Cyber Astra (Cyber Security Threats Detection)

Ms. Snehal A. Pagare[1], Ms. Hanishka C. Baviskar[2], Mr. Vaishnav S. Kedar[3], Mr. Parth D. Bhandari[4]
Lecturer, Department of Information Technology[1]
Students, Department of Information Technology[2,3,4]
Mahavir Polytechnic, Nashik, Maharashtra, India

Abstract*:* *Cyber security is a critical issue in today's interconnected digital environment where organizations face increasing threats. This content demonstrates integrated threat detection system, user-friendly network application designed to enhance the security of the organization. The system includes advanced tools and features such as Dark Web Infiltration Finder, Breach Tracker, Email Leak Finder, Nmap Scanner for IP Address and Network Scanning, SQL Injection Detector, Clickjacking Detector and Specially Designed Search Engine for Penetration Testers Use Google Dork for discovery.*

Main Features:

1. Dark Web Leak Finder: - Track organizational leaks on the Dark Web.

- Provide instant updates on compromised credentials or sensitive information. Track crime tracker:

- See crime history on maps and your organization. - Increase protection by identifying potential patterns and trends in cyber threats. It also works as an email leak finder:

- Search public and private sites to determine the status of corporate email leaks.

-Example has been updated to take steps to prevent tampering of email addresses and unauthorized access.

2. Nmap Scanner: - Fully scan IP addresses and networks to identify vulnerabilities.

-it tells us which port is open or closed, and also tells us which service is running on which port. - Use to strengthen and monitor network security.

3. SQL injection detection: - Check URLs for potential SQL injection vulnerabilities.

- Provide warnings and recommendations to reduce risks associated with SQL injection attacks.

4. Clickjacking Detector: - detects and blocks clickjacking attempts in web applications.

- Improved user interface to check for clickjacking vulnerabilities on the client or user's website.

5.Search engine for Penetration Testers: - Includes advanced Google Dork technology for targeted reconnaissance.

- Provide auditors with a useful search engine to identify vulnerabilities.

Keywords: cyber security, dark web, website security, network scanning, sql injection, penetration tester, hacker, ethical hacking, Cyber threats

I. INTRODUCTION

In today's digitally connected world, the origin of cyber threats poses a serious challenge to organizations' efforts to protect sensitive information and digital assets. As technology advances and cybercriminals become more sophisticated, the need for effective cybersecurity measures has never been greater. In response to this urgent need, the Cyber Astra Cyber Threat Detection System emerged as a solution designed to help organizations.

Cyber Astra represents the ultimate in smart and capable tools designed to detect, identify and mitigate cyber threats. Cyber Astra provides a comprehensive approach to cybersecurity that addresses the state of today's threats, from dark web monitoring to potential data leakage to network vulnerability assessment.

This entrance is the door to a difficult quest. Take an in-depth look at Cyber Astra, its main features and principles. By understanding how everything works and how it contributes to the overall benefits of the system, organizations can understand the benefits of Cyber Astra in supporting cybersecurity.

DOI: 10.48175/IJARSCT-15648

II. METHODOLOGY

A Cyber Threat Detection System involves the integration (Cyber Astra) of a variety of tools and features, each performing a unique function in identifying and mitigating cyber threats.
Here are details on how the main features work:

Dark Web Leak Finder:-

The UI was designed and the design was finalized, the format by which the leaked emails and the data will be displayed user-friendly to the user. The option by which the result file will be downloaded into text file was implemented. For scanning the domain the user will enter the domain which he needs to search in the input and all the leaked emails and other data which has been breached will be generated.

Working: System monitors regularly organization Dark Web, Forums and other sites for relevant leaks. It uses algorithms to compare collected data with an organization's dataset to identify matches, Resulting in immediate reporting of data breaches.

Nmap Scanner:-

The research was finalized for the network mapping tool, and the logic was implemented in python based technology. The user interface was designed and the testing was initialized.

Working: the system uses the Nmap tool to complete IP address and network scanning. It identifies open ports, Services running on those ports, and potential vulnerabilities. Results are compiled into detailed reports that provide better insights into improving cyber security.

