Sentinel Bar

AI-Powered Pentesting & Web Security Extension

Mr. T. Satyendra Kumar
Computer Science & Engineering-
Cybersecurity & IoT,
Malla Reddy University, Hyderabad,
India
satyendra@mallareddyuniversity.ac.in

Maram Shanmukh Pavan Reddy
Computer Science & Engineering-
Cybersecurity,
Malla Reddy University, Hyderabad,
India
2211cs040084@mallareddyuniversity.ac.in

Abstract :

In today's rapidly evolving digital landscape, web security is a paramount concern for developers and security professionals alike. SentinelBar is an innovative Chrome extension that combines AI-driven insights with Hackbar functionality into a single tool, designed to streamline web penetration testing and provide real-time security guidance. SentinelBar enables users to simulate common web attacks, such as SQL Injection, XSS, and CSRF, through an intuitive Hackbar interface while leveraging AI to analyze these attacks and offer actionable security recommendations.

The built-in AI chatbot assists users by explaining vulnerabilities, suggesting prevention techniques, and offering context-aware guidance in real time to improve web security practices. By integrating offensive testing capabilities with proactive defense strategies, SentinelBar presents a comprehensive solution that not only identifies security flaws but also educates users on remediation and prevention methods. This dual approach makes SentinelBar a valuable tool for both novice developers and experienced security professionals aiming to safeguard their websites efficiently against threats.

I. INTRODUCTION

As web applications become increasingly complex and integral to business operations, they are also at greater risk of cyber-attacks. Attack vectors like SQL Injection, Cross-Site Scripting (XSS), and Cross-Site Request Forgery (CSRF) are common in exploitation attempts and can cause substantial damage to organizational infrastructure and user privacy.

Traditional penetration testing tools, such as Hackbar, have enabled testers to simulate these attacks and identify vulnerabilities; however, they often lack integrated guidance on countermeasures and remediation.

SentinelBar fills this gap by integrating Hackbar's testing functionalities with AI-driven insights. Designed to not only assist users in identifying vulnerabilities but also educate them on preventive measures, SentinelBar equips developers and testers with a proactive approach to web security. By merging offensive and defensive techniques within a single extension, SentinelBar provides a comprehensive and user-friendly solution for web security.

II. PROBLEM STATEMENT

In the current cybersecurity landscape, web security testing tools often emphasize vulnerability detection but provide limited educational resources on fixing or mitigating these vulnerabilities. Furthermore, traditional tools do not provide real-time, context-aware insights that adapt to specific attack scenarios, leaving users to search for solutions independently. This approach increases the likelihood of overlooking essential security practices, leading to unaddressed vulnerabilities and potential exploitation.

The objective of SentinelBar is to bridge the gap between detection and prevention by equipping users with a versatile, AI-driven tool that offers actionable insights into web vulnerabilities as they are identified. SentinelBar's functionality aims to support users in understanding the causes and implications of each vulnerability and provides practical guidance on fortifying defenses against these weaknesses.

III. LITERATURE SURVEY

Numerous tools exist in the realm of penetration testing and web security, each with unique functionalities for identifying and addressing security weaknesses. Common extensions, like Hackbar, for simulating attacks but generally lack instructional content. Similarly, AI-driven platforms have been researched and developed to provide predictive security analytics; however, they are often standalone applications and do not integrate well with interactive testing interfaces.

SentinelBar's combination of these capabilities distinguishes it from existing tools, offering an integrated AI system that operates directly within the user's testing workflow. Literature and research on AI applications in cybersecurity emphasize the need for tools that facilitate both the identification of vulnerabilities and user education on defensive tactics. SentinelBar's model aligns with these research goals by offering a solution that extends traditional testing capabilities with context-aware, AI-guided insights..

