Parth Parmar

Sandy Springs, GA 30350

☎ 240-733-7054 ✉ parmar.parth97531@gmail.com https://parthparmar.blog

Education

University of Maryland - College Park **Aug. 2021 – May 2023**
Masters of Engineering in Cyber Security - 3.96 GPA *College Park, Maryland*

Courses : Secure Coding, Penetration Testing, Cloud Security, Reverse Engineering, Network Security, Networks and Protocols, Hacking with C, Secure Operating Systems, Security Tools

Vishwakarma Government Engineering College **Aug. 2016 – Sep 2020**
Bachelors of Engineering in Information Technology - 8.93 CGPA *Ahmedabad, India*

Experience

Sophos **August 2023 – Present**
Threat Analyst *College Park, Maryland*

- Secured thousands of customers from threats by working on detections with Managed Detections and Response team.
- Resolved investigation cases and threat hunts in under 45 minutes.
- Conducted Threat Hunt and Incident response to thwart attackers in customer estate.
- Performed Malware analysis during Active Incidents and contributed to Threat Intelligence.
- Formulated Cyberchef Automation recipes to reduce 90% time analysts spent in de-obfuscation during investigations.
- Delivered a symposium on a novel supply chain attack around package managers, along with developing tools for hunting such activity in real time.

UMIACS **February 2022 – December 2022**
Security Engineer (Research) *College Park, Maryland*

- Collaborated on 'Data Driven Security' research project focusing on security metrics like CVSS about exploitability of vulnerabilities, providing likelihood of a functional exploit being devised for CVE in near future.
- Analyzed various data endpoints and wrote crawlers using python and tested on docker.
- Provided support for website and debug issues along with development of python modules for parsing and crawling, decreasing load time of website by nearly 70% using AWS Cloud Platform.

Tata Consultancy Services Ltd **February 2021 – August 2021**
Assistant Systems Engineer *Gandhinagar, India*

- Managed Alfresco content management solution globally for Sony Pictures Entertainment.
- Monitored 30 Production Servers and 10 QA Servers during release cycle, upgrade activities and ensured availability.
- Built Java and JavaScript based code modules for Alfresco using Secure Software Development LifeCycle. Initiated process improvement activities for performance enhancements and bug fixing.
- Awarded Alfresco champion for analyzing and fixing a multi-threaded batch job failure.

Projects

Secure IT Support Portal | *.NET Core, MySQL* **November 2022**

- Developed a secure web application based on .NET core and Secure SDLC practices.
- Performed technical Secure Code Review and Threat Modeling for the project in a staged manner.
- Authorization and Authentication were implemented for each functionality and tested on more than 40 unit test cases.

NPM registry follower | *JavaScript, Bash* **August 2022**

- Developed an automated registry follower for demonstration in symposium "Exploiting Package Managers: Attacks and Detection" with a goal to identify malicious packages in real time.
- Designed JavaScript code to collect data from public npm change stream and find IOCs for malicious packages using install scripts to get real time data.

Technical Skills

Certifications: OSCP (OS-101-50541), RHCSA- Redhat Certified System Administrator (ID-200-000024)
Languages: Python, Bash, Java, C/C++, Go lang, C#, JavaScript, SQL
Technologies/Frameworks: Network Access Control, Application Security, Security Assessments, Threat Intelligence, Data Security, Incident Response, Ruby, Firewalls, Kubernetes, Helm ,Amazon Web Services (EC2, S3 buckets, AWS Lambda, Security Monitoring, Intrusion Detection)
Competitions/Labs: Participated in various CTFs like PicoCTF, Hackthebox and Portswigger Academy