SQL Injection Detector:-

The detailed study related to the SQL Injection was conducted and the tool's logic was implemented, after the UI design the tool was Ready to implement

Working: The system Analysis URLs to find patterns that indicate attempted SQL Injection. It uses signature-based detection technology to identify potential SQL Injection Vulnerabilities. The system generates alerts and recommendations to resolve and mitigate risks associated with SQL Injection attacks whendetected.

Clickjacking Detector:-

The Clickjacking detector's tool was developed after dealing with some case studies and the final tool was implemented and hosted.

Working: The system monitors user content for possible clickjacking attempts. It uses a distortion technique to prevent malicious framing. This ensures that web applications are not embedded in unauthorized framework, thus increasing overall security against click attacks.

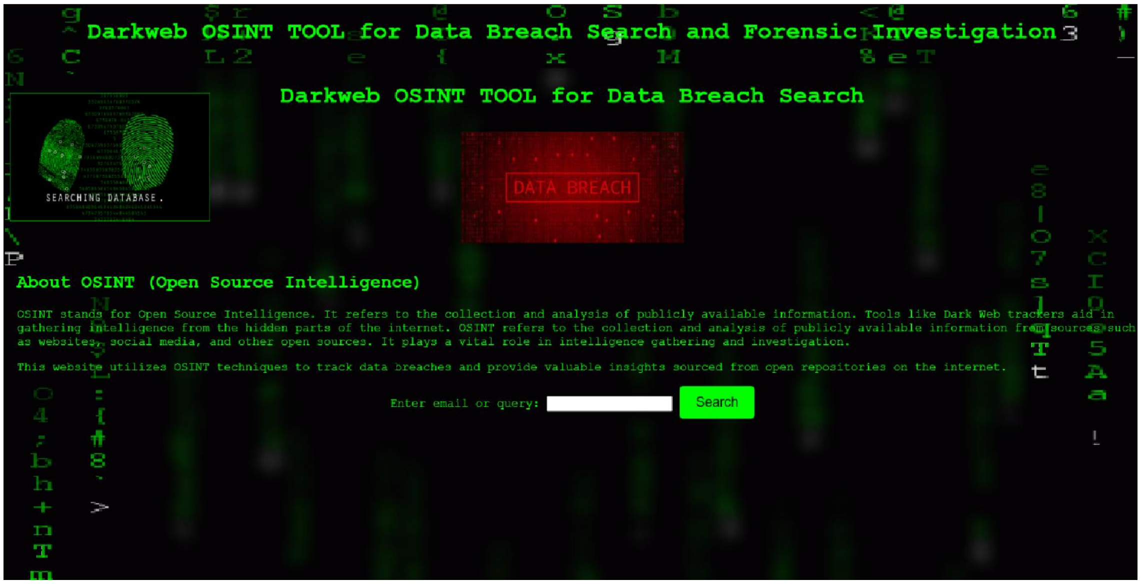
Search Engine for Penetration Testers:-

The tool was developed for the penetration testers to get while doing their workers, in which various options are available like google dorks, the tool was developed and hosted after some testings for accuracy.

Working: The system acts as a dedicated Search engine for Penetration testers. It uses advanced search technologies, including google dork queries, to perform targeted searches. This allows the penetration auditor to perform efficient and targeted searches, helping to discover vulnerabilities and potential intrusion points.

III. RESULTS

1.UI OF TOOL DARK WEB LEAK FINDER:



Darkweb OSINT TOOL for Data Breach Search and Forensic Investigation

Darkweb OSINT TOOL for Data Breach Search

About OSINT (Open Source Intelligence)

