SENTINEL BAR

AI-POWERED PENTESTING & WEB SECURITY EXTENSION

SentinelBar is a free, AI-driven extension that empowers ethical hackers to uncover vulnerabilities and strengthen defenses, providing seamless web security testing directly within the browser.

AUTHORS

Maram Shanmukh Pavan Reddy

Mr. T. Satyendra Kumar

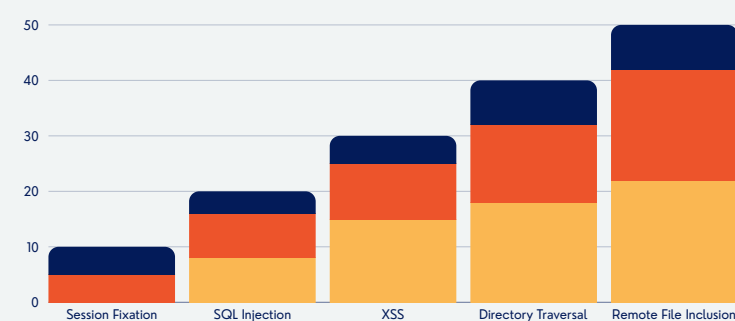**MALLA REDDY UNIVERSITY**

01. INTRODUCTION

Sentinel Bar is an AI-powered pentesting tool designed to assist ethical hackers and cybersecurity professionals in testing and enhancing website security directly within their browser. Built as a Chrome extension, Sentinel Bar offers a seamless interface for simulating attacks, analyzing vulnerabilities, and providing actionable recommendations, making it an accessible resource for anyone focused on web security.

02. OBJECTIVE

The primary goal of Sentinel Bar is to streamline the process of web security testing by integrating attack simulation and AI-driven analysis in one tool. It aims to make cybersecurity more approachable, empowering users to identify vulnerabilities and implement protective measures effectively.

TOOL INTERFACE

05. ANALYSIS

Sentinel Bar's combination of attack simulation and AI analysis provides a unique, efficient solution for cybersecurity testing. Its browser integration and guided learning features make it highly accessible, appealing to both beginners in cybersecurity and experienced professionals looking for quick, reliable insights. Here are some results which we got it from testing a website

Results are based on real world web site pentesiting

Chart categories: Session Fixation, SQL Injection, XSS, Directory Traversal, Remote File Inclusion (y-axis 0–50)

- **Offensive:** Actively testing and exploiting vulnerabilities (e.g., running payloads, simulating attacks).
- **Defensive:** Monitoring and protecting against potential threats (e.g., detecting anomalies, flagging weaknesses).

"Identify Weaknesses, Take Action."
"Monitor, Protect, and Strengthen."

04. RESULTS/FINDINGS

Testing with Sentinel Bar has shown it to be effective in quickly identifying common vulnerabilities, offering precise recommendations that significantly improve web application security. Users report a better understanding of their security posture and greater confidence in mitigating risks after using Sentinel Bar's AI-powered insights.

03. METHODOLOGY

SentinelBar operates through a multi-step process: users first simulate attacks, such as SQL injection or XSS, using the HackBar interface. The AI analysis module then evaluates the results, identifying weak points and generating recommendations. Additionally, an AI chatbot provides real-time guidance and explanations, helping users understand security concepts and the impact of each vulnerability.

SQL Injection, Cross-Site Scripting (XSS), Local File Inclusion (LFI), Remote File Inclusion (RFI), Command Injection, Cross-Site Request Forgery (CSRF), Directory Traversal, XML External Entity (XXE) Injection, Server-Side Request Forgery (SSRF), HTML Injection.

⚠ WARNING

CAUTION!
Use this extension for education purpose only

06. CONCLUSION

In conclusion, Sentinel Bar serves as a valuable tool in the field of ethical hacking, merging AI capabilities with practical pentesting functionalities. With future plans to expand its attack range and enhance AI features, Sentinel Bar aims to become an essential resource for web security testing and education.