Ushani Kumar Swamy

+91 - 9603444068
Kumarushani71@gmail.com

OBJECTIVE

To maintain a position in information security where I can use my experience and technical knowledge to help secure information systems and IT infrastructure. To be challenged and pushed to the limits in order to solve complex logic and technical problems. To perform, stay on the leading edge of technology, attacks, defenses, and security intelligence and Vulnerability Assessments.

Seeking a Challenging Career as Penetration Tester

WORK EXPERIENCE:

Organization	Designation	Duration
DBAce Technologies	Security Testing Engineer	April 2024-Present
Aujas Cybersecurity Limited	Senior Consultant-1	Jan 2023-April 2024
Tata Elxsi	Security Engineer	Sept 2022- Dec 2022
Wipro Pvt.Ltd	Security Engineer	Jun 2021 - July 2022
Accenture	Security Engineer/Analyst	Feb 2018 - June 2021

- Application Security Testing Engineer with a total of 6 years of experience in Security Assessment of Web Applications, API for multiple clients with Penetration Testing and Manual security testing for Multiple Clients.
- Performed Web application Penetration testing and Vulnerability Assessments found major bugs like Stored XSS, Insecure Direct object reference, Missing functional level access control.
- Having hands-on experience on tools Various tools such as Burp Suite, AppScan, Acunetix, Nmap, Nessus, Nexpose and Metasploit framework.

- Having In depth Knowledge about **Footprinting, Scanning, SQL Injection, XSS, Social Engineering Phishing, Reverse engineering.**
- Having good knowledge of **OWASP Top 10** Vulnerabilities.
- Worked in writing and executing Test cases based on given requirements.
- Worked on Test Management tools like JIRA.
- Experience in addressing web application security issues, such as those outlined in OWASP Top 10
- Ability to perform manual and automated testing to identify vulnerabilities.
- Proficient in understanding application-level vulnerabilities like XSS, SQL Injection, authentication bypass, weak cryptography, Session Management, etc.
- Effective Communication Skills and interested in learning new tools.
- Effective Team player and achieved **Best Team award.**
- Experience includes working with teams and clients in India.
- Played a vital role as team member and delivered multiple Web and Mobile applications and web services assessments for clients in India.
- Good Knowledge about Web/API application Security Assessment.
- Handson Experience in tools like Burp Professional, NMAP, Nessus etc.
- Well versed with Security Assessment methodologies like **OWASP** and **CVSS**, etc.
- Skilled in documenting and reporting the various vulnerabilities found in the above process and suggesting mitigations for the same.
- Performed Web/API application penetration testing and found the major bugs like Stored XSS, Insecure Direct Object Reference, Missing Functional Level Access Control.
- Having hands-on experience on tools Various tools such as **Burp Suite, AppScan, Acunetix, Nmap, Nessus, Metasploit, Wireshark** and **Nexpose, Postman.**
- Having In depth Knowledge about Foot printing, Scanning, SQL Injection, XSS, Social Engineering Phishing.
- Having good knowledge of OWASP Top 10 Vulnerabilities.
- Ability to perform manual and automated testing to identify vulnerabilities.
- Knowledge of security in both Linux and Windows environments.
- Publishing monthly dashboards, taking follow up for closure of vulnerabilities
- A Self-starter with a positive attitude, willingness to learn new concepts and accept challenges.
- exploitation and the impact of the issue.
- Reporting the identified issues in the industry standard framework.
- Experience in Security operation Center. (SOC)
- Performing scanning of APIs and integration into CI\CD pipelines for early detection of vulnerabilities.
- Working on SIEM and EDR, ITSM tools like Qradar and CrowdStrike.
- Working experience on Endpoint Security and Response tools
- Experience with tools and processes used in Cyber Incident Response and Management
- Handling Phishing and Spam Emails.
- Having skills of monitoring and troubleshooting.
- Experience in Email and Web Security Tools.
- Working in Security Operation Center (24x7), monitoring of SOC events, detecting, and preventing Intrusion attempts.
- Responding to Various security alerts for various clients and scanning for vulnerabilities using tools like NESSUS.
- Monitoring, analyzing, and responding to infrastructure threats and vulnerabilities.

- Collecting the logs of all the network devices and analyzing the logs to find suspicious activities.
- Responsible for preparing the root cause analysis reports based on the analysis.
- Analyzing daily, weekly, and monthly reports.
- Performing Real-Time Monitoring, Investigation, Analysis, Reporting and Escalations of Security Events from Multiple log sources.
- Maintain a keen understanding of evolving internet threats to ensure the security of client networks.
- Escalating the security incidents based on the client's SLA and providing meaningful information related to security incidents by doing in-depth analysis of event payload, providing.

EDUCATION

- B. Tech (Mechanical Engineering) from JB Institute of Engineering and Technology (JNTU) in 2017 with 60.9%
- Intermediate MPC from Narayana Junior College, Hyderabad in 2013 with 86%
- SSC from Omanand High School in 2011 with 79%.

SOFTWARE EXPOSURE

- Operating System : Win 9X, win 2000, Win XP, Win 2k3, Win 2k8
- Languages : C, Java
- Concept Known: Operating Systems, Security Testing Tools, SIEM, EDR
- Mark-Up Language : HTML
- Work Area : Web Application Security testing, Pentester, & SOC
- Testing Tools : Burp Suite, Postman, App scan Standard Edition, HP Web Inspect, Checkmarks, Nmap, Nessus, Nexpose

hereby declare that the information furnished above is genuine and authentic to the best of my knowledge.

Places: Hyderabad (Ushani Kumar Swamy)

BALNE SAI KUMAR

: +91 9533 418763
: reach.sai@aol.com
:Hyderabad, Telangana.

Professional Glimpse:

- Professional with close to 5+ years of Experience, with a proven track record in information security, as both an individual contributor and as a team leader.
- Experience spans across diverse projects covering, ***API Security || Web Application Security || Android Application Security || Penetration Testing || Software Composition Analysis ||***
- Detailed understanding of security policies, procedures, & processes.
- Executed multiple on-site projects and maintained the best service record.
- Experience in working on Finance, Telecom, Pharma & Life sciences, and commercial Applications.
- Strong knowledge of ***OWASP || SANS || CVSS ||***
- Interact with customers in a collaborative consultative manner to deliver results, and provide feedback and remediation recommendations on findings.
- Expertise in Establishing, engaging, and enhancing client relationships.
- Ensured client engagement and retention with timely communications and deliverable.
- Spearheaded the management of the entire SaaS product lifecycle, including SCA, SAST, and DAST.
- Evaluating and implementing security solutions across the organization.
- Experience in cost optimization on security solutions procurement.
- Keen to learn & take up new challenges in the fields of Cyber Security and project management environments.
- Excellent track record in managing services, consultants, & client relationships.

Work Experience:

Information Security Engineer-II, **Jan,24 to Till Now**
MRI Software India Pvt. Ltd.

- ✓ Performing pentests for in-house products and delivering them on time
- ✓ Managing and coordinating with the internal team for third-party pentests
- ✓ Ensuring completion of pentests for clients
- ✓ Consistently performed penetration tests for multiple clients, ensuring ongoing evaluation and improvement of their security posture.
- ✓ Managing third-party risk management tools such as BitSight and Security score card to maintain a good score.
- ✓ Active lead in developing robust processes and implementing new-age tools & techniques to consistently perform ongoing security assessments of the organizational security environments.

Information Security, **Jan,23 to Jan,24**
Sensen.ai

- ✓ Consistently performed penetration tests for multiple clients, ensuring ongoing evaluation and improvement of their security posture.
- ✓ Active lead in developing robust processes and implementing new-age tools & techniques to consistently perform ongoing security assessments of the

organizational security environments.

- ✓ In my role as an Information Security professional, I led the management of the complete SaaS product lifecycle, overseeing tasks such as software composition analysis, code review, and security testing (VAPT).
- ✓ Managed security assessments to ensure compliance to firms' security standards (i.e., OWASP Top 10, SANS 25
- ✓ Generated executive summary reports showing assessments results, recommendations and risk mitigation plans and presented them to the respective business sponsors and senior management.
- ✓ Periodic Communications with Dev team members for efficient management work
- ✓ Regular Training sessions to the teams on the latest security updates and mitigation techniques.
- ✓ Periodic training sessions for the new joiners, on tools and usages, and also on policies.
- ✓ Active participation and regular interactions with the senior management in assessing and reviewing the third-party vendors and security products, contributing to strategic and well-informed decision-making processes.
- ✓ Establishing best practices for project support, policies, and documentation.
- ✓ Identifying suitable application or service vendors across the spectrum and evaluating futures and options for further negotiations, and recommending the same to management for finalization and implementation.
- ✓ Assessing and deploying security products, a notable one is endpoint solutions across the organization.
- ✓ Maintained best track record of completing assigned projects within the scheduled milestone.
- ✓ As per the needs of the Industry and organization, Quickly learned new security tools for effective utilization.

Information Security Consultant, **Oct,19 to Jan,23**

Esec Forte Technologies Pvt Ltd.

- ✓ Profile an application, identify threats, and develop test cases to target identified threats.
- ✓ Identify vulnerabilities in the application and make recommendations on how to fix the issues andsubmit a detailed documented report.
- ✓ Capable of understanding end-user requirements from a security perspective.
- ✓ Responsible for Interaction with the client and assisting the development team to fix all loopholes in the web application. Monitor and track the progress of found vulnerabilities, maintain the history, and prepare redacted reports.
- ✓ Performed manual and automated testing on web applications.
- ✓ Act as a Point of Contact between management and technical team.
- ✓ Creating Awareness about secure coding and application security best practices.
- ✓ identify and exploit vulnerabilities in applications.
- ✓ Successfully completed all the assigned projects.
- ✓ Experience in handling relationships to secure needed information and strengthen the partnership.
- ✓ Identifying security tools and evaluating them.
- ✓ work on improvements for provided security services, including the continuous enhancement ofexisting methodology material, and supporting assets.

Education:

Bachelor of Technology (B.Tech) | |
JNTU Hyderabad. 2012 to 2016

Intermediate (+2) | |
SRR Jr. College. 2010 to 2012

Certifications:

- CAP-Certified AppSec Practitioner.
- PrivacyOps Certification.
- Practical Web Application Security Testing.
- ISO/IEC 27001 Information Security Associate.
- AWS Security Fundamentals.
- Multi-Cloud Network Associate.
- CNSS-Certified Network Security Specialist.

Technical Skills:

- **Programming Languages:** C, C++.
- **Scripting Languages:** Html, Xml, Java Scripting.
- **Operating System:** Windows, Kali Linux, Android.
- **Web application &Web service security:** Acunetix, Nets parker, Burp Suite, Soap UI Pro.
- **Mobile Penetration Testing:** Apktool, dex2jar, JD-GUI, Sign-apk, Xposed Frame Work, mobSFJADX, FRIDA.
- **SCA:** Open-source tools, black duck.
- **OSNIT Testing**: Using open-source tools in kali linux.

Personal Info:

Date of Birth	: 19th Nov, 1994.
Gender	: Male.
Marital Status	: Single.
Languages Known	: English, Hindi & Telugu.
Hobbies	: Bug hunting, Travelling & Reading self-help books.

Shubham Kumar

Shubham36.bgs@icloud.com | +91 7979865736 | connect2shubham | Gurugram, India |

Professional Summary

Impact-driven Product Security Engineer with 4.5+ years of experience, currently enhancing the security posture of large-scale, customer-facing web, mobile, and API platforms in a leading MedTech organization. Specialized in identifying and mitigating real-world vulnerabilities through penetration testing, secure code reviews, and threat modeling. Proven track record of collaborating with cross-functional teams to implement proactive security measures while ensuring compliance with industry regulations & standards. Actively expanding expertise in DevSecOps, cloud-native security, and AI security testing to address the evolving landscape of security challenges.

Professional Experience

Product Security Engineer, Stryker - Gurugram, India Sep 2023 – Present

- Performed Vulnerability Assessment & Penetration Testing (VAPT) on web applications, mobile applications, APIs, and Docker environments for a diverse range of Stryker products.
- Collaborated with divisional partners and cross-functional teams to successfully complete and deliver VAPT projects, ensuring alignment of security goals with business objectives.
- Identified vulnerabilities across critical platforms and providing actionable insights to development teams to protect critical assets and products.
- Conducted vulnerability monitoring scans using DAST tools such as Tenable and HCL AppScan, managing the triage process and generating detailed vulnerability reports for senior management and stakeholders.
- Researched third-party cybersecurity tools, conducted Proof of Concept (POC), analyzing them based on the company's use case. Presented findings to senior management for consideration and tool purchase.
- Actively promoted security best practices within the team and across product development lifecycles to minimize risks and enhance overall product security.

Consultant, Grant Thornton Bharat LLP - Gurugram, India March 2023 – Sep 2023

- Performed Vulnerability Assessment & Penetration Testing (VAPT) on web applications, mobile applications, APIs, and network environments for clients such as FinTech, Banking, Power, and Telecom sectors.
- Conducted internal and external network penetration testing, identifying vulnerabilities and misconfigurations.
- Carried out source code reviews and threat modeling to detect architectural flaws and insecure development patterns.
- Delivered comprehensive, client-ready reports with risk-based prioritization and actionable remediation guidance.
- Collaborated directly with technical teams to communicate findings and support timely, secure fixes.

Information Security Consultant, AKS IT Services Pvt Ltd - Noida, India Dec 2020 – Feb 2023

- Conducted Vulnerability Assessment & Penetration Testing (VAPT) for web applications, mobile applications and APIs across Central & State Government Ministries, Public Sector Banks, and private organizations.
- Performed internal and external network penetration testing, identifying and helping remediate vulnerabilities.
- Conducted secure source code reviews to identify and remediate vulnerabilities, ensuring early detection and reducing production risk.
- Mentored freshers offering hands-on guidance throughout the VAPT and review lifecycle.
- Delivered comprehensive reports, detailing findings, risk levels, and remediation recommendations.
- Contributed to the successful assessment of 100+ applications, ensuring alignment with security and regulatory standards.

Information Security Intern, Esec-forte Technologies, - Gurugram, India Jan 2020 – June 2020

- Gained hands-on experience in Web Application Security, learning vulnerability identification, reporting, & industry-standard documentation.

Skills

Core Competencies: Web Application Security, Mobile Security, API Security, Container Security, Penetration Testing, Vulnerability Assessment, Vulnerability Monitoring, Secure Code Review, Threat Modeling, DevSecOps & CI/CD Security Integrations & OWASP Security Standards

Tools & Framework: Burp Suite, OWASP ZAP, Postman, SoapUI, Fiddler, Wireshark, Metasploit, Nessus, Nmap, Android Studio, Frida, MobSF, APKTool, Drozer, Docker Bench, Trivy, Microsoft Threat Modeling Tool, SonarQube, Checkmarx, Jenkins, Terraform & OWASP Security Frameworks

Soft Skills: Problem Solving, Fast Learner, Adaptability, Good Listener, Leadership, Team Contribution

Education

Punjab Technical University, B.Tech in Computer Science & Engineering 2016 – 2020

Certifications

- Web Application Penetration eXtreme (**eWPTX)** by INE.
- Certified Ethical Hacker (**CEH v11**) by EC-Council.

M Santhosh Rao

mail id: muthinenisantosh@gmail.com

Mobile no: 6300619612.

PROFESSIONAL SUMMARY

- 10 years of relevant experience in Application security Testing and Vulnerabilities analysis.
- Good exposure to Security Testing of Web based applications and vulnerabilities.
- Excellent understanding of Security Concept **(OWSAP)**
- Experience in security code review of applications developed in **C, C++, JAVA & .Net**.
- Experience with Security Risk Management with TCP-based networking.
- Knowledge of common information security standards, such as: ISO 27001/27002, NIST.
- Hands on experience in working with Penetration testing tools like **Sqlmap, ZAP, Acunetix, KALI Linux testing suite.**
- Ability to apply experience and expertise to problem solving in a complex technical environment.
- Strong knowledge in analysis of web applications, scanning and vulnerability Assessment reporting.
- Conduct **Threat Modeling** to identify security risks in application architectures, data flows, and system designs.
- Utilize frameworks like **STRIDE, DREAD, PASTA, and MITRE ATT&CK** to assess threats and recommend mitigations.
- Analyse application security vulnerabilities found through testing and collaborate with development and other internal technical teams to provide mitigation steps to reduce the risk.
- Preparing Vulnerability Assessment Report.
- Manual verification of testing results

- Black box/Grey box Web Application Security Testing.
- White Box Security Testing /Source Code Analysis.
- Ability to multitask and manage shifting priorities
- Communicate effectively in English, both verbally and written, in a business environment
- Self-starter, independent thinker but a good team player

AREAS OF EXPERTISE

- Penetration Testing
- Customer Relationship Management Skills
- Escalation Management
- Automated/Manual Code Reviews
- Dynamic Web Application Vulnerability Assessments
- Reporting & Analytics.

TECHNICAL SKILLS

Tools	HP Fortify, Burp-Suit, Acunetix Web Scanner, SQL Injection Tools and Kali Linux, ZAP Proxy, Qualys, Coverity
Office Tools	MS Office (MS Excel, MS Word, MS PowerPoint, MS Visio)
Web Technologies	HTML, JavaScript
WebServer	Apache, IIS 6.0/7.0
Databases	DB2,Oracle 11c/10g/ 9i, SQL Server 2005/2008, MS Access
Environments	Windows NT/98/95/2000/XP, UNIX (Sun Solaris), Linux
Languages	Unix Shell scripting, Python, Java.
Network Tools	Nmap, Wire Shark, Nessus.

EDUCATION

- **B-Tech (IT) From Aurora's Engineering College, JNTU, Hyderabad 2009**

PROFESSIONAL EXPERIENCE

1. Capgemini Technology Solutions India Ltd, Hyderabad. Jan 2021-Till date

Consultant (B2)

- Vulnerability Assessment of online applications to identify the vulnerabilities in different categories like Input and data Validation, Authentication, Authorization, Auditing & logging.
- Conduct network Vulnerability Assessments using tools to evaluate attack vectors, Identify System Vulnerabilities and develop remediation plans and Security Procedures
- Provide remediation guidance and recommendations and coordinate with Development Operations, IT and other teams as needed to provide oversight to the remediation and/ or mitigation of enterprise vulnerabilities
- Working with Different SAST tools to identify code vulnerabilities and provide a remediation support to the Applications teams
- Working with DAST tools to identify vulnerabilities in non-prod and prod environments and provide a remediation support to the App teams.
- Performing manual and automated Web penetration testing using Burp Suite Professional and Enterprise Edition and manual methods testing for SQL injection, Cross Site Scripting and Cross Site Request Forgery.
- Helping the App teams to integrate the Applications for coverity scan.
- Working on EVM Vulnerabilities reported by Qualys and doing a manual analysis on vulnerabilities and share with respective Asset Owners for Remediation of Vulnerabilities.

2. Loylogic Technologies India Pvt Ltd, Pune. Mar 2020- Dec2020

Sr. Information Security Engineer.

Responsibilities:

- Monitor and respond to alerts indicating security incidents and research new and emerging threats to pre-emptively eliminate the possibility of system breach.
- Conduct both self- assessments and coordinate third party risk assessments of technology infrastructure and operational processes and controls for assigned areas
- Conduct recurring scans and audit and track mitigation activities through to completion.

- Conduct scheduled, targeted IT compliance audits and vulnerability scans and pen tests for the organization
- Performed manual and automated Web penetration testing using Burp Suite Professional and Enterprise Edition and manual methods testing for SQL injection, Cross Site Scripting and Cross Site Request Forgery.
- Security assessment of online applications to identify the vulnerabilities in different categories like Input and data Validation, Authentication, Authorization, Auditing & logging.
- Conduct network Vulnerability Assessments using tools to evaluate attack vectors, Identify System Vulnerabilities and develop remediation plans and Security Procedures
- Provide remediation guidance and recommendations and coordinate with Development Operations, IT and other teams as needed to provide oversight to the remediation and/ or mitigation of enterprise vulnerabilities
- Establish appropriate security and compliance management calendar, schedule engagements and track activities to completion. Maintain history of scans and activities for future reference
- Maintain and report out on the Information Security Risk Register
- Manage and maintain ISO 27001, PCI DSS, GDPR and any future security standards and compliances.

3.Digital Minds Software Solutions, Hyderabad. **Feb 2015- Feb 2020**

Sr. Application Security Analyst.

Responsibilities:

- Involved in Analyze the requirements, Generating scenario to validate requirements
- Conducted application penetration testing of 50+ business applications
- Conducted Vulnerability Assessment of Web Applications
- Responsible for performing security code reviews and application risk assessments for customer facing applications. Audited applications written in multiple languages, including Java/JSP, PHP, and Utilized OWASP and Ounce Labs formal methodology to conduct code reviews and risk assessments.
- Web Penetration testing to prove Software Security Vulnerabilities with IBM Appscan, Burp Professional and Manual Fuzzing and Penetration Testing with AppScan and Firefox plug-ins.

