AJIN ABRAHAM

Security Research and Engineering

Bangalore, India
+919633325997
ajin25@gmail.com
ajinabraham.com
github.com/ajinabraham

SUMMARY

Highly self motivated and out of the box thinking individual with strong proficiency in Computer Security and Applied Security Research. Authored some of the well known open source security tools like Mobile Security Framework, an automated pentesting platform for mobile applications, OWASP Xenotix XSS Exploit Framework, an advanced cross site scripting detection and exploitation framework, Droid Application Fuzz Framework, an android browser and pdf fuzzing framework and NodeJsScan, a SAST for Node.js web applications. OWASP Xenotix and MobSF were among the Top 10 Security tools by ToolsWatch for the years 2013, 2014, 2016 and 2017.

Published security research at notable security conferences around the globe including BlackHat Europe, BlackHat Asia, Hack In the Box, OWASP AppSec AsiaPac, OWASP AppSec EU, Nullcon, ClubHack, Sacon, c0c0n, Ground Zero Summit, Hack In Paris and PHDays

Areas of interest include runtime security instrumentation, web and mobile application pentest, code and architectural reviews, security tool development, security automation, breaking and fixing security products, fuzzing, reverse engineering and exploit development.

SKILLS

Security

Security Research, Secure Code Review, Penetration Testing, Vulnerability Assessment, Threat Modelling, Secure Architecture/Design Review, Security Automation, DevSecOps, Web Security, Mobile Security (Android, iOS, Windows, Tizen), Framework and Server Security, AWS Security, Container Security, Exploit/PoC Development, Windows and Linux Exploit Research, Network Security, Malware Analysis and Reverse Engineering.

Security Engineering and DevSecOps

Python, JavaScript, Golang, Node.js, Lua, Java, Ruby, C, C++, Android, MASM, VB.NET, C#, ASP, PHP, Bash, Electron, HTML5, CSS3, Bootstrap, Foundation, JavaScript frameworks, AWS, GCP, Docker, Kubernetes, Ansible, Supervisor, Git, Perforce, Jenkins, MySQL, PostgreSQL, MSSQL, MongoDB, Memcached and Redis.

WORK EXPERIENCE

Security Researcher

2017-Nov - Present

TrendMicro

Security Researcher, Eliminating web vulnerability classes one at a time.

- Evangelized and spearheaded Product Security related initiatives, discussions and tasks.
- Conducted independent security research, developed or improved novel defence techniques against Deserialization remote code execution and Expression language injection in web applications.
- Worked on integrating and testing IPS and RASP technologies for the next generation security product that focus on containerized environments.
- Developed a test suite that evaluate IPS rules by repeating HTTP packet from PCAPs.
- Conducted AWS Infrastructure pentest and security assessment focussing on IAM, Lambda, EC2, EBS, RDS, S3, CloudFormation, Fargate/ECS and EKS.
- Implemented Docker container scan service that performs periodic vulnerability scan of docker images.

Product Security Engineer

2015-Sep - 2017-Oct

IMMUNIO

Product Security, Security Engineering and Research

- Member of Security Research and Development team responsible for designing and developing cutting edge security defences with runtime instrumentation (Python, Ruby, Java, Node.js, Lua and JavaScript).
- Researched and developed or improved novel defence techniques against DOM XSS, Verb Tampering, Layer 7 DDoS, Session Hijacking and Credential Stuffing in web applications.
- Published an academic research paper titled *Injecting Security into Webapps at Runtime.*
- Developed a Differential Pentest POC based on context learning capabilities of RASP that reduced automated DAST scan times from hours to minutes.
- Developed a framework for benchmarking RASP, WAF and other security products.
- Discovered bypasses and edge cases in RASP agents and developed fixes or provided remedies.
- Developed in-house fuzzers for automated vulnerability or bypass detection in RASP agents.
- Performed vulnerability analysis and reverse engineering of interesting Zero Days or CVEs and published detailed technical blogs at https://www.immun.io/blog/author/ajin-abraham

Founder

2015-Dec - 2017-Oct

OpSecX

Founded OpSecX Security Education Platform

Created OpSecX, an online platform for self paced application security education. The e-learning platform captured 8000+ students from 90+ countries. The venture started to run on profit from second month of it's launch and continue to run profitably.

