PIYUSH KUMAWAT

+91-8562808965
piiiiyush22@gmail.com
linkedin.com/in/piyush-kumawat

EXECUTIVE SUMMARY

Product Security Engineer with 3.5+ years of experience in penetration testing and willing to achieve a challenging position in an environment where I can use my technical, academic skills and utilize my techniques to the optimum level to be able to fulfil personal as well as organizational goals.

HIGHLIGHTS

- 3.5 years of work experience as Application Security Engineer
- Expertise in the following fields
    - Web Application Penetration testing (Grey and Black Box)
    - Web Services & API Security
    - Network Penetration Testing
    - Android and iOS Penetration Testing
    - Cloud Security Configuration Review
    - DevSecOps
    - Source Code Review
    - Secure Design Reviews
    - Threat modelling
- Expertise in using tools such as Burp Suite, Nessus, App Scan, Metasploit, SqlMap, Nmap, OpenVas, Dirb and other security tools.
- Expertise in SAST or SCA tools configurations such as Coverity, Checkmarks, Findbugs, Whitesource, Blackduck, Sonarqube and other code analysis tools
- Continuously learning new technologies such as Secure Development and Threat Modelling.
- Experienced in handling US/Canada and EU based Clients.
- Hands-on on Microsoft Azure, AWS platform, Google Cloud Platform and Alibaba cloud for Cloud configuration reviews.
- Working with the clients to remediate the vulnerabilities and helping them secure their organization.
- Excellent Reporting Skills.

- Excellent oral and written communication skills
- Experience working both as a part of team and independently.

EXPERIENCE

Product Security Engineer

OLA | Jan 2022 – Present | Bangalore

Brief Description

- Perform Threat Modelling, Dynamic Application Security Testing (DAST) and Static application security testing (SAST) on Web applications of different OLA's business groups (OLA Money, OLA Electric, OLA Mobility, OLA Avail Finance, etc.).
- Perform Web Application security assessments for identifying and remediating OWASP top 10, MITRE ATT&CK and Business Logic Vulnerabilities.
- Run scans using tools such as Burp Suite.
- Manage the Bug Bounty Process of OLA.

Roles and Responsibilities

- Performed white box tests as per OWASP top 10 framework for Web Applications.
- Performed Automated and Manual Tests and removed False positive issues.
- Work with developers to remediate the open findings.
- Mapped the risks as per business criticality and impact of vulnerability on application.
- Raise Jira tickets which includes Description, Remediation, Steps to Reproduce and screenshots for the Reported Findings.
- Raise a Jira Ticket which provide detailed technical summary of the findings with appropriate recommendations, Steps to reproduce and Screenshots.
- Assessed the closure of security risk by conducting retest on the web applications, web services and mobile assessments.
- Managing the GDPR or PCI-DSS Audit dependencies on Application Security.

Security Services Associate Consultant

Synopsys Inc. | June 2019 – Jan 2022 | Bangalore

Brief Description

- Perform Dynamic Application Security Testing (DAST) for Web applications.
- Perform Web Application security assessments for identifying and remediating OWASP top 10, MITRE ATT&CK and Business Logic Vulnerabilities.
- Run scans using tools such as Burp Suite, Nessus, App Scan, Metasploit, SqlMap, Nmap, OpenVas, Dirb, Nikto and other security audit tools.
- Continuously learning new technologies such as Mobile penetration testing, Secure Development, Threat Modelling and Cloud Configuration review.

Roles and Responsibilities

- Performed black box and grey box security tests as per OWASP top 10 framework for Web Applications.
- Performed Automated and Manual Tests and removed False positive issues.
- Mapped the risks as per business criticality and impact of vulnerability on application.
- Sent daily updates of identified vulnerabilities and provided support for revalidating them in parallel with actual testing.
- Provided executive reports with detailed technical summary of the findings with appropriate recommendations.
- Assessed the closure of security risk by conducting retest on the web applications, web services and mobile assessments.
- Managing DevSecOps environment by configuring various tools such as CheckMarx, WhiteSource, and Burp in a CI/CD environment.
- Performs Cloud Configuration Review on various Cloud Platforms (AWS, Azure, GCP Ali Cloud).

Cyber Security Intern

Synopsys Inc. | Jan 2019 – May 2019 | Bangalore

- Engaged in the learning of various pen test, application stacks, working of typical N-tier application OWASP Top10 in WEB, Mobile, etc. Data flow in complex applications successfully.
- Successfully automated multiple security tools in a unified platform for the Organization using Jenkins in a CI/CD pipeline.

System / Network Admin Intern

Shah Technical Consultants Pvt. Ltd. | March 2017 - April 2017 | Jaipur

- Manages Network and Server for the Organization.
- Provide proactive solutions for the technically challenging problem of the Organization.

PROJECT

Security Tools Automation

- Automated different open source and paid SAST, SCA and DAST tools in Jenkins pipeline to perform a security scan efficiently on a source code base.

Windows Administrator Learning App

- Successfully deployed android application for learning windows administration in Windows Server (20k+ Download).
    - https://play.google.com/store/apps/details?id=com.techdreamers.Windows_Server

Certifications

- AZ-500 - Microsoft Certified Azure Security Engineer Associate
- Az-900 - Microsoft Certified Azure Fundamentals
- Oracle Cloud Infrastructure 2019 Certified Architect Professional
- Oracle Cloud Infrastructure 2019 Certified Architect Associate

ACADEMIC BACKGROUND

MSC. Digital Forensics & Information Security

Gujarat Forensics Sciences University | 2017 – 2019 | Gujarat, Gandhinagar

BCA (IT-Infrastructure Management System & Cloud Technology)

Poornima University | 2014 – 2017 |Jaipur, Rajasthan

HOBBIES & INTRESTS

- Managing personal security blog.
  - https://securitycipher.com
- Travelling & Trekking.
- Trying various cuisines.
- Playing online PC and Mobile games.
- Bug Hunting in leisure time.