Penetration Tester, Senior

Key Role:
Conduct hands-on penetration testing beyond automated tool validation, with a focus on Web applications. Conduct scenario-based and functional security testing during authenticated and unauthenticated testing. Develop comprehensive and accurate reports and presentations for both technical and executive audiences. Perform documentation and logging of activities, including Wireshark logs, when applicable. Communicate findings and strategy to client stakeholders and technical staff. Apply security testing and penetration testing techniques and mindset to a wide range of projects.

Basic Qualifications:
- Experience with Metasploit, BeEF, Nessus, or Tenable SC.
- Experience with a database scanner, including Imperva, Guardium, or AppDetective.
- Experience with at least one of the following: Java, JavaScript, Perl, Python, Ruby, Bash, C or C++, C#, PHP, or SQL.
- Experience with Windows and NIX environments.
- Knowledge of applications, database, Web server design, HTML, and implementation.
- Knowledge of Burp Suite Pro and Kali Linux tools relevant to penetration testing.
- Knowledge of open security testing standards and projects, including OWASP.
- Ability to convey results clearly in formal technical reports and deliver briefings.
- Ability to conduct a Web app pen test without the use of a vulnerability scanner or exploit framework using a browser and a proxy and editor.
- Ability to obtain a security clearance required.

Additional Qualifications:
- BA or BS degree
- Offensive Security Web Expert (OSWE) or SANS GIAC Web Application Penetration Tester (GWAPT) Certification

Clearance:
Applicants selected will be subject to a security investigation and may need to meet eligibility requirements for access to classified information.

Terp Techs is an Equal Opportunity Employer.
EOE/Minorities/Females/Veterans/Disabled are encouraged to apply.