- Conducted security assessment of including Java/JSP, ASP.NET,Web Applications
- Performed manual and automated Web penetration testing using Burp Suite Professional and Enterprise Edition and manual methods testing for SQL injection, Cross Site Scripting and Cross Site Request Forgery.
- Created custom scripts to take out certain security vulnerabilities, used regular expressions to search for sensitive data, like credit card numbers and social security numbers.
- Responding to inquires/issues from end users related to active directory
- Generated and presented reports on Security Vulnerabilities to both internal and external customers.
- Security assessment of online applications to identify the vulnerabilities in different categories like Input and data Validation, Authentication, Authorization, Auditing & logging.
- Vulnerability Assessment of various web applications used in the organization using Paros Proxy, Burp Suite, and Web Scarab.
- Proficient in understanding application level vulnerabilities like XSS, SQL Injection, CSRF, authentication bypass, cryptographic attacks, authentication flaws etc.
- Performing onsite & remote security consulting including penetration testing, application testing, web application security assessment, onsite internet security assessment, social engineering, wireless assessment, and IDS/IPS hardware deployment.
- Conduct network Vulnerability Assessments using tools to evaluate attack vectors, Identify System Vulnerabilities and develop remediation plans and Security Procedures.
- Identifying the critical, High, Medium, Low vulnerabilities in the applications based on OWASP Top 10 and SANS 25 and prioritizing them based on the criticality.

PERSONAL DETAILS

Name	M Santhosh Rao
Father name	M Ranga Rao(late)
Dob	14-02-1987.
Marital Status	Married

Address Flat no:504, Akhilesh Towers, Road no5,
SS homes, Ameenpur, Hyderabad.

Date: M Santhosh Rao

GAURANG BHATNAGAR

Contact

Phone: +91-8860824808

Email: gaurang8492@gmail.com

Linkedin: https://www.linkedin.com/in/iamgaurangbhatnagar/

Tech Writeups (Blog)

https://offsec.space/posts/

Certifications

- **OSCP** (OS-101-19281)
- **eWPTX** (8818929)
- **eCPPT** (4902001)
- **eWPT** (EWPT-224)
- **eMAPT** (EMAPT-71)
- **eJPT** (EJPT-200175)

Career Highlights

- **9+ years** in offensive security domain, holding a Master's degree in Cyber Security from a National University.
- Authored **InsecureShop vulnerable Android app** and **Mobile Nuclei Templates**; developed tools for **mobile security scanning.**
- Active contributor to open source, with presentations at security conferences.
- Specialized in **vulnerability triage**, **source code review, devsecops, fuzzing** and **penetration testing** across multiple cybersecurity domains.

Experience

R&D Engineer Software 3 – *Feb 2024 to Feb 2025*
Broadcom, *Pune, India*

- Transitioned from VMware to Broadcom's Enterprise Security group as part of the acquisition.
- Led the enhancement of existing security tools, leveraging Semgrep for comprehensive secret scanning and code review.
- Fuzzed Windows and Linux binaries to uncover security vulnerabilities.
- Integrated and deployed security tools within the CI/CD pipeline to automate security checks.

Security Response Engineer (MTS 3) – *Mar 2022 to Feb 2024*
VMware, *Bengaluru, India*

- Worked as a member of VSRC (VMware Security Response Centre) where I worked alongside Technical Program Managers to validate Bug Bounty Submissions.
- Worked as a key member of the mobile security team to enhance the security posture of VMware's mobile applications through collaborative risk assessments and mitigation strategies.
- Managed VMware's bug bounty program, executed penetration tests, performed source code reviews, and researched new attack vectors.

Security Consultant – *Oct 2019 to Mar 2022*
Optiv, *Bengaluru, India*

- Executed application security engagements for USA and Canadian clients.
- Conducted technical Peer-Reviews on the Pentest reports.

GAURANG BHATNAGAR

Core Skills

- Vulnerability Triage
- Secure Code Review
- Android Vulnerability Research
- Android Userland Fuzzing

Security Experience

- Mobile application
- Web Application
- API
- Network
- Firmware
- IOT
- Source Code Review
- Cloud Security
- Fuzzing

Programming Languages

- Python
- Java (Android)

Security Consultant – *Jan 2016 to Jun 2019*
***Ernst & Young**, Gurugram, India*

- Performed penetration testing on various entry points such as IoT, Web applications, Mobile applications, Networks, Systems, and Wireless networks.

Notable Accomplishments

- Researched various mobile attack vectors and developed an intentionally vulnerable Android application named "InsecureShop".
- Contributed "nuclei templates" to quickly identify mobile application security issues.
- Listed among Google's Top 50 researchers in 2017 as part of their vulnerability reward program. (Best Rank #50 in 2017 | Profile)
- Winner in one of the levels of the practical international web hacking challenges organized by InfoSec institute in 2015. (Reference)
- Received multiple Security Hall Of Fame and acknowledgements from 50+ reputed firms including well-known giants like Apple, Google, and Yahoo.

Conference Talks/Publications

- Presented research on Android application security at SourceZeroCon 2021 titled "**Deep Dive into Android Static analysis and Exploitation**" (Slides | Video)
- Presented a talk on API Security at combined Null and Owasp meet titled "**Pentesting Rest API's**" (Slides)
- Published articles on:
  - MITM issues in mobile apps in Pentest Magazine titled "**Exploiting certificate validation flaw in mobile apps**" (Publication)
  - IoT device exploitation in Pentest Magazine titled "**Pentesting an IoT based biometric attendance device**" (Publication).

Education

- **Masters in Technology (M.Tech)** – May 2014 to May 2016
  Cyber Security & Incident Response
  National Forensic Sciences University (*Gandhinagar, India)*

- **Bachelors in Technology (B.Tech)** – May 2010 to May 2014
  Electrical & Electronics Engineering
  Sharda University (*Greater Noida, India)*

Divya Gangolu

Email:divyagangolu15@gmail.com
Mobile: +91 8374108398

SUMMARY

I am a passionate Information Security Consultant with solid technical background and a highly analytical mind as well as a Bachelor of Engineering Degree, having experience in InfoSec domain of 3 years, performed VAPT on 30+ web and mobile applications. Looking forward to enhancing my knowledge in the wide field of Cyber Security.

Team player with an open and direct style of communication who uses humor, listening skills, broad knowledge, and interests to create a pleasant working environment

AREAS OF STRENGTH

BUSINESS:

Strong understanding of OWASP/CVSS scoring system standards.

Security policies, procedures, and processes.

Managing services, consultants, and client relationships.

Professional Skills:

Security Tools: Burpsuite, OWASP Zap, Post Man, Soap UI, SQL Map, Nmap, Dirb, Acunetix, MobSF, Drozer, Frida, Jadx, Postman, SonarQube, CheckMarx and many more.

Security Distros : Kali Linux

Programming Skills: HTML, Javascript.

PROFESSIONAL SUMMARY

Information Security Consultant with Around 3 years of experience in Application Security.

- Currently working in Qseap Infotech Pvt.Ltd,(Navi Mumbai) as Information Security Consultant from May 2022.
- Strong Hands-on Experience in manual and automated Vulnerability Assessment, Penetration Testing.
- Hands on experience with Web Application, Web service and Mobile, Thick client Application Security Testing.
- Done Penetration Testing for several industries like: Health, Finance, Telecom, Government & commercial various others.
- Interactive with team members and confident during client meetings.
- Assist application teams in performing vulnerability assessments and documenting findings, adhering to RBI guidelines and industry best practices.

- ✦ Prioritize security vulnerabilities based on severity and Impact, and identify potential risks.

WORK EXPERIENCE

1. Qseap Infotech Pvt Ltd as a Information Security Consultant. (From: May 2022 to Present)

Roles & **Responsibilities:**

- Conducting Manual Vulnerability Assessment and Penetration Testing for Web Applications, Mobile Application, Web Services APIs and Thick client Testing.
- Responsible for Scanning Applications Using an Automated Vulnerability Scanning Tools
- Manually Verify Result Generated by Scanner
- Manual Penetration testing by using various tools.
- Prepare & Explain Reports to the Client
- Provide Assistance to Development Team for Mitigating the Vulnerabilities.
- Performed Source Code Review for 2 Projects
- Research and track current security vulnerabilities and related projects
- Responsible to Initiate, Run and Execute the Project

ACADEMICS

- Completed **B. Tech (Electrical & Electronics Engineering)** from Vaagdevi Engineering College. 2015-2019.
- Completed **Intermediate (MPC)** from SVS Junior College. 2013-2015
- Completed **10th** Std from Sadhana High School in the year of 2013

ACHIEVEMENTS&ACTIVITIES

- Received praise from clients for conducting a range of VAPT (Vulnerability Assessment and Penetration Testing) tasks.

ADDITIONAL INFORMATION

DOB: 15/10/1998
Address: Warangal, Telangana

I hereby declare that the above information is true to the best of my knowledge.

Sanket Pawase

Computer Engineer | Penetration Tester | Cyber Security | CEHv12

+91 9359030206 sanketpawase92@gmail.com www.linkedin.com/in/sanket-pawase Pune, Maharashtra, India

Summary

An aspiring Computer Engineer and Cybersecurity specialist with 8 months of hands-on experience in penetration testing, network security, and vulnerability assessments through internships. Skilled in using tools like Burp Suite, Nessus, and Metasploit to identify and address security vulnerabilities and implement strategies for web application and network protection. Certified in CEH v12 by EC-Council and committed to continuous learning, with experience in developing machine learning-based security firewalls to enhance cybersecurity defenses.

Education

Bachelor of Engineering (BE), Computer Science

Sir Visvesvaraya Institute of Technology, Nashik — 06/2020 - 06/2024

- CGPA: 8.14/10

Higher Secondary (XII), Science

Chandaneshwar Vidyalaya & Junior College, Chandanapuri — 06/2019 - 06/2020

- Percentage: 60.00%

Secondary (X)

Devgad Vidyalaya Hiwargaon Pawasa — 06/2017 - 06/2018

- Percentage: 82.60%

Experience

Penetration Tester Intern

Hacktify, Remote, (1 Month) — 07/2024 - 08/2024

- Executed penetration tests on 10+ web applications, employing methodologies like Reconnaissance, Scanning, Enumeration, Exploitation, and Reporting to identify and address vulnerabilities.
- Diagnosed critical issues (SQL, XSS, IDOR, CSRF), improving overall application security by 40%.

Cybersecurity Intern

ShadowFox, Remote, (1 Month) — 06/2024- 07/2024

- Conducted 10+ network scans to uncover active hosts, services, operating systems, service versions, and open ports to identify vulnerabilities..
- Analyzed 200+ network packets with Wireshark to identify potential security threats and gather insights into network traffic patterns

Penetration Tester Intern

CFSS - Cyber & Forensics Security Solutions, Remote, (1 Month) — 03/2024 - 04/2024

- Audited file upload functionalities in 6+ web applications, uncovering critical risks and recommending security improvements.
- Assessed 10+ multi-factor authentication (MFA) implementations to evaluate their effectiveness against common attack vectors.

Cybersecurity Intern

(AICTE)All India Council for Technical Education, Remote, (3 Month) — 05/2023 - 07/2023

- Improved expertise in 10+ network protocols, firewalls, and IDS/IPS by simulating real-world threat scenarios.
- Conducted 20+ network security assessments, identifying vulnerabilities in network configurations, monitoring traffic for anomalies, and implementing security best practices.
- Acquired proficiency in 4 core SOC functions, including threat detection, incident response, threat intelligence, and security monitoring, ensuring effective cybersecurity operations

Cybersecurity Intern

Teachnook, Remote, (2 Month) — 02/2023 - 03/2023

- Studied 10+ countermeasures against DDoS attacks, significantly reducing system downtime during such incidents.
- Assessed 5+ social engineering techniques, including phishing and tailgating, strengthening defenses against human-based security breaches.

Projects

Neural Network web Security Firewall

- Designed a machine learning-powered firewall that detected and blocked 98% of malicious web traffic in real-time. Applied CNNs to analyze traffic patterns, identifying anomalies and preventing SQL injection, XSS.
- Integrated LSTMs for time-dependent attack detection, improving system defenses against advanced threats by 40%.
- This firewall protected against 5+ types of attacks, including SQL injection, XSS attack, OS command injection, file inclusion attack, and DoS attack on the web.

Keylogger

- Developed a keylogger tool that records 100% of keystrokes on a computer system.
- This project focuses on creating a keylogger for ethical purposes, monitoring and analyzing 5+ user input events daily to detect unauthorized access or potential security breaches..
- The tool captures and logs 8+ types of data keystrokes, system information parameters, periodic screenshots, and other sensitive information storing everything in a secure file and sending consolidated email alerts.

Skills

- **Technical Skills:** Ethical Hacking, Network Security, Penetration Testing, Information Security, Web Application Security, Vulnerability Assessment, Cryptography, Network Assessments, Intrusion Detection.
- **Tools:** Burp Suite, Nessus, Metasploit, OpenVAS, Nmap, Wireshark, OWASP ZAP, SQLmap, John the Ripper.
- **Networking:** TCP/IP, OSI Model, VPN, Firewall, IDS, IPS.
- **Standards:** OWASP, MITRE ATT&CK.
- **Programming Languages:** Python.
- **Operating Systems:** Windows, Kali Linux, Parrot OS.
- **Non-Technical Skills:** Problem Solving, Communication, Teamwork, Collaboration.

Certifications

- **Certified Ethical Hacker (CEHv12)** – EC-Council
- **Digital Forensic Essentials (DFE)** – EC-Council
- **Network Defense Essentials (NDE)** – EC-Council
- **Ethical Hacking Essentials (EHE)** – EC-Council
- **Security Operations Fundamentals** – Palo Alto Networks
- **Cloud Security Fundamentals** – Palo Alto Networks
- **Network Security Fundamentals** – Palo Alto Networks
- **Cybersecurity Fundamentals** – Palo Alto Networks

Achievements

- **Hall of Fame** – Bugcrowd (Lime Bug Bounty Program)

Languages

- **English** (Proficient)
- **Hindi** (Proficient)
- **Marathi** (Native)

Bhavani Prasad Sharma Siddanthi

Information Security Analyst

Hyderabad, India
9381811400 - siddanthibhavani@gmail.com

Links
LinkedIn

Certifications

CERTIFIED ETHICAL HACKER v12

AWS CERTIFIED CLOUD PRACTITIONER (CLF-C01)

NETWORK SECURITY ASSOCIATE NSE 1&2

CERTIFIED APPSEC PRACTITIONER (CAP)

Professional Summary

- Working as an Information Security Analyst at Cognizant with 2.5+ years of expertise.
- Possess dedicated experience in Vulnerability Assessment and Penetration Testing, specializing in both manual and automated assessments.
- Experience includes Web Application, Mobile Application, Source code review.
- Have good understanding about various Security Standards/Frameworks like OWASP Top 10 and SANS 25.
- Have excellent interpersonal skills and proven ability of working with different levels of management.
- Involved in Information gathering, test planning, test execution, false positive analysis, reporting vulnerabilities, fixed recommendations.
- Proficient in writing Interim reports, Final Summary reports and delivered walkthrough on the security test report with the stake holders

Work Experience

Programmer Analyst, Cognizant, Hyderabad

07/2022 - Present

- Conducted vulnerability assessments on 10+ Web and Android applications using Burp Suite and OWASP ZAP, leading to a 30% reduction in potential risks.
- Defined security testing scope utilizing test design principles, security tools, and comprehensive understanding of business requirements and application workflows.
- Performed DAST, SAST, API, and Mobile Security Testing for web and Android applications, adhering to OWASP Top 10 standards.
- Conducted False Positive analysis on automated scan results to ensure accuracy and reliability.
- Compiled Final Security Test Executive Summary Reports detailing business impact, severity ratings, OWASP mappings, reproduction steps, evidence, and remediation recommendations.
- Retested applications post-fix implementation by the development team to verify vulnerability remediation.

Education

Bachelor of Technology, CMR College of Engineering and Technology

06/2018 - 06/2022

- CGPA - 8.6

Technical Skills

- Security - Vulnerability Assessment, Penetration Testing, DAST, SAST, MAST, API, OSINT.
- Frameworks - OWASP, SANS.
- Tools - Burp Suite, ZAP, Nessus, Postman, MobSF, Frida, Nmap, Wireshark, SQL Map.
- Operating systems - Windows, Kali Linux, Parrot Security.

Key Achievements

Risk reduction through Assessments

- Successfully reduced the potential risks by 30% through effective vulnerability assessments

Conducted Security Awareness trainings

- Took initiative and conducted a comprehensive security awareness training program, resulting in a 35% reduction in security incidents such as Phishing and other social engineering attacks.

SANKARAN S

CSSLP | APPSEC | DEVSECOPS

CONTACT DETAILS

E-mail :
gannysan@protonmail.ch

Phone : 90030 31822

CERTIFICATIONS

- Certified Secure Software Lifecycle Professional (**ISC2**)
- **AWS** Certified Security - Specialty (SCS-C01)
- Certified Ethical Hacker (v11) - **EC-Council**
- API Penetration Testing - **APIsec University**
- **Qualys** Certified - Vulnerability Management

PROFESSIONAL SKILLS

- Software Composition Analysis
- **Open Source Security**
- SAST(Checkmarx,Veracode, Black Duck)
- **DAST** (BurpSuite, ZAP)
- IL4 | FedRAMP
- Scripting (**Python** | **Bash**)
- **Vulnerability Management** (AlienVault, Qualys, Nessus/Tenable)
- **AWS**, **Azure**, O365 Security & Compliance
- EDR | MDM | DLP | WAF
- **SIEM** (AlienVault, Splunk)
- Darktrace | Varonis | Threat Locker

EDUCATION

Bachelor's in Electronics and Communication engineering

ABOUT ME

CSSLP with 5.5+ years of expertise in securing SaaS, threat modeling, and vulnerability mitigation. Proficient in integrating security across the SDLC to deliver compliant, resilient, and scalable solutions. Strong collaborator with a focus on proactive risk management and effective stakeholder communication.

WORK EXPERIENCE

EVERI | JUL 2023 - NOV 2024
Senior Application Security Engineer

Application Security Testing and Risk Management
Perform threat modeling, static code analysis, and software composition analysis on Everi product lines to enhance software security. Partner with developers and QA to address license risks, promote secure coding practices, and offer remediation support. Enhancing the security posture of the company's products through risk evaluation, design reviews, and security metrics.

CHRONUS | JUN 2021 - MAY 2023
Security and Compliance Engineer

Security Compliance and Assessments
Worked with DevOps on DoD IL4 for security gap assessments and control implementation (FedRAMP). Conducted end-to-end web application and API security assessments, including SAST/DAST/IAST, and threat modeling.

Cloud Infrastructure Security
Optimized and secured cloud infrastructure with continuous security audits, monitoring, and configuration standards (DISA STIGS & SRG).

Implementation and Management of Security Controls
Implemented NIST 800-53 and FIPS security controls; maintained POA&M for vulnerability tracking and remediation. Managed SCA for open source component identification, license compliance & vulnerability management.

GAVS TECHNOLOGIES | JUN 2019 - APR 2021
Application Security (DevSecOps)

Application Security Testing and Management
Conduct static/dynamic app testing, code reviews, threat modeling, and penetration testing. Manage security assessments to ensure compliance with standards like OWASP Top 10 and SANS25.

Collaboration and Training
Draft policies, SOPs, and reports for various processes.
Experience with Security Frameworks NIST, CIS, PCI DSS, HIPAA, and GDPR standards.

HARIKRISHNA MANDALAPU

Penetration Tester | Certified Ethical Hacker | Immediate Joiner

+91-8074329587 iamharikrishna23@gmail.com

Career Objective

To secure a Penetration Tester role where I can leverage my 6+ years of expertise in vulnerability assessment, penetration testing, and security analysis to identify and mitigate risks. I aim to contribute to organizational cybersecurity by utilizing advanced tools, adhering to OWASP and SANS standards, and integrating security into CI/CD pipelines for proactive risk management.

Professional Summary

Certified Ethical Hacker (CEH) with 6+ years of experience in Vulnerability Assessment and Penetration Testing (VAPT) across web applications, APIs, and mobile platforms. Proficient in tools like Burp Suite, OWASP ZAP, HCL AppScan,Hp Web Inspect, Nmap, Kali Linux, and Veracode, with expertise in DAST, SAST, and SCA methodologies. Skilled in identifying and remediating vulnerabilities aligned with OWASP Top 10, SANS Top 25, and CVSS scoring. Experienced in leading team, managing end-to-end client communication, and preparing daily, weekly, and monthly reports. Strong communicator with a proven ability to deliver actionable insights and mentor junior team members.