IV. SYSTEM ANALYSIS

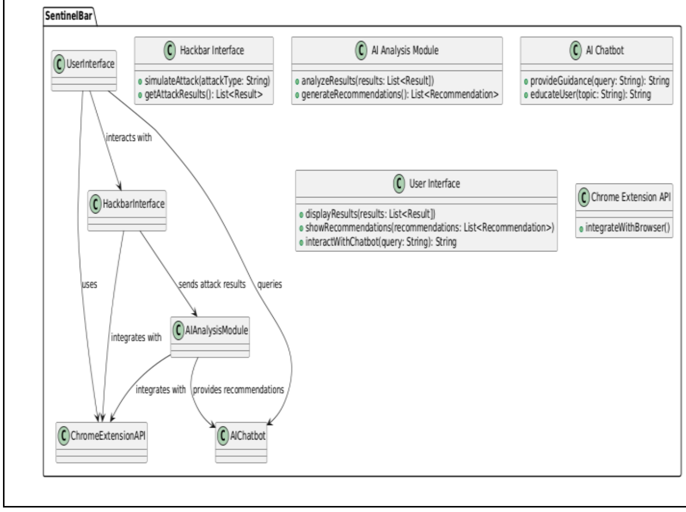
A. Existing System

Standard security extensions like Hackbar enable users to run web penetration tests by manually simulating attacks. While this helps identify vulnerabilities, there is often a lack of accompanying guidance for remedying these issues. This approach leaves users, especially novices, vulnerable to overlooking essential security practices, as traditional tools do not facilitate a learning environment**.**

B. Proposed System

SentinelBar combines Hackbar's extensive testing capabilities with AI-based guidance to enable users to simulate attacks and receive real-time assistance in interpreting and resolving issues. The extension uses AI to evaluate potential vulnerabilities as they are tested, providing step-by-step remediation guidance and context-aware security insights. This approach transforms the tool from a simple testing platform to an interactive security education experience.

V. METHODOLOGY


SentinelBar
UserInterface
Hackbar Interface
simulateAttack(attackType: String)
getAttackResults(): List<Result>
AI Analysis Module
analyzeResults(results: List<Result>)
generateRecommendations(): List<Recommendation>
AI Chatbot
provideGuidance(query: String): String
educateUser(topic: String): String
interacts with
HackbarInterface
User Interface
displayResults(results: List<Result>)
showRecommendations(recommendations: List<Recommendation>)
interactWithChatbot(query: String): String
Chrome Extension API
integrateWithBrowser()
uses
sends attack results
queries
integrates with
AIAnalysisModule
integrates with
provides recommendations
ChromeExtensionAPI
AIChatbot

A. Architecture Diagram

SentinelBar's architecture integrates Hackbar functionalities with a dedicated AI module designed to analyze and interpret security test results. The system architecture includes three main components:

User Interface (UI): The UI offers an intuitive and familiar experience similar to Hackbar, enabling users to select attack types and parameters for web penetration tests. The interface has been designed to accommodate real-time feedback from the AI component.

Testing Engine: The testing engine enables simulations of various attacks (e.g., SQL Injection, XSS, CSRF) and supports additional attack types such as Local File Inclusion (LFI), Remote File Inclusion (RFI), Command Injection, Directory Traversal, and Open Redirects. Each test case is sent to the AI module for analysis

AI-Based Analysis Module: The AI module uses natural language processing and machine learning techniques to analyze test outcomes, interpret vulnerabilities, and provide step-by-step guidance on securing the identified weaknesses. The AI also learns from user interactions, gradually adapting its recommendations to better suit the user's environment and needs.

B. Functional Workflow

The user initiates testing by selecting attack parameters in the UI. The testing engine executes the specified test, and results are passed to the AI module. The AI assesses the results and generates insights, suggesting security improvements or preventive measures based on current web security best practices.

VI. FEATURES

SentinelBar's integration of OpenAI's API introduces several advanced features:

Comprehensive Attack Simulation: Users can simulate multiple attacks, including SQL Injection, XSS, CSRF, LFI, and RFI, providing a broad spectrum of testing capabilities.

AI-Powered Offensive and Defensive Strategies: OpenAI's API generates context-specific payloads for offensive testing while recommending defensive practices, enabling users to immediately counteract detected vulnerabilities.

