Ishaq Mohammed

Application Security Enthusiast

https://ishaqmohammed.me/

I am an Experienced Security Enthusiast with over 5 years of demonstrated skills in Application Security Engineering and Automation, Penetration Testing, Vulnerability Assessment and Secure Code Review. I sometimes play ctfs on hackthebox, lab.pentestit.ru, root-me.org, and Web Security Academy and also do open source security research, more about my work and learnings can be found on my blog

EDUCATION

MUMBAI UNIVERSITY **JUNE 2013 TO MAY 2016**

Bachelor of Science in Information Technology (B.Sc. (I.T.))

EXPERIENCE

APPDIRECT, PUNE **MAR 2020 TO PRESENT**

Application Security Engineer

- Performed pentesting and security reviews of AppDirect products and services
- Setup & Organized CTFs & Trainings for internal teams & security champions
- Designed and documented the security champions program
- Evaluated tools available widely to integrate and implement SSDLC
- Worked on the POC for Github Advanced Security and Detectify
- Managed private bug bounty program
- Reviewed over 800+ subdomains for subdomain takeover issues
- Reviewed and validated over 2.2k AppDirect repositories for leaked secrets
- Conducted internal PCI segmentation testing and vendor security assessments
- Conducted phishing campaigns across AppDirect employees
- Coordinated with engineering team to ensure that solid security practices are applied in the SDLC
- Proactive research on latest vulnerabilities and exploits

QUALYS, PUNE **MAR 2018 TO MAR 2020**

Application Security Analyst

- Performed pentesting of Qualys products and services
- Performed security reviews of inhouse extensions and plugins
- Performed regular dynamic and static security testing for product builds
- Automated software composition analysis using open-source tools
- Proactive research on latest vulnerabilities and exploits

SECURELAYER7 TECHNOLOGIES, PUNE **SEPT 2016 TO FEB 2018**

Information Security Consultant

- Performed automated and manual vulnerability assessment and penetration testing across internal, external networks and applications as per standards using both commercial and open source tools
- Creating and setting up pentest labs

TOOLS

Burpsuite, Nmap, Github Advanced Security, Sonarqube, Dependency-Check, Dependency-Track, Nessus, WhiteHat Sentinel, Docker, Kubernetes, Maven, Gradle, Jenkins, Git

PROJECTS

- MavenDependencyCheck
- CSV Injection Vulnerable Script
- Race Condition Vulnerable Web Application

AWARDS & ACHIEVEMENTS

Certifications/Courseworks

- Certified DevSecOps Professional(CDP)
- Golang Bootcamp
- Kubernetes for the Absolute Beginners

CVEs

- CVE-2019-10349 - Stored XSS vulnerability in Dependency Graph Viewer Plugin
- CVE-2019-6804 - Rundeck Community Edition - Cross-Site Scripting
- CVE-2017-14618 - PHPMyFAQ 2.9.8 - Cross-Site Scripting
- CVE-2017-14619 - PHPMyFAQ 2.9.8 - Cross-Site Scripting
- CVE-2017-15284 - OctoberCMS 1.0.425 (Build 425) - Cross-Site Scripting
- CVE-2017-15878 - KeystoneJS 4.0.0-beta.5 - Cross-Site Scripting
- CVE-2017-15879 - KeystoneJS 4.0.0-beta.5 - CSV Excel Macro Injection
- CVE-2017-16807 - Kirby CMS < 2.5.7 - Cross-Site Scripting
- CVE-2017-18048 - Monstra CMS 3.0.4 - Arbitrary File Upload / Remote Code Execution
- CVE-2017-18049 - SilverStripe CMS 3.6.2 - CSV Excel Macro Injection

Presentations

- Garage4Hackers: Talk on CSV Injection Attacks
- Infosecgirls Workshop: Web Application Security

Vulnerability Publications

- ExploitDB
- SSD Advisory – Monstra CMS RCE

EXTRACURRICULAR ACTIVITIES

- Active participant, Null & OWASP Chapters
- Curator – DevSecOps Newsletter
- Reviewer - Free Docker Security Course