Job Details

Job Title: Penetration Tester

Company Name: Riseup Labs

Share

Riseup Labs is Hiring a Penetration Tester!

📍 **Location:** Remote
🏢 **Company:** Riseup Labs

Are you passionate about identifying vulnerabilities, safeguarding platforms, and ensuring data security? 🚀 Join **Riseup Labs**, where we work on cutting-edge projects and help us enhance our security posture with your expertise!

Job Responsibilities:

As a Penetration Tester, you will:

1. **Input Validation & Injection Attacks**
   - Identify vulnerabilities like **SQL Injection**, **XSS**, **CSRF**, and **Command Injection** across web applications and APIs.
2. **Authentication & Authorization**
   - Test for broken authentication, privilege escalation, session management flaws, and URL manipulation vulnerabilities.
3. **Payment Gateway Security**
   - Assess **Stripe integration** for PCI DSS compliance, API misconfigurations, replay attacks, and webhook authentication.
4. **API Security**
   - Detect BOLA issues, enforce rate limiting, prevent API key leakage, and sanitize API inputs.
5. **Cryptography**
   - Analyze encryption methods, key lengths, and secure storage for sensitive credentials.
6. **Data Storage and Privacy**
   - Identify unencrypted sensitive data and log vulnerabilities.
7. **Denial of Service (DoS)**
   - Test for DoS risks, including request flooding and database query abuse.
8. **Infrastructure & Deployment**
   - Validate endpoint protection, security headers, subdomain/DNS configurations, and deployment vulnerabilities.
9. **Framework & Third-Party Libraries**

- Conduct network testing, OWASP Top 10 vulnerability assessments, social engineering simulations, and wireless security tests.

Job Requirements:

Technical Skills:

1. **Proficiency in Security Tools**: Metasploit, Burp Suite, Nmap, Wireshark, Nessus, etc.
2. **Programming Knowledge**: Expertise in scripting languages like Python, Bash, Ruby, or JavaScript.
3. **API Security**: Strong understanding of API endpoint testing and secure integrations.
4. **Cloud Security**: Experience securing cloud platforms (e.g., AWS, Azure, or Google Cloud).
5. **Web and Network Security**: In-depth knowledge of OWASP Top 10, TCP/IP, DNS, firewalls, and VPN security.
6. **Compliance Knowledge**: Familiarity with PCI DSS, GDPR, and industry security standards.
7. **Vulnerability Management**: Experience with identifying, exploiting, and remediating vulnerabilities.

Certifications (Preferred but Not Mandatory):

- Certified Ethical Hacker (CEH)
- Offensive Security Certified Professional (OSCP)
- GIAC Penetration Tester (GPEN)
- CompTIA PenTest+
- Certified Information Systems Security Professional (CISSP)

Soft Skills:

- **Analytical Thinking**: Ability to identify complex security issues and provide actionable recommendations.
- **Communication**: Document findings clearly and effectively communicate them to technical and non-technical stakeholders.
- **Problem-Solving**: Creativity in uncovering hidden vulnerabilities and recommending solutions.

Experience & Education:

- **Work Experience**: 3+ years of penetration testing, ethical hacking, or related fields.
- **Education**: Bachelor's degree in Cybersecurity, Computer Science, or related disciplines (or equivalent experience).

🔗 **Ready to apply?**
Join us and make a difference in cybersecurity. Submit your application today!

Submit your CV/ Resume at: wasif.zaman@riseuplabs.com

Deadline: 02 February, 2025

Other Jobs

View All

TECLA

Jr. Manual QA Analyst

Remote

Not Specific

Publish Date: 23 March, 2025

LifeMD

Quality Assurance Auditor

Full Time Remote

Publish Date: 03 March, 2025

MailerLite

Senior Test Automation Engineer

Full Time

Remote Worldwide

Publish Date: 09 February, 2025