Experience

QAonCloud | Chennai, Tamil Nadu | Sep 2023 – Present

Designation: QA Specialist - Security

Client: Avanti Finance, Geekladder

- Conducted manual and automated penetration testing for web applications, mobile apps, and APIs using tools like Burp Suite Professional, OWASP ZAP, and Postman.
- Integrated security testing tools (e.g., Burp Suite, OWASP ZAP) into CI/CD pipelines using Jenkins and GitLab CI to enable continuous security validation during the development lifecycle.
- Identified and reported critical vulnerabilities (e.g., SQL injection, XSS, CSRF, XXE) aligned with OWASP Top 10 and SANS Top 25 standards.
- Tested REST and GraphQL APIs for vulnerabilities such as insecure endpoints, broken authentication, and data exposure using Postman and Burp Suite.
- Conducted mobile application security testing using tools like Jadx GUI, APK Tool, Frida, Objection, and Android Studio to identify issues like insecure data storage, hardcoded secrets, and weak encryption.
- Collaborated with DevOps teams to automate security testing processes, ensuring timely detection and mitigation of vulnerabilities in CI/CD pipelines.
- Prepared detailed penetration testing reports with exploitation steps, risk levels, and remediation recommendations for stakeholders.
- Managed client communications by presenting vulnerability findings, risk assessments, and remediation strategies to ensure alignment with project objectives and client expectations.
- Conducted training sessions for junior team members on penetration testing tools, methodologies, and OWASP Top 10 vulnerabilities.

Orion Innovation | Hyderabad, Telangana | Apr 2022 – Sep 2023

Designation: QA Engineer

Client: KPMG

- Conducted vulnerability assessments and penetration testing for web applications and APIs using tools like Burp Suite Professional,Postman and Qualys Guard.
- Identified and reported critical security vulnerabilities, including account takeover, remote code execution (RCE), XXE (XML External Entity) attacks, XSS, CSRF, and insecure authentication, in alignment with OWASP Top 10 standards.
- Utilized Qualys Guard for automated vulnerability scanning and prioritized findings based on CVSS scores and risk

levels.

- Prepared detailed vulnerability assessment reports with risk analysis, exploitation steps, and remediation recommendations.
- Proactively connected with clients to gather requirements, understand application functionalities, and ensure comprehensive testing coverage.
- Managed end-to-end testing processes independently, from planning and execution to reporting and follow-up on remediation efforts.

Accenture | Bangalore, Karnataka | Apr 2018 – Dec 2021

Designation: Security Delivery Senior Analyst

Client: ATT, BMS and HESS

- Conducted Dynamic Application Security Testing (DAST) using tools like HCL AppScan and HP WebInspect to identify vulnerabilities in 120+ web applications.
- Performed False Positive (FP) analysis on scan results to ensure accurate and actionable findings for clients.
- Prepared detailed vulnerability assessment reports and shared them with clients, providing clear explanations of risks and remediation steps.
- Conducted Static Application Security Testing (SAST) using Veracode to identify security flaws in application source code.
- Tested applications in alignment with the OWASP Top 10 framework, ensuring comprehensive coverage of common vulnerabilities.
- Maintained a database of identified vulnerabilities using ThreadFix for efficient tracking and management.

Education

Bachelor of Technology in Electronics & Communication Engineering

Vignan's Lara Institute of Technology & Science (VLITS) | JNTU Kakinada, Andhra Pradesh | Aug 2012 – May 2016

Certifications

- Certified Ethical Hacker(CEH)
- AWS Cloud Practitioner
- Azure Fundamentals(AZ-900)

Skill Set

Technical Skills: Vulnerability Assessment, Penetration Testing (VAPT), DAST, SAST, SCA, Web/API/Mobile Penetration Testing, CI/CD Integration

Tools: Burp Suite, OWASP ZAP, HCL AppScan, Veracode, Qualys Guard, Nmap, Kali Linux, Postman, Jadx GUI, MobSF, Frida, Metasploit, Dirbuster, Hp WebInspect, Acunetix, SonarQube, Jenkins

Frameworks/Standards: OWASP Top 10, SANS Top 25, CVSS, CVE, CWE

Programming Languages: Python, Java, HTML, JavaScript

Awards: Ace Award, Spot Award, Best Crewmate Award

Declaration

I consider myself familiar with all above mentioned aspects. I am also confident of my ability to work in a team. I hereby declare that the information furnished above is true to the best of my knowledge.

Signature

(HariKrishna.M)

THEJA. P

Professional Summary:

- Having **7.5** years of experience as a security admin on various access management technologieslike **Okta CASiteMinder,PingFederate,PingAccess, PingOneCloud,OneLogin, AzureAD, TruU Fluid Identity.**

- On boarding new applications in **Okta** and providing the support to the applications.
- Integrated many applications in Policy server by creating new policies.
- Providing the L1 and L2 support and meeting the SLAs for the issues.
- support and meeting the SLAs for the issues report deported by the by the application teams or customers.
- Installed AD agents to sync the users from AD to **Okta** and monitor the services.
- Implemented inbound federation in Okta and users can redirect to third party IDP.
- Creating policies in Okta to enable specific group of users and applications.
- Migrating the apps from **PingFederate** to **Okta** and working closely with stake holders for smooth migration.
- Creating OIDC policies to map to the Oauth clients.
- Gathering requirements from application team to onboard application in Okta IAM.
- Integrated SaaS based applications and provided the support to end users.
- Strong understanding of Authentication, Authorization, MFA, SSO, Federation, and Directory Services concepts
- Good Communication and interpersonal skills.
- Joining CAB meetings for getting change approvals.
- Working with CA for any major issues and providing paramagnet solution for respective issues.
- Weekly report pulling for tracking purpose.

Skills:

Operating System	**: Solaris 9 &10, Windows 2008, 2012, 2016, RHEL.**
ITIL Tools	**: JIIRA, HRMaestro, ServiceNow**
Tools	**:CASiteminder,Activedirectory,PingAccess,PingFederate, PingOne Cloud, SVN, New Relica, OneLogin,AZURE AD, PingDirecotry, Preempt (Crowdstrike), Okta, MFA**

Professional Experience:

- Working in Cognizant Technology solutions Pvt Ltd as Senior Associate from Sep 2018 to Till Now.
- Worked as Senior Software Engineer in CBSI India Pvt Ltd from from June 5th, 2018 Sep 2018.
- Worked as Ping Identity Consultant in Verti system India Pvt Ltd from 19th June 2017 to 3rd June 2018.

Project	:	**Web and Federation based apps on boarded**
Client	:	**Confidential**
Duration	:	**Aug 5th, 2020, to Till Date**

Integration of internal / external applications of customer to the existing **PingFederate** infrastructure and enable the SSO. On boarded new applications in **Okta** and worked on Migrating apps from **PingFederate to Okta**

Key Activities:

- Participation in the on-boarding application meetings and provide feedback to client.
- Analysing the client requirement and SP Metadata for the on-boarding of the SP to the existing IDP of **Okta**.
- Support to the existing on-boarded applications and debug when issues arise.
- Support to the operations team during the deployment of the configuration on the production.
- Participated actively in Change meetings to implement the changes in higher environments.
- Integrated web-based apps to protect the applications using **Okta Access Gateway**.
- Troubleshooting the issues related to Okta and worked with end users closely to resolve the issues within SLA.
- Involved in **Okta from classic to Identity Engine** upgradation and performed health check after the upgradation.
- Created custom authentication policies, session controlling for the specific applications.
- Worked on MFA and resolved the issues related to MFA based issues.
- Worked on PingDirectory and installed oem agents in all PinDirectory servers to monitor the server's health check.

- Preparing deployment document to integrate an application within **Okta** Environment.
- Worked on different types of protocols **OAUTH, OpenID Connect,** and **Saml**.
- Migrated the applications from **PingFederate to Okta** from lower env to Production.
- Troubleshooting the issues related to **Okta** and resolving user sync issues and using expression passing the custom values as attributes.
- Configuring the application in **Okta** Dashboard and mapping the attributes and shared the IDP metadata to app team/vendor to update from their end.
- Involving onboarding calls with the stakeholders and explain the use cases and workflow of the authentication.
- Creating the policies in **PingFederate** as per the requirement and enabling MFA for the applications.
- Configuring the policies in **Okta** and provide MFA for the users and supporting end to end.
- Having good working experience on **Oauth** and **SAML, ODIC** protocols and integrating the apps as per the app specific requirement.
- Integrated SCIM based applications in **Okta** and worked on automated user provisioning to third party applications.
- Monitoring the user synchronization and resolving **Okta** sync issues if the user belongs to different region.
- Documentation of the different technical and process-oriented issues over the application migrations.
- Involved in **DR activity** and documented the procedure to follow the instructions.
- Configuring the required adapters and PCV to integrate PingID with PingFederate.
- Having strong knowledge on Okta, CA IDM.
- Worked exclusively with different teams and users to get them registered with **OKTA**.
- Worked on integrating Okta with commercial Billing applications.
- Worked on troubleshooting the issues encountered in Okta during the application integration with SAML, provisioning of users, importing of users etc.
- Worked with **OKTA** support by opening cases on several issues.
- Worked on provisioning users from **OKTA** to AD and importing users from AD to **OKTA**.
- Worked on implementing pre-empt product and installing DC sensors on **Pre-empt** management servers.
- Good working experience on documentation and following the client specific guidelines.
- Coordinating with vendor and involved in Preempt DC sensors upgrade.
- Worked on integration **PingFederate** with **Preempt** and deployed preempt adapter in PingFederate and configured polices.
- Integrated Azure with Preempt for MFA.

- Creating the policies in PingFederate and tested different types of authentication methods.
- Deploying Jar files into PingFederate and configuring new policies as per the application requirement.
- Worked on Migration project from **PingFederate to Okta** **Project #2:**

Title : Global Applications Security -IDAM
Period : June 2018 to June 2020
Environment : PingOneCloud, JIIRA, PingFederate IAM, Active Directory.

Description:

Configuring the applications with in PingFederate and providing end to end support to the applications in Test and UAT and PROD Env.

Key Activities:

- On boarding the application connections (IDP and SP) and troubleshooting the Issues.
- Managing the **PingFederate IAM** Services in server and managing the logs (Audit, server) for reports and troubleshooting purpose.

- Creating Customer connections from PingOneSSO for SaaS apps.
- Integration different applications on IdP Side in Dev/Prod.
- Troubleshooting the issues related to SAML based connections.
- Configuring applications for sso and provisioning.
- Customize the pages to match brand.
- Creating Adapters, Service Provider and Identity Provider connections, replicating configuration archive, exporting Metadata, importing and exporting SSL s using Ping Federate.
- Worked on OAUTH Grant types for the OAuth Clients to get the Access Token.
- Worked on migrating applications from **PingFederate IAM** 8.3 to 8.4 version.
- Updating ACS urls as per the requirement in **PingFederate IAM.**
- Mapping the adapters and creating the data stores as pcv.
- Monitoring OneLogin AD connector servers and renewing certificate for all the four **AD connector servers.**
- Worked on migration from **One Login** to **Azure AD.**
- Migrated 42 Form Based applications from **One Login** to **Azure AD.**
- Integrated internal SAML based application in **Azure AD** as well as in **OneLogin.**
- Adding new applications in AzureAD and assigning the specific security groups to access the applications from Azure dashboard.

- Enabling MFA as per business requirement.
- Worked on SAML **Singning certificate** updates in UAT and PROD.
- Worked on Migraiton Project from Ping to Okta.
-

Project#1 **: IDAM**
Environment **: CA Siteminder12.52, Directory, Solaris 10, Linux, Windows Server 2008/2012.**
Period **: 2017 Sep to June 2018**

Description:

Configuring the applications with Site minder and providing Authentication, Authorization single sign on services. Providing L1 support to the application integrated with Site minder environment.

Key Activities:

- Onboarding new applications in CA Siteminder and providing the support to the applications.
- Good experience in troubleshooting the CA **Siteminde**r and web agent issues.
- Installing and configuring the web agent in apache and IIS webservers and configuring the web agent to communicate with **Siteminder**.
- Configuring the policies for the applications to provide authentication and authorization.
- Configuring authorization policies for directories/file.
- Creating the attributes and new object classes.
- Involved in SSO Enabling Web based applications and there after supporting these applications.
- technically for any error/ issue reported.
- Creation of policies on the Policy Servers with the help of Site Minder Objects like in Realms,
- Agents, Authentication Schemes, Policies to protect the resource and give access only to required users by configuring groups for the specific application.
- Working on user specific issues and contacting users for their concerns.
- Managing Change Advisory Board meeting to get approvals.

`

Vemula Vamshi

Medium: *https://vamshi-vemula.medium.com*
Tryhackme: *https://tryhackme.com/p/vamshivemula444*
Pentesterlab: *https://pentesterlab.com/profile/geek_444*

Email: *vamshivemula444@gmail.com*
Mobile: *+91 8096265545*
LinkedIn: *https://www.linkedin.com/in/vamshivemula444*

EXPERIENCE

- **Zomato** Gurgaon, India (Hybrid)
  Security Engineer I (Full-time) *Nov 2023 - Present*
  - Worked on over 220+ internal security audits/assessments, including manual VAPT, secure code reviews, and threat modeling, across Zomato, Blinkit, Hyperpure, District, and FeedingIndia.
  - Led 22+ comprehensive security audits, performing end-to-end service reviews to identify and mitigate critical vulnerabilities.
  - Proactively identifying critical security issues and maintaining security posture across multiple services and applications.
  - Collaborated with developers to mitigate the identified vulnerabilities and helped the dev team to prevent security issues during the idealization phase.
  - Worked on internal security automations that include script writing and research.
  - Managed OnCall responsibilities, including secret detection monitoring, leaks monitoring (internal tool vinifera) and handling Hackerone Bug Bounty Program (Triaging and resolving the reports).
  - Performed vendor onboarding reviews, including VAPT on third-party assets and security documentation verification, to prevent supply chain attacks/breaches.
- **Apna** Bengaluru, India (Remote)
  Security Engineer Intern (Full-time) *July 2023 - Nov 2023*
  - Performing VAPT (Pentesting) on apna mobile application and web applications.
  - Integrating and monitoring SAST and DAST tools with CI/CD pipelines.
  - Source Code Review and Closely working with developers to mitigate the vulnerabilities.
  - Monitoring web application traffic via reblaze WAF and implementing security rules.
  - Reviewing and evaluating external VDP(Vulnerability Disclosure Policy) reports.
  - Worked with wazuh (SIEM) tool configuration and set-up a few security policies for company laptops to monitor security events and enhance security.
- **Seclance** Bengaluru, India (Remote)
  Offensive Security Consultant/ VAPT Intern (Full-time) *Feb 2023 - May 2023*
  - Worked on over 5+ pentest projects.
  - Performed vulnerability assessment and penetration testing on various assets including Web, Infra, API and Mobile.
  - Managed a team of interns as lead by reviewing the team findings and drafting the professional pentest report.

EDUCATION

Bachelor of Technology B.Tech - (Computer Science & Engineering) GPA: 8.0 *Aug 2019 - July 2023*
Jawaharlal Nehru Technological University Hyderabad - (TKREC) Hyderabad, India

SKILLS SUMMARY

- **Languages (Prog.):** Python, Javascript, Golang
- **Security Skills:** Web Application Security, Mobile Application Security, Network Security, VAPT, SAST, DAST, Secure Code Reviews (Manual)
- **Tools:** Burp Suite, Nmap, Docker, Metasploit, Nessus, MobSF, Postman, Acunetix, Git
- **Web Technologies:** HTML, CSS, SQL, Node.js
- **Platforms:** Linux, AWS, GCP

ACHIEVEMENTS

- Received performance-linked cash bonuses twice during my work at Zomato.
- Reported multiple vulnerabilities and acknowledged by various programs include FreeCharge, Byjus, FirstCry, Bigbasket, Flipkart, etc.
- Hands-on Pentesting and Application Security knowledge with Tryhackme, PentesterLab, Portswigger Academy and Hackthebox platforms, Solved over 280+ Labs.
- Ranked 4th Position in Cyber Secured India (Cyber Security & Digital Forensics) Internship Program and made it to top 10% in CIT- ISAC Hackathon.
- Solved 300+ coding problems on leetcode, GfG, Coding Ninjas and Hackerrank using Data Structures and Algorithms.

CODING PROFILES

- Leetcode: *https://leetcode.com/vamshi_vemula/*
- GitHub: *https://github.com/vamshi-vemula*

PROJECTS

secretX Tool - *(Golang)* GitHub (Private)

- Developed a Golang based automation tool for tracking organization's employees activity and detect secrets in public repositories (Github, Docker, Huggingface)
- The tool only requires an organization github username as an input and it traverses over all the github repos of org including commits, PRs, discussions, contributors, public members and finds users.
- By using employee usernames, the tool will scan all the public github, Docker, HuggingFace repos using Trufflehog.
- Verified secrets will be notified via slack webhook and slack bot to the specified channel with scan output file.

Crypter Tool - *(Python, Tkinter)* GitHub | Demo

- A GUI based Image Steganography tool for transmitting secret information without affecting unintended users.
- Added extra layer of confidentiality by adding password protection for steganography images using AES encryption.

Personal Portfolio Website - *(HTML, CSS, Javascript)* GitHub | Live

- Designed and developed a good looking responsive portfolio website and hosted on Google Firebase Cloud Hosting.

AKSHARA M

CYBERSECURITY VULNERABILITY MANAGEMENT LEAD ANALYST

CONTACT

+91 80893 93893
akshararadhakrishnanclt@gmail.com
linkedin.com/in/Akshara
Kochi, Kerala, India

SKILLS

- Infrastructure vulnerability scanning
- DAST, SAST
- Policy compliance scanning
- Cloud & On-Prem Security
- Change Management
- Incident Resolution
- Automation (Python, C, C++)
- Reporting & Documentation
- Operating System (Windows, Linux)

TOOLS KNOWN

- Qualys
- Tenable (Security Center, VM, Nessus)
- CrowdStrike
- Rapid7 InsightVM
- Microsoft Defender
- Invicti
- Hadrian
- Snyk
- JFrog
- JIRA, ServiceNow, Fresh service

EDUCATION

College of Engineering, Vadakara
2018-2022
B. Tech CSE (Honors) – 8.3 CGPA

CERTIFICATIONS

Microsoft certified: Security Operations Analyst Associate (SC-200)

Qualys Guard Certified Specialist (VMDR)

REFERENCES

Sreejith K
Senior Technical Consultant
Sreejith.061@wipro.com
+91 94477 12627

PROFILE

Cybersecurity Analyst with 3 years of experience in vulnerability management, risk assessment and security compliance across cloud and on-prem environments. Skilled in threat detection, web application security, policy compliance scanning and automation. Proven ability to lead team, optimize security operations and enhance organizational security posture. Currently serving notice period.

EXPERIENCE

Vulnerability Management Lead Analyst

Wipro Limited (May 2022 – Present)

- Leading a 6-member team, successfully delivering security assessments across cloud and on-premises environment, for 10000+ Ips and 20+ applications per month, maintaining 95% on-time project delivery rate.
- Experience in deploying, configuring and managing vulnerability assessment tools.
- Conducted Dynamic Application Security Testing (DAST) using Tenable VM and Invicti, identifying vulnerabilities based on OWASP top 10 & SANS top 25.
- Executed Static Application Security Testing (SAST) using Snyk, to identify vulnerabilities in source code.
- Leveraged JFrog to scan and manage vulnerabilities in software artifacts.
- Engaged agent-based scanning in Qualys and InsightVM.
- Worked on Policy compliance, enhancing adherence of security benchmarks.
- Knowledge in change management process, including raising, assessing and implementing change requests.
- Migrated EOS vulnerability scanners from CentOS to Oracle Linux, upgraded scanners, and migrated RHEL servers to maintain compliance.
- Troubleshot and resolved scan and server level issues related to TVM tools.
- Proficiency in Python to automate reporting tasks, reducing manual report generation time by 50%.
- Acted as Transition SME, leading smooth KT and transfer of process, tools and responsibilities.
- Managed the remediation process by prioritizing vulnerabilities and coordinating with relevant teams to implement timely fixes.
- Analyzed threat intelligence feeds to author comprehensive vulnerability advisories, notifying threats and recommending remedial actions.
- Prepared customized reports, summaries, SOPs and status report decks.
- Experienced in handling various customers across different geographies.
- Resolution of requests and incidents within SLA.
- Mentored Junior analysts by providing guidance, training and support.

ACHEIVEMENTS

- Wipro Beyond Boundaries award for excellent client feedback.
- Wipro Habit Flagbearer award for due diligence and proactive approach.
- Wipro Inspiring performance award for team leadership and positive attitude.

