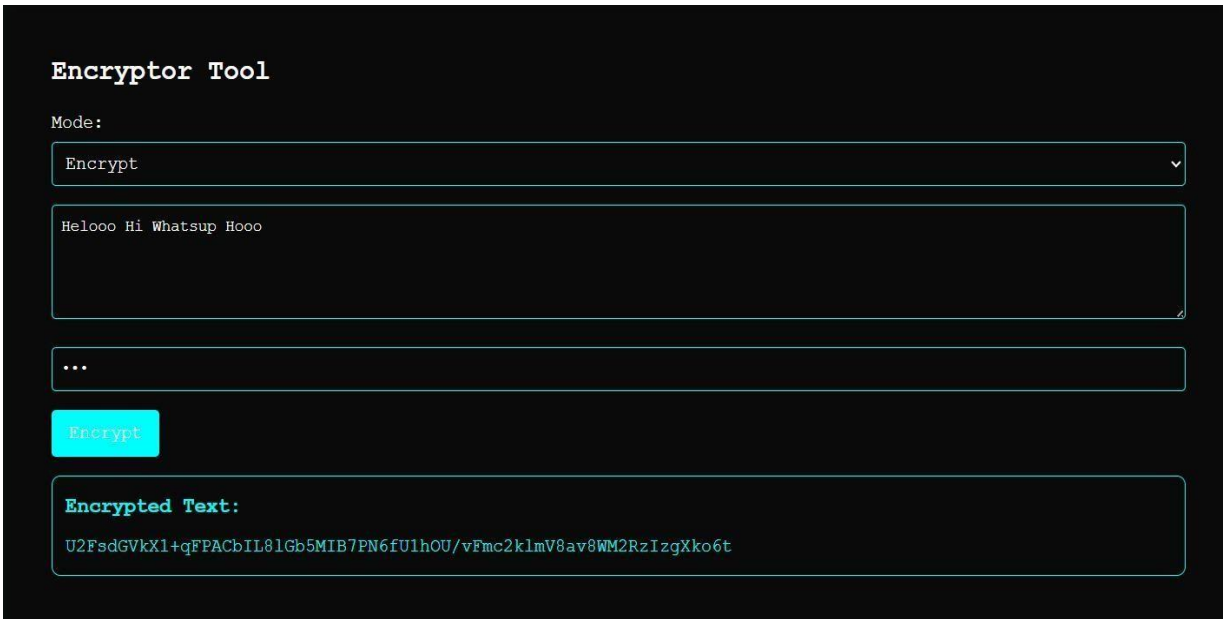


Fig 5.2.9.3-2 Encrypt

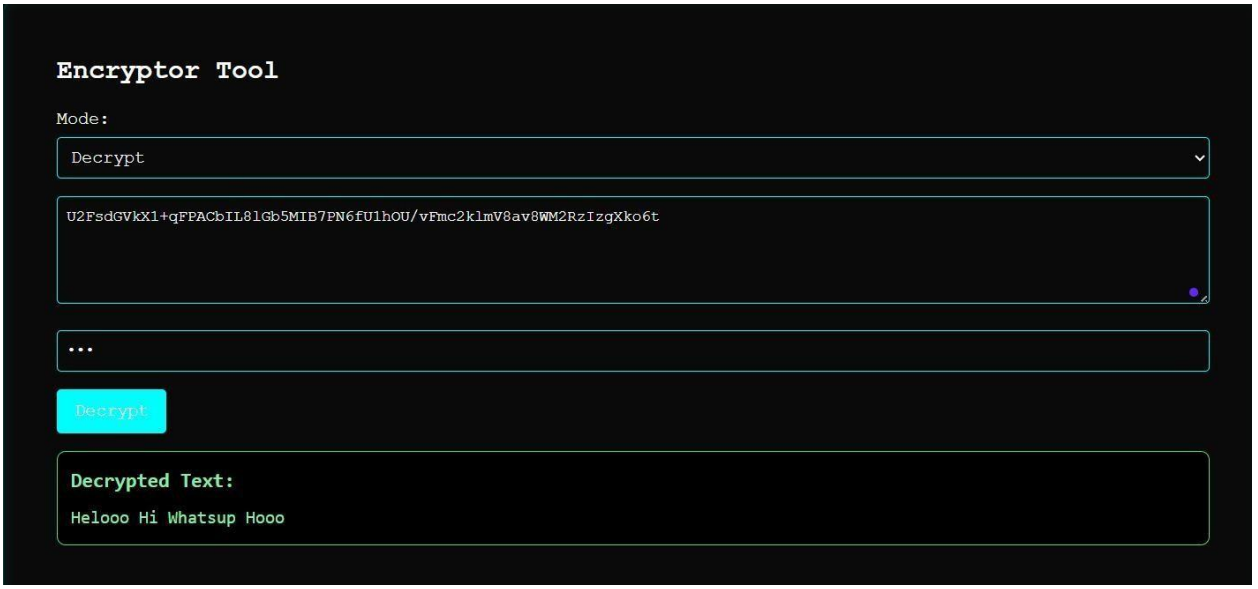


Fig 5.2.9.3-3 Decrypt

5.2.9.4 Digital Forensic Case : Disk Imager

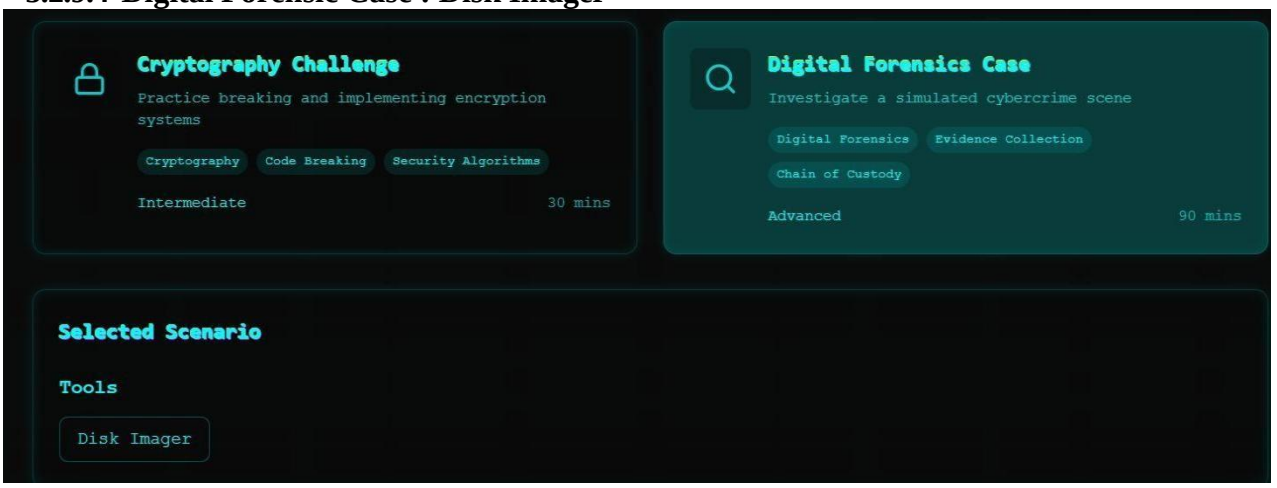


Fig 5.2.9.4 Digital Forensic Case

Fig 5.2.9.4-1 Disk Imager

5.2.9.5 Logs :

```
▸ 0: {toolName: '📄 PCAP Viewer', clickedAt: '2:40:40 PM'}
▸ 1: {toolName: '💾 Disk Imager', clickedAt: '2:40:42 PM'}
▸ 2: {toolName: '⚙️ Static Analyzer', clickedAt: '2:40:43 PM'}
▸ 3: {toolName: '🔑 Key Analyzer', clickedAt: '2:40:44 PM'}
▸ 4: {toolName: '🔒 Encryptor Tool', clickedAt: '2:40:44 PM'}
▸ 5: {toolName: '⚙️ Static Analyzer', clickedAt: '2:40:45 PM'}
▸ 6: {toolName: '🔍 Dynamic Analyzer', clickedAt: '2:40:46 PM'}
▸ 7: {toolName: '📄 Log Analyzer', clickedAt: '2:40:47 PM'}
```

