**Offensive Security Analyst**

**Job Type:** Remote/Full-time

**Salary:** $6,500 - $12,000 per month

**About Us:**

Global Risk and Security (GR&S) at Oracluless enables business strategy, protects client and Oracluless interests (e.g., assets and data), and stewards a strong risk culture. Our teams leverage enterprise-wide insights, deep expertise, and trusted advice so that across Oracluless, leaders and crew drive faster, stronger, risk-informed decisions.

At Oracluless, we pride ourselves on being a global leader in cutting-edge technology solutions, helping organizations navigate complex digital landscapes while mitigating risk and securing critical assets. We serve diverse clients across industries, offering comprehensive cybersecurity strategies that not only safeguard their operations but also drive sustainable growth. Our innovative approach combines industry best practices with proprietary tools, positioning us at the forefront of the cybersecurity domain.

We are passionate about fostering a collaborative, innovative, and learning-driven work environment. Our team is composed of top-tier cybersecurity professionals who bring varied backgrounds, perspectives, and expertise, ensuring we stay ahead of evolving cyber threats. Through continuous learning and knowledge sharing, we empower our employees to grow their careers while making an impactful contribution to our mission of building a safer digital world.

At Oracluless, we believe in the power of proactive security and risk management. By staying agile and future-focused, we not only protect our clients from emerging threats but also support their long-term strategic goals, enabling them to operate with confidence in today’s ever-evolving technological landscape.

**Job Overview:**

We are seeking an Offensive Security Analyst with advanced expertise in web application penetration testing to join our team. In this role, you will be responsible for identifying and exploiting security vulnerabilities within web applications, APIs, and cloud environments, helping to protect our organization's assets from sophisticated cyber threats. As a key member of the offensive security team, you will conduct red team operations, simulate attacks, and collaborate with cross-functional teams to improve security posture and mitigate risks. This position demands hands-on experience, technical proficiency, and a strong understanding of the latest vulnerabilities, attack techniques, and exploitation methods.

**Pay:**

* Competitive monthly salary based on experience and qualifications
* Performance bonuses and profit-sharing opportunities

**Shift and Schedule:**

* Regular business hours
* Occasional on-call requirements for urgent assessments

**Responsibilities:**

* Perform comprehensive web application penetration testing and vulnerability assessments across internal and external web applications.
* Identify, exploit, and document security vulnerabilities in web applications, APIs, and cloud environments, providing detailed risk assessments and recommendations for remediation.
* Simulate real-world attacks to evaluate application security controls and detect potential threats.
* Collaborate with development and security teams to offer actionable guidance on fixing vulnerabilities and strengthening security posture.
* Prepare detailed penetration testing reports and clearly communicate findings to technical and non-technical stakeholders.
* Continuously research and stay current on emerging vulnerabilities, security trends, and attack vectors in the web application landscape.
* Assist in security incident response by identifying and analyzing vulnerabilities that may be exploited during an attack.
* Conduct threat modeling and provide input on security requirements for application development.
* Develop and maintain custom scripts and tools to enhance penetration testing efforts.
* Mentor junior security team members and contribute to the overall knowledge base of the security team.

**Education Requirements:**

* Bachelor’s degree in Computer Science, Information Technology, Cybersecurity, or a related field
* Relevant certifications (e.g., CEH, OSCP, CISSP) are preferred

**Skills and Qualifications:**

* Proven experience in web application penetration testing, with a strong background in identifying vulnerabilities, performing manual testing, and using automated tools.
* Deep understanding of web application security concepts, including OWASP Top 10, secure coding practices, authentication and authorization mechanisms, session management, and input validation.
* Proficiency in using security tools such as Burp Suite, OWASP ZAP, Metasploit, and other custom scripts for penetration testing.
* Strong knowledge of web technologies such as HTML, JavaScript, CSS, AJAX, and HTTP/HTTPS protocols.
* Hands-on experience with exploiting common web vulnerabilities like SQL injection, XSS, CSRF, SSRF, RCE, XXE, and IDOR.
* Familiarity with security testing methodologies, frameworks, and standards (e.g., OWASP, PTES, NIST, MITRE ATT&CK).
* Strong scripting and programming skills (e.g., Python, JavaScript, Bash, PowerShell) to develop custom exploits and automate tasks.
* Strong analytical and problem-solving skills, with the ability to think like an attacker and identify creative ways to exploit vulnerabilities.