ARNAB ROY

+1 (857) 317-1327 ◇ arnab.cyberapp@gmail.com ◇ linkedin.com/in/arnab-roy-/ ◇ Website

EXPERIENCE

Information Security Analyst Jun 2024 - Present
Intello Group *Boston, MA*

- Configured and optimized SIEM platforms (Splunk and Azure Sentinel) to correlate security events across 200+ endpoints, creating custom detection rules that reduced alert fatigue by 35% and improved mean time to detection.
- Led security architecture reviews for 5 critical business applications and IT infrastructure projects, identifying design flaws and recommending secure architecture patterns that prevented potential breaches, ensured secure-by-design principles and reduced remediation.
- Reviewed and restructured identity and access management policies, implementing role-based access controls and conducting quarterly user access reviews that identified and removed 60+ instances of excessive privileges, strengthening the organization's security posture.
- Designed and implemented an end-to-end vulnerability management program using Nessus and OWASP ZAP, prioritizing critical vulnerabilities based on business impact and reducing the average patch deployment time.

Associate Security Researcher Jun 2023 - Jun 2024
Semgrep *Boston, MA*

- Developed 600+ security rules for software package managers including npm, Maven, PyPI, and GoMod, addressing critical and high vulnerabilities in the software supply chain.
- Performed incident response activities and executed vulnerability scans to identify and remediate weaknesses, resulting in a 35% improvement in threat detection accuracy.
- Automated rule generation processes, improving integration of vulnerability data from various sources, boosting efficiency and accuracy of Semgrep's security responses by 25%.

IT Audit Analyst Co-op Jul 2022 - Dec 2022
Fidelity Investments *Boston, MA*

- Led comprehensive audits across 12 databases, enhancing data collection and retention processes while resolving security and compliance issues in alignment with corporate policies.
- Spearheaded security audits with a thorough review of IAM policies, reducing permission creep by eliminating 30 redundant users and roles.
- Managed Datadog dashboards and alert systems to ensure swift incident detection and response, improving overall incident response efficiency by 8%.

EDUCATION

Master of Cybersecurity Northeastern University Sep 2021 - May 2023
Relevant Coursework: Network Security, Software Vulnerability, Security Risk Management, Computer System Security

PROJECTS

Tor Network Crawler Jan 2024

- Created a research crawler that uses Tor to recursively search.onion sites. It complies with legal and ethical research requirements by using PostgreSQL for data persistence, multi-threaded content extraction, and XML-to-JSON data conversion.

Reconnaissance Paper Oct 2021 - Nov 2021

- Conducted reconnaissance of an organization's 700 websites using Passive Open-Source Intelligence Tools including Spiderfoot, Shodan, and Censys to identify IP addresses vulnerable to Remote Code Execution.

SKILLS

Programming Languages : C, C++, C#, Java, Python, JS, Go, Bash, Powershell
Technologies: AD, AuditBoard, AWS, Azure, Azure Sentinel, Burp Suite, Censys, Citrix VPN, Azure, Azure Sentinel, CrowdStrike, Datadog, Docker, Fedora, Flask, Git, GitHub Actions, GitHub Security Advisory, Hunter.io, Kali, Kubernetes, MacOS, MariaDB, Metasploit, Nessus, Nikto, NMap, PEASS-ng, Pfsense, Power BI, Redis, RSA Archer, Semgrep, Sentry, Snort, Spiderfoot, Splunk, SwaggerAPI, SwaggerHub, Symantec, Ubuntu, VMWare, Wireshark, Windows, YARA

CERTIFICATES AND PUBLICATIONS

- CompTIA CySA+ Apr 2024
- OWASP Boston BASConf CTF Winner Mar 2024
- AWS Certified Cloud Practitioner Jul 2022
- AI based MEC for IoT Feb 2022
- CompTIA Security+ Jul 2021

RAJA KOTHA **+91-9603584141**

APPLICATION SECURITY ENGINEER – VAPT ENGINEER **rajakotha2229@gmail.com**

Summary:

A Cyber Security Enthusiast with 5 years of experience and seeking a position as an Application Security engineer/Penetration Tester/VAPT Engineer.

Interested in Web applications, Mobile application penetration testing, Network penetration testing,

Api security testing, implementing security controls on the application, and finding security postures of applications at all levels.

- Performed penetration tests on various kinds of applications like Block chain, Web3 applications, E-Commerce application, Banking application, financial application and IPR applications, Live applications like cricket.com etc.
- Proficient in understanding Application level, Api level, code level and network level vulnerabilities.
- Experience in using a wide variety of network security tools to include Wireshark, Nmap, Nessus etc.
- Experience in using different kinds of web application security tools like Kali Linux, Burp suite, OWASP ZAP, Metasploit etc.
- Experience in supply chain security process, so third-party software meets the standards.
- Experience in doing Red-Team assessments on the applications and infrastructure.
- Worked on improvements for provided security services, including the continuous enhancement of existing methodology.
- Implemented Shift Left Approach and Integrated Automation tools to improve the security posture of applications during development.
- Worked with stake holders in reproducing and addressing security vulnerabilities.
- Worked with application developers to validate, assess, understand root cause, and mitigate vulnerabilities.
- Performed VAPT on test environment as well as on live environment.
- Prepared Comprehensive Penetration testing reports so that every stake holder can easily understand, which includes all vulnerabilities, steps to reproduce, other ways to occur, possible mitigations, CVE ID's, and references.
- Strong understanding of IT security standards, OWASP 10, SANS 25 and MITRE FRAMEWORK.
- Strong understanding of OSI, TCP/IP model and Network basics.

Experience:

Karnataka Bank Limited: Application Security Engineer: February 2025 – Currently Working

- Performed Application security testing on both External and Internal applications of Karnataka Bank Limited.
- Performed Network security testing on Internal Network of Karnataka Bank Limited.
- Performed Threat modelling on the applications of Karnataka Bank Limited.
- Performed Security testing on the implementation of API gateway.
- Performed WIFI scanning of the routers implemented in the office premises.
- Performed Vulnerability Analysis of the servers and applications using Nessus Tool.
- Prepared documentations on Enterprise Security Architecture for RBI Audit.

Head Digital Works: Application Security Engineer (CONSULTANT): October 2024 – February 2025

- Performed Application security testing of Web applications like cricket.com, A23.com, hdw.com and found many vulnerabilities.
- Performed Network security testing of Internal Network.
- Performed Network level penetration testing of all external facing domains (Nearly 100 Domains) to check the secured visibility of domains to external users.

Mai Labs Private Limited: Security Engineer: March 2023 – Currently Working

- Found numerous vulnerabilities at Network Level, Code Level, Api Level, and application level.
- Performed web application security testing of blockchain applications like MyIpr, Kalp Studio, Kalptantra.
- Performed threat modelling on block chain architecture i.e., Kalptantra.
- Performed Api security testing of all block chain Api's.
- Performed Secure code analysis on Golang applications and Python applications.
- Implemented Gosec tool in CI/CD pipeline.
- Performed security analysis on integration of microservices into application.
- Prepared comprehensive penetration report which includes all the vulnerabilities, scenarios how it was found, all scenarios how it can occur, steps how it can be reproduced to exploit, possible mitigations, and their CVE ID'S.

Accedian Technologies Private Limited: Security Analyst: June 2020 – March 2023

- Found numerous bugs and vulnerabilities both at client side, server side and covered threats at all the 7 layers of OSI.
- Found various Business logic vulnerabilities in the applications.
- Performed Blackbox testing on different types of applications which include E-Commerce applications, Fintech applications, Block chain applications, Banking applications, Blog websites and applications which are internal to companies.
- Performed secure code analysis of different languages like java, python, and Golang.
- Performed API security testing on Api's which are in development level and for deployed applications.
- Prepared comprehensive penetration report which includes all the vulnerabilities, scenarios how it was found, all scenarios how it can occur, steps how it can be reproduced to exploit, possible mitigations, and their CVE ID'S.

Skills:

- Web application penetration testing
- Api security testing
- Mobile Application penetration testing
- Threat Modeling
- Security Analysis
- Network Penetration Testing

Tools:

- **Web Application Security:** Burp suite, Owasp Zap, Metasploit.
- **API security:** Postman.
- **Mobile Application Security:** Burp Suite, MobSF, Frida, Geny Motion.
- **Threat Modeling:** Microsoft Threat modeling tool, Threat Modeler.
- **Network Security**: Nmap, Nessus, Metasploit, Wireshark.
- **Operating Systems:** Linux, Windows.
- **Security Standards:** Owasp 10, Sans 25.

Languages:

- Python.
- Bash Scripting.

SHAHIN SK

Mobile No: +91- 6281102992

Email ID: shahin.sk.appsec@outlook.com

Objective

To excel and attain a challenging position in IT industry on Information security that Uses my Technical, Analytical and Management skills for successful mutual growth.

Summary

- 3.5 years of strong experience as security engineer in security assessments (Web Based Applications, Web services, Penetration Testing and Vulnerability Assessment.)
- Hands on experience in experience in Application Security Testing particularly focused on performing technical activities such Application security Assessment, Vulnerability Assessment, Penetration Testing, and Mobile Application Security Testing.
- Excellent understanding of the web application security approach
- Proficient in application security concepts, familiar with OWASP Top 10 & SANS 25
- Security Assessment based on OWASP framework and reporting the identified issues in the industry standard framework.
- Strong knowledge on Security Assessment, Risk Assessment.
- Able to perform black box/grey box security assessment of web applications and using automated and manual approach
- Evaluating the application's security for industry best practices to overcome risks and defining policy and verifying whether it follows all given policies.
- Implement Secure SDLC process in application development teams to improve security.
- Understanding the technical designs to analyze and identify security threats in design.
- Effectively communicate with internal teams and external client to deliver functional requirements like implementation strategy & approach, integration design and support.
- Experience in conducting vulnerability assessments.

Experience

- Working with Accenture, Hyderabad, from Nov 2021 to till date.

Educational Qualifications

- B. Tech from JNTUK Tirumala Engineering college in 2021.

Summary of Major Skills

- **Industry Standards**: OWASP-Top 10, SANS 25.
- **Tools:** Burp Suite, SQLMAP, OWASP ZAP, WebInspect Nessus, App Scan, Acunetix, and NMAP.
- **Web Vulnerability Scanner**: Burp Suite, Web Inspect, Nessus
- **Network Security Scanner:** Nessus, Nmap.
- **Platforms:** Windows, Linux.

Projects

Project : EMIRATES NATIONAL BANK
Role : Analyst

Responsibilities:

- Perform Security Testing on all projects in Web Platform. This includes Web applications, web services.
- Working as a secret analyst we are performing the DAST, SAST, NSST security scans testing security scans.
- Prepared comprehensive security report detailing identifications, risk description and recommendations.
- Preparing reports and sharing with developers and management based on the issues identified.
- Worked closely with development and product management for vulnerability remediation.
- Vulnerabilities validated through manual testing by using Proxy Tools.
- Ensuring overall quality of the project and On-time delivery
- Interacting with clients on status updates on a weekly basis.
- Performed manual assessment on tool-based results.
- Providing trainings to developers on writing secure code best practices
- Performed Black box and Grey box penetration testing.

Project : ALD-Automotive
Role : Associate

Responsibilities:

- Performing the multiple test cases by using the Burp-Suite Proxy and discussing with the team to confirm the high and critical level of vulnerabilities.
- Preparing reports and sharing with developers and management based on the issues identified.
- Worked closely with development and product management for vulnerability remediation.
- Vulnerabilities validated through manual testing by using Proxy Tools.
- Interacting with clients on status updates on a weekly basis.
- Performed manual assessment on tool-based results.
- Tracking of secure analysis reports and driving them to closure.

Project: CITI BANK

Role : Associate

Responsibilities:

- Performed Dynamic application Security analysis of the web applications using Burpsuite
- Identified and risk rated vulnerabilities
- To carry out web application security testing (Gray box and Black box) and reporting the vulnerabilities
- Expert working knowledge of OWASP Top 10 vulnerabilities analysis
- Recommendations to mitigate the weaknesses discovered during the assessment.
- Discussing and Taking follow up with respected team to get the vulnerabilities close
- Delivery of Technical and Executive Reports

Harshit R. Sharma

harshit.cybersec@gmail.com +916353617691 n0desNc0des India

PROFILE

A cybersecurity enthusiast since childhood, I bring a deep passion for securing digital landscapes. My technical proficiency spans ethical hacking, penetration testing, and network security. I actively seek challenges and remain committed to continuous learning, always staying ahead of emerging threats. Eager to make a significant impact in the cybersecurity field, I am poised to contribute my skills and dedication to safeguarding the digital world.

EDUCATION

Bachelor of Technology CSE - Cyber Security, 2020 – 2024 | Hyderabad, TS
Sphooorthy Engineering College

Intermediate, Narayana Junior College 2018 – 2020 | Hyderabad, TS

SSC, Narayana E- Techno School 2018 | Hyderabad, TS

PROFESSIONAL EXPERIENCE

Cyber Security Intern, 02/2024 – 08/2024 | Hyderabad
Centre for Development of Advanced Computing (C-DAC)

- Developed a Python3 web crawler with support for .onion sites, using bs4 for parsing and ThreadPoolExecutor for concurrent crawling.
- Implemented keyword search with multi-keyword support, error handling, and link saving for iterative searches.
- Initiated frontend development with Django, Tailwind, and Daisy UI (paused).
- Designed and developed an XSS Vulnerability Scanner in Python3 to detect stored and reflected XSS, with multi-payload injection and concurrent scanning.
- Added form-based login functionality and began implementing token-based authentication.
- Researched onion sites, web traffic patterns, and DOM-based XSS detection techniques.
- Performed VAPT on an Android application, including SSL pinning bypass of the APK.
- Collaborated with peers to troubleshoot issues and explored additional cybersecurity tools and methodologies.

SKILLS

Cyber Security

OWASP Top 10

Networking
TCP/IP, DNS, DHCP, SSH, FTP, HTTPS, SSL/TLS

Programming Languages
Python, Bash

Systems
Linux(Red Hat, Kali, Ubuntu), Windows, MacOS, Active directory

Tools
Burpsuite, Metasploit, Nmap, Nessus, Splunk, Virtualbox, CLI, VScode, Git

CERTIFICATES

- Pragmatic approach to cyber security, Futureskills Prime(C-DAC)
- Google Cybersecurity Professional Certificate(In progresss)

PROJECTS

HyperEye: Web Crawler and XSS Vulnerability Scanner, A Python-based web crawler and XSS vulnerability scanner that automates security testing, detects vulnerabilities, and stores results using MongoDB. Optimized with concurrent processing for efficient scanning and analysis.

- **Programming (Python, Bash):** Developed a web crawler and XSS scanner using Python.
- **Database Management (MongoDB):** Stored and managed scan results, crawled links, and vulnerabilities.
- **Web Scraping & Parsing:** Extracted and analyzed web data using *requests* and *BeautifulSoup*.
- **Concurrent Programming & Multithreading:** Optimized scanning performance with ThreadPoolExecutor for parallel processing.

Web-weaver
- This python tool is a basic web crawler designed to recursively explore and extract hyperlinks and subdomains from a specified target URL.
- It is implemented using requests library for making HTTP requests and extracting webpage content along with re library for regular expression based parsing and urllib to join links.
- My main aim while building this tool was that the tool crawls links without any repetition and redundancy.

Vuln-Detective
This Python project is vulnerability scanning tool with finds possible cross site scripting vulnerabilities including Reflected and Stored XSS using the requests, BeautifulSoup, urllib, re libraries. This tool specifically targets DVWA application which is vulnerable web application for practicing and learning web security testing.

AWARDS

Sphoorthy Cyber Security CTF
Participated in an Ethical Hacking and Cyber Forensics workshop at my college where I won the Capture the Flag (CTF) competition held on the final day. Caught all the flags in the given time frame. The prize money was awarded by the guest lecturers.

LANGUAGES

- English
- Hindi
- Gujarati
- Telugu

ORGANISATIONS

Teach For India, Volunteer Hyderabad, TS
- Led student travel to another city for *Conference of the Birds* play.
- Managed logistics, safety, and overall experience for the group.

REFERENCES

Mr. Ajith Menon, *Senior Security Engineer,* Plume Designs Inc
ajithmenoninfosec@gmail.com, +917356454428

Kaustubh Trivedi

Gurugram | kaustubh.trivedi@hotmail.com | 6393779733 | linkedin.com/in/Kaustubh-Trivedi
github.com/Kaustubh-Trivedi

Techncal Skills

Languages: Python, Java, SQL, JavaScript

Security Tools: AppScan, AKAMAI WAAP, Prisma Cloud, Qualys, Nessus, SonarQube, BurpSuite

Cloud Security Tools: GuardDuty, Secret Manager, KMS, Cloudtrail, Lambda, IAM, CloudWatch

DevSecOps Tools: EKS, ECS, Jenkins, Github, Terraform, CodeCommit

Core: Code Review, Secure SDLC, Threat Modeling, SAST/DAST, API Security testing, Pentesting

Experience

Product Security Engineer, MaxHealthcare – Gurugram, India July 2022 - Present

- Reviewed **30+ code repositories** across multiple languages (Python, Java, JS), identifying and helping fix **100+ critical vulnerabilities** including XSS, SSRF, IDOR.
- Automated **SAST & DAST scans** for 30+ microservices, integrating tools like SonarQube, ZAP, and Snyk into CI/CD pipelines (GitHub Actions, Github) — reduced manual testing overhead by 70%.
- Implemented container scanning for 100+ Docker images used in production, identifying 20+ CVEs proactively.
- **Led security architecture reviews for 10+ critical applications**, identifying design flaws early and reducing post-deployment vulnerabilities by 60%.
- Implemented **secret scanning** across 50+ repositories using [e.g., GitHub Advanced Security / TruffleHog / Gitleaks], preventing 20+ exposed credentials from reaching production.
- Designed and integrated **SBOM** generation using Syft/CycloneDX into build pipelines, achieving 100% open-source component visibility across microservices.

Security Engineer Intern, Tracelay Network – Banglore, India May 2022 – July 2022

- Collaborated with the Qualys team to deploy an enterprise-wide **vulnerability management** platform, enabling automated scanning, asset discovery, and risk-based remediation across 1,000+ endpoints.
- Led the migration of critical application infrastructure into a **secure DMZ environment**, significantly reducing external attack surface and aligning with network segmentation best practices.
- Implemented data privacy controls aligned with GDPR and DPDP regulations for S3 bucket, including PII classification, consent tracking, and data retention policies — reducing regulatory risk exposure by 60%.
- Deployed Armis for real-time asset discovery and threat detection across unmanaged IT, OT, and IoT environments, enhancing visibility and reducing blind spots by 90% across 5,000+ devices.

Technical & Leadership Projects

Cloud Native Application Security with PALO ALTO Prisma Cloud

- Led the implementation of Palo Alto Prisma Cloud to secure cloud-native applications across multi-cloud environments (AWS, GCP), detecting and remediating misconfigurations and vulnerabilities in real-time; **improved overall security posture by 70%** and enhanced compliance with industry standards (e.g., CIS, NIST).
- Tools Used: Prisma Cloud, Defender

Org-wide Cybersecurity Audit Project – in collaboration with EY

- Led a year-long organization-wide audit engagement with EY, collaborating across AppSec, Cloud, and Infra teams to **close 80% of findings** and elevate security posture to meet ISO/NIST benchmarks.
- Skill Used: Leadership, Communication

API Security with AKAMAI

- Led end-to-end integration of Akamai API Security for 30+ critical APIs, enabling real-time protection against BOLA, injection, and credential abuse while **reducing API-related incidents by 65%**; implemented granular

threat detection and access control policies to block 200+ anomalous requests daily.

- Tools Used: AKAMAI API Security, JIRA

Web Application Firewall with AKAMAI

- Deployed and fine-tuned Web Application Firewall (WAF) using Akamai WAF, creating custom rulesets to block SQLi, XSS, and bot attacks; **reduced malicious traffic by 80% across 33 production applications**.
- Tools Used: AKAMAI WAF, XML

Educations

Dr. A. P. J. Abdul Kalam Technical University, B.Tech in Computer Science & Engineering — Aug 2017 – Aug 2021

Achievements

Certified Practical Ethical Hacker, CISSP

A Self-Motivated Accomplished Person with good knowledge on cyber security, Application security and DevSecOps with experience of little over 9 years.

Work History

2024-03 - 2024-10

Technology Lead

Broadridge, Bangalore

- Collaborated with cross-functional teams to assess application security postures, identify critical vulnerabilities, and spearhead targeted remediation efforts across a diverse application portfolio, resulting in a 30% reduction in security risks and significantly strengthening the organization's overall security framework.
- Led shift-left security initiatives by integrating security practices early in the software development lifecycle (SDLC), which resulted in a 20% decrease in security-related issues during development and improved risk mitigation for high-priority applications.
- Spearheaded the mitigation of BitSight findings by recommending and implementing strategic solutions, achieving 100% remediation within set timelines and contributing to significant improvement in the organization’s public security rating.
- Collaborated with development teams to identify and resolve bottlenecks in the remediation process for vulnerabilities identified in security testing, proposing alternative solutions that were aligned with business objectives and accelerating vulnerability resolution by 25%.
- Engaged with newly acquired product teams to assess and address their security needs, ensuring seamless integration of security protocols and reducing time-to-compliance by **10%** for new product rollouts.

