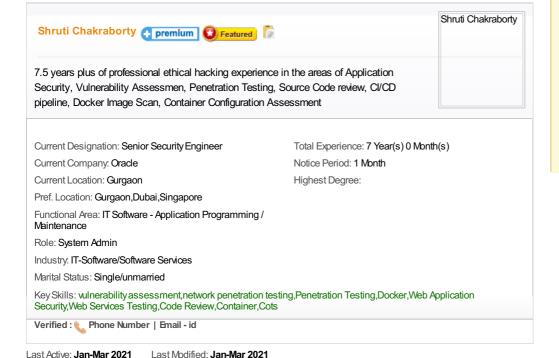


1800 102 2558 | +91 9818882211







Jump to Section

Work Experience | Education | IT Skills |

Summary

B.Tech (Computer Science) with 6.9 years plus of professional ethical hacking experience in the areas of Application Security, Vulnerability Assesment, Penetration Testing, Source Code review, Definning Test Cases for new exploit etc in cross-domain platform that covers the banking sector, finance, E-commerce etc. Worked for US, Indian clients covering end-to-end SDLC life cycle of real time applications like understanding business logic, scope closure, functional specification documents, verification and validation, release and maintenance

Work Experience

Oracle as Senior Security Engineer May 2020 to Till Date

This project involves SAST, DAST, Web Application Pentest, Webservice PT, Vulnerability Management Dashboard, Docker Image and DoCker Container security for the Oracle SaaS products

Deloitte as Solution Delivery Advisor Dec 2015 to Feb 2020

Banking Industry - Banking and e-commerce application assessment Technology & Environment : Advanced Java, Oracle 10g, DB2, Red Hat Linux. Tools: Veracode, Fortify, Burpsuite, HP WebInspect, Postman, Swagger Parent Organisation: Deloitte USI

Project Duration: 11st April, 2015 to Till date.

Project Description:

project involves third party security assessment. To be more precise, COTS product assessment of different vendors that are deployed on the client environment along with network assessment. Also, performed source code review of applications hosted on client environment using fortify tool. Contributions:

Primary role is assessment of the COTS product using Veracode, source Code Review using Fortify tool, API pentesting using postman & swagger, application penetration testing.

For COTS Fortify tool, API pentesting using postman & swagger, application penetration testing.

COTS:

Onboarding of the applications and interacting with vendors to understand the scan scope of those applications

Executing false-positive & false-negative analysis of the issues observed

Followup with te vendor to ensure closures as per SLA

Final report preparation of COTS product against open issues

Source Code Review:

Onboarding of the applications and interacting with developers to understand the scan scope of those applications

Creating project on Fortify Software Security Centre (SSC) as a part of onboarding of

Important

· Using Free CV Search you have access to featured candidate profiles of Naukri. You can browse through the profiles and email the candidates of your choice directly using the email option provided. To prevent misuse of candidate information, contact details and attached resume of the candidates have been withheld

ine application

Scaning of the applications using Fortifytool

Manual analysis of the issues identified as a part of false positive review

Creating report which demonstrates the final risk rating of the application Jenkin integration with Fortify SCA using Jenkin as CI/CD pipeline

Uploading the security issues in JIRA & Qtest tool

Application Pentest:

Custom & legacy application penetration testing

Automated scan using HP Webinspect followed by manual assessment Uploading the security issues in JIRA & Qtest tool

False positive & false negative analysis followed by report preparation

API Pentest:

Accessing the collection or swagger project file for security threats

Automated scan of collection file followed by manual analysis

Uploading the security threats in JIRA & Qtest tool

IBM India Pvt Ltd as Security & Privacy Consultant (GBS)

Apr 2013 to Dec 2015

2. Telecom Industry - Telecom application testing

Technology & Environment: Advanced Java, Oracle 10g, DB2, Red Hat Linux.

Tools: Burp professional, Nessus, Nmap, Openssl, Wireshark etc.

Parent Organisation: IBM India Pvt. Ltd.

Project Duration: 1st Jully, 2013 to 9th December 2015.

Project Description:

This project involves application security audit, VA & PT & Grey-Box of the telecom applications. application testing was focused on critical telecome applications. The applicatiobs are web applications

with different end-user objective. This applications gives the complete support to the back office

executive. Underlying system audit through complete end-to-end VA & PT activity.

My Contributions:

Page 3 of 4

Primary role is Appsec, VA & PT and Risk analysis.

GAP assessment and creating threat profile along with the test plan.

Analysing & testing the telecom applications (Grey-Box testing) for identifying vulnerabilities

in the application that reveals sensitive data to an adversary.

Peform VA & PT for internal and external network of the complete assets.

Report making for both application testing and network penetration testing.

Interacting with the development team & server team to fix the vulnerabilities.

Test case creation for application & business logic

^ Back to Top

Education

UG: B.Tech/B.E. (Computer Science) from west bengal university technology in 2012

PG: in 0

^ Back to Top

IT Skills

Skill Name	Version Last Used Experience
Burpsuite, HP WebInspect, Owasp ZAP	
Nessus, OpenSSL, Qualys, SSLScan	
Nmap, Wireshark	
Postman, Swagger, SoapUI	
Windows (xx), Unix(xx), Linux	
JIRA, qTest	
DOCKER	0 0 Year(s) 0 Month(s)

^ Back to Top

Languages Known

Language	Proficiency	Read	Write	Speak
English				
Hindi				

^ Back to Top

Affirmative Action

Work Authorization

Physically Challenged: No

Job Type: Permanent Employment Status: Full time

^ Back to Top

All rights reserved © 2021 Info Edge India Ltd.

Careers - About Us - Clients - Terms & Conditions - FAQ's - Contact Us - Report a Problem - Site Map - Resources
Our Partners: Jeevansathi Matrimonials - ICIClcommunities.org - 99acres - Real Estate In India
All rights reserved © 2021 Info Edge India Ltd.