

**Job Title:** Associate Application Security Consultant

**Reports To:** Penetration Testing Team Lead

**FLSA Status:** Full-Time Exempt

**Prepared Date:** May 2011

**Salary Range:** Industry standard, commensurate with experience

IOActive is a cutting-edge firm that blends opportunities for career and personal advancement with a positive and challenging work environment. We seek talented people with broad, robust skill sets from around the world to join our diverse, growing team of consultants. IOActive's highly experienced and technically skilled consulting teams work with organizations to mitigate information asset and mission-critical system security risks in their complex, interconnected business environments.

Our consultants deliver high-quality, and on-time services and products for our client engagements. They have gifted technical minds with deep experience in programming and application security, infrastructure security, tool development, and source/code architecture review. Our consultants identify, test, and articulate client vulnerabilities; provide practical recommendations; and adapt to new technologies and practices that raise the bar of computer security standards.

### **What Candidates can Expect:**

- Performing web application assessments for various customer business units with differing objectives and constraints ranging from integration to incident response.
- Exposure to a wide variety of web applications and technologies as well as spoken languages; however, multilingual skills are not necessary.
- Responsibility for helping protect one of the largest user bases on the Internet.
- Exposure to and opportunities to participate in cutting-edge research.
- A hands-on learning environment in which to grow both technical and professional skill sets.

### **Desired Consultant Experience and Traits:**

- A passion for breaking web applications.
- An unrelenting desire to expand, hone, and master offensive security skills and knowledge by way of training, receiving mentorship, self-study, shadowing and assisting in more advanced engagements, and seeking out additional ways to contribute and grow beyond what is asked and expected.
- A solid methodology and the skills required to detect and exploit web application vulnerabilities, bypass WAFs, IPS, et cetera with and without the assistance of tools.
- Ability to demonstrate, present, deliver, explain, and defend findings.

- Competence with Microsoft Word, Excel, and PowerPoint expected.
- Understanding of security principles, policies, and industry best practices.
- Strong communication and technical assessment skills, particularly with regard to projects and cross-functional teams.
- Demonstrated ability to think quickly and take risks commensurate with responsibility.
- Ability to work with all levels of management and technical personnel to further the engagement's goals.
- Experience with active listening and building relationships.
- Experience working in high-pressure client environments with aggressive deadlines.
- Ability to learn quickly and implement new technologies or processes in rapid, demanding, and changing environments, establishing realistic yet aggressive timeframes.
- Ability to feel comfortable working with unproven/challenging new concepts.
- Desire to learn new and different approaches.

IOActive is an equal opportunity employer.