CMSCAN

Vulnerability Scanner for CMS

"Automating the CMS vulnerability scanning"

TEAM MEMBERS

- Durgesh Sahu

Bio

Durgesh Sahu

Class - CSE - 6th

Roll no. 301202220065

What ?

What this project is about?

Why ?

Vision of this project?

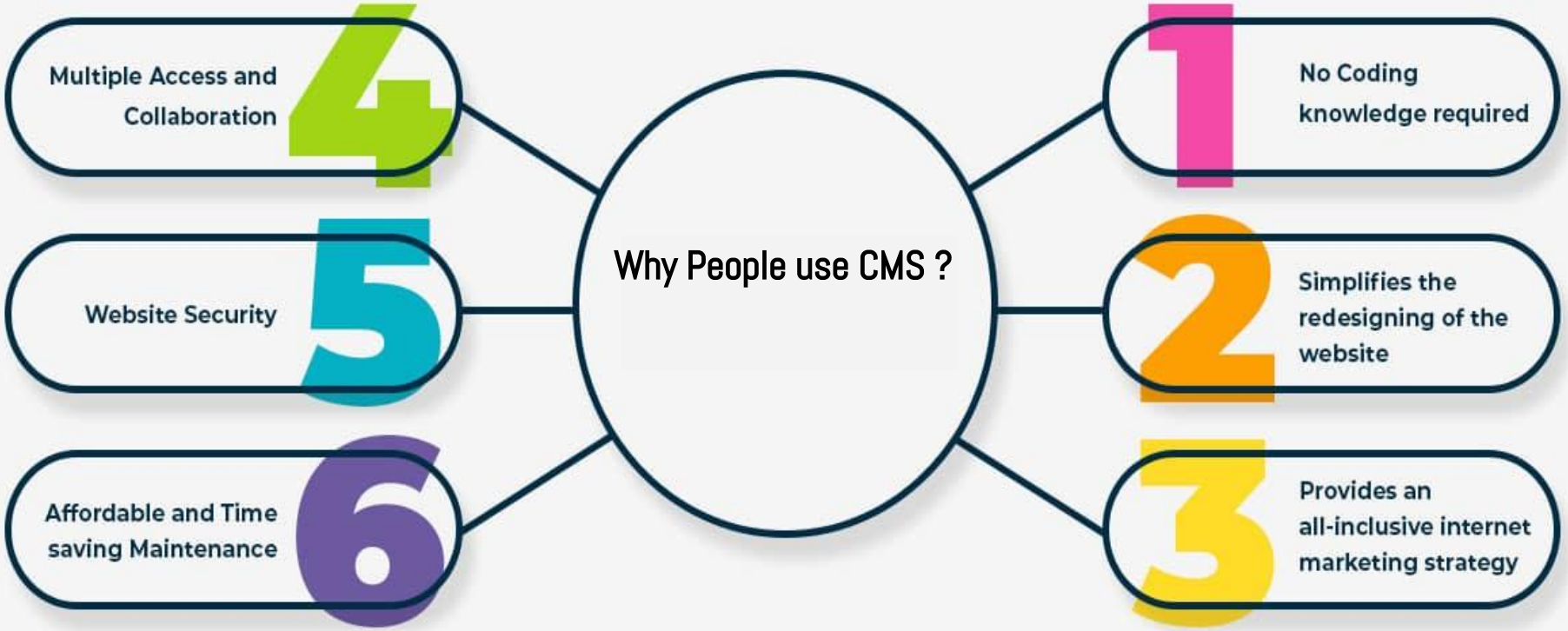
How ?

How to use it?

What is CMS

A content management system (CMS) is software that helps users create, manage, and modify content on a website without the need for technical knowledge. In other words, a CMS lets you build a website without needing to write code from scratch (or even know how to code at all).

E.g - Wordpress, Joomla, Droopal, Magenta etc.


Why People use CMS ?
1
No Coding knowledge required
2
Simplifies the redesigning of the website
3
Provides an all-inclusive internet marketing strategy
4
Multiple Access and Collaboration
5
Website Security
6
Affordable and Time saving Maintenance

BUT !!!!!!!

As the majority of CMS platforms are open source, they are vulnerable by nature. CMS built on an open source framework have its benefits like collaborative environment, sharing and modifying the source code together and many more.

But the main concern is that there is no one to take the responsibility of finding and patching the CMS security vulnerabilities on time. Because it’s free and no one takes accountability for dealing with security issues, the final product often has critical security vulnerabilities. Some of these security vulnerabilities are found by either security researchers or attackers.

What is CMSCAN?

- CMSAN is a automated script including popular vulnerability scanner for CMS(Content Management System)
- A tool with collection of automation tools e.g. wpscan, joomscan, vbscan, droopescan.
- A tool that provides a centralized Security Dashboard for CMS Security scans.

Why CMSCAN ?

- The aim of this project is to provide a automated scanning solution for identifying and assessing vulnerabilities in popular Content Management Systems using populer CMS scanner
- It Simplify Vulnerability Assessment & Pentesting for Content Management System
- User friendly dashboard to analyze assessment report
- Cost-Effective Solution for web admin/developer
- It even provide schedule based scanning and has the ability to sent email reports.