2022-05 - 2024-01

Associate Manager

Atos-Paladion, Bangalore

- Lead Secure code review team to ensure smooth delivery of the projects
- work as an SME/SPOC for the clients and aid with remediation of issues reported during the security assessments.
- Perform security assessments on Web, Mobile and API assets of the organization.
- overseeing subordinates and aiding them by providing necessary support

Mohanvamshi Kodali

Technology Lead

Contact

Address
Hyderabad India

Phone
7093662106

E-mail
mohanvamshi.kodali@gmail.com

Skills

- Web Application Security
- Mobile Application Security
- Secure Code Review
- Threat modelling
- Network pentest
- Basic understanding of DevSecOps
- Java based applications development knowledge
- Organizing CTF event
- Experience in zero-day hunting

Tools

- BurpSuite
- Postman
- Checkmarx
- Fortify
- IriusRisk
- Nessus
- Archer EGRC tool
- MobSF

2020-09 - 2022-04

SSE- Application Security Analyst

Ivitesse, Hyderabad

- Perform application security assessments.
- Perform threat modelling to identify security issues in the products early in the SDLC phase
- work with issue remediation team to manage the already reported security issues

2019-04 - 2020-05

Senior Software Engineer

Loginsoft, Hyderabad

- Perform Grey-Box assessments of web applications
- Worked on CVE deep-dive process to ingest data into Nexus tool
- Take part in CVE hunting occasionally

2017-10 - 2019-03

Cyber Security Analyst

NseIT, Mumbai

- As part of ISRC team I was posted at a client location
- At client location my job role includes performing grey box assessment of web applications
- Perform SAST scans using MicroFocus fortify tool.

2016-10 - 2017-10

Security Analyst

Paladion Networks, Mumbai

- Perform Security assessments of web and mobile applications
- Organize CTF activities.
- Monitor Cyber security drills organized as per RBI guidelines

2015-10 - 2016-10

Research Associate

Team Lease (IDRBT), Hyderabad

- As part of Cyber Security Team my roles include Developing intentionally vulnerable web applications to host cyber drills as per RBI guidelines.
- Perform grey box assessments for small and medium scale banks.
- Manage IB-Cart Portal, which is a platform for all banks to share security incidents

Education

2010-06 - 2014-06

Bachelor of Technology: Computer Science

Bomma Institute of Science and Technology - Khammam

Accomplishments

- Achieved a CVE (CVE-2020-21142) for reporting a vulnerability in open-source software.
- Received an acknowledgement from Dell for reporting a security issue in their website
- Received an acknowledgement from Lenovo for reporting a security issue in their website
- Received acknowledgement from Intel for reporting security issues on their website

Bhagya Laxmi K

Sr. Security Analyst-L1

Email: bhagyalk.5570@gmail.com
Contact: +91 8712374884

Career Objectives:

Information Security professional seeking a career position within an organization, where my professional experience, education and abilities would be an advantage for the growth of employer and myself.

Professional Summary:

- Over all 4**+** years of experience in Information Security and currently working as Security Analyst (Security Operation Centre team)
- Hands on experience on Threat analysis, Remediation of malware and **Security monitoring and Operation.**
- Experience on **SIEM (Security Information and Event Management) tools** like Monitoring real-time events using **IBM QRadar, Splunk** tools and SentinelOne.
- Preparing daily, weekly and monthly reports as per client requirement.
- Investigating and creating cases for the security threats and forwarding it to the Onsite SOC team for further investigation and action.
- Experience on performing log analysis and analysing the crucial alerts on an immediate basis.
- Filling the Daily health checklist.
- Installation of Application Software and Antivirus software.
- Installing Operating Software such as Windows.
- Good knowledge on networking concepts including OSI layers, subnet, TCP/IP, ports, DNS, DHCP etc.
- Good understanding of security solutions like Firewalls (Palo alto, checkpoint, Fortinet, Cyber am), DLP, Anti-virus, IPS, Email Security etc.
- Hands on experience with Q radar SIEM tool for logs monitoring and analysis.
- Training: Security plus, SIEM (Q radar SIEM), Incident Life cycle.

Work History:

Sr.SECURITY ANALYST– 08-03-2021 To Till date

Client: Tata Communications Limited, Hyderabad

Responsibilities:

- Monitoring security alerts using Splunk SIEM.
- Analysed Phishing emails and performed IOC-based triaging.
- Created and escalated incidents based on severity levels.
- Followed runbooks and SOP's for incident response
- Performed log correlation and trend analysis.

- Served as Security Analyst in SOC operations for real-time monitoring, analysing logs from various security/Industrial appliances by using HP ArcSight ESM console, ArcSight Logger and troubleshooting of logging issues.
- Administering various incidents/security alerts triggered in the SIEM tool.
  • Responsible for log & event analysis, incident investigation, reporting.
  • Responsible for Integration of OS logs from windows and Unix flavoured (RHEL/HPUnix/CentOS).
  • Integrating new Devices with SIEM (IBM QRadar) along with Database to collect real time logs.
  • Troubleshooting log source devices for any issues on log collection.
  • Case study and Implementation of basic correlation rules.
  • Creation of reports, dashboards and rules fine tuning.
  • Determine the scope of security incident and its potential impact to Client network, assessment of risk; recommend steps to handle the security incident with all information and help them to mitigate the risks and threats.

Messaging Gateway TrendMicro IMSVA –

• Monitoring and sending alerts of inbound the threats detected by DDI and escalating to the respective team.
• Checking email sender's reputation and accordingly set bad and good sender list to restrict the access.

Anti-DDOS - Radware DefensePro

• Monitoring the Radware and analyzing threats.
• Blacklisting and Whitelisting IP's on Radware based on business requirement.
• Analyzing the Weekly/Monthly Reports.

Anti-APT – Trend Micro DDI, DDA

• Monitoring and sending alerts of inbound the threats detected by DDI and escalating to the respective team.
• Detecting the C&C Communications and Lateral movements.

Incident Management
• Raised incidents or service requests through HP Service Manager and get it closed by follow ups with respective teams

Team Supervision
• Leading & monitoring the performance of team members to ensure efficiency in operations and to meet organisational targets.
• Identifying and implementing strategies for building team effectiveness by promoting a spirit of cooperation within the team.

- Recognizing areas of improvements, organizing training programs and mentoring new team members.

Technical Skills:

- Application Security – Web Security
- **SOC** (Security Operation Centre)
- **SIEM** (Security Information and Event Management) Tool: **IBM Qradar, Vulnerability Assessment** Phishing Email Analysis, NMAP, TrendMicro and Anti DDOS , SPLUNK, ArcSight
- **EDR Tools:** Sentinel One, Crowd Strick
- **Ticketing Tools:** Service Now
- **OS Knowledge:** ,Linux
- **Protocols:** TCP/IP,DNS,HTTP,SMTP
- **Others:** MITR ATT&CK,IOC Detection, Email Header Analysis
- Create, Modify and Update Security Information Event Management (SIEM) Tools.
- Perform Cyber and Technical Threat Analyses.
- Monitoring for external threats and alerting Client's IT groups regarding intrusions or suspicious activity.
- Threat hunting for security loopholes and security incidents with various threat hunting tools.
- Managing the incidents created and follow ups till closure of security incidents on manage Engines portal.
- Preparing Monthly and Weekly reports.
- Preparing Run Books, SOP, Advisory.
- Firewalls and network security principles

BAJAJ ALLIANZ GENERAL INSURANCE CO LTD, Hyderabad, INDIA **Period: Oct 2006 - Jul 2017**

Sr.ExecutiveData Analyst

Responsibilities:

- Assisted in the preparation of insurance portfolio reports, financial risk analyses, and premium collections tracking.
- Designed and implemented Excel-based automation tools to streamline data aggregation and reporting tasks.
- Conducted variance analysis and provided insights into claims trends, underwriting performance, and loss ratios.
- Coordinated with underwriting and claims teams to provide accurate data for regulatory compliance and business forecasting.

- Responsible for the allocation of insurance expenses and analysis of data for insurance renewals.

- Accounted for all invoices and their monthly portions of expense.

- Allocated insurance premiums to cost centers based on risk exposures by using various models.

long-term debt and long-term leases. Performed various other responsibilities.

- Performed quality review audits of the various areas within credit operations.

- Assisted in ensuring adherence to the established procedures/regulations.

- Analyze output from audits and be proactive in researching areas of concern by following through on analysis and making suggestions on improvements.

- Measured and reported the progress of credit operations toward the realization of the service level goals set by management.

- Made independent decisions regarding the performance of representatives monitored.

- Took ownership of unresolved customer issues and followed through to completion.

- Compiled and analyzed information and data in order to give feedback to the necessary departments.

- Responsible for daily sales analysis by product sales channel.

- Managed marketing incentive program reporting, producing accurate and timely list pulls on all compliance sales communications.

- Improved rewards point process efficiency by 93% thru process requirements gathering, design, development, testing, and automation of an access database.

- Provide Daily status updates to higher management along with participation in weekly defect review meetings with team members through ou A.P, Telangana and Odisha.

- Generating & compiling the detailed MIS reports daily.

- Created quantitative and statistical business models by using MS-Excel's data analysis program, statistical and financial functions.

- Coordinate with the team to resolve the issues pertaining to RTM & MIS.

- Coordinating with Teams, to get the issues Resolving, follow ups, Updating the Clients on time.

- Preparing and updating the IMD data as per requirement for H.O (Related Codes issuance) by coordinating with Relationship Managers.

- Coordination and follow-ups with Clients, vendors etc.
- Management and coordination with internal and external Clients for all lines of business.
- Handling and conducting meetings with internal/external Clients.
- Related reports maintenance / MIS / Claims MIS all over Business.

Technical Proficiency

- MS Office(Excel, Word, Power Point)
- Power BI, Power Platform
- Excel (Macros, Pivot Tables, Look up's)

Soft Skills

- Analytical Thinking
- Problem-Solving
- Communication & Presentation
- Team Collaboration
- Time Management

Education:

- ➢ Masters: Master of Business Administration from Osmania University, Hyderabad, INDIA - 2005.
- ➢ Bachelors: Bachelor of Science in Computers from Osmania University, Hyderabad, INDIA – 2003.

Personal Details:

Father Name	:	K.Sathaiah
Date of Birth	:	04-04-1981
Languages	:	English, Telugu ,Hindi
Address	:	H.No:3-3-67/A, Baghameer, Kukatpally, Hyderabad..

Declaration:

I Bhagya Laxmi declare that the above-mentioned information is correct to the best of my knowledge and belief.

Place:Hyderabad Signature

K.BhagyaLaxmi

Vijay Bandari

Cyber Security Researcher | Malware Analyst | SOC (L2)

Hyderabad, Telangana vijaypbandari@gmail.com

Phone: 9581519018, 7702543272

LinkedIn: https://www.linkedin.com/in/vijay-bandari-a65413193/

Aspiration

Seeking a dynamic environment that will enhance my expertise in Cybersecurity with 5.3 years of related experience, I am eager to secure a challenging role where I can leverage my skills to achieve and surpass organizational objectives. Envisioning a rewarding position offering continual learning opportunities and challenges, I aim for a role that fosters both personal and professional advancement.

Professional Experience

LTIMindtree, Hyderabad, Telangana, India Feb 2023 – Present

Cyber Consultant

Extensively engaged in the identification and comprehension of various malware types and their delivery techniques. Responsibilities include providing investigation, triage, and mitigation for detected security events. Additionally:

- Working on Static and dynamic analysis of PE & Non-PE samples.
- Determining samples and adding detection in AV signature.
- Validation of determination by other researchers from different teams.
- Working on FP and FN alerts for determination and validation.
- Working on samples belonging to different environments such as Windows, Linux, Android, MAC OS, Java.
- Analyzing different scripts such as batch, python, ruby, powershell, JS, XML, HTML, PHP, etc.
- Analysis of Microsoft office related documents (File types such as doc, docx, xls, ppt, etc)
- Writing static/generic signatures for Malware, PUA (Potentially Unwanted Applications), UWS (Widely known as Riskwares) samples.
- Working on different client tasks which includes signature analysis, Signer Hash analysis and specific malware families for better coverage of Automation.
- Working on testing, integration of Copilot with Microsoft Defender.
- Collaborated with a team of Microsoft for development of a tool, used for determination of samples and also enabling researchers in sample analysis by providing scan results of Microsoft as well as third party AVs, vital metadata about sample.
- Conducting sessions on malware campaigns such as Whispergate, Qakbot, etc. for almost 4 teams with 100% capacity.
- Training of new joiners/juniors on file analysis and signature writing.
- Working with packed samples such as UPX, MPress, Themida, Enigma, VMProtect, etc., and AutoIT samples as well.
- Reviewing technical reports of different determination provided by client and performing Vulnerability Assessments on the same.
- Providing Network Security protocols focusing on protecting industrial control systems (ICS) and operational technology (OT) from cyber threats, ensuring the safety and reliability of critical infrastructure like power grids and manufacturing plants.
- Reviewing different Pull request of signatures before publishing and documenting all the reports.

Mindtree Ltd. – Hyderabad, India

EDR | Threat Researcher Feb 2022- Feb 2023

- Served Part of the Security Researcher team as a Microsoft Defender for Endpoint (EDR).
- Analyzing machine event data to identify False Positives (FP) and True Positives (TP), and creating reports based on analysis.
- Writing suppression rules to mitigate False Positives and fine-tuning False Positive detectors.
- Recommending changes to the source code of EDR detectors to address False Positives.
- Creating new EDR detections and triaging False Negatives for undetected suspicious or malicious threat campaigns.
- Testing newly developed detectors across various scenarios and telemetry to assess detection quality before production.
- Actively hunting for advanced targeted attacks using large datasets and Microsoft's Threat Intelligence IOCs.
- Involved in various stages of incident response, including in-depth analysis and Root Cause Analysis (RCA) submission on security incidents.
- Hands-on experience with network management solutions and firmware updates.
- Emulating APT group behaviours and attacks to validate detections and align them with the ATT&CK framework.
- Handling customer and client detection issues, providing prompt and accurate feedback.

Tollplus India Private Ltd., India

CSA System Analyst Nov 2019 - Nov 2021

To review the higher-priority security incidents escalated by triage specialists and do a more in-depth assessment using threat intelligence tools.

- worked round the clock in a security operations centre.
- Using OSINT tools to investigate harmful phishing emails, domains, and IPs. Then, depending on your findings, suggest appropriate blocking.
- Surfing security blogs to explore emerging and changing threats and vulnerabilities.
- To conduct security testing, use vulnerability assessment tools like Nessus and NMAP.
- Conducting real-time monitoring of URLs and traffic behaviour, making daily adjustments to database records through CRUD operations based on analysis.
- Re-scan systems to prevent new infections. Return systems to the network if there are none.
- Using Splunk for log analysis.
- Performed the high level Gap and Risk assessments in the process.
- Examine DNS, web, email, and firewall logs to find and stop attack attempts.
- Developed and optimized automation rules and playbooks within SIEM, analysing cybersecurity data to identify trends and collaborating with management to develop service improvement strategies.

Key Skills

- Malware Analysis - Developed and implemented new methods of detecting and analysing malicious activity, leveraging knowledge of malware, network security, reverse engineering, and digital forensics. Writing signatures for intended files.
- Email and URL analysis - Scan suspicious emails for malicious content by isolating and implementing ways to harden frames and reduce their attack surface.
- Vulnerability Assessment - Being adept in discovering vulnerabilities, misconfigurations, and possible attack vectors creating in-depth reports that identify weaknesses in security.

- Incident Response and Digital Forensics – Investigating and analyzing evidence and Classify security events, conduct indepth forensic analysis, and suggest appropriate course of action, and coordinate incident response activities. To ensure efficient incident handling, create and maintain standard operating procedures for the Security Operations Center (SOC).
- SOC – Well versed in cryptographic techniques, IDS, IPS, Network security, Splunk, Firewall, Arcsight, Incident handling and documentation. Knowledge and experience working with various security tools like SIEM, EDR tool, WAF, Email Protections tools, etc
- Well versed in Network security concepts.

Education

- Bachelors in Computer Science (July 2015 - August 2019) Osmania University
- Board Of Intermediate Education (2013 - 2015) NRI Academy

Certifications:

Certified Ethical Hacker (CEH)

Secure Delivery for Infrastructure Security

Protecting Cloud Infrastructure

Essential Incident Response

Securing Infrastructure Architecture

Achievements:

- Recognized as a “STAR PERFORMER” during 2023 and 2024 annual awards in LTI Mindtree.
- I was a recipient of the coveted “TOP PERFORMER” award for efficiently performing QC checks in Mindtree.
- Worked in CDC (Cyber Defence Centre) in RED team and blue team. Knowledge in OWASP Top10 vulnerabilities.

Personal Profile:

- Date of Birth : 17th February 1997
- Languages Known : English, Telugu and Hindi

Declaration: I hereby declare that all the information furnished above is true to the best of my belief.

Place: Hyderabad

Bandari Vijay.

Kasireddy Bala Naga Mounika

Cyber Security Engineer

Mounikakasireddy13@gmail. +91 9603344839 Hyderabad, India

https://www.linkedin.com/in/bala-naga-mounika-kasireddy-496862225/

PROFESSIONAL SUMMARY

Dedicated Cybersecurity Professional with **3 Years** of proven experience in penetration testing and vulnerability assessments across various environments. Proficient in utilizing industry-standard tools and techniques to identify and mitigate security risks. Strong communicator adept at collaborating with cross-functional teams to enhance security posture and ensure compliance with relevant standards.

SKILLS

Burp suite | Nessus | Nmap | Wireshark | Python | Metasploit | Kalli Linux | SonarQube

WORK EXPERIENCE

- **Capgemini, Hyderabad - Software Engineer** December 2021 – Present

PROJECTS

Guruland

December 2023 - Present

Client: PropertyGuru Groups

Role: Security Testing

Roles and Responsibilities

- Conducted regular scans and assessments of applications and systems to identify security vulnerabilities, prioritizing remediation based on risk analysis.
- Collaborated with cross-functional teams to implement patches and mitigations, reducing vulnerability exposure by 80%.
- Developed and maintained vulnerability reporting processes, providing stakeholders with insights into security posture and remediation progress.
- Implemented SAST tools to analyze source code for security vulnerabilities during the development lifecycle, improving early detection and remediation efforts.
- Provided training and support to development teams on secure coding practices based on SAST findings, leading to a 80% reduction in vulnerabilities in new releases.
- Utilized SCA tools to identify vulnerabilities in third-party libraries and open-source components, ensuring compliance with licensing requirements.

ICCI Application August 2022 – December 2023

Client: ICCI

Role: GUI /Pentesting.

Roles And Responsibilities

- Conducted comprehensive penetration testing of the Icci application, identifying security vulnerabilities across various components.
- Utilized a combination of automated tools and manual techniques to assess potential security risks and provided detailed reports on findings.
- Collaborated closely with development and operations teams to assist in the remediation of identified vulnerabilities, ensuring timely resolution and compliance with security standards.
- Developed risk assessment strategies to prioritize vulnerabilities based on potential impact, enhancing the overall security posture of the application.
- Documented testing processes and findings, presenting complex technical issues in an understandable manner to non-technical stakeholders.

CAREER HIGHLIGHTS

- Received the Wow Award from Capgemini management as part of annual appreciation for outstanding contributions to project success and team collaboration.

EDUCATION

Bachelor of Technology in Information Technology,
Qis institute and Technology, 2021

Varun Kumar Y

Phone Number: *8790550540* Mail Id: Varun.cs2022@gmail.com

SUMMARY

- 3.5 years of experience into IT and 2.2 years of experience into security testing (Web applications, Mobile Applications, Api, Network)
- Conducted vulnerability assessment of multiple servers and network devices.
- Assisting in review of business solution architectures from security point of view which helps avoiding security related issues/threats at the early stage of project
- Coverity and verifying vulnerabilities to eliminate false positives
- Learned Agile environment based on CI/CD and using development approach.
- Skilled using Various Tools for web application penetration tests such as **Burp Suite, OWASP ZAP, Wireshark, Nmap, Nessus.**
- Proficient in understanding application-level vulnerabilities like **XSS, SQL Injection**, **authentication bypass, weak cryptography, Session Management**, etc.
- Skilled in executing **OWASP top 10 test cases**.
- Learned application architecture review form few projects.
- Mentoring and training the team members/interns on application vulnerability assessment
- Publishing monthly dashboards, taking follow up for closure of vulnerabilities.
- Manual web application penetration testing using Burp Suite.
- Proficient in identifying application-level vulnerabilities like **XSS, SQL Injection, CSRF, IDOR, Authentication & Authorization bypass and Cryptographic flaws** etc.
- False positives removal by analysing the results from automated scanners.
- Reporting the vulnerabilities with evidences, business impact and remediation steps.
- Used Nessus and Nmap to perform network wide security assessments.
- Provided details of the issues identified and the remediation plan to the stakeholders.
- Using standards like **CVSS** (Common Vulnerability Scoring System) to provide the severity (Critical, High, Medium, Low) rating to the vulnerabilities identified.
- Reporting the identified issues in the industry standard framework.
- Learned security assessments (Web Based Applications, Web services, Penetration Testing and Vulnerability Assessment.)
- Update with the new hackings and latest vulnerabilities to ensure no such loopholes are present in the existing system.
- A self-starter with a positive attitude, willingness to learn new concepts and accept challenges.