Application Security Consultant

2015-Oct - 2017-Oct

Envestnet | Yodlee

Web and Mobile Security, Security Architecture and DevSecOps

- Involved in security architecture and design review of new products.
- Conducted pentest and code review of Yodlee's fintech web and mobile applications written in Java, Objective C, PHP, Node.js, and Golang.
- Coordinated with engineering team to ensure that solid application security practices are followed in the SDLC process.
- Conducted zero day exploit analysis and implemented interim code patch or WAF rule before vendor support/software update is available.
- Automated security assessments, developed security tools and secure libraries to be used within the organization (Python, Golang, .NET, JavaScript).
- Implemented DevSecOps pipelines to keep security in pace with agile development environment.
- Mentored and trained a team of freshers in Application Security and Security Engineering.
- Designed Security CTF competitions for improving competence of team members.

Application Security Engineer

2014-June - 2015-Sep

Yodlee

Web and Mobile Security, Security Assessment and Automation

- Conducted threat modelling, pentests, manual and automated code reviews and security certification of hybrid mobile applications (Android, iOS), web applications (Java, Node.js) and SDKs (Android, Node.js, JavaScript).
- Developed open source security tools for automated security testing of mobile and web applications. Major open source contributions include YSO Mobile Security Framework, NodeJsScan, and OAuth 1.0a Request Proxy (Python, .NET, Java, JavaScript).
- Worked with engineering team to ensure that secure SDLC is followed and all Yodlee applications are built with security controls right from the early design and implementation phase.
- Performed application security research and published the research findings at multiple security conferences.

EDUCATION

MBA in Information Security Management
2015 - 2018

University of Madras, India

Pursuing Master of Business Administration (MBA) in Information Security Management

Bachelor of Technology in Computer Science
2010 - 2014

Kannur University, India

- First Class, CGPA -74.38%
- Computer Science Branch Topper Award 2010-2014.
- Best Outgoing Student Award 2010-2014.
- Best Speaker Award at Forchsung International Conference 2014.
- One among the Top 3 Finalist of Mar Baselios Youth Excellence Award 2014.
- MalBoxie Project won 2000 USD from MetaScan for the valuable security project to community category.

AWARDS & ACHIEVEMENTS

- OWASP Xenotix XSS Exploit Framework ranked 5th in ToolsWatch Top Security tools of 2013 and 2014
- Yodlee MVP Award within 8 months of joining the Security team
- 3 Performance Spot Awards from Envestnet Yodlee.
- Mobile Security Framework - MobSF ranked 5th in ToolsWatch Top 10 Tools of 2016
- Mobile Security Framework - MobSF ranked 9th in ToolsWatch Top 10 Tools of 2017
- Nullcon BlackShield Luminaire award 2017 for the most talked about person in most of the 1337 conferences and communities, one who has made a significant contribution to the security landscape and has been an inspiration to others.
- Quoted in BBC News
  Mobile Security: http://www.bbc.com/hindi/india/2015/02/150219_android_phone_hackers_tk
  Drone Safety and Security: http://www.bbc.com/hindi/india-42366906

RESEARCH PUBLICATIONS

- Detecting and Exploiting XSS with OWASP Xenotix XSS Exploit Framework - Nullcon, BlackHat Europe
- Abusing Exploiting and Pwning with Firefox Add-ons - OWASP AppSec AisaPac
- Xenotix xBOT: The Layer 7 SSL Encrypted Bot with Google as C&C - Ground Zero Summit
- Hacking Tizen: The OS of Everything - Nullcon, HITB
- Automated Mobile Application Security Assessment with MobSF - c0c0n, Nullcon, BlackHat Asia, OWASP AppSec EU
- Injecting Security into WebApps at Runtime - Nullcon, Sacon, HackInParis, PHDays