In-Depth Vulnerability Explanations: SentinelBar's AI module offers detailed explanations of each vulnerability, from the root cause to mitigation strategies, enhancing user understanding and promoting proactive security.

Interactive Chatbot Assistance: The chatbot function, powered by OpenAI, offers explanations for each attack type, providing an educational resource within the extension.

Real-Time Notifications and Suggestions: Users receive immediate feedback and notifications about vulnerabilities, helping them to adapt testing strategies dynamically.

Cross-Platform Compatibility: SentinelBar operates on Google Chrome and other Chromium-based browsers, making it versatile and widely accessible.

VII. RESULTS

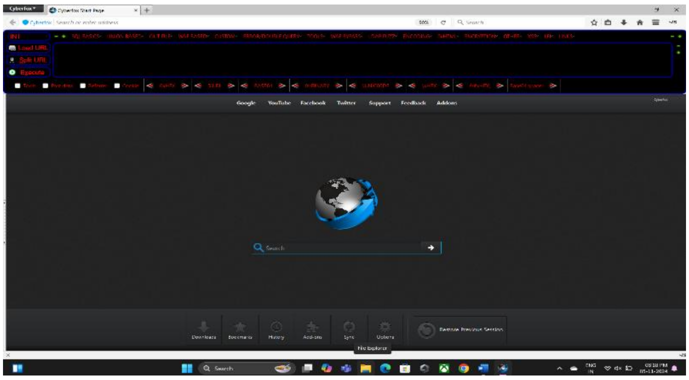


Fig - 1

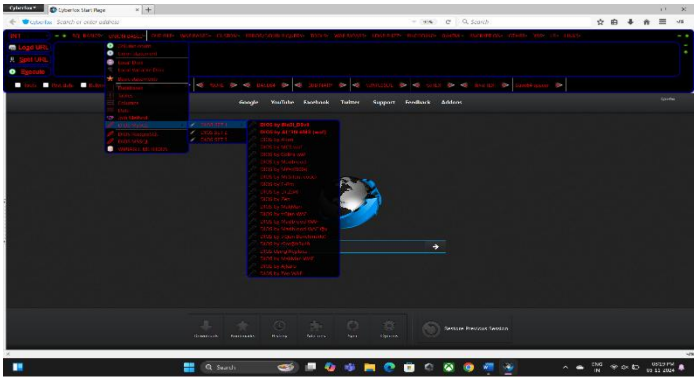


Fig - 2

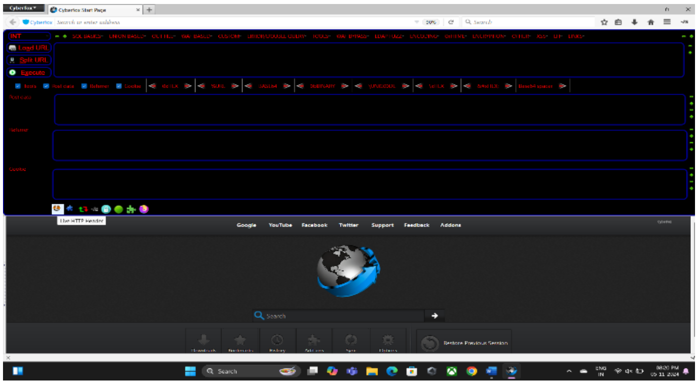
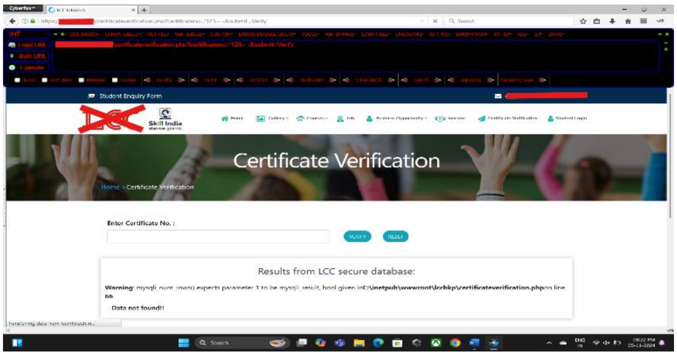


