Pradeep Jairamani

Linkedin Profile: https://www.linkedin.com/in/pradeepjairamani/
Github Profile: https://github.com/pradeepjairamani

Professional Summary

- Information security analyst with the ability to protect systems from internal and external threats.
- Proficient in red teaming, network vulnerability assessment, web application security testing, wireless security testing, kubernetees security assessment, docker security and serverless security.
- Reported multiple vulnerabilities and received acknowledgments from tech giants and also produced CVE reports for various content management systems. (CVE-2018-6890 (WolfCMS), CVE-2018-6905 (Typo3CMS), CVE-2019-12425, CVE-2019-0235 (Apache Ofbiz), CVE-2019-16888(Konakart), CVE-2019-19892 (OpenMRS))
- Expertise in automation of Web and Network application vulnerability analysis using Python.

EDUCATIONAL QUALIFICATIONS

Year	Degree/Certificate	Institute/School
2018	B. Tech Computer Engineering	Poornima University, Jaipur
2014	XII (CBSE)	Defence Public School, Jaipur
2012	X (CBSE)	Defence Public School, Jaipur

Work Experience

Colortokens LLP ***(Sep'19-Present)***
Profile: Security Engineer
Job Responsibilities

- Worked on RASP (Runtime application self-protection) based application security product's (Colortokens XSecure) capabilities and improved signatures and behavioral methods for detecting security vulnerabilities.
- Worked on Docker security and kubernetees security tools like Clair, docker-bench, kube-bench, kube-hunter, anchore-cli, cilium, etc
- Worked on serverless security penetration testing (OWASP top 10 for serverless)
- Worked as a security engineer to perform web application penetration testing on multiple client locations and found critical vulnerabilities including Privelege escalation, SQL injection, Insecure direct object reference, XSS, CSRF, File upload, Remote command injection etc.
- Worked on multiple open source applications for increasing application security coverage and reported multiple vulnerabilities including SSRF, CSRF, Host header injection, Clickjacking, XSS. (CVE-2019-12425 (Apache Ofbiz), CVE-2019-16888(Konakart), CVE-2019-19892 (OpenMRS))

Ernst & Young ***(June'18-Aug'19)***
Profile: Security Analyst (IIC Advisory)
Job Responsibilities

- Worked for industry in the field of Healthcare, Pharmaceutical, Telecommunication, Beverage, Manufacturing, Consultancy, Banking and Hotel industry.
- Performed Red team assessments for clients in research centres, manufacturing plants, telecommunication firms, beverage industry, hotel chains, technical consultancy firms and hospital network.
- Conducted phishing drills with 30000+ users for clients in technical consultancy, manufacturing and. software development firms
- Performed Configuration review and endpoint security review for multiple clients in banking sector and manufacturing firms.
- Worked on a range of assignments related to Vulnerability assessment and Penetration Testing in Web and Infrastructure (Grey Box and Black Box) with telecommunication, manufacturing and Banking sector in India and Europe

- Created Boot2Root network challenge for Annual Information security summit 2018 CTF Hackathon hosted by Data Security Council of India & EY.
- Received 2 EY Kudos award for exemplary performance.
- Contributed in EY knowledgebase about active directory reconnaissance and initial foothold techniques using SMB relay attacks.
- Received EY cyber security Bronze Badge.

A Leading Healthcare firm:

- Performed Red team assessment and physical security testing. Compromised windows active directory environment and gained access to all the servers including windows endpoints, Linux servers, cameras, routers and switches

A Leading Manufacturing Firm:

- Conducted Wi-Fi Security Assessment, Network VA/PT and successfully compromised local windows active directory environment, Microsoft Azure active directory environment, Linux servers, routers, switches and camera devices.

