POOJA A. GAONKAR

Domain – Expertise in PCI-DSS Requirements, Application security Assessment, IT security solutions.

6+ years of comprehensive experience in IT security services (VAPT and Application security), IT security auditing (PCI DSS, ISO 27001, RBI, SEBI, HIPAA, GDPR) Team Management, IT security solutions consulting, Network Security, Risk assessments, SOC Operations, Network and Application Security architecture review for international clients from multiple disciplines such as Banking, Financial, Stock Exchange and IT services.

Core Competencies

- Vulnerability Assessment & Penetration
- Network, Operating System & Database
- Configuration Reviews and Hardening
- Payment Gateway App Security Assessm
- Application Security Code Review
- Identity & Access Management
- Threat modelling
- Web, Mobile & Application Security Assessments
- Secure Network Architecture Reviews-Firewall
- Router, Switch Rule Base Reviews
- Wireless Security Assessments
- IT system and process audits, ISO, PCI, Internal Audits, Risk Assessments, Gap-Assessments

Trainings and Certifications

- ✓ CISSP
- ✓ ISO Lead Auditor ISO / IEC 27001
- ✓ EC-Council Certified Security Analyst (ECSA) v9
- ✓ PCI -Associate Qualified Security Assessor
- ✓ Certified Ethical Hacker (C|EH) Version 8
- ✓ Qualys guard Training Certification
- ✓ Cisco Certified Network Associate (CCNA)

Professional Experience

❖ **Aujas Networks Pvt Ltd.** **March 2020 to till present**

Designation: - Senior Information Security Consultant

Description: During tenure she was deployed at **National stock exchange** as Information security advisor and managing team of security testers within A**ujas**.

- Ensure that controls are adequate to meet legal, regulatory, policy, standards, and security requirements (ISO, RBI, PCI, SEBI etc.)
- Review the status of the information security program with higher level managers / stakeholders.
- Communicate with and report to (as required) all internal and external stakeholders.
- identifying vulnerabilities and security loopholes in the existing implementation.
- Define guidelines and conduct vulnerability assessment and penetration testing with team.
- Represent security group during external and internal IT Security and IS audits related to application security.
- Lead security solution evaluation, purchase and implementation.
- Gap assessment for new technology.
- Provide security solution or compensatory controls to reduce the risk for the vulnerabilities identified during application penetration testing, Vulnerability assessment and source code review analysis.
- Managing the team of security testers where reviewing their performance, training on their weak areas.
- Part of read teaming establishment.
- Conducting trainings for web application PT, Mobile (android) application PT and codebashing training of checkmarx.

+91 9821523513
poojagaonkar7@gmail.com

❖ **Reserve Bank of Information Technology (4 months)** **Nov 2019 to March 2020**

Designation: - Information Security Manager

Description: Working as manager who handles the technical team and performs the audits with regulatory.

Responsibilities Include:

- Conduct Information System audits for regulated entities as per the schedule with a focus on payment systems such as SWIFT, UPI, IMPS, ATM, Internet Banking, Mobile Banking, Core Banking System.
- Support in maintaining audit checklist and documents, trend analysis, preparing presentations etc.
- Review/Assess the security architecture, IT security controls for compliance against published framework and RBI standards.
- Audit IT processes including change management, configuration management, backup management, identity & access management, capacity management and security incident management
- Conducting audit of Information security policies, procedures and processes to identify design gaps.
- Coordinate with security intelligence framework to obtain latest threats & vulnerabilities
- Prioritizing security vulnerabilities identified in ethical hacking, penetration testing and application / system testing based on business impact and update Security operations team for mitigating them.
- Define security guidelines for application development (secure SDLC, Secure coding practices etc.)
- Handling the team which conduct internal / third-party Ethical Hacking / Vulnerability Assessment / Penetration Testing, Red Team assessment on business-critical assets and processes.
- Work with SoC team to define event correlation rules related to application threats and vulnerabilities, ensure all events related to application threats are tracked to closure

During the tenure, she has worked across the Indian sub-continent

❖ **CONTROLCASE INTERNATIONAL PVT. LTD (5 years)** **Nov 2014 to Nov 2019**

Designation: - Senior Information Security Consultant

Description:

Security assessments of client IT environments against various industry standards and regulations including PCI, GDPR, ISO 27001, and HIPAA. Working as the consultant for assignments which included small to large service providers in payment services, e-commerce merchants, Banks, Payment gateways in various geographies like Asia and Africa.

Responsibilities Include:

- Assisted implementation (**Gap Assessment & Remediation**) PCI DSS for clients, currently supporting service provider clients in India etc. for onsite / offsite remediation assistance.
- Interface with clients to review and analyze complex systems (**Applications, operating systems, databases, and Networking devices**), to identify risks, exposures, define and implement compensating controls
- Performing various technical security assessments, educating the client on the inherent risks, and providing meaningful **hardening and mitigation strategies**.
- **Managing certification projects** along with team to ensure clients meet their compliance and certification goals
- Able to analyze cardholder data flows (business and application data flows) and accordingly identify the risks to **cardholder data**
- Produce final reports on compliance to detail the controls observed during security assessments in accordance with various security standards and regulations. **ROC and AOC**, **Executive summary, Gap analysis and risk analysis** with reports writing.
- Develops valuable and trusting relationships with internal business partners by executing efficient audit work and offering suggestions to enhance risk management based on an enterprise-wide view of technology risk management
- **Perform user access reviews, physical access reviews, internal production access reviews** and user attestations according to schedule
- Reviewing security testing reports for security services like **VAPT, APT, and MAPT.**
- **Security Penetration Testing**- As per PCI requirements.
- Provide in-house training to clients on **PCI DSS awareness.**

