



# INTERNSHIP TASKLIST

## BLUE TEAMING



CLOUD  
SECURITY

NETWORK  
SECURITY

CYBER  
SECURITY

**2025**  
JANUARY  
BATCH

# ***Internship Pre-requisites before starting your tasks:***



- 
1. **LinkedIn Profile Update:** Ensure that your LinkedIn profile is updated to reflect your technical skills, and update your experience section to include "HACK SECURE Cyber Security Intern."
  2. **LinkedIn Post:** It's not mandatory to post the offer letter on LinkedIn, but if you wish at the end of the internship, you can post your offer letter and tag us.
  3. **Completion of Tasks:** Complete the required tasks as specified in this Task List.
  4. **Proof of Work:** At HACK SECURE, we value Proof of Work (POW). You need to get validated from your mentor before you submit your respective tasks in the Task Submission Forms.

**Note:** Do not upload your Report in LinkedIn, this would allow others to copy your work. If the team finds out that you have posted your report in LinkedIn, your internship would be terminated.

After completing all the above steps, proceed with your task completion. Kindly note that all the details and reports you submit will be thoroughly verified before you receive the Certificate.

---

# **TASK LEVEL INTERMEDIATE**

---

- 1).** Find all the ports that are open on the website <http://testphp.vulnweb.com/>
  
- 2).** Brute force the website <http://testphp.vulnweb.com/> and find the directories that are present in the website.
  
- 3).** Make a login in the website <http://testphp.vulnweb.com/> and intercept the network traffic using Wireshark and find the credentials that were transferred through the network.
  
- 4.)** Perform SQL injection on the login or search page of <http://testphp.vulnweb.com/> and check if the website is vulnerable to SQLi by extracting database information.
  
- 5.)** Inject malicious JavaScript payloads in input fields (such as the comment section or search box) to see if the website is vulnerable to stored or reflected XSS attacks.

# **TASK (CTF)**

---

## **1. IR Playbooks**

- Incident Response Phases: Identification, containment, recovery, and lessons learned.
- IR Tools: Log analysis, network forensics, and endpoint monitoring.
- Playbook Creation: Build customized incident response playbooks.

## **Investigation with Splunk**

- Detection Focus: Monitor Exchange exploit attempts, lateral movement, and persistence mechanisms.
  - Response Actions: Investigate data exfiltration patterns and credential dumping activity.
- Tools: Use Splunk, Sysmon, and Windows Event Logs.



**Congratulations!**

🚀 Here's a Glimpse of Your Future Achievement



***Hack Secure, boosting your Experience  
with  
this impactful internship!***

*Lakshay Jain*  
Co-Founder & CEO

*Aryan Thakur*  
Founder & MD