

CMSCAN

(Vulnerability Scanner for Content Management System)

A Synopsis Submitted to

Chhattisgarh Swami Vivekanand Technical University Bhilai (C.G.), India



For fulfillment of the award of Degree

Bachelor of Technology

In

Computer Science And Engineering

By

Durgesh Sahu (Roll No :- 301202220065)

Enrollment No. BJ5755

Under the guidance of

Prof. Khushboo Shrivastava

Asst.Pro., Department of CSE, RITEE Raipur(C.G.)



RAIPUR INSTITUTE OF TECHNOLOGY, RAIPUR(C.G.)

Department of Computer Science and Engineering

Chhatauna, MandirHasaud, Raipur, (C.G.)

DECLARATION BY THE CANDIDATE

I the undersigned solemnly declare that the report of the thesis work entitled "CaptureTheFlag" is based my own work carried out during the course of my study under the supervision of Miss Khushboo Shrivastava ma'am, Asst. Prof., Department of CSE, RITEE, Raipur.

I assert that the statements made and conclusions drawn are an outcome of the project work. I further declare that to the best of my knowledge and belief that the report does not contain any part of any work which has been submitted for the award of any other degree/diploma/certificate in this University /deemed University of India or any other country.

Name	Course	RollNo.	EnrollmentID	Signature
Durgesh Sahu	Btech-CSE(5th)	301202220 065	BJ5755	



RAIPUR INSTITUTE OF TECHNOLOGY, RAIPUR(C.G.)

Department of Computer Science and Engineering

Chhatauna, MandirHasaud, Raipur, (C.G.)

CERTIFICATE BY THE SUPERVISOR

This is to certify that the report of the thesis entitled "CaptureTheFlag" is a record of research work carried out by bearing Roll No: 301202220065 & Enrollment No.: BJ5755, Roll No: 301202220068 & Enrollment No.: BJ5781 Under my guidance and supervision for the award of Degree of Bachelor of Technology in Computer Science and Engineering of Chhattisgarh Swami Vivekanand Technical University, Bilai (C.G.), India.

To the best of my knowledge and belief the thesis

- i) Embodies the work of the candidate himself.
- ii) Has duly been completed.
- iii) Fulfils the requirement of the Ordinance relating to the B.E. degree of the University and
- iv) Is up to the desired standard both in respect of contents and language for being referred to the examiners.

(Signature of the HOD)
Mr. Vivek Kumar Sinha
Asst. Prof. Head Of The
Department
Raipur institute of technology

(Signature of the Supervisor)
Miss Khushboo Shrivastava
Asst.Prof. Department of CSE
Raipur institute of technology

Forwarded to Chhattisgarh Swami Vivekanand Technical University,Bilai

(Signature of the Principal)
Raipur Institute Of Technology, Raipur



RAIPUR INSTITUTE OF TECHNOLOGY, RAIPUR(C.G.)

Department of Computer Science and Engineering

Chhatauna, MandirHasaud, Raipur, (C.G.)

CERTIFICATE BY THE EXAMINERS

The Thesis entitled "Untitled" submitted by Durgesh Sahu (Roll No.: 301202220065 Enrollment No.: BJ5755) has been examined by the undersigned as a part of the examination and is hereby recommended for the award of the degree of Bachelor of Technology in Computer Science and Engineering of Chhattisgarh Swami Vivekanand Technical University, Bhilai.

Internal Examiner

Date:

External Examiner

Date:

ACKNOWLEDGMENT

The pleasure, the achievement, the glory, the satisfaction, the reward appreciation and the construction of my project cannot be thought of without the few, who apart from their regular schedule spared their valuable time. A number of persons contribute either directly or indirectly in shaping and achieving the desired outcome. I owe a debt of gratitude to Mr. Vivek Kumar Sinha (HOD) for providing me with an opportunity to develop this project. Through her timely advice.

Constructive criticism and supervision she was a real source of inspiration for me.

I express my sincere thanks to my guide, Miss Khushboo Shrivastava Asst. Prof. Department of Computer Science & Engineering, Raipur institute of technology for his valuable guidance, suggestions and help required for executing the project work time to time. Without his direction and motivation, it would have been nearly impossible for me to achieve the initial level of target planned.