OWASP Foundation ***(Mar'18-Present)***

Profile: Project Leader and Google Summer of Code Intern

Project URL: https://github.com/zdresearch/OWASP-Nettacker

Job Responsibilities

- Vulnerability research for adding more exploits and reconnaissance tools.
- Python Development (Create and implement service scanner, SPF (Sender Policy Framework) Record Testing for Mail Servers, FTPVulnerabilities, CMS vulnerability detection and brute forcing, Password List Generator, Enhancing Language Library, HTTP/HTTPS vulnerabilities, Honeypot Detection)

Provensec LLC. ***(Aug'17-Apr'18)***

Profile: Information Security Analyst and Python Developer

Job Responsibilities

- Finding vulnerabilities in network and web applications for small and medium organizations.
- Lead Python developer in Provence Network Scanner, SIEM-Pro, Internal scanner ISO.

Nex-G Exuberant Solutions PVT LTD. ***(Nov'16-Jan'17)***

Profile: Big Data and Hadoop Intern

Job Responsibilities

- Setting up Hadoop and Zookeeper for the Infrastructure.
- Working on fetching data from HBase using Hive and Pig.
- Automating log sending to database using Flume and Scoop.
- Maintaining 100% uptime of the servers using Zookeeper.

Independent Security Researcher ***(Jan'13-Present)***

- CVE-2018-6890 WolfCMS
  https://github.com/pradeepjairamani/WolfCMS-XSS-POC
- CVE-2018-6905 Typo3CMS
  https://github.com/pradeepjairamani/TYPO3-XSS-POC
- Listed as a Security Researcher for finding critical vulnerabilities in various websites.:
  - Twitter Security Acknowledgment
  - Apple Security Acknowledgment
  - Microsoft Security Acknowledgment
  - Ebay Security Acknowledgment
  - Blackberry Security Acknowledgment
  - Telekom Security Acknowledgment
  - AT&T Security Acknowledgment
  - Adobe Security Acknowledgment
  - Nokia Security Acknowledgment

PROJECTS

Provensec Network Scanner

(Jan'18 - Present)

- Vulnerability research for adding network vulnerability assessment scripts
- Performs a Service and version detection of the client's machine.
- Finds exploits from MongoDB for service and version.
- Dynamically finds plugins from the plugin directory after fetching results from Database.
- Launches the scan and converts the output in Text/Json and XML format.

SIEM-Pro (Security Information and Event Management) ***(Aug'17 - Oct'17)***

- SIEM-Pro is a product which works as a LIDS.(Log based Intrusion Detection System) It has the functionality of Log Management , Intrusion Detection, Intrusion Prevention.
- It is a system for 24/7 hours Protection for your Systems.
- It keeps all your assets Logs and Errors at one place So you can manage your assets easily.
- Automating Nmap Scripting Engine Scripts.
- Searching exploits using Nmap scan results.
- Finding difference in day-to-day scans and if any difference is found, a mail is send to the user automatically.
- Interactive NMAP scanning

Password List Generator ***(May'17 – May'17)***

A Python script which creates a password list for brute force attacks according to the data entered by the user.

TECHNICAL SKILLS

Programming	Python
Vulnerability Research	OWASP Testing guide for Web application vulnerabilities, Mobile application vulnerabilities Red team assessment, Network penetration testing and Wi-fi Penetration Testing
Additional skills	Buffer Overrun, Exploit development, Phishing drills and Machine Learning
Tools	Metasploit Framework, Nmap, Bloodhound, Burp Suite, Wireshark, OSSEC

Achievements

- Lead Contributor and Freelance trainer with 100+ students at IT expert Training
- Organized seminar on Cyber Security with "Police and People Council" at various schools and colleges.
- Stock Market Analysis and Prediction got selected by Department of Science and Technology, Government of India. Link
- Interview published in Hindustan Times on 3rd Dec 2012 regarding cybercrime awareness.

Personal Details:

Name:	Pradeep Jairamani
Nationality:	Indian
Date of Birth:	28th May 1996
Email Id:	pradeepjairamani22@gmail.com
Contact Number:	+91-9166556249

Date: 23-June-2020 **PRADEEP JAIRAMANI**