CareerCross by JAC Recruitment

Michael Page www.michaelpage.co.jp

Security Testing Engineer

Security Testing Engineer

Job Information

Recruiter
Michael Page

Job ID
1514193

Industry
Internet, Web Services

Job Type
Temporary

Location
Tokyo - 23 Wards

Salary
5 million yen ~ 6 million yen

Refreshed
December 30th, 2024 12:25

General Requirements

Career Level
Mid Career

Minimum English Level
Daily Conversation

Minimum Japanese Level
Business Level

Minimum Education Level
Bachelor's Degree

Visa Status
Permission to work in Japan required

Job Description

Our client, a global leader in e-commerce and digital services, is looking for security engineer who will responsible for testing of security aspects of Web Application/API.

Client Details

Our client is global technology company, known for its e-commerce platform, online banking, digital content, and telecommunications services.They operates in multiple countries, so understanding cultural differences and multilingual support might be beneficial.

Description

- Perform security testing to identify vulnerabilities in web applications and APIs.
- Follow industry standards, including the OWASP Web Security Testing Methodology.
- Utilize tools like Nmap and Nessus to conduct thorough network scans and detect potential vulnerabilities.
- Create detailed vulnerability tickets to report the findings.
- Share the results in a debriefing meeting for team collaboration and awareness.

Job Offer

- A dynamic, energetic working environment with good work/life balance
- Open culture and job rotation available to enable internal career development
- Competitive salary and benefits package
- Opportunity for growth and advancement within the company
- Collaborative and supportive team environment

To apply online please click the 'Apply' button below. For a confidential discussion about this role please contact Ayaka Iwaki at +81 3 6832 8658.

Required Skills

- Experience of Web application penetration testing, network scanning.
- Familiarity with tools like Nmap, Nessus, and other network scanning tools to identify vulnerabilities in networks and infrastructure.
- Experience with penetration testing techniques to actively exploit vulnerabilities and determine potential impact.
- Proficiency in reporting vulnerabilities clearly and effectively, both in writing (e.g., creating vulnerability tickets) and during meetings (e.g., debriefing sessions).

Company Description

Our client is global technology company, known for its e-commerce platform, online banking, digital content, and telecommunications services.They operates in multiple countries, so understanding cultural differences and multilingual support might be beneficial.