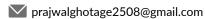# PRAJWAL GHOTAGE

PROFILE

I am a web developer and cyber security enthusiast. My interests lie in web app penetration testing and I love learning new technologies. I am also into public speaking and delivering presentations. Currently I can build websites using the MERN Stack and am familiar with web app penetration testing.

- github.com/mirai-cmd
- prajwalghotage2508@gmail.com
- linkedin.com/in/prajwal-ghotage
- Portfolio Website

EDUCATION

KLS GOGTE INSTITUTE OF TECHNOLOGY
BE, Computer Science and Engineering(2020 - 2024)

Belagavi, Karnataka
- CGPA : 9.04

GSS SCIENCE COLLEGE

PU II, Science (2018 - 2020)

Belagavi, Karnataka
- Result : 90%

SKILLS

- **Frontend** : React.js , TailwindCSS
- **Backend** : Node.js, MongoDB
- **Security** : Metasploit Framework, Burpsuite , Nmap
- **Platforms** : Windows, Kali Linux, Fedora
- **Dev Tools** : git, VSCode, VirtualBox
- **Public Speaking**

LEADERSHIP

- Chair, IEEE Computer Society
- Vice President and Co-founder, Cybersecurity Club of KLSGIT
- Member of Rotaract Club of GIT

CERTIFICATIONS

- Ethical Hacking - NPTEL

EXPERIENCE

PENETRATION TESTER

Eyesec Cybersecurity Solutions Pvt. Ltd.
Jul 2022 - Sep 2022
- Performed a VAPT of client's web applications.
- Analysed system logs, leading to discovery of a hacker present in the system.
- Formulated and submitted a thorough report with remediation methods for the discovered vulnerabilities.
- Used a thorough questionnaire to get an in depth description of client systems in detail from the concerened staff

PROJECTS

HACKER SPACE   GitHub   Live

React.js, Bing NewsAPI, MaterialUI, Context API

- A web app using **React.js** to view news articles on cybersecurity using **Bing News Search API**.
- Users can search for relevant articles by the title of article.
- Articles can also be sorted by date and sources in alphabetical order
- Implemented pagination on news articles and utilized **MaterialUI** to enhance user experience

PYSCAN   GitHub
Python Sockets, Argparser, MultiThreading

- A command line port scanner written in python using **Python Sockets** and **Argparser** for command line arguments.
- Multiple options available including host discovery
- Users can provide custom port ranges and can also scan individual port numbers.
- **MultiThreading** speeds up scanning process initiating scans on multiple ports at a time