

Application Penetration Tester

**Do you have what it takes to join the elite security testing team?
If you answered “Yes” we’d love to put you to the test!**

Canary Trap is always on the lookout for professionals to join our growing team. This role is responsible for coordination with stakeholders, security testing of technology, communication of findings and completion of day to day tasks associated with a penetration testing program. The Application Penetration Tester will participate in internal application assessments, API testing, and referring any customer facing applications for independent assessments.

Qualified candidates must possess the required certifications, expertise and experience along with interpersonal skills necessary for success.

Job Responsibilities & Description:

- Conduct initial penetration test scoping/kick off meetings with stakeholders
- Conduct web application, API, mobile and network penetration testing within the designated scope and rules of engagement
- Provide consultation on appropriate remediation actions
- Must be intimately familiar with the OWASP standard testing guide.
- Maintain communication with customers to ensure a quality engagement.
- Provide reports on application security
- Must have a comprehensive understanding of the HTTP protocol, System Development Lifecycle (SDLC) and Web Programming for multi-tier web applications and web services.
- Scripting and/or programming experience in Java or Angular JS
- Intermediate knowledge of operating systems (Windows, Linux) and SDLC frameworks
- Experience with different HTTP proxy tools, Web Browsers and in-depth understanding of authorization and authentication frameworks.
- Experience and knowledge of performing security tasks within regulated environments (SOX, HIPAA, NIST)
- Experience and knowledge of security frameworks (NIST CSF, ISO 27001)
- Certifications such as GIAC Web Application Penetration Testing (GWAPT) or OffensiveSecurity Certified Professional (OSCP) are preferred.
- Strong attention to detail, data accuracy, and data analysis.
- Strong organizational and project management skills.



- Self-motivated and operates with a high level of integrity.
- Previous experience working in large scale environments with diverse technologies.

- Bachelor's degree in Computer Science, Information Technology, Cyber Security, or related discipline or equivalent experience
- Minimum of 5 years of IT experience
- Minimum of 2 years Information Security experience, with previous penetration testing or application security background
- This description is not a comprehensive listing of activities, duties or responsibilities that may be required of the employee and other duties, responsibilities and activities may be assigned or may be changed at any time with or without notice.

Have what it takes to Join Canary Trap?

Submit your resume/CV to careers@canarytrap.com along with a personal letter.