Cybersecurity Internship Program

Offered by: Tinos Software and Solutions LLP

Duration: 3 Months (Paid)

Location: Palarivattom / Remote

Application Deadline:25/02/2025

Internship Overview

The **Cybersecurity Internship Program** at **Tinos Software and Solutions LLP** is a **three-month paid training** designed for individuals seeking hands-on experience in **Web Application Security, Mobile App Security (Android/iOS), and Software Security Testing**. Interns will work on **real-world security projects, perform security assessments on applications, and gain exposure to industry-standard tools and techniques**.

Internship Objectives

By the end of the internship, participants will be able to:

- Conduct **penetration testing on web and mobile applications (Android & iOS)**.
- Perform **software security assessments** and identify vulnerabilities in applications.
- Utilize **industry-standard cybersecurity tools** such as Burp Suite, OWASP ZAP, MobSF, Frida, and Metasploit.
- Identify, exploit, and document security vulnerabilities using **ethical hacking methodologies**.
- Understand corporate security frameworks, **secure coding practices, and risk**
- **mitigation strategies**.

Internship Curriculum

Month 1: Foundations & Web Application Security

Week 1: Introduction to Cybersecurity & Ethical Hacking

- Fundamentals of **cybersecurity, threat landscapes, and attack vectors**
- Understanding **software security assessment methodologies**
- Setting up a **penetration testing environment** (Kali Linux, Burp Suite, OWASP ZAP)
- Introduction to **OWASP Top 10 vulnerabilities**

Week 2: Web Application Security & Testing

- Web technologies overview (HTTP, API security, session management)
- OWASP Top 10 vulnerabilities in detail (SQL Injection, XSS, CSRF, SSRF, IDOR)
- Hands-on **web security testing using Burp Suite & OWASP ZAP**
- Security misconfigurations in **modern web applications and frameworks**

Week 3: API Security Testing & Secure Development Practices

- Common **API security threats and vulnerabilities**
- Testing REST and GraphQL APIs for security flaws
- Secure coding practices for web and software development
- Case study: **Real-world API security breaches and their impact**

Week 4: Web Application Security Assessment

- Conducting a **full security test on a live web application**
- Exploiting vulnerabilities and simulating attacks
- Generating **professional security assessment reports**

Month 2: Mobile Application & Software Security Testing

Week 5: Android & iOS Application Security

- **Android security architecture, APK analysis, and reverse engineering**
- iOS security, jailbreaking concepts, and testing frameworks
- **Hands-on security analysis using MobSF, Frida, and Objection**
- Identifying **insecure data storage, API vulnerabilities, and authentication flaws**

Week 6: Software Security Testing & Secure Code Review

- **Secure coding best practices for software applications**
- Identifying **insecure dependencies, buffer overflows, and privilege escalation issues**
- Introduction to **static and dynamic code analysis tools**
- Hands-on **secure code review techniques**

Week 7: Advanced Exploitation Techniques

- **Privilege escalation in applications and operating systems**
- Reverse engineering fundamentals and **binary exploitation basics**
- Malware analysis and **secure software development lifecycle (SSDLC)**
- Case study: **Security analysis of popular applications**

Week 8: Advanced Mobile Security Testing

- **Bypassing authentication mechanisms in mobile apps**
- Reverse engineering Android & iOS applications
- Advanced **Frida scripting for mobile security**
- Practical mobile application security assessment

Month 3: Security Assessments & Enterprise Security

Week 9: Security Auditing & Compliance Standards

- **Understanding ISO 27001, NIST, GDPR, and PCI-DSS compliance**
- Conducting **security audits for web and mobile applications**
- Risk assessment methodologies and **remediation strategies**

Week 10: Exploit Development & Zero-Day Research

- **Introduction to exploit development and fuzzing techniques**
- Real-world vulnerability analysis and proof-of-concept (PoC) development
- Case study: **Analysis of recent security vulnerabilities**

Week 11: Incident Response & Risk Management

- **Cyber incident handling and vulnerability management**
- Threat intelligence gathering and adversary profiling
- Secure application deployment strategies

Week 12: Final Security Assessment & Evaluation

- Conducting a **live penetration test on a real-world application**
- Preparing a **professional security assessment report**
- Final presentation and evaluation
- Internship completion and certification

Internship Benefits

- **Paid, full-time internship** with hands-on experience in cybersecurity
- Mentorship from **experienced security professionals**
- Exposure to **real-world cybersecurity challenges and projects**
- Opportunity to work on **security assessments in a corporate environment**
- Internship **completion certificate**
- Potential opportunity for **long-term employment at Tinos Software and Solutions LLP**

Application Process

1. Submit your **resume and cover letter** to **support@tinos.co.in**.
2. Include **relevant cybersecurity projects**, such as **GitHub repositories, security research, or penetration testing experience**.
3. Shortlisted candidates will be required to complete a **technical assessment**.
4. Selected applicants will undergo a **technical interview** with the cybersecurity team.
5. Successful candidates will receive an **official internship offer**.

Contact Information

📧 Email: **support@tinos.co.in**

🌐 Website: **https//:tinos.co.in**

📍 Location: **Palarivattom/Remote**

phone :**+91 7907358458**