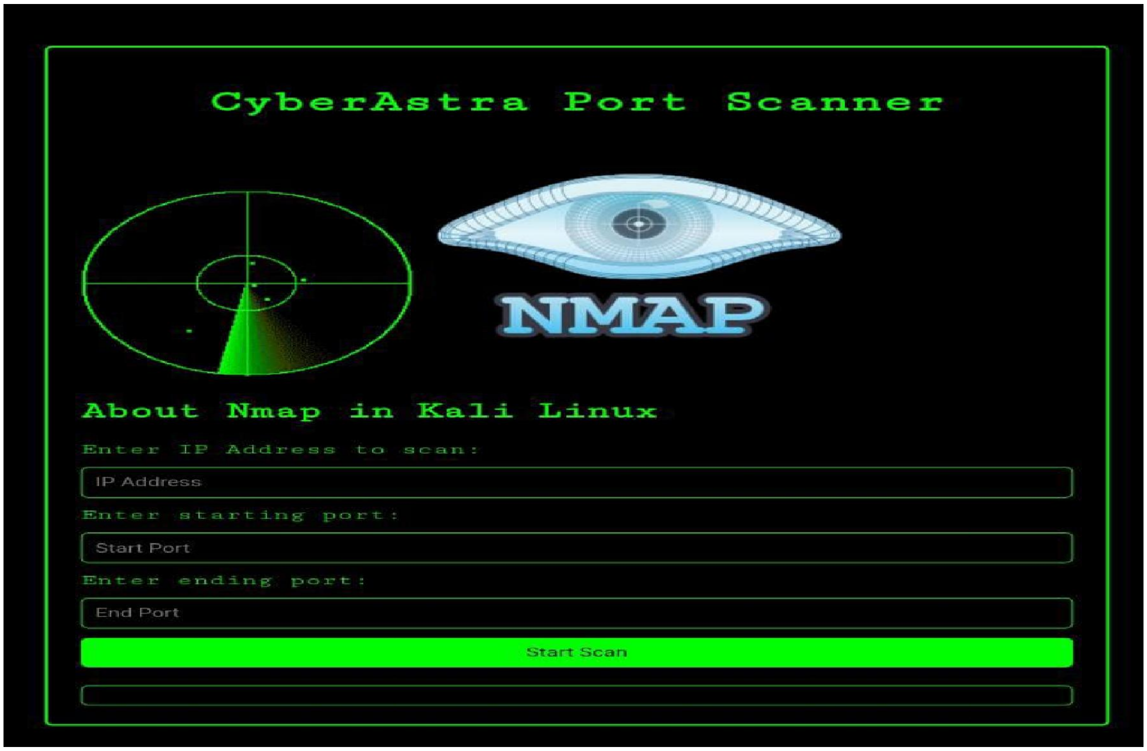
OSINT stands for Open Source Intelligence. It refers to the collection and analysis of publicly available information. Tools like Dark Web trackers aid in gathering intelligence from the hidden parts of the internet. OSINT refers to the collection and analysis of publicly available information from sources such as websites, social media, and other open sources. It plays a vital role in intelligence gathering and investigation.

This website utilizes OSINT techniques to track data breaches and provide valuable insights sourced from open repositories on the internet.

Enter email or query:

Fig. 1. UI of tool Dark Web Leak Finder

2.UI OF NMAP SCANNER:



CyberAstra Port Scanner

About Nmap in Kali Linux

Enter IP Address to scan:

IP Address

Enter starting port:

Start Port

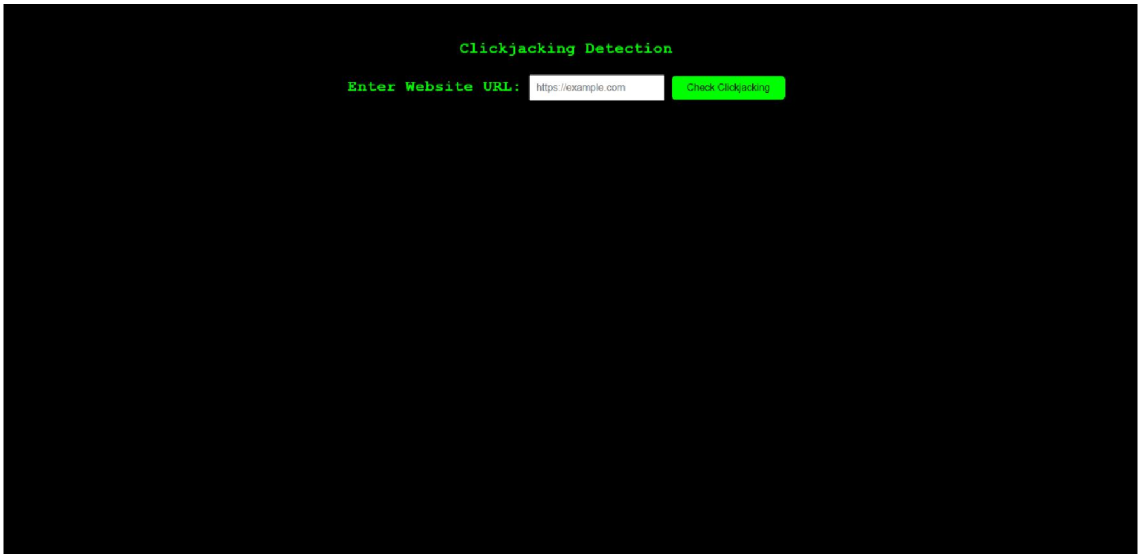
Enter ending port:

