



# CYBER SECURITY

[WWW.FUTUREINTERNS.COM](http://WWW.FUTUREINTERNS.COM)



# TIMELINE

1



**Offer Letters are sent**

2



**After 2 Weeks  
Submission form  
is mailed**

3



**Certificate and  
LoR is Processed**

4

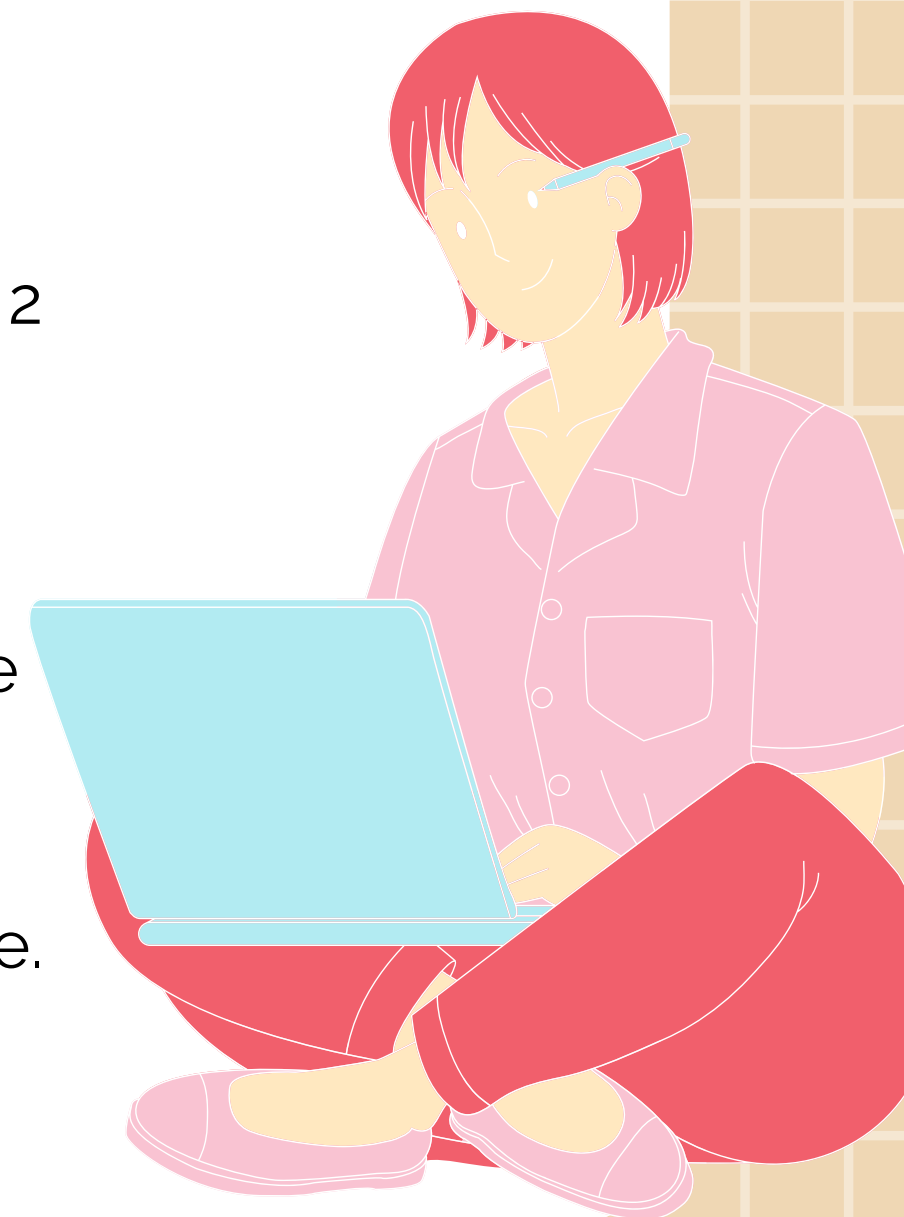


**100\$ Worth  
Goodies Access**



# IMPORTANT GUIDELINES FOR YOUR INTERNSHIP

- **Start Date:** You should begin your internship tasks only after the official start date mentioned in your Offer Letter email.
- **Domain-Specific Tasks:** Focus solely on completing tasks within your assigned domain as stated in the Offer Letter.
- **Completion Certificate:** To qualify, you must successfully complete a minimum of 2 tasks within your internship track.
- **Letter of Recommendation (LoR):** To be eligible, you need to complete at least 3 tasks in your domain.
- **Learning Resources:** The internship is self-directed. You are encouraged to choose your own learning materials to complete your tasks, as no formal training will be provided.
- **Flexibility:** This is a self-paced internship, allowing you to work at your convenience. There are no fixed timings or daily schedules.