I also express cordial thanks to Dr. Swapnil Jain. Principal, Raipur Institute of Technology. Raipur, for providing necessary infrastructural and moral support. At the last but not the least I am really thankful to my parents for always encouraging me in my studies and also to my friends who directly or indirectly help me in this work

(Signature of the Student)

Name: Durgesh Sahu

Raipur Institute Of Technology, Raipur

TITLE

“Automating the automated CMS vulnerability scanning”

CMSCAN: A Comprehensive Automated Content Management System (CMS) Scanner for Enhanced Website Security

ABSTRACT

CMSCAN is a automated linux tool developed as a college project that aims to provide a comprehensive scanning solution for identifying and assessing vulnerabilities in popular Content Management Systems (CMSs) like WordPress, Drupal, Joomla, vBulletin websites for Security issues. By integrating well-known CMS scanners like wpscan, droopescan, vbscan and joomscan offers an efficient and user friendly interface for security professionals and website administrators to identify potential security risks in their CMS-based websites. This synopsis presents an overview of CMSCAN, highlighting its features, advantages, and potential applications.

INTRODUCTION

As the Internet continues to evolve, Content Management Systems (CMSs) have revolutionized the way websites are created and managed. However, the popularity of CMSs has also attracted the attention of malicious actors, making website security a top priority for organizations and individuals alike. CMSCAN, a comprehensive CMS scanner, emerges as an indispensable tool for effectively identifying and addressing vulnerabilities within popular CMSs.

CMScan combines the capabilities of well-established individual CMS scanners, including WPScan for WordPress, JoomScan for Joomla, Droopescan for Drupal, and VBSscan for vBulletin. By consolidating these scanners into a single, integrated tool, CMSCAN streamlines the vulnerability assessment process, empowering security professionals to proactively protect CMS-based websites from potential exploits.

Key Features of CMSCAN:

Automated CMS Detection: CMSCAN intelligently identifies the underlying CMS powering a website, eliminating the need for manual identification and streamlining the scanning process.

User-Friendly Web Interface: CMSCAN provides a intuitive web-based interface that simplifies the navigation and operation of the tool, enabling both experienced security professionals and novice users to leverage its capabilities effectively.

Comprehensive Reports: CMSCAN generates consolidated reports that highlight identified vulnerabilities and potential security risks specific to the detected CMS, aiding in prioritization and remediation efforts.

Time Efficiency: By leveraging multiple scanners simultaneously, CMSCAN significantly reduces the time required for vulnerability identification and analysis, enabling prompt mitigation measures.

Potential Applications:

CMSCAN finds relevance in various security-focused scenarios, offering benefits such as:

Website Security Auditing: CMSCAN facilitates comprehensive security audits of CMS-based websites, enabling security professionals to identify vulnerabilities and recommend appropriate measures for mitigation.

Penetration Testing: Penetration testers can utilize CMSCAN to simulate real-world attacks, pinpointing potential entry points and assisting in strengthening website security.

Secure Website Development and Maintenance: CMSCAN supports secure website development and maintenance practices by ensuring that CMS installations and updates are performed with a thorough understanding of potential vulnerabilities.

Security Awareness and Education: CMSCAN serves as an educational tool to raise awareness about the inherent vulnerabilities in popular CMSs, empowering website administrators and developers to implement best practices for secure website management.

OBJECTIVES:

- Develop a comprehensive CMS scanner by integrating popular individual scanners.
- Streamline vulnerability identification process by automating CMS detection and execution of appropriate scanners.
- Enhance website security by identifying and highlighting CMS-specific vulnerabilities.
- Provide a user-friendly web-based interface for easy navigation and result analysis.
- Facilitate security audits and penetration testing with comprehensive vulnerability reports.

REQUIREMENT :

HARDWARE REQUIREMENT:

- A Laptop or Desktop
- PROCESSOR INTEL i3 or pentium (3rd preferable)
- RAM 4GB
- ROM 500 gb HDD/SSD

SOFTWARE REQUIREMENT:

- Linux/Window OS (linux recommend)
- Python >= 3
- Docker >= 20.10.23 (if need of prebuilt container)

Conclusion

In conclusion, the CMSCAN project has been successfully implemented and thoroughly tested, demonstrating its capability to meet the specified requirements to a great extent. The machine delivers a comprehensive scanning solution for CMS-based websites, empowering users to identify and address vulnerabilities effectively.

Looking ahead, the project team plans to release new features of CMSCAN that will incorporate new technologies, overcome potential difficulties, and introduce additional exciting features for an enhanced user experience. The aim is to continuously improve the tool's functionality and keep pace with evolving security challenges.

Thank You !