GIRISH

Information Security Consultant

CERTIFICATION

CEH (Certified Ethical Hacker)

ICSI | CNSS (Certified Network Security Specialist)

ICS security from DHS

SKILLS:

- Broad Knowledge of Vulnerability and Risk Management
- In-Depth knowledge of network and application vulnerabilities and ability to articulate their impact to business users
- Ability to Automate Testing process using any scripting or programming languages (php, Python, shell)
- Ability to conduct web application and mobile security assessments and handle vulnerability remediation of applications
- Perform, review and analyze security vulnerability data to identify applicability and False Positives
- Ability to recognize, value, and include different perspectives, experiences, approaches, and cultures in achieving organizational goals
- Ability to conduct source code reviews of applications and provide remediation to help the development team fix vulnerabilities.

EDUCATION

BACHELOR OF ENGINEERING
Computer Science and Engineering (CSE),

WORK EXPERIENCE

Domain: Information Security.
Designation: Information Security Consultant.
Experience: 4+ Years

NUMBER OF PROJECTS

More than 100+ projects handled in the security categories such VAPT, Red Team, GRC, forensics, Osint etc.

Multiple Corporate Trainings for MNCs

Multiple Trainings for technical Colleges

ROLES

- Vulnerability Assessment and Management (VA & VM) of Network and Applications
- Configuration Audit
- Network Penetration Tester
- Web Application Penetration Tester
- IOT Penetration Tester
- Cloud Security
- Security testing of REST, GraphQL and SOAP APIs.
- Penetration testing of Mobile Applications (iOS and Android).
- Static Application Security Testing (Secure code review)

RESPONSIBILTIES

- Planning, Execution and Manage projects or contribute to committee or team work.
- Understanding of web application security concepts and standards, checking for vulnerabilities in application as per OWASP and SANS guidelines.
- Performing Vulnerability Assessment of Servers, Network devices, Access Points, Firewalls and Security devices.

TOOLS

- KALI LINUX
- BURPSUITE
- NESSUS
- NMAP
- WIRESHARK
- SQLMAP
- METASPLOIT
- POSTMAN
- SOAPUI
- FRIDA
- MOBLEXER
- MOBSF
- FIDDLER
- ADB
- SonarQube
- Fortify

- **Performing Manual/Automated Penetration Testing of internally and externally accessible Web and Mobile Applications.**

- **Performing Security testing on REST, GraphQL and SOAP API Services by using Manual and Automated Tools.**

- **Identify information security weaknesses and/or gaps in the client operations and work with the stakeholders to bring information security operations up to industry standards and best practices.**

- **Create detailed risk assessment reports which explain identified security weaknesses, describe potential business risks, present prioritized recommendations for remediation, and estimate costs and effort levels for remediation.**

- **Provide customer consultation involving validation evidence, exposure, remediation, recommendations and risk posture to both executive management and technical teams.**

- **Collaborate with development teams to prioritize and remediate vulnerabilities throughout the software development lifecycle and to improve security program.**

- **Help inspect security vulnerabilities associated with open-source and 3rd-party functional libraries.**

ACHIEVEMENTS

HALL OF FAME: https://english.pratilipi.com/hall-of-fame
(V/R)DP: GoodGrid, Ricoh, Shaadi, BornBabies, Atlassian(confluence) etc
Pentest Report Generator: https://github.com/ari5ti/security-report-generator

DECLARATION

I hereby declare that above information is to best of my knowledge and belief. I bear the responsibility for the correctness of above-mentioned particulars.