Deepak Kumar
Senior Security Consultant

A security enthusiast with 7.3 years of experience mainly in 'Application Security' domain. Currently I am part of EY GDS Technology Consulting, mainly responsible for Leading teams in Appsec engagement(s). I explore and learn emerging technologies while I am actively engaged on projects.

✉ deepakr.hooda@gmail.com   📱 +91 8050660458   📍 Gurgaon, India

WORK EXPERIENCE

Senior Security Consultant
Ernst & Young GDS

2017 - Present   *Gurgaon*
EY

Achievements/Tasks

- Led a team of 20+ security consultants (Lead & Engagement Manager role) for an Appsec engagement for a leading European pharmaceutical client.
- Led a team of 8+ security consultants (PMO role) for an Appsec engagement for a leading Indian telecom client.
- Independently assessed 50+ applications from threat modeling & secure architecture review perspective.
- Independently assessed over 10+ applications from vulnerability assessment perspective.
- Active involvement in coaching the team members for Application Security topics.
- Took initiatives to improve overall project quality, delivery and operational aspects. Created questionnaires for various security assessments.

Security Consultant
SecurEyes Techno Services Pvt Ltd

2013 - 2017   *Bangalore*
Achievements/Tasks

- Part of application security team & conducted security audits (vulnerability assessment & ATM audit) for major banking clients (4+) in Middle East.
- Part of application security team & conducted security audits (penetration testing & vulnerability assessment) for major banking clients (2+) in India.
- Part of application security team & conducted security audits (penetration testing & vulnerability assessment) for Government websites / clients.
- Mainly dealt with vulnerability assessments of web based (60+), mobile based (8+) and thick client (6+) applications to assess against OWASP Top-10 (but not limited to) framework.

SKILLS

| Technical Lead | Secure Architecture Reviews | Threat Modeling (STRIDE) | Penetration Testing | Salesforce |

| Cloud Security (AWS & Azure) | OWASP & SANS Top 25 | SAP | Vulnerability Assessments (Nessus) |

MAJOR PROJECTS

Application Security Assessment - One of the leading European Pharmaceutical client (2018 - 2020)

- Assessed applications (cloud based, in house developed, COTS product) against STRIDE & CAPEC framework to carry out the threat modeling & secure architecture reviews.
- Creation of data flow diagram (DFD) using Microsoft Threat Modeling Tool. Representation of data labels, key components, trust boundaries, communication protocols as part of DFD creation.
- Information gathering and Analysis work by conducting interviews with relevant stakeholders & reading relevant technical documents. The analysis work comprise of evaluating over 150+ questions from security domains, such as authentication & authorization, session management, encryption (at rest & in transit), deployment, change management, patch management, backup and recovery, logging and monitoring, input validation, integration / interface security, API security, cloud security.
- Draft report creation followed by a readout discussion to finalize the treatment and mitigation plan for the identified risks.
- Handled other key responsibilities such as internal QA of draft reports for other team members, weekly / daily stand up with client and onsite, tracking the quality / delivery / operational aspects, interviews, utilization tracking, internal KT sessions for new team members, resolution for escalations etc.

MAJOR PROJECTS

Application Security Assessment - One of the leading Indian Telecom client (2017-2018)
- Carried out the vulnerability assessments of live applications, both internet facing and intranet / internal facing.
- Project involved application understanding, threat profiling, manual audit against the OWASP categorization, interaction with development team to assess / analyze the observed vulnerabilities, proposed mitigations, documenting reports recommending most feasible solution for remediation of risk.
- Handled other key responsibilities such as internal quality assurance of reports for team members, dashboard creation for weekly stand up meeting with client, training sessions for team member on critical / high severity risks, overall project monitoring.

Application Security Audit - Two Largest Banks in KSA
- Performed security audit testing of SADAD Online Payment system. This OLP system has 3 modules i.e. merchant, customer and public website. The merchant module is for the merchants to view and perform certain operations on transactions made by the bank customers. The bank users can login to view and manage the transactions made by them. Further the public website is accessed by the users to make a payment. The vulnerability assessment of various Database and Web servers is conducted based on the current implementation of SADAD-OLP solution. Finally, the report was presented to the client with detailed description of vulnerabilities found and along with best suitable mitigation.

Application Security Audit - External Annual Audit on behalf of SAMA Risk Assessment
- Performed application security audit of RIB (Retail Internet Banking), CIB (Corporate Internet Banking), Payment Gateway and 25+ internal banking applications during the annual SAMA compliance test activity for 4 nationalized banks. The project involved application understanding, threat profiling, manual audit against the OWASP categorization and Business Rules Validation, reporting with feasible recommendations, interacting with the development team towards the mitigation of the observed vulnerabilities. Also, performed the ATM security audit for the 3 ATMs selected for the activity which involved meetings with various stakeholder and physical visit to the ATM headed by the vendor and bank personnel.

Application Security Audit - Three Leading Private Sector Banks in India
- Performed application security audit of RIB (Retail Internet Banking), CIB (Corporate Internet Banking), Credit Card System, Payment Gateway and 20+ internal banking applications. The project involved application understanding, threat profiling, manual audit against the OWASP categorization and Business Rules Validation, reporting with feasible recommendations, interacting with the development team towards the mitigation of the observed vulnerabilities. Apart from OWASP, certain controls present in the bank's security baseline were also assessed such as logging, cryptographic, interface, data protection, change management and segregation of duties.

Application Security Audit - Various Govt. Ministries across the country (NIC Audit Project)
- Part of the the NIC random audit project that involved security audit of 30+ critical NIC websites. The project involved blackbox application penetration testing audit against the OWASP categorization, reporting with feasible recommendations, interacting with the development team towards the mitigation of the observed vulnerabilities. Also, led the team towards successful completion of the activity.

HONOR AWARDS

ECS (Exceptional Client Service) award for outstanding client service.
EY

Extra Miller & Spot awards while leading the team.
EY

Star Performer award of the year.
SecurEyes

Achievers Award for Quick Learner of the year.
SecurEyes

CERTIFICATES

Certified Scrum Master

Certified Ethical Hacker

ISO 27001:2013 (Lead Auditor)

EDUCATION

Master of Computer Applications
Sir MVIT College, VTU

2010 - 2013   *Bangalore*