End Port

Fig. 2. UI of tool Nmap Scanner

DOI: 10.48175/IJARSCT-15648

3.UI of Tool Clickjacking Detector:

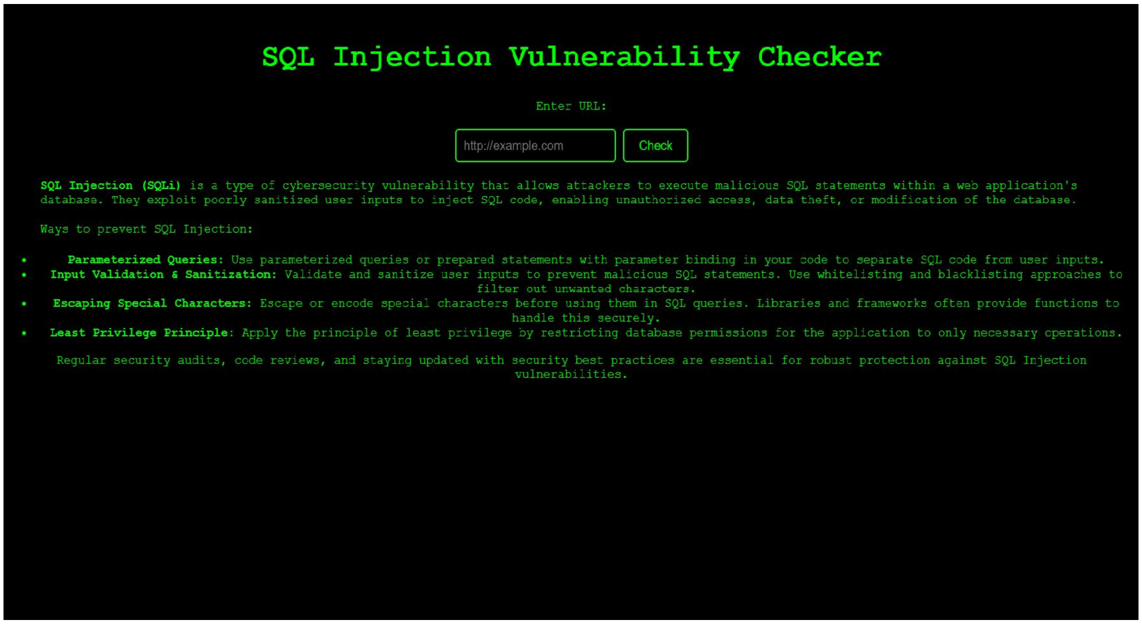


Clickjacking Detection

Enter Website URL:

Fig. 3. UI of tool Clickjacking Detector

4.UI OF TOOL SQL INJECTION DETECTOR:



SQL Injection Vulnerability Checker

Enter URL:

SQL Injection (SQLi) is a type of cybersecurity vulnerability that allows attackers to execute malicious SQL statements within a web application's database. They exploit poorly sanitized user inputs to inject SQL code, enabling unauthorized access, data theft, or modification of the database.

Ways to prevent SQL Injection:

- **Parameterized Queries:** Use parameterized queries or prepared statements with parameter binding in your code to separate SQL code from user inputs.
- **Input Validation & Sanitization:** Validate and sanitize user inputs to prevent malicious SQL statements. Use whitelisting and blacklisting approaches to filter out unwanted characters.
- **Escaping Special Characters:** Escape or encode special characters before using them in SQL queries. Libraries and frameworks often provide functions to handle this securely.
- **Least Privilege Principle**: Apply the principle of least privilege by restricting database permissions for the application to only necessary operations.

Regular security audits, code reviews, and staying updated with security best practices are essential for robust protection against SQL Injection vulnerabilities.