EDUCATION DETAILS

Master's (Cybersecurity) Royal hollway university of London. 2022 to 2024.

Professional Experience

Worked as Jr. consultant, in Capgemini from April 2022 to Dec 2022.

Workedd as Trainee in KPMG From Nov 2019 to March 2022.

Key projects

Client: Life Insurance

Roles & Responsibilities:

- Conducted web application penetration testing on business applications
- Perform infrastructure security assessments by analysing the networks, enumeration of services on hosts and identify vulnerabilities.
- Exploitation of identified vulnerabilities in network hosts by using existing exploits or manual methodologies.
- Manual web application penetration testing using Burp Suite.
- Proficient in identifying application-level vulnerabilities like XSS, SQL Injection, CSRF, IDOR, Authentication & Authorization bypass and Cryptographic flaws etc.
- False positives removal by analysing the results from automated scanners.
- Reporting the vulnerabilities with evidence, business impact and remediation steps.
- Responsible for timely delivery of status updates and final reports to clients.
- Work closely with developers and network/system administrators while fixing the findings.
- Vulnerability management by keeping track of reported issues and ensure fixing.

Client: E-Commerce

Roles & Responsibilities

- Using web application vulnerability scanners to perform automated assessments.
- Manual penetration testing of the applications to identify vulnerabilities based on OWASP standard.
- Manual web application penetration testing using Burp Suite.
- Performed security testing on **APIs using Postman**.
- False positives removal by analysing the results from automated scanners.

Using standards like **CVSS (Common Vulnerability Scoring System) to provide the severity (Critical, High, Medium, Low)** rating to the vulnerabilities identified

DECLARATION

I consider myself familiar with all above mentioned aspects. I am also confident of my ability to work in a team. I hereby declare that the information furnished above is true to the best of my knowledge.

Varun Kumar Salibindla

Phone Number: *7093146957* Mail Id: VarunKumar.cs2021@outlook.com

SUMMARY

- 3 years of experience into security testing (Web applications, Mobile Applications, Api, Network)
- Conducted vulnerability assessment of multiple servers and network devices.
- Assisting in review of business solution architectures from security point of view which helps avoiding security related issues/threats at the early stage of project
- Coverity and verifying vulnerabilities to eliminate false positives
- Learned Agile environment based on CI/CD and using development approach.
- Skilled using Various Tools for web application penetration tests such as **Burp Suite, OWASP ZAP, Wireshark, Nmap, Nessus.**
- Proficient in understanding application-level vulnerabilities like **XSS, SQL Injection**, **authentication bypass, weak cryptography, Session Management**, etc.
- Expertise in Attack surface management to mitigate the Risk from cyber criminals.
- Skilled in executing **OWASP top 10 test cases**.
- Learned application architecture review form few projects.
- Mentoring and training the team members/interns on application vulnerability assessment
- Publishing monthly dashboards, taking follow up for closure of vulnerabilities.
- Manual web application penetration testing using Burp Suite.
- Proficient in identifying application-level vulnerabilities like **XSS, SQL Injection, CSRF, IDOR, Authentication & Authorization bypass and Cryptographic flaws** etc.
- False positives removal by analysing the results from automated scanners.
- Reporting the vulnerabilities with evidences, business impact and remediation steps.
- Used Nessus and Nmap to perform network wide security assessments.
- Provided details of the issues identified and the remediation plan to the stakeholders.
- Using standards like **CVSS** (Common Vulnerability Scoring System) to provide the severity (Critical, High, Medium, Low) rating to the vulnerabilities identified.
- Reporting the identified issues in the industry standard framework.
- Learned security assessments (Web Based Applications, Web services, Penetration Testing and Vulnerability Assessment.)
- Update with the new hackings and latest vulnerabilities to ensure no such loopholes are present in the existing system.
- A self-starter with a positive attitude, willingness to learn new concepts and accept challenges.

EDUCATION DETAILS

B Tech - HINDUSTHAN UNIVERSITY (2018 – 2022).

Professional Experience

Working as SECURITY ANALYST, in Cognizant from May 2022 to Till Date.

Certifications

- Azure Security Engineer Associate (AZ 500) – Issued by Microsoft
  Issued : June 2024 – June 2025
- Google Associate Cloud Engineer - Issued by Google
  Issued : May 2024 – May 2022
- Ethical Hacking Essentials (EHE) – Issued by EC-Council
  Issued : Feb 2024
- Network Security and Database Vulnerability - Issued by IBM
  Issued : Aug 2020

Key projects

Client: Life Insurance

Roles & Responsibilities:

- Conducted web application penetration testing on business applications
- Perform infrastructure security assessments by analysing the networks, enumeration of services on hosts and identify vulnerabilities.
- Exploitation of identified vulnerabilities in network hosts by using existing exploits or manual methodologies.
- Manual web application penetration testing using Burp Suite.
- Proficient in identifying application-level vulnerabilities like XSS, SQL Injection, CSRF, IDOR, Authentication & Authorization bypass and Cryptographic flaws etc.
- False positives removal by analysing the results from automated scanners.
- Reporting the vulnerabilities with evidence, business impact and remediation steps.
- Responsible for timely delivery of status updates and final reports to clients.
- Work closely with developers and network/system administrators while fixing the findings.
- Vulnerability management by keeping track of reported issues and ensure fixing.

Client: E-Commerce

Roles & Responsibilities

- Using web application vulnerability scanners to perform automated assessments.
- Manual penetration testing of the applications to identify vulnerabilities based on OWASP standard.
- Manual web application penetration testing using Burp Suite.
- Performed security testing on **APIs using Postman**.
- False positives removal by analysing the results from automated scanners.

Using standards like **CVSS (Common Vulnerability Scoring System) to provide the severity (Critical, High, Medium, Low)** rating to the vulnerabilities identified

DECLARATION

I consider myself familiar with all above mentioned aspects. I am also confident of my ability to work in a team. I hereby declare that the information furnished above is true to the best of my knowledge.

CONTACT

mariamal468@yahoo.in
Mariamal Ganesan | LinkedIn
+919600204297

EDUCATION

Bachelor of Engineering (CSE)
Anna University | 2020

CERTIFICATIONS

- CHFI | EC-Council Certification
- Certified Penetration Tester

TECHNICAL SKILLS

- General Tools: Confluence, Jira, ServiceNow, Sharepoint, Microsoft office.
- SBOM Tools: Blackduck, Finite State
- Proxies/Sniffers Tools: Burp Suite, OWASP ZAP
- Source Code Review: SonarQube & Sonarcloud, Dependency checker
- Malware Analyzer: MetaDefender Cloud & Core.
- OS: Windows, Linux, Kali Linux
- Thread Model Tool: Microsoft TM

SOFT SKILLS

- Highly collaborative and customer service oriented
- working to solve complex Product Security related problems creatively
- Strong interpersonal skills, team player, service oriented
- Strong organizational, analytical, and communication skills.
- Hands on experience on project management skills.
- Ability to manage multiple tasks and priorities in a fast-paced environment

Mariamal Ganesan

Product Security Engineer with 4+ years of experience working in IT Security services organization. Committed to continuous improvement and contributing to team success. Works closely with security vendors, consultants and the wider security research community with the objective of ensuring that the company's security testing programs remain up to date, relevant and comprehensive.

EXPERIENCE

Product Security Engineer (Mid-Senior level) | Sep 2023 - Present
Hitachi Energy Technology Services Pvt Lmt, *Bangalore.*

- **Security Tooling:** Evaluated and implemented SAST/DAST/SCA tools, automating security testing within the SDLC.
- **Cross-Functional Security Integration:** Collaborated with Development, DevOps, and IT Security teams to integrate security early in the SDLC, prioritize security features/bugs, and ensure their implementation.
- **Vulnerability Remediation Ownership:** Owned the vulnerability remediation lifecycle for products, ensuring adherence to timelines, criticality-based prioritization, progress tracking, and process improvement; facilitated stakeholder alignment on delivery dates.
- **Security Policy & SDLC Integration:** Implemented security policies, standards, and guidelines to embed security into the SDLC design phase.
- **Product Release Support:** Provided comprehensive security support for all release types (Emergency, Maintenance, Standard), including digital code signing (PKI), malware scan report generation, vulnerability prioritization, threat modeling, security assessment review, and VAPT execution.
- **Vulnerability Exception Management:** Managed and documented exceptions for identified vulnerabilities when necessary.
- **Global Team & Multi-Project Management:** Collaborated effectively with a US-based global team, managing 10+ concurrent product and work streams.
- **Incident Response & Remediation:** Assisted in application security incident response, including root cause analysis and defining remediation strategies.

Product Security Engineer (R&D group) | Dec 2021 - Sep 2023
NEC Corporation India Pvt Lmt, Bangalore.

- Conducted in-depth security assessments and evaluations of proposed security solutions across various domains.
- Developed and maintained comprehensive benchmarking criteria and methodologies for evaluating security solutions based on features, functionality, performance, pricing, and vendor support.
- Leveraged industry resources like Gartner, Forrester, and vendor websites to identify and analyze competitive solutions.
- Performed comparative analyses of security solutions, identifying strengths, weaknesses, and areas for improvement.
- Prepared detailed reports and presentations summarizing findings, recommendations, and ROI analysis for executive-level decision-makers.

Penetration Tester Intern | April 2021 - Nov 2021
Invesics Cyber Forensic LLP, *Ahmedabad.*

- Performed regular penetration testing on internal applications, including vulnerability scans and manual assessments.
- Sharpened analytical skills by accurately identifying and eliminating false positives from automated vulnerability scanning reports.
- Verified the effectiveness of implemented security patches by retesting applications after fixes were deployed.
- Created detailed vulnerability reports and communicated risks and remediation steps to relevant development teams.

NAFEESA A

LinkedIn

Email: anafeesa07@gmail.com
Mobile: +91 9176520647

EXPERIENCE

Cyber Security Analyst - Vulnerability Assessment Dec 2022 - Present
PrimEra Medical Technologies Hyderabad, India

Roles and Responsibilities:

- Facilitated the onboarding of newly acquired site devices for security scanning, ensuring all systems, endpoints, and infrastructure were integrated into the existing security framework for vulnerability assessments.
- Collaborated with IT teams to inventory and classify assets based on criticality and risk, facilitating a more efficient and prioritized scanning process across various environments.
- Configured and tailored Tenable scans to ensure targeted vulnerability assessments for newly onboarded devices, aligning scan profiles with device types and operational roles to enhance the accuracy of results.
- Analyzed scan results, prioritized vulnerabilities based on severity and potential business impact, and provided detailed reports to relevant stakeholders for timely remediation.
- Coordinated remediation efforts with Site IT teams, working together to ensure that vulnerabilities were addressed according to organizational risk tolerance and security policies.
- Developed and maintained risk register for vulnerabilities that could not be immediately remediated, documenting the risks, mitigation strategies, and justifications for deferred action, while ensuring ongoing monitoring.
- Generated regular vulnerability management reports for leadership, providing insights into the security posture of newly integrated assets and outlining progress on remediation efforts.
- Developed and implemented Python scripts to automate the vulnerability scanning process, streamlining the scheduling and reporting of scans, and significantly reducing manual effort while enhancing the efficiency and accuracy of vulnerability management.
- Provided ongoing KT to new team members by assisting in their training and development, sharing best practices in vulnerability management, scanning processes, and effective use of security tools to enhance team competency.
- Developed and maintained detailed documentation for security processes, configurations to ensure consistency and compliance with industry best practices and regulatory requirements.
- Developed and implemented a new process for external attack surface management, enhancing the organization's ability to identify, assess, and mitigate risks associated with exposed assets and potential vulnerabilities in the external environment.

Associate Cyber Security Analyst - Vulnerability Assessment Feb 2022 - Nov 2022
PrimEra Medical Technologies *Hyderabad, India*

Roles and Responsibilities:

- Provided hands-on expertise in configuring tailored Tenable scans for different devices including but not limited to Windows, Unix/Linux, network devices and other endpoint devices, ensuring targeted assessments and improving the accuracy of vulnerability detection.
- Analyzed scan results, prioritized vulnerabilities based on risk, and recommended actionable solutions to mitigate threats and strengthen defenses.
- Monitored and assessed emerging security threats and vulnerabilities, ensuring that the organization remained updated on evolving risks and promptly applied necessary patches or mitigations.

Associate Cyber Security Analyst - Network Security Sept 2021 - Jan 2022
PrimEra Medical Technologies *Hyderabad, India*
Roles and Responsibilities:

- Configured Fortinet Firewall rules to ensure a secure network environment, tailoring settings based on specific use cases and organizational needs.
- Implemented and maintained NAC policies to regulate access to the network, ensuring only authorized users and devices are allowed entry based on security compliance.
- Implemented website whitelisting/blacklisting policies to provide a controlled and safe browsing environment, enhancing both security and user productivity.
- Provided IT support to users across the organization, resolving technical issues remotely via ServiceDesk and ensuring quick turnaround on tickets through efficient troubleshooting and problem resolution.

INTERNSHIP

Cyber Security Intern Apr 2021 - Aug 2021
Valentia Technologies *Hamilton, New Zealand*
Roles and Responsibilities:

- Conducted comprehensive vulnerability assessments on internal network assets using a variety of open-source and commercial tools, ensuring a thorough evaluation of potential security risks.
- Mapped network services and ports across internal systems to detect potential exposure points and misconfigurations.
- Monitored emerging vulnerabilities and threats, recommending timely mitigation strategies and security patches to maintain the integrity of network assets.

EDUCATION

M.Sc. in Cyber Forensics & Information Security Jan 2022 - Present
Institute of Distance Education, University of Madras *Chennai, India*

B.Tech in Electronics and Communication Engineering Aug 2016 - Aug 2020
B.S. Abdur Rahman Crescent Institute of Science and Technology *Chennai, India*

TOOLS

- Tenable Security Center/Nessus, Qualys, Rapid7, Acunetix, Burp Suite, NMap, Wireshark, AMASS and various OSINT tools for Vulnerability Assessment and Management.
- MS Office Suite, Service Now, Service Desk, Zendesk, Jira and various ITSM tools.
- Windows, MacOS, Unix/Linux and its distributions.

SKILLS

- Understanding vulnerability management tools to enhance security.
- Using vulnerability data to drive decision-making.
- Problem-solving skills to improve assessment processes.
- Strong analytical and interpersonal communication skills.
- Engaging cross-functional teams on security objectives**.**

CERTIFICATIONS

- eLearnSecurity Junior Penetration Tester
- Certified Web Application Security Professional by Network Intelligence
- Fortinet’s Certified NSE 1, NSE 2, NSE 3 Network Security Associate

ABHISHEK CHAURASIYA

+918879722755
Gmail
Mumbai, Maharashtra
Linkedin

SUMMARY

Cybersecurity professional with experience in CTF challenges and internships, focused on penetration testing, network security, and vulnerability assessments. Proficient in Red/Blue Teaming, SQL Injection, and tools like Burp Suite and MITRE Framework. Dedicated to securing information systems and driving continuous improvement in cybersecurity practices.

TECHNICAL SKILLS

- Python
- JAVA
- Snort
- Imperva (WAF)
- Kali Linux
- Metasploit
- Wirershark
- CloudSEK
- Burpsuite
- Nmap
- OSINT's
- Qualys
- Nessus Community/Professional
- SQLi (SQL Injection)
- OWASP TOP 10/OWASP API
- Mimikatz
- Linux System Hardening
- Windows Hardening
- Active Directory Hardening
- Network Device Hardening

WORK EXPERIENCE

Protiviti Global Consulting Pvt Limited

Consultant 2 in Security and Privacy ***(Client: AB-InBev)*** • November 2023 - Present

- **Troubleshot** and **resolved complex client issues** related to **External DNS**, including **DNS record misconfigurations** and **propagation delays**.
- **Optimized DNS infrastructure** by implementing **DNS load balancing** and **failover strategies** to ensure high availability and reliability.
- Collaborated with clients to secure DNS services against **DNS spoofing**, **cache poisoning**, and **DDoS attacks**, utilizing techniques like **rate-limiting, geolocation blocking, and filtering.**
- **Configured geolocation-based policies, ACLs,** and DNS-based firewall rules to restrict access to specific regions or IP addresses, improving client security posture.
- Managed and configured Imperva WAF to protect client websites from **OWASP Top 10 vulnerabilities, SQL Injection, Cross-Site Scripting (XSS), and DDoS attacks.**
- Composed rules for **optimizing Cloudsek's fraud prevention** and monitoring tools, **enhancing detection and response capabilities.**
- Analyzed WAF logs and traffic patterns to detect and mitigate evolving cyber threats; **successfully blocked 90% of potential attacks** by fine-tuning security rules.
- Implemented **vulnerability management** protocols using **Qualys**, effectively **mitigating high and medium-risk vulnerabilities**.
- Implemented and maintained **threat mitigation policies** to defend against **credential stuffing**, **web scraping**, and **bot attacks**, enhancing website security and performance.

CyberNX Technologies Private Limited

AppSec Intern(VAPT) • August 2023 - November 2023

- Developed reports **documenting** the findings for **Vulnerability Assessment and Penetration Testing(VAPT)** and offered **remediation** recommendations.
- Utilized **automated tools** and **manual pen-testing** for potential security vulnerabilities.
- Utilized tools such as **Burpsuite Professional**, **Nessus Professional**, and **OSINT** for Vulnerability Assessment and Penetration testing.
- Conducted **Black Box**, **Grey Box**, and **White Box** Testing on various projects, including those involving **Zero Trust Security**, **Intranet**, and **Web Applications**.
- Conducted security assessments and generated a **Secure Configuration Report** to ensure compliance with information security laws.

Skills and Expertise

- Participated in various **Capture The Flag (CTF)** challenges involving both **Red and Blue Teaming** and practical experience in **IoT Hacking**.
- Utilized tools such as **VirusTotal, Censys, and the MITRE Framework**.
- Implemented **SQL Injection techniques** on platforms like **Bug Bounty** and **CTF challenges**, covering **In-Band SQLi**, **Error-Based SQLi**, and **Union-Based SQLi**. Also investigated other injection methods, including **Blind SQLi** with **Authentication Bypass**, **Boolean-Based SQLi**, **Time-Based SQLi**, and **Out-of-Band SQLi**.
- Used **Burp Suite Community** to evaluate **OWASP Top 10** vulnerabilities, employing features like **Repeater**, **Proxy**, **Intruder**, **Decoder**, and **Comparer**.
- Engaged in **Privilege Escalation** CTF challenges, focusing on areas such as **Kernel**, **Exploits**, **SUDO**, **SUID**, **Capabilities**, **Cron jobs**, **PATH**, and **NFS**.

EDUCATION

Higher Secondary School Certificate

Bunt's Sangha's S.M.Shetty junior college, Mumbai, Maharashtra • **Grade - A**

Bachelor of Information Technology (B.E.IT)

Shree L.R.Tiwari Engineering • **Grade - A**

HOBBIES

- *Tech Enthusiast, Nature Lover, Puzzler, Gamer, Optimistic. CTF Player*

Achievements and Awards

- Certified by Tryhackme in ***Cyber Advent 2022*** & ***Cyber Advent 2021.***
- Top **1%** in **Tryhackme**.
- Published Final Year project in **IJRASET** for **Forest Fire Prediction System** using **Machine Learning**.
- Achieved certification in **Offensive Pentesting on TryHackMe**.

CERTIFICATION

- Offensive Pentesting
- Security Engineer

PROFILE

- *Tryhackme* & *IJRASET*

Lokesh Jakku

+91 7658961324 Lokesh0696@gmail.com

SUMMARY

Cyber Security Analyst with 4.8 years of professional experience and proven knowledge in penetration testing and vulnerability assessment of Web Application, Web Services, Mobile Application, Source Code Analysis with keen interpersonal, communication and organizational skills.

