Hrishikesh Nate

Mumbai-400031
Cell: +91-
8097108406,7039172503
Email: ihrishikeshnate@gmail.com

Career Profile:

Working as a Security Researcher, Web Developer having 4.8 years of experience in finding vulnerabilities, building secure web applications, and creating tools to protect against cyber threats. My work has taught me the importance of attention to detail, problem-solving, and staying up-to-date with the latest security concepts and practices.

Career Objective:

Achieving an apical position in Cyber Security Profession. Looking for an opportunity to work on challenging and interesting modules and projects. Motivated and eager to upgrade my career with a growth-oriented, technically-advanced organization as an Information Security Researcher.

Professional Experience:

- Working as a Senior Security Engineer at **Paytm** Financial technology company (July 2021-Present) Bangalore.

  Achievements:

  - The tool fetches data from AWS Route 53 and compares it with a local database, identifying new domains and differences. It then performs a scan on the new domains using open-source tools, allowing for the proactive identification of potential security vulnerabilities or other issues. This tool can provide valuable insights for security and IT teams managing AWS environments.
  - The most recent Development is the file-share portal which is now in production and allows file sharing and maintains logs for files shared among registered users this tool was developed to monitor and centralize file sharing within the organization with all security and audit requirements.
  - The **“Github Crawler”** is a tool that allows users to query GitHub search results without being limited by the rate limits imposed by the open GitHub API. By bypassing these limits, users can obtain search results more quickly and efficiently, all from the comfort of their terminal. This tool can be particularly useful for developers and researchers who need to search for specific code snippets, repositories, or other information on GitHub.
  - The open-source dashboard I developed integrates Jira tickets, providing management with a comprehensive and analytical view of the Jira ticketing process, including duration metrics. This tool can help organizations using Jira to streamline their ticketing processes and optimize their workflows by identifying areas for improvement and potential bottlenecks. With this dashboard, management can make data-driven decisions and improve overall efficiency and productivity.
  - **“Spyonic”** is a homegrown product I developed that integrates various open-source bug bounty tools, allowing users to identify and remediate low-hanging fruits caused by security misconfigurations. With this tool, organizations can proactively detect and address vulnerabilities, reducing the likelihood of a successful attack. By combining multiple bug bounty tools into one platform, Spyonic can

provide a comprehensive security assessment and help organizations prioritize and focus their remediation efforts.

- The **"Slack app"** I developed takes user input in the form of a domain and performs a self-assessment for S3 takeover. The assessment includes checks for default metrics/actuator paths and the use of custom wordlists using Dirsearch. By automating this process within Slack, organizations can quickly and easily assess their S3 security posture and identify any potential vulnerabilities or misconfigurations. This tool can help organizations reduce the risk of a successful attack and ensure that their S3 buckets are properly secured.
- This automation process crawls the latest CVEs from the OpenCVE API and stores them for later use. It then uses a **Qualys** script to that queries to identify the latest vulnerabilities, to match them against the CVEs previously collected. This process can help organizations proactively identify and address potential vulnerabilities before they can be exploited. By automating the collection and matching process, this tool can save time and improve the overall security posture of an organization's infrastructure.

Job Role & Responsibilities:

- Conducting security testing of web applications and APIs using SAST and DAST techniques.
- Developing and maintaining automated security testing scripts for web applications and APIs.
- Analyzing security test results and identifying potential vulnerabilities or security weaknesses.
- Providing guidance and recommendations to development teams on security best practices and vulnerability remediation.
- Collaborating with cross-functional teams, including developers, architects, and project managers to ensure security requirements are met throughout the development lifecycle.
- Participating in security incident response activities as needed.
- Staying up-to-date with the latest security trends, vulnerabilities, and threat landscape.
- Providing training and education to other team members on security best practices and emerging security technologies.
- Leading to security-related projects and initiatives, such as security automation and tool development.

- Working as a Senior Security Executive in **Justdial Limited** (July 2018 –July 2021) in Bangalore.

Job Role & Responsibilities:

- Web Application Penetration Testing.
- API Pen Testing.
- Vulnerability Assessment & Penetration Testing for Internal and External Networks.
- Monitored the use of data files and regulated access to protect secure information.
- Monitored computer virus reports determining when to update virus protection systems (Quarterly VA-PT)
- Conducted penetration testing and located system vulnerabilities before they could be exploited.
- Monitored the organization's networks for security breaches and investigated violations.
- Expertise in security policies.
- Expert in Automation Scripts.

Achievements:

- Automated the whole IP Blocking and Releasing process.
- Implementation of Rules based on Crawling behavior.

- Worked as an intern at **Justdial Limited**.

  Job Role & Responsibilities:

  - SIEM module.
  - Worked on MVC Projects.
  - LAMP Architecture.

Government Association:

- Tested Maharashtra State government's websites for vulnerabilities and reported to the respective authorities with appropriate optimal solutions for the same.
- Developed an OSINT Tool called OsintORK for ease in the digital investigation for authorities and to help fraud online traces of reformation regarding the subject of the case.
- Dark-Web Deep monitoring.
- Collected requirements as per department needs and developed a Social Media Monitoring Web Application for collecting complaints regarding offensive posts.
- Included modules to generate automated letters/ reports/notices based on actions taken by the respective authority and dynamically change content as per the sections of the India Penal Court criminal procedure code and IT Act.
- Automating and Optimizing Infrastructural Work.

Technical Proficiency:

- Web Application Penetration Testing. (DAST & SAST).
- API Penetration Testing.
- Vulnerability Assessment & Penetration Testing .
- Android Penetration Testing.
- Networking.
- Automation & Scripting.

Certifications & Training:

- EC-Council: - CEH V10 (ECC3150269784).
- CCNA Routing & Switching.
- CCNP Security (ASA).
- CNSS(Network Security).
- Microcontroller 8051 Key skills.

Software Languages & Tools:

Security Tools:

DAST: Burp Suite, Postman
SAST: Checkmarx
VA: Nessus, Faraday, Qualys

WAF: Akamai CDN.

Cloud: **AWS** EC2, S3, Route 53 (Basics)

Front-end Languages:

HTML5, CSS3, JavaScript, Ajax.

Back-end Language:

Bash, Python, PHP, Groovy.

Database:

MySQL, PostgreSQL

Framework:

Flask, Django.

Educational Summary:

Examination	Specialization	University/ Board	Year
B.E	Bachelor of Electronics & Telecommunication Engineering	Mumbai University	2018
HSC	Science	Maharashtra Board	2014
SSC	General	Maharashtra Board	2012

Technical Project Accomplishments:

• Cloud Computing and Firewall on Raspberry Pi.
• Quadcopter configuration and assembling using Arduino.
• Testing Payloads and Malware on Windows 10 and antivirus.
• Testing WPA, WEP, and WPA2 wifi.
• Practice in Capture the Flag challenges from Vuln Hub, Hack The Box, and Over The Wire. • Darknet Crawler.

Social:

- https://www.linkedin.com/in/hrishikesh-n/
- https://twitter.com/hrishikesh_nate
- https://github.com/ihrishikesh0896

Personal Details:

Name: Hrishikesh
DOB: 19-08-1996
Nationality: Indian
Languages : English, Marathi, Hindi.