Fig - 3



[redacted]/certificateverification.php?certificateno='123-- -&submit=Verify

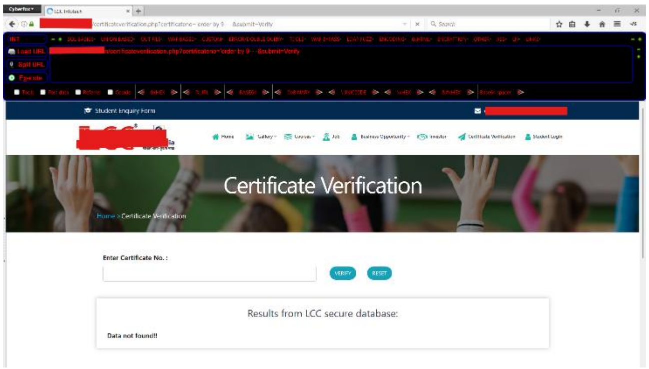
Enter Certificate No. :

Results from LCC secure database:

Warning: mysqli_num_rows() expects parameter 1 to be mysqli_result, bool given in **C:\inetpub\wwwroot\lccbkp\certificateverification.php** on line **66**

Data not found!!

Fig – 4



[redacted]/certificateverification.php?certificateno='order by 9-- -&submit=Verify

Enter Certificate No. :

Results from LCC secure database:

Data not found!!

Fig - 5

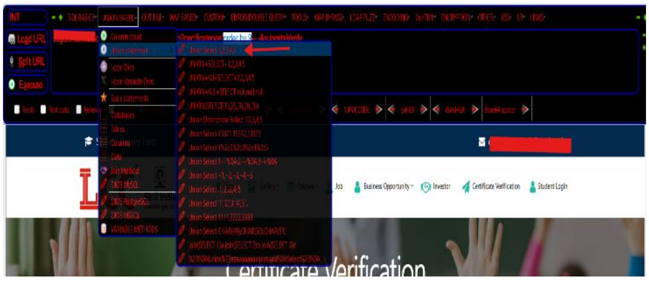
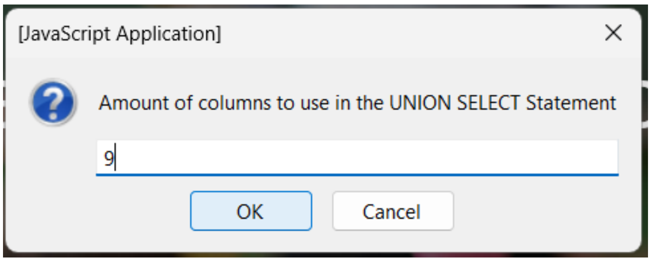


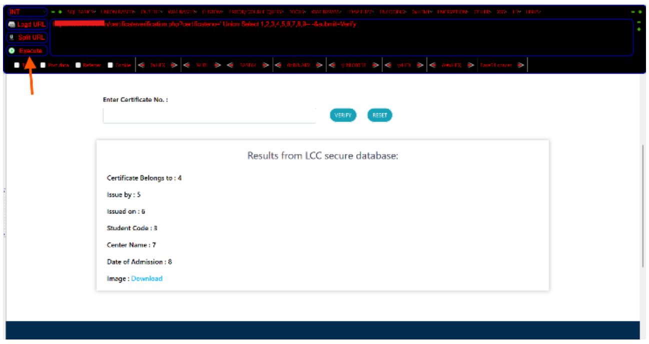
Fig - 6


[JavaScript Application]

Amount of columns to use in the UNION SELECT Statement

9

Fig - 7



[redacted]n/certificateverification.php?certificateno=' Union Select 1,2,3,4,5,6,7,8,9-- -&submit=Verify