# TASK SUBMISSION GUIDELINES

## GitHub Repository:

- You are required to maintain a public GitHub repository to document all tasks you complete.
- Use the following naming convention for your repository:
- "FUTURE\_TrackCode\_TaskNumber"
- Example: If you are pursuing a Cyber Security Internship and working on Task 2, your repository name should be "FUTURE\_CS\_02".



# COMPLETION GUIDELINES

- **Task Submission Form:**
  - A Task Submission Form will be provided around the middle of your internship month. Use this form to submit your completed tasks.
- **Programming Language and Tools:**
  - You are free to use any programming language, tool, or framework to complete your tasks, depending on your preference and expertise.
- **Recommended Tools for Cybersecurity Interns:**
  - **Programming Languages:** Python, Java, C, or Bash
  - **Cybersecurity Tools:** Wireshark, Metasploit, Burp Suite, Nmap
  - **Platforms:** Kali Linux, VirtualBox, AWS, or other cloud platforms
  - **Text Editors and IDEs:** VS Code, Sublime Text





# BUILDING YOUR PROFESSIONAL LINKEDIN PROFILE

## 1) Showcasing Your Internship:

- Post your internship offer letter on LinkedIn to announce your journey with Future Interns.
- Update your LinkedIn profile by:
  - Adding "Intern at Future Interns" in your headline.
  - Listing "**Future Interns**" as your current company in the work experience section.

## 2) Task-Based LinkedIn Posts:

- After completing each task, it is MANDATORY to create a LinkedIn post.
- Your post should summarize the task, highlight what you learned, and include relevant insights, screenshots, or visualizations.
- To enhance your post's visibility and engagement, consider adding a video demonstration of your work (optional but recommended).





# **CYBER SECURITY**

**TRACK CODE: CS**

# TASK 1

## WEB APPLICATION SECURITY TESTING

- ◆ **Task:** Conduct security testing on a sample web application to identify vulnerabilities like SQL injection, XSS, and authentication flaws.
- ◆ **Skills Gained:** Web application security, ethical hacking, penetration testing.
- ◆ **Tools:** OWASP ZAP, Burp Suite, SQLMap.
- ◆ **Deliverable:** A detailed security report with identified vulnerabilities and mitigation strategies.

[Full Details](#)





## TASK 2



# SECURITY ALERT MONITORING & INCIDENT RESPONSE

- ◆ **Task:** Monitor simulated security alerts using a SIEM tool, identify suspicious activities, classify incidents, and draft an incident response report.
- ◆ **Skills Gained:** Log analysis, alert triage, incident classification, SOC operations basics.
- ◆ **Tools:** Elastic Stack (ELK), Splunk Free Trial, sample log files.
- ◆ **Deliverable:** Incident response report with alert analysis, incident classification, and remediation recommendations.

[Full Details](#)



## TASK 3

# SECURE FILE SHARING SYSTEM

- ◆ **Task:** Build a file upload/download portal with AES encryption to secure files at rest and in transit.
- ◆ **Skills Gained:** Web development, encryption implementation, secure file handling, key management.
- ◆ **Tools:** Python Flask or Node.js (Express), PyCryptodome or Node.js Crypto module, Git & GitHub, Postman/curl.
- ◆ **Deliverable:** GitHub repo, walkthrough video, and a security overview document.

[Full Details](#)



# Thank you



**EMAIL**

[contact@futureinterns.com](mailto:contact@futureinterns.com)



**WEBSITE**

[futureinterns.com](http://futureinterns.com)



**LinkedIn**

[linkedin.com/future-interns/](https://linkedin.com/future-interns/)