VEDANT ROY

Senior Associate
PwC AC
Bangalore

Mobile No: 8114728917
E-mail: vedantroy42@gmail.com
LinkedIn: https://www.linkedin.com/in/vedant-roy-230598129/
Blog: https://ghostonsecurity.in
Github: https://github.com/ved009

Objective:

Securing applications and infrastructure to make products and environments more robust and secure. Looking forward to working in an organization where I can put my creative methodologies and out of the box thinking and be a team player.

Professional Summary:

- Professional experience of 5.5 Years.
- Experience in Penetration testing of Web Applications, APIs and Perimeter, Vulnerability Management, Threat Modeling, Attack surface management and client-side source code review.
- Work Experience as a Penetration Tester and a Developer
- Published Articles and Blog Posts in Eforensics Magazine.
- Part of management group of OWASP Patna Chapter
- Learning and Development Manager for the whole Cyber Defense Team of PwC AC Bangalore location consisting of 200+ employees.
- Part of Microsoft Mentors program where helping the team from Asia region to migrate from Google Workspace to Office 365.
- Part of a Cyber Vigilance team associated with TCS Hackquest.

Technical Qualification:

- **Programming and Scripting Languages:** Python, HTML/CSS,SQL, Golang and Bash
- **Tools:** Burp Suite, Nmap, Winhex, Wireshark,OWASP ZAP, Autopsy, Metasploit Framework, Nessus, Checkmarx, SD Elements
- **Operating Systems:** Windows, Kali Linux, Ubuntu
- **Certifications:** CEH V10, CNSS, AZ 900, SC 900, Fortinet NSE 1 and 2, AWS Certified Cloud Practitioner, AWS Certified Security Specialty(In Progress) and BSCP(In Progress)
- **Trainings:** Autopsy, Comptia Security+

Professional Experience:

APRIL 2021 — PRESENT
PRICEWATERHOUSECOOPERS ACCELERATION CENTER
Projects Summary: _Penetration Testing of Web Applications (Internal and External), Services (APIs) and Perimeter_

Short term Engagements:

#American Investment Bank- This project involves performing Threat Modeling of their Production applications and in development apps which will be deployed over the internet. Most of the applications are moving to the public cloud which requires checking their cloud configurations along with their existing configuration of Technology Stack. This in depth visibility allowed us to win a contract for both web application and network penetration tests which span for a number of years and are cyclic in nature.

#American Consumer Company- This project involves the penetration testing of web applications and perimeter penetration testing. Most of the work is included in the SDLC life cycle including apps built on frameworks like Salesforce, wordpress and google sites. I have been working on this project for more than 6 months and reported numerous bugs that disclosed PII information and direct access to internal servers.

American Insurance Client - This project involves the penetration testing of web applications and perimeter penetration testing. I have been working on this project for 2 months and reported numerous bugs like Account Takeover and unauthenticated file Deletion of a VPN server.

#American healthcare Client – This project involves Setup and Management of VM workstation along with developing step by step guidelines for the client team to manage the workstation once developed. I developed several workflows to prioritize assets, define remediation timeline according to NIST standard, detection and removal of dead assets from CMDB, installation and deployment of scan agents in the assets and scheduling scans on priority of Assets.

#Canadian Insurance Bank - This project involves the penetration testing of web applications. I have been working on this project for 2 months and reported numerous bugs like Stored XSS and Information Disclosure in the Salesforce SAAS App using Aura objects.

DEC 2018 – APRIL 2021
TATA CONSULTANCY SERVICES
Projects Summary: _Penetration Testing of Web Applications (Internal and External), Services (APIs) and Perimeter_

Long term Engagement:

#European Healthcare Client - This project involves the penetration testing of web applications, thick clients and internal services. Most of the work is included in the SDLC life cycle along with some requests for testing SAAS clients like salesforce, Azure and Word press. I have been working on this project for more than 1.5 years and reported numerous bugs that likely disclosed user medical data and other sensitive information.

Short term Engagements:

#Banking Infrastructure - This engagement involved penetration testing of a web application (User and employee interface) along with the whole network infrastructure of the bank. 17 different unique bugs were reported over the whole life cycle.

#Industrial IOT platform and Management - The application is developed internally which includes a customizable management system for power plants, Aqua farming and other similar infrastructures. 11 different unique bugs were reported over the whole life cycle.

#On prem User management network infrastructure - The application is developed internally for user management for project allocation to various projects and real time reports(notifications) to the end users of upcoming projects and status of applied projects. 29 different unique bugs were reported over the whole life cycle.

#Energy Company - An external client with branches over different countries and it provides energy related solutions. I have been part of the project over 2 life cycles and penetration testing included web application, source code review and network infrastructure.

Projects Summary: _Center of Excellence (COE) - Development_
#On Prem vulnerability scanner tool - I am a part of the development team where my module consists of the integration of OSINT resources to perform penetration testing.

#Vulnerable Labs Development - I am part of an R&D team where we develop vulnerable Labs in accordance with OWASP Top 10 as a practice hub for other team members and to understand the vulnerability in more depth.

Jan 2018 – APRIL 2018
Research Summary: _Electronics and Radar Development Establishment(LRDE) - DRDO_

Worked on the implementation of Motion compensation algorithms for Inverse synthetic aperture radar (ISAR) using MATLAB. These algorithms are used to form an image of a moving target by predicting the image parameters from the data collected by the aperture.They are mainly used to generate high resolution remote sensing imagery.

Educational Qualification:

Examination	Year of Passing	Name of Institute	CGPA / %
B.Tech(ECE)	2018	CUSAT, Kochi	7.13
12th Board	2013	Shivam Convent, Patna (CBSE)	77.6%
10th Board	2011	S.T Joseph's High School, Patna (CBSE)	79.8%

Achievement and Awards:

- INTIGRITI – Current Global Rank – 4463 (Global rank keeps on changing as vulnerabilities are reported.)
- NCIIPC – Reported over 500+ vulnerabilities through National Critical Information Infrastructure Protection Center Portal (NCIIPC RDVP) on various public websites owned and maintained by the Government of India.
- Hall of fame/Vulnerabilities Identified and Reported - Dutch Government, NCIIPC(Q3), Nokia, Australian Government Department of Social Services, Vodafone, Zeotap, Meesho, Empire Flippers, Agicap, Microstrategy, TomTom, GeoTab, Swisscom, Verazial ID, Bentley Systems, BBC, ACT Fibernet and GeeksforGeeks
- Published articles on "Passive Information Gathering '' and "Introduction to Bug Bounties" on Eforensics Magazine and Blog.

Personal Details:

Date of Birth	:	20 Dec, 1995
Marital Status	:	Single
Father's Name	:	Mr. Ramakant Roy
Mother's Name	:	Mrs. Himbala Roy
Present Location	:	Bangalore
Home town & Birth place	:	Patna(Bihar), India
Languages	:	Hindi, English