KEY SKILLS

Web Application Penetration Testing • Black Box Security Testing • White Box Security Testing • Static and Dynamic Application Security Testing • SAST • DAST • OWASP Top 10 • REST and SOAP API Testing • Source Code Analysis • Manual Testing • Automated Testing • Mobile Application Testing • Network Vulnerability assessment • Cryptography

TOOLS TECHNICAL PROFICIENCIES

• Burp Suite Professional • Fortify • POSTMAN • OWASP ZAP (Zed Attack Proxy) • Nmap • SQLmap • Frida • Objection • MOBSF • Nessus • Drozer •Apktool • JADAX • Dex2jar • Metasploit

PROFESSIONAL EXPERIENCE

Infosys, Hyderabad, India **February 2022- Present**

Role: Senior Associate Consultant

- Performed the penetration testing and Vulnerability assessment on Web applications, API's, Mobile security (Android & iOS) and network vulnerability assessment and source code review.
- Followed Industry standards methodologies of OWASP TOP 10 to meet the security compliance and performing the false positive manual analysis.
- Good Hands on experience of DAST and SAST analysis of Web application and Mobile applications and Source code review.
- Tools expertise on Burp suite professional/Community, Postman, OWASPZAP, NMAP, Nessus, MOBSF, JadxGUI, adb, Objection,Frida,3utools, grapefruit, Fortify and kali Linux.
- Proficient in creating detailed and clear reports on vulnerabilities. Review and evaluate the vulnerability reports and assessing and prioritizing vulnerabilities based on impact and exploitability.
- Collaborate with cross-functional teams, including developers and product managers, to understand project requirements and design effective test strategies.
- Experience in having client business calls to understand the requirement of security testing and providing the best solution and Participation of RFPS as well.
- Collaborated with the team mates to providing the knowledge on Security testing and validated the reports of final review.
- Ability to explore, learn and apply technologies to increase business prospects Quick learner, good at communication & Interpersonal Skills
- Worked in total 5 client's Security projects so far in Infosys

Paralok Information security, Hyderabad, India **June 2021 – Dec 2021**

Role: Information security analyst

- Conducted Penetration test on Business-Critical Web Applications, API's, Network assessment in Automated well as Manual (Using Burp Suite Professional) Manner (Plan, Discover, Attack, Report).
- Experienced in security testing on the Web Applications and Web Services and Good Manual analysis of the false positive analysis and business flows.
- Interacted with customers to understand their requirements and Queries.
- Managed whole penetration test activity from scheduling walkthrough call to Explaining discovered vulnerabilities to Developers and helping them to remediate.
- Proficient in identifying various critical vulnerabilities like RCE, SQL Injection, XSS, Code Injection, CSRF, IDOR, Session Hijacking, Authentication & Authorization Flaws, Remote & Local File Inclusion, Malicious File Upload, Business Logic Vulnerabilities and many more.

- Experienced in performing the static and dynamic analysis testing of Android and iOS applications using Mobsf, Drozer, Objection and SSL pinning attacks.
- Perform the network vulnerability assessment for the IP and Hosts by using the Nmap and Nessus tool and Metasploit.

OTP talenq Pvt Ltd, Hyderabad, India **March 2020 – April 2021**
Role: Intern as cyber security analyst

- Learned the new technologies of cyber security and work flow of the Business requirements.
- Learned the Usage of the security testing tools and methodologies.
- Performed the retest of the Fixes and existing Vulnerabilities for quarterly audit.
- Hands on experience on real-time project and submitted the reports of the findings.

CERTIFICATION: **Certified** in **Ethical Hacking** (**CEH**), **certified appsec practitioner (CAP)**

ACADEMICS:

Completed B.Tech in Electronics and Communication Engineering from Kakinada Institute of Technology and Sciences, affiliated to Jawaharlal Nehru Technological University- Kakinada, May -2017.

ANKUR VERMA

Location: Pune, Maharashtra, India | **Mobile:** +91 9716548996 | **Email:** hackankur@gmail.com | **LinkedIn:** https://www.linkedin.com/in/hackankur/

PROFESSIONAL SUMMARY

Experienced security professional with 7 years in application security, penetration testing, and vulnerability assessment across web, mobile, and thick client applications. Expertise in OWASP Top 10, security tools, manual testing methodologies, and client communication. Skilled in identifying, documenting, and remediating security issues, with proven experience in training and mentoring team members.

PROFESSIONAL EXPERIENCE

TIAA Global Capabilities | Associate | Pune | Jan 2024 - Present

- Performed security assessments on 70+ MDM and Intune mobile applications, including third-party apps, using tailored test cases to identify vulnerabilities across Android and iOS platforms
- Conducted end-to-end Android/iOS mobile app assessments using SAST and DAST, along with malware analysis in source code, uncovering vulnerabilities of varying severity
- Utilized specialized tools including NowSecure, MobSF, Frida, Jadx-Gui, Apktool, ADB, and Drozer to identify and report weaknesses across mobile builds
- Presented detailed vulnerability findings and remediation strategies to engineering teams and leadership, improving secure development practices
- Led onboarding and technical training for junior team members on mobile penetration testing methodologies
- Delivered regular security awareness sessions to internal users and customers (audience size: 10-250), contributing to measurable improvement in application security scores

Ernst and Young Global Services | Security Associate | Gurgaon | Apr 2021 - Dec 2023

- Performed end-to-end manual and automated VAPT on 90+ web, mobile, API, thick client, and browser extension applications, uncovering vulnerabilities across all severity levels
- Executed vulnerability scans using SAST/DAST tools, followed by manual validation to eliminate false positives and ensure high-fidelity findings
- Reviewed Minimum Security Baseline (MSB) controls and performed security assessments aligned with secure SDLC practices for backend and cloud-based environments
- Conducted thick client assessments using Eco Mirage, Wireshark, and Fiddler, targeting binary analysis, privilege escalation, DLL hijacking, and local storage vulnerabilities
- Created custom scripts and in-house Python tools to automate testing workflows, including a utility to download iOS IPA files directly from the App Store
- Delivered security architecture reviews during design phases to proactively identify flaws before development began
- Presented vulnerability impact, risk context, and mitigation strategies to developers, product owners, and leadership to drive secure coding practices
- Authored comprehensive security reports aligned with OWASP Top 10 and NIST 800-53, with tailored remediation plans for clients

Cyber Root Risk Advisory Pvt Ltd | InfoSec Associate | Gurgaon | Apr 2019 - Apr 2021

- Conducted risk assessments and vulnerability analysis across diverse domains including e-commerce, government, BFSI, hospitality, and CMS platforms
- Designed and executed proof-of-concept (PoC) testing, recommending tailored security solutions aligned with business requirements
- Identified critical vulnerabilities based on OWASP Top 10 standards, ensuring secure and compliant client application deployments
- Collaborated with technical teams to develop mitigation strategies during pre-deployment and production phases
- Interfaced directly with clients to explain security methodologies, assessment results, and remediation plans
- Performed static and dynamic application testing using Burp Suite and Acunetix, applying both manual and automated techniques
- Developed concise vulnerability reports and actionable remediation plans for rapid implementation

Goods and Service Tax Network | Desktop Support Engineer | Delhi | Nov 2017 - Jun 2018

- Provided desktop and endpoint support including patch management, F5 VPN configuration, and IP phone troubleshooting for government users
- Resolved IT issues, incidents, and service requests through ticketing systems, maintaining SLA compliance
- Diagnosed and repaired hardware and software issues across user devices, ensuring operational continuity

TECHNICAL SKILLS

- **Security Testing:** Web/Mobile/API/Thick Client VAPT, Risk Assessment, Browser Extension Security, Malware Analysis
- **Security Standards:** OWASP Top 10, NIST 800-53, ISO 27001
- **Tools:** Burp Suite, Nmap, Metasploit, Wireshark, NowSecure, MobSF, Frida, Objection, Jadx, ADB, Drozer
- **SAST/DAST:** Checkmarx, HCL AppScan, Qualys, Aquasec, Netsparker, Acunetix, OWASP ZAP
- **Programming:** HTML, PHP, Python
- **Operating Systems:** Kali Linux, Windows, iOS, Android

CERTIFICATIONS

- ISO 27001 Lead Auditor
- CNSS (ICSI)
- Network Security Associate 1 & 2 (Fortinet)
- C-DAC Certification

EDUCATION

- **PG Diploma in IT Infrastructure Systems and Security** | C-DAC, Pune | 2018 - 2019
- **B.Tech in Computer Science Engineering** | Accurate Institute of Management & Technology | 2012 - 2016

SHIVA PRASAD REDDY K

E-mail:shivaprasadreddy36@gmail.com LinkedIn: https://www.linkedin.com/in/shiva-prasad-reddy/ Phone: 7204459227

PROFESSIONALEXPERIENCE

Altruista Health Services Pvt. Ltd., Hyderabad, Telangana, India **Jan2020–Sept2022**

Software Engineer-1, SecOps Team, Engineering Department

- Testing Static Application Security of web application and API source code manually and using automated testing suites.
- Testing Dynamic Application Security of web applications and APIs using automated testing suites.
- Developing and maintaining a code security module in C# and .Net containing the secure implementation of commonvulnerable functions that can be utilized by developers.
- Automating activities related to Secure Code Analysis and integrating them with the DevOps pipeline Training newdevelopers in Code Security and Secure Coding Practices.
- Increased efficiency, usability, and accuracy of existing automation.
- Experience in using Veracode, Acunetix, Sonarqube, Burp Suite, TeamCity, OWASP ZAP, JIRA, Bitbucket,and Confluence.

Security Code Review Expertise

Performed detailed security code reviews to identify and address vulnerabilities, ensuring applications were secure against common threats like SQL injection, cross-site scripting (XSS), and insecure authentication. Used a combination of automated tools and manual techniques to evaluate code, align with security best practices, and comply with industry standards such as OWASP Top 10. Worked with development teams to provide recommendations and implement secure coding practices, improving the overall security and resilience of applications.

Cognizant **Sept 2022-Present**

Program Analyst, Malware Analysis

- Reverse Engineering and malware Analysis for the Android [Play-Store] Applications.

Key Skills

- Reverse Engineering, Static Analysis, Dynamic Analysis, Behavioral Analysis, Secure Code Review

Process

- Conducted static and dynamic malware analysis for apps flagged as suspicious on the Play Store.
- Identified vulnerabilities in applications and third-party libraries used by Android apps.
- Performed manual and automated code reviews to detect embedded malware.
- Monitored app network traffic to identify data exfiltration or unencrypted transmission of sensitive information.
- Delivered detailed technical reports on malware functionality and mitigation strategies.

INTERNSHIPS

BSNL RTTC Mysore **Feb2018**

Wireless Communication: Gained knowledge on working process of various technologies used in wireless communication in recent times.

INDUSTRIAL PROJECTS.

Code Security Analysis integration with Pipeline **July2020-February2021**

Objective: Analyze, incorporate, test, and implement a system into the CI/CD pipeline to scan the codes for Code Security flaws at early stages there by reducing vulnerabilities in the application

Technology/Tools Used: PowerShell, Veracode-Pipeline Scanner, Bitbucket

SecurityModule **Jan2020-May2020**

Objective: Develop a module that contains secure implementations of various C#/.Net functions and that can be consumed by alldifferent modules of the product.

Technology/Tools Used : C# , Java

Sonarqube Automation Module **Nov2021-Sept2022**
Objective: Develop an automation module that contains secure implementations of various C#/.Net functions and that can be consumed by all different modules of the product. And integrating it in CI/CD pipeline for better results.
Technology/Tools Used: Sonarqube, Teamcity.

Reverse Engineering in Malware Analysis **Sept2022-Present**

TECHNICALSKILLS

1. **Programming Language**: C#, .Net Framework, SQL, Power Shell, HTML, CSS, and Java.
2. **Technology/Techniques/Tools**: Veracode, Acunetix, Burp Suite, TeamCity, SonarQube, Quokka, HTTP Tool Kit.
3. **Software**: Jira, Bitbucket, Confluence.
4. **Operating System:** Microsoft Windows, Microsoft Windows Server.

Certifications

- CompTIA Security+(**SY0-601**)
- CISSP [**Certified Information System Security Professional**]

ACADEMIC QUALIFICATION

B.E [Electronic and Communication Engineering] **2015-2019**
Bellary Institute of Technology and Management (6.5/10 CGPA)

Nihal Tikka

Hyderabad
+918886669725 • nihaltikka@gmail.com

Professional Summary

Results-driven cybersecurity professional with over 5 years of experience in web application penetration testing, mobile penetration testing, and API security. Expertise in identifying and mitigating security risks across web applications, APIs, and mobile platforms. Proven track record of leading cross-functional teams to enhance security postures and delivering actionable insights that reduce potential security breaches. Passionate about continuous learning and contributing to the cybersecurity community.

Skills

- Web Application Penetration Testing
- Mobile Penetration Testing
- Vulnerability Assessment and Penetration Testing (VAPT)
- Collaboration with Cross-Functional Teams
- Security Tools: Burp Suite, SQLmap, Nmap, OWASP ZAP, Onapsis, Nessus

Work Experience

Senior Associate Consultant December 2022 - Present
Infosys

- Conducted in-depth web application penetration testing, mobile penetration testing, ethical hacking, API security assessments, and DAST using Burp Suite and Nessus, successfully identifying and exploiting 70+ security vulnerabilities, ensuring heightened security for clients.
- Performed DAST, source code review, and mobile penetration testing, identifying vulnerabilities in web and mobile applications, helping clients secure their platforms from potential exploits.
- Delivered detailed vulnerability reports with risk assessments, PoCs, and actionable remediation steps, leading to a 30% reduction in potential security breaches.
- Reduced false positives from automated DAST scanners through rigorous false-positive analysis, improving issue triage efficiency and resolution times.
- Collaborated with development teams to implement secure coding practices and conducted secure code reviews, achieving a 90% reduction in repeat vulnerabilities within 6 months.

Associate January 2020 - December 2022
Cognizant Technology Solution

- Conducted comprehensive Vulnerability Assessment and Penetration Testing (VAPT) for web applications, APIs, and mobile applications, identifying critical security vulnerabilities across different platforms.
- Executed penetration testing using industry-standard tools like Burp Suite, SQLmap, Nmap, and OWASP ZAP to uncover vulnerabilities in web applications and mobile environments.
- Delivered actionable insights in detailed vulnerability reports, complete with risk assessments and PoCs, resulting in a 30% reduction in potential security breaches.
- Reduced 60% of erroneous issues reported by automated scanners through rigorous false-positive analysis, streamlining issue triage and resolution processes.
- Collaborated with 20+ cross-functional development teams to remediate security vulnerabilities, driving swift resolution and enhancing the security posture of applications.

Certifications

- CEH Master
- Azure Security Engineer
- Purdue Applied Cybersecurity Essentials

Education

BTECH 2015-2019
JNTUH

- Coursework: Java, Computer Networks, Algorithms, Database Management Systems, Principles of Programming Languages, Operating Systems, Information Security

SUJITH BUDDHARAJU

Email: sujithbuddharaju@gmail.com **Phone**: +91-9160080708

Career objective

Cyber security professional with OSCP Certified and over 5+ years of proven industry experience involving in vulnerability and Penetration Testing. Seeking a challenging role to further enhance my expertise, and contribute to safeguarding critical systems.

PROFESSIONAL EXPERIENCE

Successive Digital
Senior Security Engineer (Dec 2024 - Feb 2025)
Client: US - Telecommunication

Roles and Responsibilities

- Conducted extensive penetration tests on applications and infrastructure to uncover security vulnerabilities.
- Performing automatic and manual network penetration testing using industry-standard tools.
- Automatic PT using Qualys and Qualys WAS for identifying and prioritizing security vulnerabilities.
- Manual PT leveraging Kali Linux, Metasploit , and Burp Suite for in-depth exploitation, and validation of discovered vulnerabilities.
- Communicated risk levels associated with vulnerabilities, aiding clients in informed decision-making regarding risk acceptance.
- Prioritized vulnerabilities based on OWASP Top 10 and SANS 25, guiding remediation efforts effectively.
- Trained junior staff on penetration testing methodologies and security best practices.
- My primary focus in offensive security is to identify vulnerabilities by thorough reconnaissance, vulnerability analysis and realistic exploitation while ensuring minimal disruption to business operations.
- Understanding the application flow and proficient in finding Business Logic Flaws.
- I tailor reports for different audiences by providing brief overview for non-technical stakeholders, emphasizing business risks and strategic recommendations, while including technical details and stepbystep guidance for IT and security teams.

KPMG

Assistant manager (Feb 2023 - June 2024)
Client: Public Sector Bank

Roles and Responsibilities

- In DAST, Performed VAPT for web, API, and mobile applications.
- Performing vulnerability assessment and penetration testing on Network Infrastructure.
- My primary focus in offensive security is to identify vulnerabilities by thorough reconnaissance, vulnerability analysis and realistic exploitation while ensuring minimal disruption to business operations.
- Identified critical vulnerabilities which include XSS, Authentication Bypass, Privilege escalations etc.
- Understanding the application flow and proficient in finding Business Logic Flaws.
- I tailor reports for different audiences by providing brief overview for non-technical stakeholders, emphasizing business risks and strategic recommendations, while including technical details and step-by-step guidance for IT and security teams.
- Working with stakeholders (Server Team, Network Team, and Application Team) to provide clarifications and remediation strategies on vulnerabilities reported.
- Conducting configuration reviews for Network Infrastructure and Database using CIS Benchmarks.
- In SAST, performing manual source code analysis for (CI/CD) pipelines, using tools Check Marx.
- Real time involvement with developer's team for change request/change management Timely delivery, clear communication to client and Quality review of deliverable.
- Peer review proactiveness to approach managers for proposals, business development works etc.
- Work on large or non-traditional proposals on client requirements.
- Assisted my team with internal cyber audits, Facilitated by RBI.
- Ran vulnerability and compliance scanning on test machines and reviewed security standard and Minimum Security Baseline for the client. Assisted on Monthly conference call to discuss implementation and upgrade of critical infrastructure.
- Collaborate, deliver professional offline presentations to the clients on cyber awareness, highlighting top vulnerabilities and associated tools.

APPSECCO

Security Consultant (Oct 2022 - Jan 2023)

Roles and Responsibilities

- Performed dynamic and static analysis of web application. Analyse systems for potential vulnerabilities that may result from improper system configuration, hardware or software flaws.
- Conducted white/grey box penetration testing on the financial systems using Kali Linux.
- Reviewed security documentation and make recommendation. Assisted in conference call meeting with Developer to mitigate vulnerability findings.
- Port scan servers using NMAP and close all unnecessary ports to reduce the attack surface
- Perform red-teaming attack simulations against external customer's networks
- Maintain persistence on internal networks for goal-oriented results, providing value by identifying
- Detailed attack chains that could be utilized by real attackers
- Complete in-depth research and development, establishing new approaches to ever-changing attack landscape
- Utilize new techniques to identify and exploit vulnerabilities in customer networks
- Create comprehensive and accurate reports and presentations for both technical and executive audiences.

Performed live packet data capture with Wireshark to examine security flaws. Used LDAP injections techniques of exploiting Web applications that use client supplied data

Aujas Cybersecurity

Consultant (Aug 2021 - Aug 2022)
Client: One of the Leading Stock Exchanges in India
Security Tools: Burp Suite Pro, HXD, Echo mirage, Process hacker, Wire shark, Nmap, Postman, Gidra, mobsf etc

Roles and Responsibilities

- Black box and Grey Box Assessment of Web Applications, Mobile, API and Thick client applications.
- Working with stakeholders (Server Team, Network Team, and Application Team) for the remediation of the vulnerability in remediating the vulnerabilities.
- Providing clarifications on the notified vulnerability.
- Delivering guidance and remediation actions to stakeholders by delivering clear, actionable suggestions based on their technical expertise
- Assist the development with source code to address the Security Requirement.
- Proficient in understanding and executing the application-level vulnerabilities attacks like – XSS, CSRF, Remote Code execution, SQL injection, SSRF, Session hijacking, Variable manipulation, LFI, RFI, Privilege escalation, Authorization Bypass.
- Creating proof of concept (POC) for the vulnerability findings and creating formal reports.
- Understanding the application flow and proficient in finding Business Logic Flaws.
- Recommend corrective measures and ensure the adequacy of existing information security controls. Develop risk remediation plans and security procedures.

Aspion Technologies Private Limited

Security Analyst (Jan 2019 – Jul 2021)
Client: largest ecommerce company in US.

Security Tools: Burp Suite Pro, Rapid7 AppSpider

Roles and Responsibilities

- Performed penetration testing for web applications using manual and automated tools.
- In total handled around 200+ Applications in Web application security, Mobile Appsec, API, Thick Client and penetration testing.
- Scheduled Scanning of Web application using Rapid7 AppSpider, accunetix.
- Identified critical vulnerabilities including Stored XSS, CSRF & Privilege Escalations etc.
- At the end, providing a detailed report with all explanations of vulnerabilities including POC's & relevant Screenshots.
- Ability to identify and resolve top OWASP security vulnerabilities.
- Excellent understanding of the web/Mobile application security Testing & secure code reviews.
- Identified business logic vulnerabilities and checked the resilience of application.
- Profound knowledge of vulnerability scans for DAST and SAST using App Spider & Checkmarx.
- Performed penetration testing for web applications using manual and automated tools.
- Conducting Vulnerability Assessment and Penetration Testing through manual or automated tools and providing the recommendations towards the mitigation of vulnerabilities.

