Arkaprabha Chakraborty

Portfolio: arkaprabhachakraborty.github.io
Github: github.com/ArkaprabhaChakraborty
Address: 188 Barui Para Lane, Kolkata 700108, West Bengal, India.
Date of Birth: 17-05-2001

Email: chakrabortyarkaprabha998@gmail.com
Mobile: +91-86218-94194
TryHackMe: tryhackme.com/p/Arkaprabha
Nationality: Indian

Skills

Languages	**Advanced:** Java, C++, Python, Bash scripting **Intermediate:** Ruby, Golang, Javascript, Perl, SQL
Concepts	OOP design pattern, Compiler Design, Operating System, DBMS, Computer Networking, Test Driven Development, REST API, Virtualization
Tools	Kubernetes, Docker, Git, GitHub, JIRA, CMake, Jenkins, Gradle, Linux
Cloud Platforms	Google Cloud Platform, Microsoft Azure, Amazon Web Services
Others	BurpSuite, ZAP, ffuf, wfuzz, Metasploit, SQLMap, PEASS-NG

Education

2019 - 2023 **Bachelor of Technology - Computer Science Engineering**
Kolkata, India BP Poddar Institute of Management and Technology
Courses Taken: Operating systems, Compilers, Computer networks, Artificial Intelligence, Data Structure and Algorithm Design, Database Management Systems, Distributed Systems, Cyber Security, Cloud Computing & Cryptography
(SGPA: 9.2/10.0)

Work Experience

PricewaterhouseCoopers(PwC) - India Kolkata, India
Cyber Security Associate April 2024 - Present

- Network Penetration Testing Engagement: Conducted Network Penetration Testing Engagement with a renowned pharmaceutical company in India.
- Proficient in application security assessment, conducted web application pentesting for 7+ clients in EMEA and US region and successfully identified critical vulnerabilities such as privilege escalation, remote code execution, SQL Injection, authentication bypass, XSS and business logic issues, while adhering to OWASP top 10, NIST, PCI/DSS and ISO/IEC 27000 standards
- Skilled in Android application security testing, conducted assessments for 3+ clients, successfully identified high severity bugs based on OWASP standards such as privilege escalation, insecure local storage, authentication bypass and IDOR attacks.
- Conducted red teaming projects for clients at PwC, performing vulnerability assessment and penetration tests for 17+ clients and covering more than 5000 IPs, using tools such as Nessus, Tenable One, Burp Suite Enterprise, OWASP ZAP, Metasploit, Cobalt Strike, Covenant, Sliver C2 and Nmap. Collaborated with development teams and stakeholders to successfully identify and remediate critical vulnerabilities.

Cyber Security and Privacy Specialist - Threat and Vulnerability Management July 2023 - April 2024

- Red Team Assessment on a Power Company: Collaborated with the red team in PwC India over a red teaming assessment of Azure Active Directory Infrastructure of a reputed Power and Electricity supply company
- Motocorp Security Assessment: Conducted a black box network and web assessment for a leading automotive (motorbikes) company, evaluating their infrastructure and applications. Developed POCs for security vulnerabilities and collaborated with developer teams for remediation.
- Vendor Security Assessment of a Reputed Private Bank: Conducted a black box web application security assessment for a major private bank vendor in India, breaching and decrypting sensitive data with a custom tool, earning client appreciation.
- Azure Pipeline Security Assessment: Conducted a grey box web application security assessment on an Inventory Application deployed on Azure Kubernetes Service, identified multiple critical vulnerabilities, including gaining access to the container environment and misconfigured Azure SQL Database, Blob, and Disk services, and guided the DevOps and Developer teams to mitigate 99% of the associated risks by implementing best practices.
- **Awards Received:** Advisory Team Excellence Award, STAR&R: Dazzling Debut and Above and Beyond Award for excellent and timely delivery of quality penetration testing services

Internships and Fellowship Experience

PricewaterhouseCoopers(PwC) - India Kolkata, India
Cyber Security Intern - Threat and Vulnerability Management Jan 2023 - July 2023

- Financial Institution Network Security Assessment: Conducted network security assessments on a prominent financial institution's internal VPC network. Discovered misconfiguration in their desktop jumphost interface (thick client), leading to a foothold and identification of 2 critical privilege escalations.
- Automotive Industry Security Assessments: Conducted comprehensive security assessments of web, Android, and iOS applications, identifying vulnerabilities and proposing remediation strategies. Collaborated with cross-functional teams to design, implement, and deploy secure features that enhanced application security and user data protection.
- Building Custom Security Tools: Assisted in the development of automated vulnerability detection tools, improving the efficiency of the vulnerability assessment process.

OWASP Foundation Remote, India
Google Summer of Code Contributor May 2022 - Sept 2022

Worked on **Zed Attack Proxy (ZAP)**, formerly known as OWASP ZAP, a former OWASP Foundation's flagship project and current Software Security Project (SSP). [Link]

- Developed and currently maintaining the parameter digger add-on for ZAP which can find 25000+ vulnerable parameters in under a minute. Developed cache poisoning detection at scale with heuristic methods for comparison of responses and reporting vulnerable parameters. Incorporated a carpet bombing attack option for users to carry out cache poisoning DDoS attacks.
- Improved ZAP's Active Scanning and XSS scan rule by adding 3 new reflected XSS checks, 2 new stored XSS checks and SSTI checks
- Enhanced ZAP's automation framework by creating new job rules and URL presence tests. Implemented URL presence tests within the framework to trigger conditional workloads and tests.

Data Consultants Corporation Remote, India
Security Engineer Intern Nov 2021 - Apr 2022

- Worked on setup and maintenance of Appsec pipeline built with CodeQL, semgrep SAST for static analysis, OWASP ZAP and wfuzz actions for DAST
- Set up a DAST pipeline using OWASP ZAP and Google Cloud Engine with modifiable contexts to support short, defined scans when a merge request(MR) is made on the main branch or a change has been committed to an MR
- Set up netbox on an Azure VM instance with isolated postgreSQL and redis instances for easily accessible network documentation.
- Created custom modules for Netbox auto-update with Azure VNet SDKs

Projects

Veracity(Ongoing)

A blogging platform like Twitter and Medium which is mainly made for journalists to voice their stories. Veracity is based on the Nostr protocol so that governments or individuals with power cannot alter the content.

Security Notes Link

Information security notes that can help students or working professionals to be better at web applications and network security testing. This is still under active development with content being added almost every day.