❖ **CONTROLCASE INTERNATIONAL PVT. LTD**

Designation: Information Security Consultant

+91 9821523513
poojagaonkar7@gmail.com

Responsibilities Handled:

- **External & Internal Vulnerability Assessments and Penetration Testing** with the help of tools like Nmap, Nessus, Nexpose, Qualys, Metasploit, Backtrack, Kali, etc. post which performing manual testing for confirming and exploiting the reported vulnerabilities, open ports, OS fingerprinting, etc. using various methods.
- **Manual Web Application (thick &web api**) **Security Assessments** for all possible vulnerabilities with the help of tools like Burp Suite, SQLMap, Fiddler, OWSAP ZAP, Netsparker, Acunetix, IBM AppScan, Eco mirage, Process monitor, process explorer, soap UI etc. and providing a detailed report with methodology and screenshots of the vulnerabilities identified while providing strong mitigating solutions with detailed risk and impact of the same.
- Conduct Mobile applications **IOS/Android/Windows/POS security testing** and **Application Security Code Review** with check Marx tool.
- **Threat modelling** of the Project by involving before development and improving the security at the initial phase.
- **Secure Network Architecture Review** of WAN, LAN, VLAN, network configuration reviews, access controls review, failover implementation and based on the understanding of the current network and business requirements in depth, proposal of a secure and redundant network for the organization. Also, conducting **Firewall Rule Based Audit** after understanding the network and business needs / requirements. Routers and switches Rule Base Reviews.
- **Cyber Security Assessment** which included activities such as VAPT, Process, Procedures and Policies Audit, IT Security Architecture, Network Security Configuration, Component Level Security Configuration of OS and DB, Mail Security, Firewall Configuration, Active Directory Security Configuration, Data Leakage Prevention Review, Disaster Recovery Planning, Wireless Security, Workstation Security, Antivirus and Patch Management Server Review and Remote Access.
- **Payment Gateway Testing** integrated with the Bank's Payment Gateway for all possible vulnerabilities with the help of tools like Burp Suite, Wireshark, Paros, etc. and providing a detailed report with methodology and screenshots of the vulnerabilities identified while providing strong mitigating solutions with detailed risk and impact of the same.
- Performed **Wireless Security Audits** for industry leading BPOs and Call Centre mainly inIndia.
- Keep track of new vulnerabilities on various network and security devices for different vendors Knowledge of security bug classification frameworks such as CVSS and experience applying security bug classification methods in development and QA.

During the tenure, she has worked across the Indian sub-continent and other international countries such as Africa Middle east and ASIA Pacific region.

❖ **Lucideus** **June 2014 to December 2014**

Designation: Information Security Consultant Intern

Description: Lucideus is an IT Risk Assessment and Digital Security Services provider.

Responsibilities Handled:

- Conduct Vulnerability Assessments on systems, web applications and network devices, Penetration Testing
- Conduct Mobile application security testing for android.
- Reverse engineering and android application Development
- Python scripting for automation
- Regular expressions for scripts
- Tools development and research
- Log analysis and Attacks research.
- Logging and monitoring

❖ **Freelancing**: Black-box and grey box testing for Web and mobile applications, VAPT.

Responsibilities Handled:

Performing vulnerability assessment and penetration testing on the application providing comprehensive report on findings and action items to fix the identified vulnerabilities. Hall of frames from below clients. Conduct training for

Android application penetration test for various clients. Trainings conducted for android application PT.
Clients: Stupid Sid, ALLCARD, FNB, Visionael, Clear trip
Digisec360 – Consulting projects
GB hackers: Security research, cyber security blogger and Author
Overview: updating with new attacks with research, blog writing of vulnerabilities which are exploited, and overview of android application penetration testing.
URL: https://gbhackers.com/author/pooja-gaonkar/

Education

- B.E(**Electronics & telecommunication**) from Mumbai University with 73.94% in Distinction Class (JULY-2014).
- HSC (**Computer Science**), S.S.C Maharashtra Board, with 83.33% in Distinction Class (MARCH-2010).
- SSC from SSC Maharashtra Board, with 90.46% in Merit Class (June-2008).
- Held Joint Cultural Secretary position in Students Council of college from 2012 to 2013
- Held Campus Brand Ambassador position in Stupid Sid from 2013 to 2014

HONORS & AWARDS

- ControlCase Appreciations for exceeding expectations and delivering a project single handed in the absence of Senior Manager also for showing real dedication and hard work on a global client project
- Multiple Client Appreciations while at ControlCase for project completion on time with excellent quality.
- Client Appreciation while at ControlCase for work done on onsite activities in Africa & Jordan.
- Client Appreciation while at Rebit for work done on onsite activities at NPCI & various banks.
- Hall of frames and Appreciation mails from various clients for bug bounties
- Nominated for Merit-cum-Medal Award for Securing **79.86%** in B.E SEM 8 at ytcem-Mumbai University
- Nominated for Merit-cum-Medal Award for Securing **90.46%** in SSC at shardashram vidyamandir

Personal Details-

Date of birth	**:**	November 20, 1992
Gender	**:**	Female
Nationality	**:**	Indian
Marital Status	**:**	married
Languages Known	:	English, Marathi, Sanskrit and Hindi

I confirm that the information provided by me is true to the best of my knowledge and belief.

Place: Mumbai. Pooja Gaonkar
Date: August 2020. Signature

+91 9821523513
poojagaonkar7@gmail.com

+91 9821523513
poojagaonkar7@gmail.com