DIGITAL PASTIMES

- Following security blogs and participating in professional events.
- Knowledge sharing through professional presentations.
- Engaging in continuous learning through certifications and training programs.

TECHNICAL SKILLS

- Passionate Skills : Red Teaming, Product security, Penetration Testing
- Web Vulnerability Scanners : Acunetix, AppSpider & Checkmarx
- Network Security Scanner : Nmap and Nessus
- Open Source Tools : Kali Linux, metasploit, Sublister, Assetfinder, Uniscan, OWASP ZAP
- Programming Languages : HTML 5, Python, JavaScript, PHP, Java
- Common Industry Standards : OWASP, SANS, NIST, ISO 27001, CIS

CERTIFICATIONS

- **OSCP** (offsec certified professional)
- **CEH V12** (certified ethical hacker – ECC6154278390)
- **eCPPT V2** (eLearnSecurity Certified Professional Penetration Tester)

EDUCATION

Rabindranath Tagore university – Bhopal, India 2016-2018
Master of Business Administration: Information Technology

MADHUR SHARMA

Ph.: +917018343280, 9459750604
Email: madhursharma3@gmail.com

LinkedIn Profile: https://www.linkedin.com/in/madhursharma7/

PROFESSIONAL SUMMARY

Experienced Cyber Security Professional with over 4 years of experience specializing in Cyber Security, Web Application Penetration Testing & API Security, Network Security and Vulnerability Assessment & Management who is determined to stand between businesses and threat actors. A lifelong student of developments in new technologies in the landscape of IT & cybersecurity. Adept at assisting in every stage of vulnerability & threat detection, from preventive measures to vulnerability mitigation and remediation.

PROFESSIONAL WORK EXPERIENCE

ERNST & YOUNG (EY) LLP, Bangalore (India)

Position - Cyber Security Consultant *Jun 2021 – Present*

- A Cyber-Security professional with over 4 years of expertise in **Web Application Penetration Testing** using **Burp Suite/OWASP Zap** and on numerous web applications across different domains.
- Performed comprehensive **Secure Focused Code Reviews** to identify security vulnerabilities in the source code of the application and priortized the development teams to fix them in the earlier phases of SDLC.
- Performed **API Penetration Testing** using Burp Suite and **Postman** to assess the security of RESTful and SOAP APIs & Applications, identifying vulnerabilities, and assessing the overall security posture of the application.
- Demonstrated ability to identify top OWASP security vulnerabilities, including injection attacks (e.g., SQL injection & , cross-site scripting (XSS)) and Account Takeovers, Broken-Access Control & IDORs, Broken authentication, Cross-site request forgery (CSRF) and sensitivie data exposure.
- Collaborated with the various development teams to help them in understanding the impact and the steps to reproduce the vulnerabilities detected in the penetration test and recommended the mitigation to fix/remediate the vulnerabilities resulting in the reduction of the overall attack surface in the application/server.
- Actively participated and investigated numerous false positives vulnerabilities that were detected in vulnerability scans on daily basis and providing continuous support in remediation methods to various teams.
- Performed Secure Configuration Assessment by leveraging the frameworks such as CIS & NIST benchmark hardening controls and suggested remediation for failed checks and worked on false positives checks to increase the overall compliance KPI in the organization.
- Have good experience and expertise with various vulnerability assessment and management tools such as **Qualys, Tenable.sc and Nessus**.
- Have good working knowledge in the Infrastructure Penetration Testing and Android application penetration testing.
- Experience in dealing with the scanning of Zero-Day & Public Exploitable vulnerabilities and determining the affected assets in an organization and driving different teams for the remediation within defined SLAs.
- Worked in an agile way on **JIRA** tool for managing the vulnerability remediation status by creating Tasks, assigning it to the respective teams and maintaining SLAs.

GLOBAL TECHNOLOGY AND INFORMATION SECURITY (GTIS) PVT. LTD, Gurgaon (India)

Position – Information Security Analyst Intern *Nov 2020 – Jun 2021*

- Scanning the infrastructure, network and web application assets across the organization regularly to identify critical and exploitable vulnerabilities and helping various engineering teams to fix them.
- Created Dashboards and widgets in the Qualys which are belonging to the respective OS platforms according to client's requirement for better visibility of tracking the vulnerabilities added recently in the organization's assets.
- Tested CIS benchmark hardening, scanning and suggested remediation for failed checks to increase CIS compliance percentage for Linux and Windows OS.
- Created vulnerability reports and formulated monthly metrics and weekly decks representing data on vulnerabilities and presented it to clients to effectively identify threats and vulnerabilities to the company.
- Have good experience and expertise with various vulnerability management tools such as **Qualys, Rapid 7, Tenable Nessus** and also worked with android application security testing tool MobSF and JadX.
- Collaborated with multiple geographical clients for global cloud agent rollout for the installation of vulnerabilty management software in cloud (agents) & on-premise assets and start vulnerability remediation on them.
- Worked with Remediation of several Zero-Day & Exploited in the wild vulnerabilities and have been updated regularly of new CVE's emerging in the threat landscape.

HIGHEST EDUCATION

University of Petroleum and Energy Studies, Dehradun (India) *Jul 2014 - Jun 2020*

Int. B. Tech Computer Science Engineering + LL.B. with specialization in Cyber Laws – 70.01% (First class)

TECHNICAL & SOFT SKILLS

- **Technical**: Burp Suite, Postman, OWASP Zap Proxy, Snyk, Visual Studio, Nmap, Metasploit, SQLmap, Kali Linux, Hydra, Qualys, Acunetix, Tenable.sc, JaDX, MobSF, MS Office.
- **Key Skills:** Cybersecurity, Web Application Penetration Testing**,** Secure Code Review, Android Application Penetration Testing, Network Security, Vulnerability Assessment & Management, SAST, DAST, Threat Modeling & Cloud Security.
- **Programming Languages:** Core Java, JavaScript, Python.
- **Strengths:** Adaptability, Agile, Problem-solving & Motivated.

CERTIFICATIONS / COURSES

- **eJPT** (eLearnSecurity Junior Penetration Tester)
- Certified Ethical Hacker (**CEH Practical**)
- Certified AppSec Practitioner (**CAP**)
- Certified Network Security Specialist (**CNSS**)
- Azure Fundamentals (Az-900)

ACCOMPLISHMENTS

Honors and Awards-

- Multiple Client Appreciation Notes from various international companies.
- **1** Business Extraordinarie Team Award by EY & 1 Rising Star Achievement Awards by GTIS for my continuous learning in cyber security.

LANGUAGES KNOWN

English, Hindi & Punjabi.

SAI PRAKASH GUNDALA

CYBERSECURITY ANALYST

saiprakashgundala@gmail.com

Phone: +91 7416955244

PROFILE SUMMARY

- Security Analyst with a run of 3.2+ years of professional experience in information security.
- Expertise in Vulnerability management, Web Application Security (SAST & DAST) & Network Penetration Testing, Cloud Security.
- Expertise in tracking vulnerabilities overseeing governance, ensuring compliance with vulnerability management frameworks
- Web Application Security Testing, Vulnerability Assessment and penetration testing conducted for wide range of business applications in financial/government /private sector domain against standards such as OWASP Top 10.
- Expertise in VMS to perform VA scans, proposing remediations and categorizing vulnerabilities.
- Good knowledge on networking concepts, cyber security concepts and cyber kill chain.

SKILL SET

- **Vulnerability Assessment & Pen Testing–Kali Linux, Nmap, Wireshark, Jok3r, testssl, Nessus, Metasploit Pro**
- **Vulnerability Management- QualysVMDR, Rapid7InsightVM**
- **Web application security - Burp suite, Acunetix, OWASP ZAP, HCL AppScan**
- **Cloud Security – Microsoft Defender for Cloud, CSPM for Azure, AWS**
- **Ticketing Tools – ServiceNow**
- **MS Office – MS Excel, Word, PowerPoint, Power BI**

EXPERIENCE

❖ **Infosys Limited - Hyderabad, India.**

❖ **Cybersecurity Analyst -27th Jan 2025 – Present.**

Client: Confidential (Retail Industry).
Vulnerability Management: Qualys VMDR, GRC

- Conducting vulnerability scans using Qualys and prioritizing vulnerabilities based on risk.
- Coordinate with Infra and Application teams to ensure timely remediation of finding security vulnerabilities.
- Providing technical guidance and assistance to the teams on vulnerability mitigation strategies.
- Define and vulnerability management policies, procedures and SLAs for mitigation.
- Maintain a formal process for risk exceptions, document justification and tracking compensating controls for vulnerabilities.
- Track and follow up on remediation progress ensuring compliance with internal and regulatory security standards.
- Develop and maintain dashboards using Excel and PowerBI to provide visibility into vulnerability trends, risk exposure and remediation status.
- Present security reports to the stakeholders including leadership.
- Regularly assessing and enhancing the security posture of organization by continuous improvement/monitoring.

❖ **Yash Technologies Pvt. Ltd. - Hyderabad, India.**

❖ **Cybersecurity Analyst - 8th Feb 2022 – 24th Jan 2025.**

Project 1
Client: Confidential (Health Care Sector)
Web & Network Penetration Testing:

- Performing network penetration testing on client's network infrastructure.
- Finding the open ports by using nmap.

- Performing PT on targets by using Burpsuite, Acunetix, OWASP ZAP and other CLI tools.
- Performing SAST &DAST testing on web applications to find known vulnerabilities like SQLI, XSS, CSRF etc.
- Participating in code review meetings to address potential security vulnerabilities.
- Performing automated scans on web applications by using different applications.
- Performing false positive analysis after automated scans and performing manual PT.
- Proposing mitigations for vulnerabilities.
- Report the which ports are opened and vulnerability findings in their infrastructure and applications.
- Creating customized reports about that which ports are opened and what are possibilities of vulnerabilities will be happen and proposing remediations.

Project 2

Client: Yash Technologies Pvt. Ltd.

Vulnerability Management: CyberCNS

- Onboarding assets into the tool.
- Onboarding the Authentication credentials to perform authentication scanning on different platforms.
- Responsible for conducting vulnerability assessments for networks, applications and operating systems using Rapid7 Insight VM and CyberCNS to find vulnerabilities.
- Proposing troubleshooting steps to the assets which are not alive and authentication failures.
- Identifying critical flaws in applications and systems that cyber attackers couldexploit.
- Manually validating report findings to reduce false positives.
- Preparing reports and working with respective teams and assist with the remediations of the identified vulnerabilities.

Project 3

Client: Confidential (Health Care Sector)

Vulnerability Management: Qualys VMDR

- Asset baselining and finalizing the assets to perform VA scans with the help of customer.
- Asset Onboarding.
- Scheduling discovery scans and producing report to the customer with the newly added assets in the scope.
- Scheduling VA scans for different platforms like Windows, Linux/Unix/CentOS, MacOS servers and Endpoints.
- Performing Ad-hoc scans based on customer requirement and for Zero Day Vulnerabilities.
- Creating alerts for different vulnerabilities.
- Creating different option profiles for different OS platforms.
- Asset tagging and grouping.
- Creating custom dashboards in Qualys VMDR by using QQL.
- Preparing custom report templates as per customer requirement.
- Producing VA reports to the different platform POC's and helping them to remediate those vulnerabilities.
- Categorizing and removing false positive vulnerabilities and proposing remediation.
- Troubleshooting the assets those are not alive and which are getting authentication errors.
- Performing CIS benchmark compliance scan on windows servers and endpoints.
- Responsible for conducting vulnerability assessments for different platforms and producing VA reports to the POC's.
- Responsible for creation of new users to the Qualys and removing unnecessary access (RBAC).
- Preparing custom reports as per custom requirement then help them to remediate vulnerabilities as per SLA.
- Performing rescan on ad-hoc basis for remediate assets.
- Helping to the customer to create auth credentials for different platforms by giving pre-requisites.
- Finding solutions for the issues getting in the solution i.e., Qualys by raising support case in the Qualys or getting in touch with TAM.
- Proposing troubleshooting steps to the assets which are not alive and authentication failures.
- Identifying critical flaws in applications and systems that cyber attackers could exploit.
- Risk analysis and prioritizing vulnerabilities as per SLA.
- Manually validating report findings to reduce false positives.
- Preparing reports and working with respective teams and assist with the remediations of the identified vulnerabilities.
- Preparing vulnerability trends and data points using Excel and Power BI.
- Presenting weekly data to the senior management by using PowerPoint presentations.

Project 4
Client: Confidential (Manufacturing Industry)
Cloud Security: Microsoft Defender for Cloud

- Implementing MDC for Azure based servers.
- Enabling required plans for the different resources to monitor cloud security posture management.
- Creating alerts by using Azure Monitor.
- Monitoring the critical alerts for all resources in the subscriptions as per the created alerts.
- Suppressing the alerts that are not required.
- Notifying the stakeholder regarding vulnerabilities that are found in VM's, Servers, Databases etc.
- Enabling Azure benchmark policy to the all subscriptions.
- Hardening the Azure based resources as per Azure benchmark policy.
- Proposing the recommendations for policy scans.
- Helping the customer to improve the cloud security posture.

❖ **Belcan India Pvt. Ltd. - Hyderabad, India.**

❖ **Junior Engineer – Dec 2021-Feb 2022.**

Client: Confidential (Aerospace Sector)

- Analyzing 2D drawings of Aero Engines
- Finding Hazardous materials in the Aero Engines.
- Report the Hazardous materials with composition to the customer.
- Preparing the tracker that have hazardous materials along with the part number,

CERTIFICATIONS

- CEH from EC-Council
  Validity: 12-12-2022 to 11-12-2025
- Computer Networks Security from EC-Council
- QUALYS VM Foundation
- Qualys VMDR

ACADEMIC DETAILS

- **2019:** B. Tech in Mechanical Engineering from G. Pullaiah College of Engineering & Technology. Kurnool, Andhra Pradesh.
- **2016**: Diploma in Mechanical Engineering from ESC Govt Polytechnic. Nandyal, Andhra Pradesh.
- **2013**: SSC from Shyam Vidya Vihar EM High School. Nandyal, Andhra Pradesh.

PERSONAL DETAILS

Date of Birth: 21st Jul1997
Languages Known: English, Telugu and Hindi
Present Address: H. No:28/1245 B12, Sri Sri Nivarthipuram, Noonepalli, Nandyal, Andhra Pradesh – 518501.

I hereby confirm that the above information is correct to the best of my knowledge.

Place: Hyderabad
Date:

Sai Prakash Gundala.

Rutvik Shah

rutvikshah2412@gmail.com | 8490047099

EDUCATION

NATIONAL FORENSIC SCIENCE UNIVERSITY
M.Sc. Digital Forensics and Information Security
2021-2023 | Gandhinagar, Gujarat

A. D. PATEL INSTITUTE OF TECHNOLOGY
B. Tech Computer science and Engineering
2015-2019 | New Vallabh VidhyaNagar

RESEARCH JOURNAL

SMART BANNER ADVERTISEMENT USING DYNAMIC PRICING
International Research Journal of Engineering and Technology
Issued Aug 2019
Credential ID: Volume 6 Issue 8

LINKS

portfolio: /rutvikshah.vercel.com
LinkedIn: /rutvikshah2412
Github: /rutvikshah2412
Try Hack Me: /1azyc0d3r

SKILLS

TECHNICAL

• CNAPP • ASPM • VAPT
• DevSecOps • Secure SDLC
• Networking • OSINT
• SRE Practices - Security
• MS SharePoint/Power Apps/Power Automate
• Jira/ Confluence

Familiar:
GitHub • Jenkins • CI/ CD/ CT • AWS Cloud • BASH • Java • Python

MANAGERIAL

• Stakeholder Management & Cross-Functional Collaboration
• Security Product Evaluation & Procurement
• Budgeting & Resource Allocation
• Security Metrics and key Risk Indicators (KRIs)
• Vendor Management and Coordination.

PROFESSIONAL EXPERIENCE

CREDABLE – EQUENTIA SCF TECHNOLOGIES PRIVATE LIMITED
Senior Engineer - SRE — Feb 2023 - Present

- Managed Application Security Posture and CNAPP for continuous security monitoring and compliance across 10+ apps and Cloud Account.
- Conducted VAPT for web apps, APIs, cloud infrastructure to identify and mitigate threats.
- Optimized 5+ security tools for enhanced threat detection and proactive risk mitigation.
- Integrated security practices into DevSecOps, Achieved 90% automation of code scans and enforcing secure coding in CI/CD, leading to a 25% drop in critical vulnerabilities pre-deployment.
- Delivered security training to 15+ QA team members on vulnerability detection and remediation.
- Built security dashboards, offering real-time insights for informed decision-making.
- Authored 10+ remediation documentation with mitigation strategies and best practices.
- Led end-to-end security assessments, ensuring compliance with industry standards.

TATA CONSULTANCY SERVICES LIMITED (TCSL)
Assistant System Engineer (ASE) - Trainee — June 2019 - 2020

- Developed a scalable government sector application with robust architecture and design.
- Built and optimized 8 static and dynamic web interfaces for user interaction and performance.
- Developed a log management system with dynamic report generation and amendment tracking to enable monitoring of 100% user activities.
- Wrote secure, modular code, managed version control securely and enhanced UI responsiveness using the ZK (Ajax) framework improving overall user experience.

PROJECT UNDERTAKEN

- Smart Business Card.
- Smart advertisement display based on gender and age prediction.
- Exploratory study of DevSecOps (Development- Security- Operations).

PROFESSIONAL DEVELOPMENT AND ACTIVITY

- Character certificate of National Cadet Corps.
- Volunteer in the event "VFX" in SPECTRUM'18(A.D.I.T Techfest) in March, 2018.
- Participated in the "Can you root?", "ForSecCtf" in CTF'22(NFSU University) in July.
- Liaison officer responsibility in the event "7th Interpol DFEG Meeting" in October, 2022.
- Received ownership award for leading Vulnerability Assessment and Penetration Testing (VAPT) initiatives in January, 2024.

Siva Chandra Yarramsetti

Roll No.: Y21AIT522
Bapatla Engineering College, Bapatla
Linkedin Profile

+91-7013117764
chandumani5371@gmail.com

Education

- **Bapatla Engineering College, Bapatla** *2021-25*
  Bachelor of Technology in Information Technology CGPA: 7.54
- **Aditya Junior College,Mandapeta** *2019-21*
  Board Of Intermediate Education, MPC Percentage: 90.3

Personal Projects

- **DEAD-END-DETECTOR** *Jan 2023-Feb 2023*

  Technology Used : Python

  – Developed an algorithm to detect dead-end streets in a city's road network, leveraging graph theory and depth-first search techniques. Implemented the solution in Python, processing input data on the number of locations and streets to identify potential traffic bottlenecks.

- **SMART-PARK** *Jul 2023 - Sep 2023*

  Technologies Used : IoT

  – Developed a prototype system using IoT technology to display real-time parking space availability. Designed the solution to help drivers quickly locate and access open parking spots, improving overall parking efficiency. Leveraged sensors, data processing, and visualization techniques to provide a user-friendly interface for parking management.

- **SALES PREDICTION** *Jan 2024 - Feb 2024*

  Technologies Used : Machine learning

  – Utilized machine learning techniques to predict store sales based on available attributes in the dataset. Implemented normal regression and compared results with Random Forest Regressor, . Demonstrated ability to apply predictive analytics to identify key factors influencing sales and select the best-suited algorithm for the task.

- **MCQ GENERATOR** *Nov 2024 - Present*

  Technologies Used : Google AI Studio, Gen AI API

  – Developed an AI-powered system to generate multiple-choice questions based on user requirements.Utilized Generative AI APIs to dynamically create and fetch question sets, which were then formatted for seamless usability.Integrated Google AI Studio to streamline the process of transforming user inputs into customized assessments, enhancing accessibility and user experience.

Skills

Languages : Python, Java, C.
Web Technologies : HTML, CSS, JavaScript.
Machine Learning : Supervised and Unsupervised Learning Algorithms, Natural Language Processing (NLP).
Generative AI Tools : Google AI Studio, Gen AI APIs.
Database : SQL, Database Management System.
Tools : MS Word, MS Excel.

Achievements

- **UIPATH Online Certification** *(Sept 2023)*
  Achived certification on the learing plan "RPA Developer Foundation(V2021.10)".
- **Certificate of Participation** *(Sept 2023)*
  Actively Participated in the "Uiath RPA Workshop" conducted by our college.
- **NPTEL Online Certification** *(Jan 2024- Apr 2024)*
  Successfully completed the "Cloud Computing" course through NPTEL Online Certification, earning a commendable 55score.
- **Certificate of Completion** *(May 2024- Jun 2024)*
  Successfully Completed Short-Term Internship for 180 hours on MACHINE LEARNING Organized by BIST TECHNOLOGIES PVT. LTD in Collaboration with the Andhra Pradesh State Council of Higher Education.