How to setup ?

Although, i have documented the installation process but you just have to :

1. Clone the repo or download the project
2. Run the setup.sh file
3. Run the run.sh file

If you wanna go with docker

1. sudo docker build -t cmscan ./
2. sudo docker run -it -p 7070:7070 cmscan

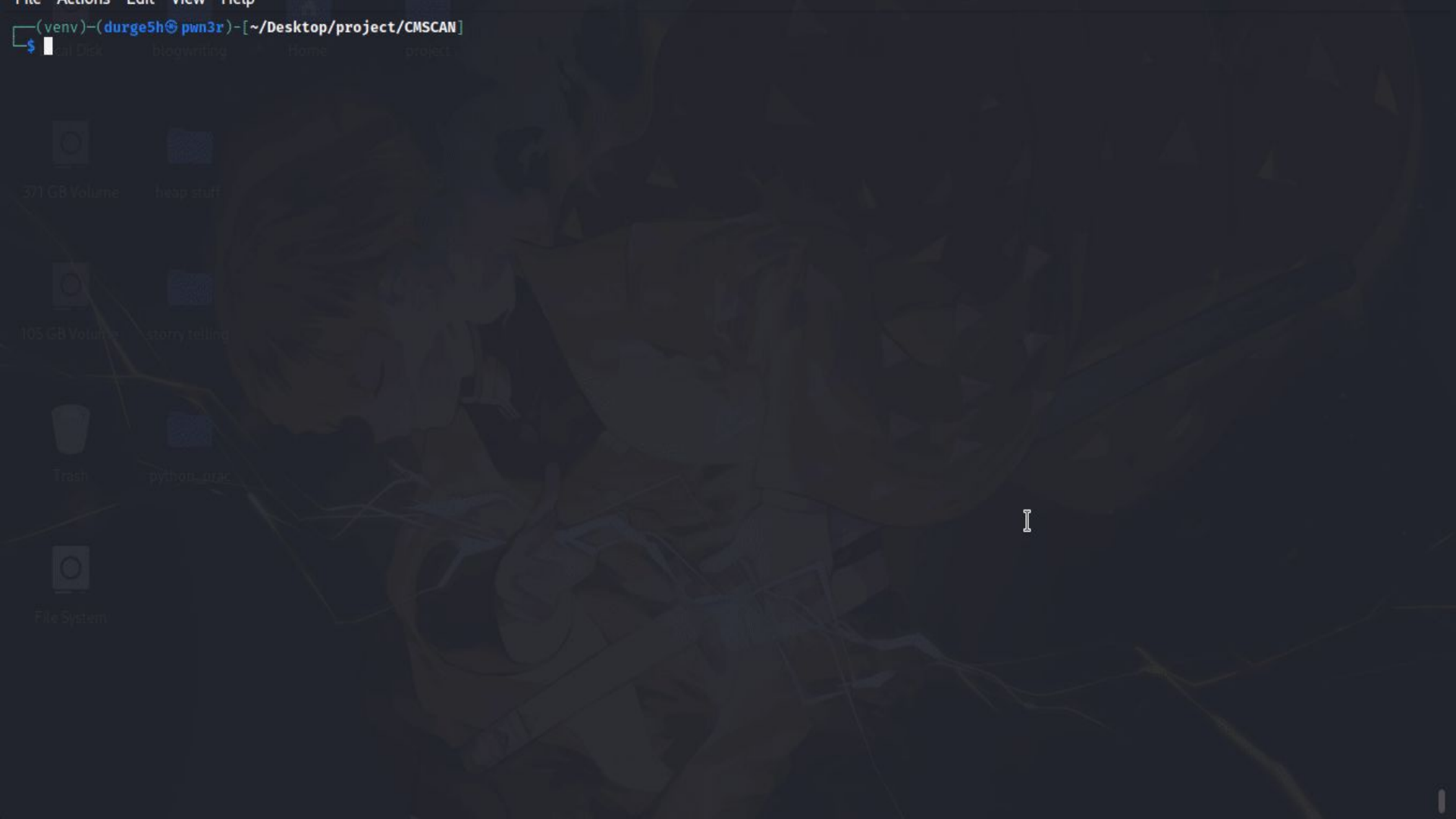
Requirement ?

Software -

- **OS** - Linux/Window(with WSL or docker) (Linux recommended)
- **Language** - Shell script, Python >= 3.9
  - Flask
  - Requests
  - Gunicorn
  - Droopescan
  - Email, smtplib,logging

Hardware -

- A Laptop or Desktop
- Processor intel ii3 or pentium (3rd preferable)
- RAM 4GB
- ROM 500 gb HDD/SSD


File Actions Edit View Help
(venv)-(durge5h㉿pwn3r)-[~/Desktop/project/CMSCAN]
$

Thanks! :)

Project : https://github.com/Durge5h/Projects

Writeup : https://sf4ult.github.io/