Fig 5.2.9.5-2 Logs : Generates Pdf's

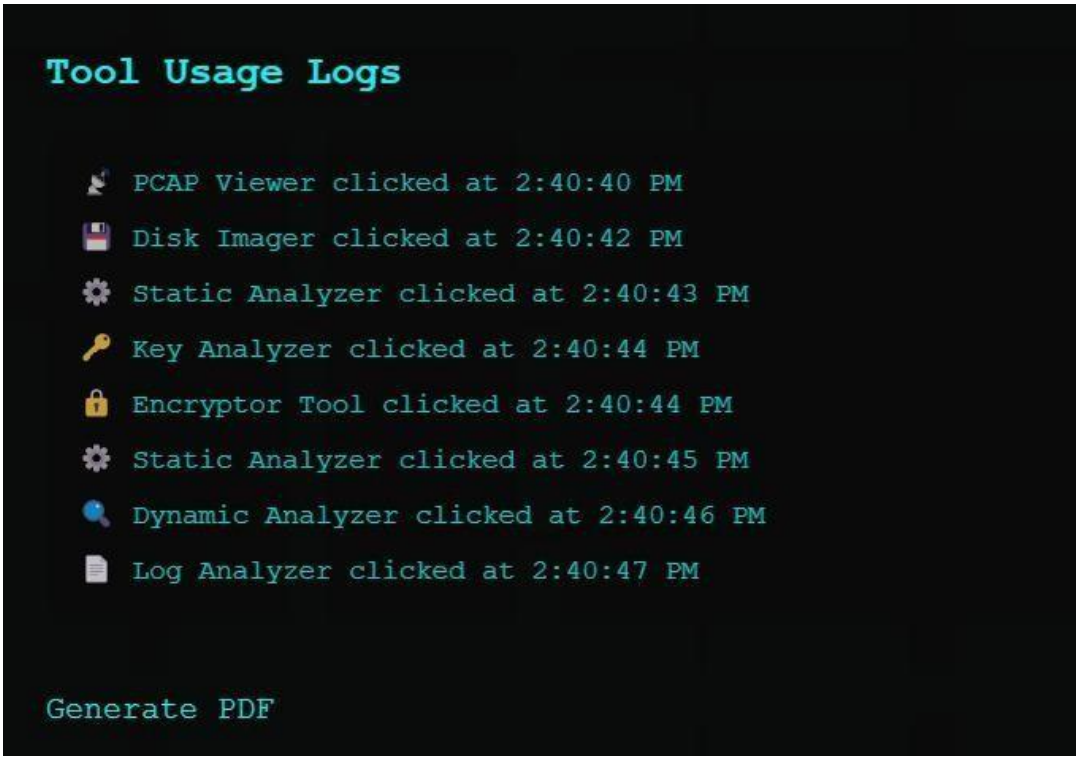


Fig 5.2.9.5-2 Logs : Generates Pdf's

Fig 5.2.9.5-2 Logs : Generates Pdf's

6. Security :

Cyber Astra is designed with security as an integral part of its architecture to safeguard user data, tools, and interactions throughout cyber investigations. A number of security layers are put in place to guarantee confidentiality, integrity, and availability of the system.

Key Security Measures Implemented:

Role-Based Access Control (RBAC): Ensures that only authorized users can access specific features and tools.

Input Validation & Sanitization: Prevents common attacks such as XSS, SQL Injection, and command injection.

HTTPS & Data Encryption: All data transmissions are secured using HTTPS and sensitive data is encrypted in transit.

Secure Tool Execution Environment: Tools are sandboxed to avoid unauthorized access to the system or user data.

7. Conclusion :

In summary, Cyber Astra is an interactive and extensive cybersecurity forensics system that is set to facilitate investigation, analysis, and educational requirements in cybersecurity. The platform offers a dynamic set of integrated tools, real-time scenario-based simulations, and visual analytics to enable users to comprehend and effectively respond to cyber threats.

8. References:

References:

