Aditya Dixit

Penetration Tester and Security Researcher

ADDRESS
Alamganj Chowki,
Gulzarbagh
Patna, India - 800007

Alamganj Chowki, , Gulzarbagh, Patna, India - 800007
+91 80951 17619
blog.dixitaditya.com
hi@dixitaditya.com
09 September 1998
zombie007o
ad17ya

Security Researcher with a keen interest in Penetration Testing Web and Mobile Applications, Bug Bounties, Automation, and AWS. Capable of Leading a Team of Pentesters, worked on 80+ Pentests with different Organizations.

WORK EXPERIENCE

Cobalt Labs, Inc.
Pentest Team Lead

(April 2021 - Present)

- Promoted as a Pentest Team Lead based on the performance to manage different teams on pentest Engagements.
- Interacting with the clients to understand their requirements, infrastructure, and applications before the start of the pentest.
- Managing a team of 3-5 pentesters, deciding on the most appropriate course of strategy and diving scope for better coverage.
- Triaging, Validating, and assigning appropriate severities on the issues reported by the team before sending them over to the client.
- Preparing the Final Penetration Test Report, summarizing the vulnerabilities, scope, approach, and overall impact on the application along with Remediations.

HackerOne Pentest
Penetration Tester

(January 2020 - Present)

- Working on Penetration Tests in different domains such as Web/Mobile apps, API, Network Infrastructures, and AWS.
- Pentesting and Collaboration among a team of 3-5 Pentesters, finding and reporting vulnerabilities.
- Assigning CVSS score to the vulnerabilities based on the CVSS parameters and the impact.
- Worked with multiple organizations in different sectors such as Blockchain, E-Commerce, Finance, Telecom, etc.

Cobalt Labs, Inc.
Cobalt Core Penetration Tester

(October 2019 - April 2021)

- Working with multiple companies on their Pentest Projects based on Web Applications, Mobile Applications, Internal and External Networks, and Cloud Audits.
- Preparation of Reports with Proof of Concepts along with a Suggested Remediation plan and its impact on the asset.
- Experience with Pentesting wide variety of products and applications in the sectors such as Finance, Healthcare, Cloud, Commerce, Education, Food, Media, etc.

Deriv Ltd.
Security Researcher

(June 2019 - Present)

- Quarterly Pentests of all the Assets of the Organization - Web Applications, Mobile Apps (Both iOS and Android), Internal and External Networks.
- Managing and Triaging on Binary.com Bug Bounty Program on HackerOne and Deriv's Bug Bounty Program on Intigriti. Collaborating with the developers in finding the root cause of the issues and getting them fixed.
- Development of Monitoring tools and Automation around scanners and Slack Bots.
- Manual and Automated auditing of the AWS Infrastructure.
- Deployment and Management of Qualys Vulnerability Management throughout the Company and its assets.
- Deployment and Management of Wazuh for Threat detection, Integrity Monitoring, and Incident Response.
- Experience with Security Onion and Nessus for Internal Network Monitoring and Scanning.
- Experience with Security Policies - Worked on Procuring EMI License, security point of contact during Audits.
- Carrying out Red Team vs Blue Team Exercises in the company to simulate actual attacks and defenses.
- Static Code Review and analysis using SonarQube and manual approaches on the code written in ASP.NET, Node.JS and Perl.

EDUCATION

Dayananda Sagar College of Engineering
Bachelors Computer Science

(August 2016 - September 2020)
8.4 CGPA

Infant Jesus' School
Higher secondary Science - Physics, Chemistry and Maths

(July 2014 - July 2016)
86%

PROJECTS

PacRecon
https://github.com/az0mb13/

Security Recon Suite developed in Go and MongoDB with features such as Subdomain Enumeration, JavaScript Files, and Parameter enumeration with automated tests for XSS, Nuclei Integration, Endpoint Brute-force, Port scanning, and Subdomain Monitoring with a Discord Bot for alerts.

Monitor-X
https://github.com/az0mb13/Monitor-X

Python-based Subdomain Monitor that scans actively and passively for new subdomains on provided hosts, keeps them in the database, and alerts if a new subdomain has been found.

Task Hijacking PoC
https://github.com/az0mb13/Task_Hijacking_Strandhogg

A Proof of Concept Android application demonstrating Task Hijacking aka Strandhogg vulnerability introduced in applications due to misconfigured launch modes for activities.

Tipster
https://github.com/az0mb13/tipster

A tool/dashboard that finds all the Liked tweets by a Twitter user and stores them in a database and allows easy search and navigation based on keywords. Developed in Python, Flask, Jinja, MongoDB, and JavaScript.

CERTIFICATIONS

Offensive Security Certified Professional (OSCP)
Offensive Security — August 2019

AWS Certified Cloud Practitioner
Amazon AWS — July 2021

Qualys Certified VMDR Specialist
Qualys — May 2021

INTERESTS AND SKILLS

Capture the Flags

Pentesting Web and Mobile Apps

HackTheBox Labs

Automation in Python, Go and JS