Satya Prakash

kayalasatyaprakash@gmail.com
+91-9949968828
linkedin.com/in/0xkayala
https://github.com/0xKayala

Summary

Dear Team,

I am Satya Prakash, a Certified Ethical Hacker with over 5.3 years of comprehensive IT security experience, specializing in Vulnerability Assessment and Penetration Testing. I bring a wealth of expertise to any organization. My strong knowledge of OWASP Top 10 and SANS Top 25 vulnerabilities, coupled with hands-on proficiency in tools such as Nuclei, Nmap, Burp Suite, Nessus, OWASP ZAP, Metasploit, Wireshark, and manual testing, allows me to effectively identify and address security vulnerabilities.

During my tenure from EC-Council to Vatins, I excelled as a Research Associate and Cyber Security Analyst for over 5+ years. This experience granted me valuable insights into Information Security, Vulnerability Assessment and Penetration Testing, along with secure operational workflows and a deep understanding of organizational processes.

Outside of my professional work, I am an active participant in CTF platforms such as TryHackMe and HackTheBox, achieving a Top 2% ranking on TryHackMe. Additionally, I actively contribute to Bug hunting platforms and Responsible disclosure programs, receiving numerous Acknowledgements, Hall of Fames and Swags for my High-quality vulnerability reports.

Eager to expand my knowledge and skills, I am motivated to leverage my expertise in my next role. With a passion for staying at the forefront of emerging technologies and industry trends, I am confident in my ability to contribute to the security and success of any organization.

Experience

Cyber Security Analyst

Vatins Systems

Apr 2023 - Sep 2023 (6 months)

➢ WAPT and NTPT ➢ API Pentesting
➢ Internal and External Pentest
➢ WhiteBox, GreyBox & BlackBox Testing
➢ Incident Management ➢ Dark Web Analysis
➢ Threat Intelligence using OSINT
➢ Report Writing and Documentation

Web Application Security Analyst

MyNextFilm

Sep 2022 - Feb 2023 (6 months)

➢ WAPT and API Pentest
➢ Internal & External Pentest
➢ Report Writing and Fix the Bug

Process Developer

Genpact

Feb 2019 - Apr 2022 (3 years 3 months)

Worked as a Process Developer - Digital Crime Unit (DCU) with the following job responsibilities:

➢ Maintain and improve upon, as necessary, the existing vulnerability management program, including maintenance of scanning tools and licensing, procedures, reporting, and client communications.

➢ Investigate and create cases for security threats while performing initial triage and escalate for further investigation and mitigation.

➢ Monitor Security Alerts and investigate phishing emails by leveraging tools such as Proofpoint or reported by the users.

➢ Scan the Internal/External Assets and report the security vulnerabilities and fix or patch them by co-ordinating with the assigned developers

Research Associate

EC-Council

Jul 2017 - Aug 2018 (1 year 2 months)

Worked on Information Security projects and developed Courseware for Industry standard certifications like CEH, CND, ECSA of EC-Council and performed security assessment on iLabs and reported the vulnerabilities found in it.

Education

Indira Gandhi National Open University

Post Graduation Diploma, Information Security

Jun 2020 - Jun 2021

Jawaharlal Nehru Technological University

Bachelor of Technology, Information Technology

Aug 2013 - Jun 2017

Licenses & Certifications

Certified Ethical Hacker (Practical) - EC-Council

Issued Nov 2022 - Expires Oct 2025

ECC5931847602

Certified Secure Computer User - EC-Council

ECC47685271912

Cybersecurity Essentials - Cisco

b69f2a68-802b-4cd2-9173-0246597168bd

Introduction to Cybersecurity Tools & Cyber Attacks - Coursera

6d299d78-9435-4834-b390-1190f1f6ee72

Network Security Associate (NSE-1) - Fortinet
taiVyECPCN

Foundations of Operationalizing MITRE ATT&CK - AttackIQ
66d5355c-86d0-4e5b-8251-86f3ac9398a0

Skills

Report Writing • Application Security • Shell Scripting • Bash Scripting • Technical Writing • Front-End Development • OWASP ZAP • OWASP Top 10 • ISO 27001 • Tenable Nessus

Honors & Awards

Secured David Tvildiani Medical University - Open Bug Bounty
Nov 2022
Bug: Reflected XSS
Link: https://www.openbugbounty.org/reports/2989403/

Acknowledged by Indian Government - NCIIPC India (A unit of NTRO)
Oct 2022
Bug: Directory Listing (Sensitive Source Code) via Exposed .git folder
Bug: Admin Login Panel Exposed via Internal Origin IP
Link: http://bit.ly/3I8Gk9y
Link: http://bit.ly/3YjU46S

Hall of Fame and Acknowledgement - Inflectra
Nov 2022
Bug: Reflected XSS
Link: https://www.inflectra.com/Company/Responsible-Disclosure.aspx

Acknowledged by Indian Computer Emergency Response Team - CERT-In
Nov 2022
Bug: Directory Listing (Sensitive Info)
Bug: Multiple Origin IPs Exposed (Internal Admin Panel)
Link: http://bit.ly/3xaAlL4 / http://bit.ly/3HOX04A
Link: http://bit.ly/3DSBbzT

Swag and Acknowledgement - CircleCI
Jan 2023
Bug: Sensitive Data Exposure
Bug: Exposed Origin IP lead access to GitLab Community Login panel (WAF Bypassed)
Link: http://bit.ly/3xlQSvG

Acknowledged by RealPage - RealPage, Inc.
Jan 2023
Bug: Exposed Origin IP Lead Access to Sensitive data [CVE-2017-5487]

Link: http://bit.ly/3YEFpCW

Swag and Acknowledgement - SIDN
Jan 2023
Bug: Exposed Origin IP Lead Access to Sensitive Portal
Link: http://bit.ly/3K71Qgm

Hall of Fame and Acknowledgement - Nokia
Jan 2023
Bug: Origin IP Exposed and SSL Host Mismatch [CWE-297]
Link: https://www.nokia.com/notices/responsible-disclosure/

Certificate of Recognition - Zyxel
Feb 2023
Bug: Multiple Sensitive Information - [CWE-200]
Bug: Multiple SSL Host Mismatch - [CWE-297]
Link: http://bit.ly/3Xs9cOA

Appreciation Letter by Panasonic - Panasonic
Jan 2023
Bug: Internal Origin IP and Jira Login Panel Exposed (WAF bypass)
Link: http://bit.ly/3Iau9sE

Swag and Acknowledgement - Nationaal Cyber Security Centrum (NCSC-NL)
Feb 2023
Bug: Sensitive Data Exposure
Link: http://bit.ly/3SAL3oc