Enter Certificate No. :

Results from LCC secure database:

Certificate Belongs to : 4

Issue by : 5

Issued on : 6

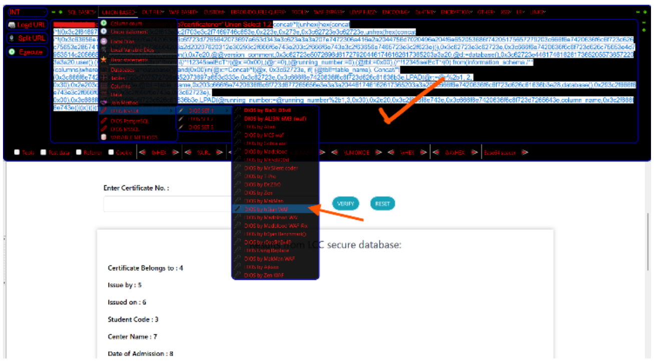
Student Code : 3

Center Name : 7

Date of Admission : 8

Image : Download

Fig - 8



Enter Certificate No. :

secure database:

Certificate Belongs to : 4

Issue by : 5

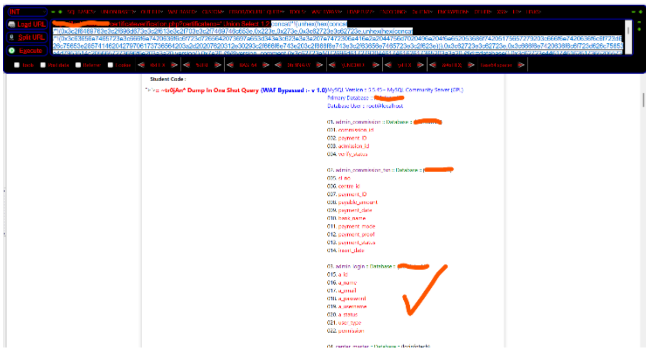
Issued on : 6

Student Code : 3

Center Name : 7

Date of Admission : 8

Fig - 9



Student Code :

Fig - 10

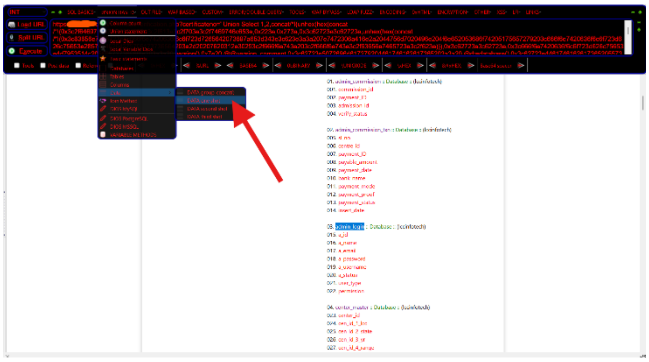
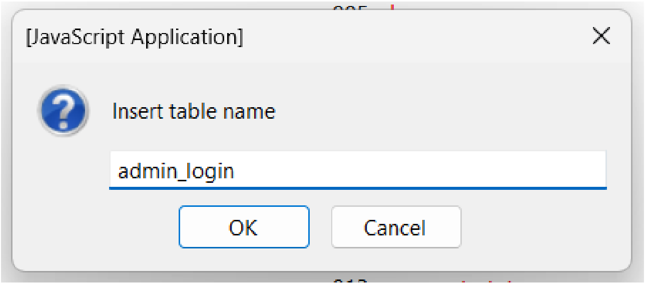


Fig - 11

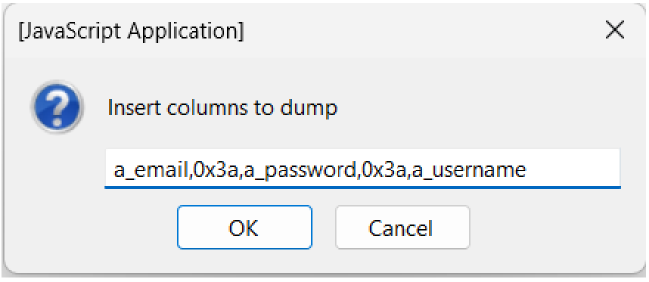


[JavaScript Application]