Fig. 4. UI of tool SQL Injection Detector

DOI: 10.48175/IJARSCT-15648

ISSN 2581-9429 IJARSCT

5.UI OF TOOL SQL INJECTION DETECTOR:

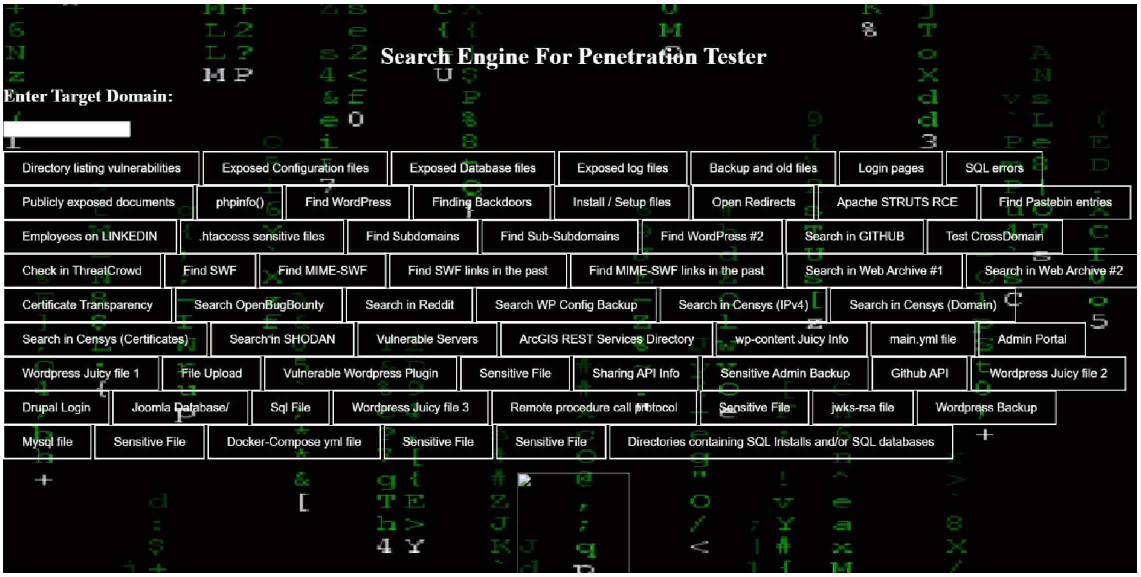


Fig. 5. Penetration Tester Search Engine

IV. CONCLUSION

The Cyber Astra (Cyber Threat Detection System) represents a way to improve the organization's Cyber Security in the evolving digital environment. Cyber Astra combines the most advanced tools and resources, enabling organizations to detect and mitigate cyber threats to protect sensitive information and property rights.

From dark Web Leak Finder's proactive monitoring to Nmap Scanner's network analysis, every feature is essential to protect against online adversaries. The system's ability to identify and respond to threats such as SQL Injection Vulnerabilities and click attempts demonstrates its effectiveness in mitigating a variety of cyber risks.

Additionally, the intrusion detection system provides auditors with the ability to conduct searches, create effective search results, and make mitigation strategies. Cyber Astra increase the efficiency and effectiveness of network security analysis and penetration testing by using new technologies such as google dork questions.

Astra is, at its core, a beacon of light in today's threat landscape, empowering organizations to maintain trust. It is dedicated to the challenging journey of cyber security. As cyber threats continue to evolve, Cyber Astra remains committed to protecting organization's assets and ensuring the integrity of the digital ecosystem.

V. ACKNOWLEDGMENT

We would like to acknowledge and give our warmest thanks to our project guide Prof. Ms. Snehal A. Pagare who made this work possible. Her guidance and advice carried us through all the stages of our project.

REFERENCES

[1]. Marco Gfeller,Lightweight Python-Based Malware Analysis Pipeline,February 9, 2023

[2]. Rick Schroeder, is it Ever Really Gone? The Impact of Private Browsing and Anti-Forensic Tools, December 9, 2020

[3]. Mrs. Ashwini Sheth, Mr. Sachin Bhosale, Mr. Farish Kurupka, Research Paper on Cyber Security, I.C.S. College, Khed, Ratnagiri, 24 April 2021

[4]. OSINT Industries LTD,30 June 2024, OSINT Industries, https://osint.industries/.

[5]. Imperva.com, https://www.imperva.com/learn/application-security/cyber-security-threats/,