Gaurav Narwani

(667) 464-1583| gauravnarwani97@gmail.com | linkedin.com/in/gauravnarwani97 | gauravnarwani.com | github.com/gauravnarwani97

- **3** years of experience in **Information Security** and **Security Automation**
- An avid blogger and eloquent public speaker with extensive experience in security packages and tools
- Seeking full time roles in the Application/Product Security domain from January 2024

Areas of Interest: Web Application Security, Security Automation, API and Microservice Security, Source Code Review, Threat Modeling, Mobile Application Security, Infrastructure and Cloud Security, Red Teaming, Cryptography, Penetration Testing

Education

JOHNS HOPKINS UNIVERSITY - *Whiting School of Engineering,* Baltimore, MD
Masters of Science in Computer and Information Systems Security; Expected Graduation: Dec 2023; GPA: 3.92/4

Relevant Coursework: Security & Privacy in Computing, Software Vulnerability Analysis, Modern Cryptography, DevOps and Secure Software Development, Blockchain, and Cryptocurrencies, Security Analytics, Network Security, Ethical Hacking

UNIVERSITY OF MUMBAI, Mumbai, India
Bachelor of Engineering in Computer Engineering; May 2015 - May 2019

Relevant Coursework: Data Structures, Computer Organization & Architecture, Database Management Systems, Operating System, Computer Networks, Software Engineering, Cryptography and System Security, Artificial Intelligence, Machine Learning

Skills

Programming Languages:	Python (*Proficient*), Java, C/C++, XML, JavaScript, HTML, CSS, PHP, NodeJS, SQL
Security Tools:	Burp Suite, Nmap, Metasploit, Beef, Hydra, Wireshark, Aircrack, Sqlmap, Nessus, Acunetix, Checkmarx, Netsparker, OWASP ZAP, RabbitMQ, Ghidra, GDB, Trufflehog, Semgrep, Microsoft Threat Modeling Tool
Certifications:	BSCP - Burp Suite Certified Practitioner, Portswigger (March 2022)

Experience

ERMPROTECT; Miami, Florida

Information Security Consultant Intern; May 2023 - July 2023

- Implemented automation solutions for Wi-Fi and Web Application Penetration Testing, boosting vulnerability detection rates. This advancement empowered pentesters to swiftly triage, prioritize, and conduct in-depth manual reviews.
- Developed an integrated audit framework for Windows, Linux, firewalls, Switches, and routers, fusing CIS benchmarks with NIST controls. This innovation streamlined processes by 60% and fortified compliance standards.

SOCIÉTÉ GÉNÉRALE; Bengaluru, India

Senior Cyber Security Analyst; December 2021 - May 2022

- Refined existing feedback and prerequisite processes to enhance throughput by 60% and worked closely with SOC in purple teaming exercises to increase attack detection mechanism by 20%
- Built scalable Nmap and Recon Automation tool in Python with multithreading to administer multiple test cases on each port discovered in the scan phase.
- Designed DAST automation architecture to incorporate tools like Burp Suite, Nessus etc. to form a secure SDLC pipeline.

Cyber Security Engineer; June 2019 – November 2021

- Enhanced vulnerability detection capabilities to uncover over 200 threat vectors, including Remote Code Execution and SQL Injection. Concurrently introduced a NodeJS reporting tool, optimizing workflows and shortening reporting time by a full day.
- Hosted security awareness programs, vulnerability mitigation meetings, weekly podcasts, and authored newsletters on the importance of secure coding, phishing emails, and physical security.

Independent Projects

Cross Pentest & Recon Automation; October 2021 – Present

- Developed using multiprocessing and priority scheduling, recon automation script in Python for automated authenticated crawl and vulnerability discovery that can handle more than 50 domains simultaneously.
- Programmed the scripts to inspect IDORs, Privilege Escalation, Cross-Site Scripting, SQL Injections, Server-Side Template Injections, HTTP Request Smuggling, and Subdomain Takeovers in real-time, incorporating the rate limit quota.

Trishul (link); March 2020

- Developed an open-source Burp extension using Jython to detect Cross-Site Scripting, SQL Injections, and Server-Side Template Injections in real-time supporting over 100 parameters in a single request.
- Having garnered more than 150 stars and 50 forks on GitHub, Trishul is widely used by Infosec Professionals, Bug Bounty Hunters and beginners for automated vulnerability detection in reconnaissance stage.

Publications & Presentations

Publications:	EspoCRM 5.6.8 (Multiple Cross-Site Scripting Issues - August 2019) - **CVE-2019-14546, CVE-2019-14547, CVE-2019-14548, CVE-2019-14549, CVE-2019-14559** Dolibarr 11.0.0-alpha (Admin Account Takeover - August 2019) - **CVE-2019-15062**
Presentations:	• Delivered a Talk on Pentesting API 101 at Worqference Conference - March 2023 • Delivered one-day training to Women in Cyber Security – October 2019

Honors & Awards

Fourth Place at Raymond James CTF - Represented Johns Hopkins University Team	October 2022
Awarded **Star of the Quarter Q1 2020** for the trait 'Curiosity'.	March 2020
Fifth Place at Brainwaves CTF Hackathon by Société Générale	February 2019
Hall of Fame: Vimeo (**4th**), Caseys (**1st**), Salesforce, Sophos, Ford, Sentiance, Under Armour, Inflectra, Roamler, Fitbit, Jet, Western Union, Humble Bundle, Puppet Labs, Overstock VDP	May 2018 – Present