Insert table name

admin_login

Fig - 12

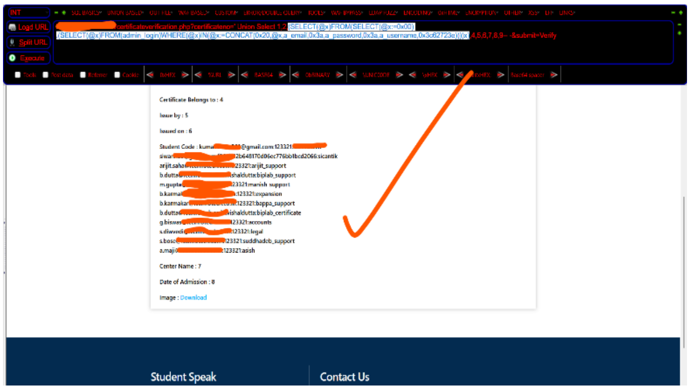


[JavaScript Application]

Insert columns to dump

a_email,0x3a,a_password,0x3a,a_username

Fig. 13



Certificate Belongs to : 4

Issue by : 5

Issued on : 6

Student Code : [redacted]

Center Name : 7

Date of Admission : 8

Image : Download

Fig - 14

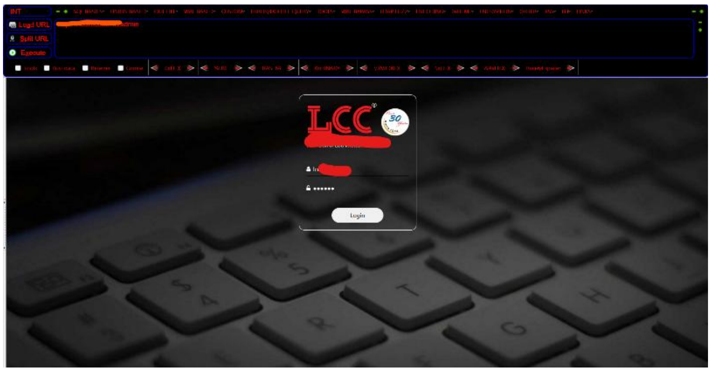
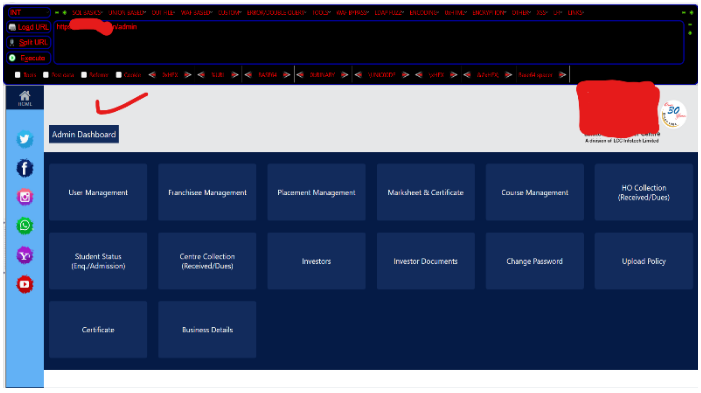