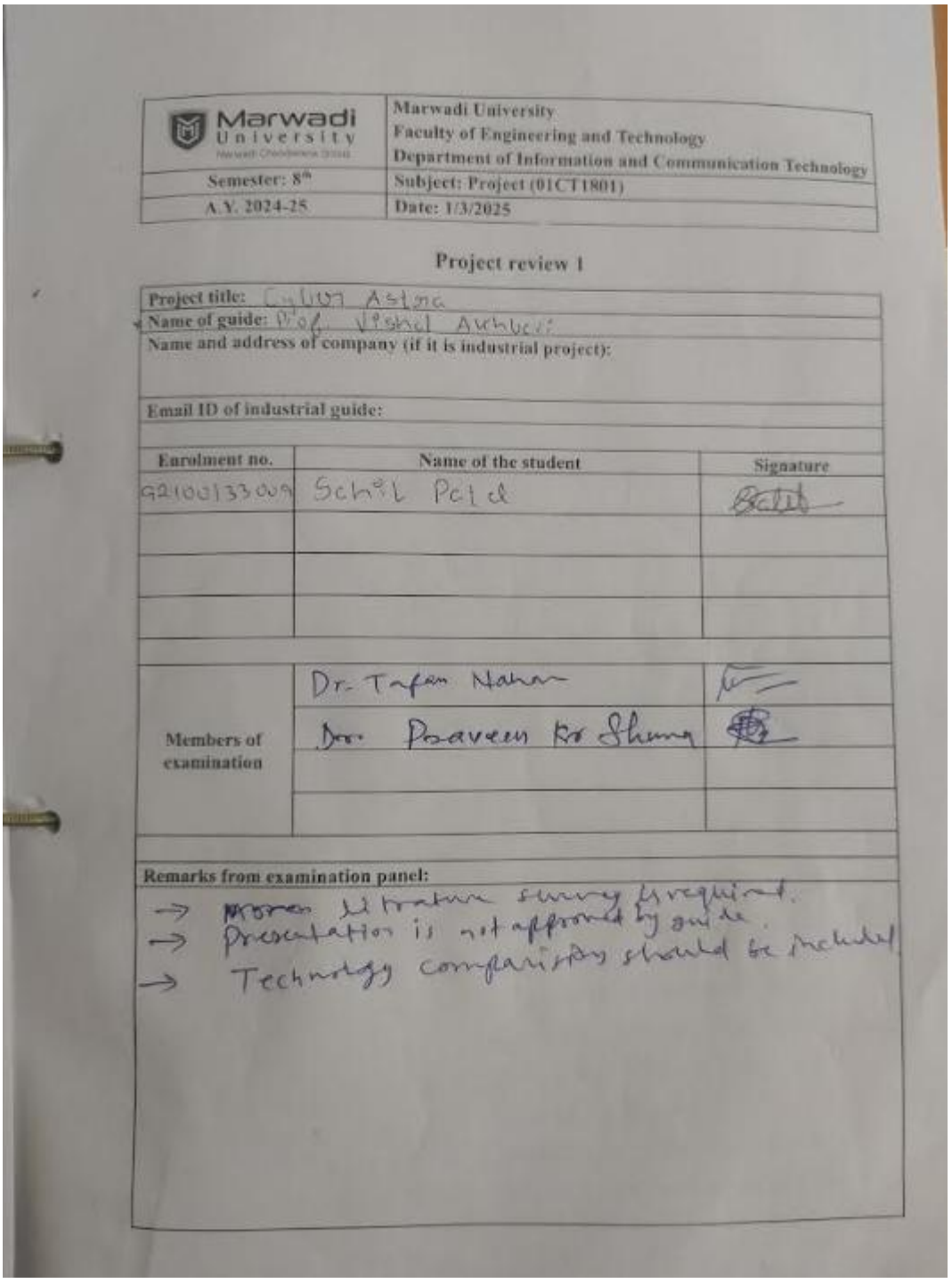
1. ReactJS Documentation – [https://reactjs.org/docs/getting-started.html]
2. Node.js Documentation – https://nodejs.org/en/docs
3. Python Official Documentation – https://docs.python.org/3/
4. OWASP Official Website – https://owasp.org/
5. Bootstrap Framework – https://getbootstrap.com/docs/
6. Visual Studio Code Docs – [https://code.visualstudio.com/docs]

Biblography:

1. 1-Mitnick, K. D., & Vamosi, R. (2017). The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data. Little, Brown and Company.
2. Harris, K. (2022). Cybersecurity Essentials for Students and Professionals. CyberEdge Press.
3. Chhabra, A. (2021). Mastering Full-Stack Development with React and Node.js. Packt Publishing.
4. Williams, J. (2023). Applied Cybersecurity and Digital Forensics. Wiley.
5. Raj, P. (2020). Practical Guide to Ethical Hacking and Cyber Security. TechAcademy Publications

9.Reviews :

Review 1 :



Marwadi University	Marwadi University Faculty of Engineering and Technology Department of Information and Communication Technology
Semester: 8th	Subject: Project (01CT1801)
A.Y. 2024-25	Date: 1/3/2025

Project review 1

Project title: Cyber Astra

Name of guide: Prof. Vishal Avhad

Name and address of company (if it is industrial project):

Email ID of industrial guide:

Enrolment no.	Name of the student	Signature
92100133009	Schil Patel	

Members of examination		
	Dr. Tapan Nahar	
	Dr. Praveen Kr Shukla	

Remarks from examination panel:

→ More literature survey is required.
→ Presentation is not approved by guide.
→ Technology comparison should be included.

Fig 9.1 Review 1

Review 2 :

Marwadi University Marwadi Chandarana Group	Marwadi University Faculty of Engineering and Technology Department of Information and Communication Technology
Semester: 8th	Subject: Project (01CT1801)
A.Y. 2024-25	Date: 29/3/2025

Project review 2

Project title: Cyber Astra

Name of guide: Vishal Akbari

Name and address of company (if it is industrial project):

Email ID of industrial guide: Naresh Makwana

Enrolment no.	Name of the student	Signature
	Sahil Patel	

Members of examination	Dr. Tapan Nahar	

Remarks from examination panel:

→ Presentation is good
→ Project must be in presentable form and good demonstration should be there.
→ project should be completed with in 10 days

Fig 9.2 Review 2