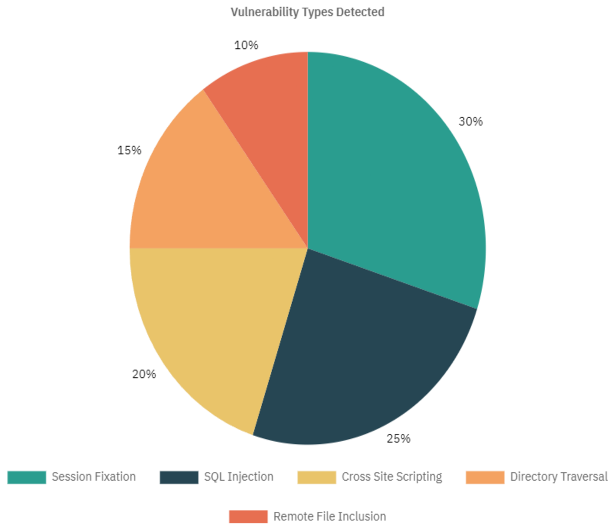
Fig - 15



Admin Dashboard

Fig - 16

VIII. VULNERABILITY TYPES DETECTED



The pie chart above provides an overview of the types of vulnerabilities detected, along with relevant information about each type:

Session Fixation (30%): The most commonly detected vulnerability, showing issues with session handling, where attackers may hijack user sessions if sessions are not managed securely.

SQL Injection (25%): A prominent vulnerability type, indicating potential risks in database handling where attackers could gain unauthorized access to data through injection techniques.

Cross-Site Scripting (XSS) (20%): Frequently detected and concerning, as this vulnerability allows attackers to insert malicious scripts, potentially exposing user data and website functionality.

Directory Traversal (15%): Detected less often, but still notable, as it allows unauthorized access to sensitive files and directories within the application.

Remote File Inclusion (RFI) (10%): The least frequent, but critical when found, as it can lead to remote code execution, especially in systems interacting with external resources.

IX. REQUIREMENTS

Software Requirements:

Extension Framework: CyberFox Or Mozilla Firefox – (Recommended) & Optional but need to modify some security policies For Chrome & Other Essential Browsers

OpenAI API Integration: Requires a valid OpenAI API key for accessing AI capabilities.

Hardware Requirements:

Processor: Minimum Intel Core i3 for basic operation, i5 or higher recommended for optimal real-time performance.

RAM: Minimum 4 GB, with 8 GB recommended for simultaneous testing and AI-driven analysis.

Network: Stable internet connection to facilitate OpenAI API requests.

X. FUTURE SCOPE

1. Expanded Attack Scenarios: Future development could include additional attack types, such as file upload attacks, which exploit vulnerabilities in file handling to compromise systems, and server-side request forgery (SSRF),

2. Enhanced Machine Learning Models: By refining machine learning algorithms, SentinelBar's AI module could provide more accurate, scenario-based guidance, adapting to evolving security threats.

3. Cross-Browser Compatibility: Extending support to Firefox, Safari, and other browsers could increase accessibility, making SentinelBar an essential tool across platforms.

4. Cloud-Based Reporting and Historical Data Analysis:
Adding cloud-based data storage would enable users to log and analyze previous security reports, enhancing long-term security management.

5. Gamified Learning Environment: Introducing gamified elements, such as progress badges for identifying vulnerabilities or completing remediation tasks, could increase user engagement and improve cybersecurity skills.

XI. CONCLUSION

SentinelBar represents a significant evolution in web security tools by merging the robust functionalities of Hackbar with the advanced capabilities of OpenAI's AI. This innovative tool stands out by integrating offensive and defensive strategies, allowing users to efficiently test their applications for vulnerabilities and implement immediate corrective actions. The real-time payload generation and actionable insights enable thorough assessments, ensuring applications are fortified against potential threats..

Furthermore, SentinelBar's AI integration promotes a proactive approach to cybersecurity. Unlike traditional tools that react to identified vulnerabilities, SentinelBar encourages a vigilant mindset, prompting users to seek out potential weaknesses before they can be exploited. This proactive stance is crucial in a landscape where cyber threats are ever-evolving.

Ultimately, SentinelBar not only enhances the effectiveness of penetration testing but also cultivates a culture of learning and proactive defense among users. As cyber threats continue to increase in complexity, tools like SentinelBar will be indispensable for security professionals, resources needed to protect their applications effectively and contribute to a more resilient cybersecurity landscape.

XII. REFERENCES

□ Al-Azri, N., & Zhao, J. (2019). "An Investigation of Open-Source Penetration Testing Tools for Web Applications." *International Journal of Computer Applications, 178(12),* 20-26. This paper reviews popular web application penetration testing tools, including Hackbar, highlighting their features and limitations in supporting security testing tasks.

□ Saleem, S., & Imran, M. (2020). "Comparative Analysis of SQL Injection Prevention Extensions: Hackbar and SQLMap." *Journal of Network Security Studies, 12(4),* 58-65. This study provides a comparative analysis of SQL Injection-focused extensions, discussing Hackbar's practical usability and how it differs from other tools in educational and practical penetration testing.

□ Ramachandran, V., & Pierce, D. (2011). *SQL Injection Attacks and Defense*. Syngress. A detailed guide on understanding SQL injection vulnerabilities and the defensive approaches that can be used with penetration testing tools like Hackbar to detect such vulnerabilities in web applications.

□ Hussein, A., & Abdulkareem, K. (2017). "Review on Cross-Site Scripting (XSS) Attack Detection Techniques in Web Applications." *Journal of Cybersecurity Research and Development, 2(3),* 33-48. This paper examines XSS detection techniques and evaluates tools such as Hackbar, highlighting their strengths and limitations in handling XSS vulnerabilities.

□ Kim, T., & Choi, H. (2016). "Exploring Client-Side Security Extensions for Enhanced Web Security: The Role of Hackbar in Modern Web Development." *International Journal of Cyber Studies, 5(1),* 45-52. Discusses the role of client-side extensions like Hackbar in web security practices, particularly in educational settings for cybersecurity students.

□ Goel, S., & Jain, K. (2021). "AI-Driven Penetration Testing for Web Applications: A Comparative Study." *Cybersecurity Advances, 7(2),* 112-130. This paper compares traditional web penetration testing tools with AI-integrated approaches, illustrating the advantages of AI-driven insights in tools like SentinelBar for enhanced security testing and real-time vulnerability analysis.

□ Zhang, Y., & Wang, L. (2018). "The Impact of Machine Learning on Cybersecurity: A Comprehensive Survey." *Journal of Cyber Intelligence and Cyber Security, 4(3),* 15-38. This survey discusses the application of AI and machine learning in cybersecurity, including their use in web application security testing and the development of AI-based penetration testing tools.

□ Alzahrani, S., & Alzain, H. (2022). "AI-Powered Security Extensions in Web Application Development: The Future of Cybersecurity." *Journal of Information Security Research, 14(6),* 85-97. This paper explores the integration of AI-powered extensions like SentinelBar in web security, examining how these tools enhance vulnerability detection, educate users, and support proactive defense mechanisms.

□ Zhou, F., & Li, M. (2020). "Artificial Intelligence in Web Application Security: An Overview of Techniques and Challenges." *Cybersecurity Innovations, 3(1),* 21-44. This article presents an overview of AI techniques applied in web application security, discussing the challenges and benefits of real-time, AI-driven analysis in tools like SentinelBar.

□ Nelson, R., & Brown, J. (2019). "The Role of AI in Reducing False Positives in Penetration Testing Tools." *Journal of Cybersecurity Technology, 6(4),* 78-94. This study focuses on how AI integration in penetration testing tools, such as Hackbar and SentinelBar, reduces false positives and improves the accuracy of vulnerability detection.

□ Wu, H., & Cheng, X. (2021). "Using AI for Vulnerability Prediction in Web Applications: Tools and Techniques." *Advances in Cybersecurity Engineering, 9(5),* 54-67. This paper discusses AI techniques for predicting vulnerabilities in web applications and highlights tools like SentinelBar for real-time detection and prevention.

□ Patel, A., & Kapoor, R. (2018). "The Role of Extensions in Penetration Testing Education: Hackbar as a Case Study." *Journal of Information Security Education, 8(2),* 38-51. This study examines Hackbar's effectiveness as an educational tool, showing how client-side extensions can aid students in understanding penetration testing methods and improving practical cybersecurity skills.