internStudio

CYBERSECURITY INTERNSHIP

TASK GUIDE

Find the gaps before attackers do.
Secure real systems, hands-on.

SIX ADVANCED PROJECTS — CHOOSE ANY TWO

01 **Web Application Vulnerability Scanner & Audit Tool**

02 **Network Intrusion Detection System**

03 **Secure Secrets & Password Vault**

04 **Web Application Penetration Test & Remediation Report**

05 **Phishing & Email Security Analyzer**

06 **Security Log Monitoring & Alerting Dashboard**

INTERNSHIP	REQUIRED TASKS	FOCUS
Cybersecurity	Complete any 2 projects	Vulnerability Assessment · Network Security · Cryptography · Monitoring

INTERNSHIP INSTRUCTIONS

Your Internship Tasks

Select and complete **any 2 projects** from the task list. All testing must be performed only against systems you own, deliberately vulnerable apps, or environments you have explicit permission to test.

Scope	Recon	Test	Exploit	Remediate	Report

EVERY PROJECT SHOULD INCLUDE

- [ ] Testing scoped only to systems you own or are authorized on
- [ ] A methodical process, not random poking
- [ ] Clear documentation of every finding
- [ ] A severity rating for each issue found
- [ ] A concrete remediation recommendation per issue
- [ ] Evidence (screenshots/logs) for each finding
- [ ] Awareness of the legal and ethical boundaries
- [ ] A professional-style write-up

BEFORE YOU SUBMIT

- [ ] Complete any 2 projects from the list
- [ ] Push tooling/code to GitHub
- [ ] Include the written assessment report
- [ ] Redact any real sensitive data from evidence
- [ ] Add a README describing scope and methodology
- [ ] Submit details via the submission form
- [ ] Share your work on LinkedIn as required

> **Suggested technologies:** Kali Linux tooling (Nmap, Burp Suite, OWASP ZAP) · Python for tooling · a deliberately vulnerable target (DVWA, Juice Shop, a VM lab).

Submit your completed work here

Once both projects are documented and pushed to GitHub, submit your project details through the official submission form.

https://forms.gle/vxL5JE8cvRXXfDBv8

> **A note on ethics.** Every project here must be run only against systems you own, deliberately vulnerable practice apps, or environments you have explicit written permission to test. Never test systems you do not control.

01 Web Application Vulnerability Scanner & Audit Tool

Build a tool that scans a web application for common OWASP Top 10 issues and produces an audit report.

REQUIREMENTS

- Detect at least four distinct OWASP-class vulnerabilities
- Distinguish confirmed findings from suspected ones
- Generate a structured, exportable report
- Test only against an authorized/deliberately-vulnerable app
- Crawl the target app systematically before testing
- Avoid destructive payloads against the target
- Rate each finding by severity (CVSS or similar)
- Recommend a specific fix per finding

Focus: Automated vulnerability discovery, structured reporting and severity-based prioritization.

02 Network Intrusion Detection System

Build a system that analyzes network traffic and flags likely intrusion attempts.

REQUIREMENTS

- Capture and parse real network traffic
- Distinguish signature-based from anomaly-based detection
- Log detected events with enough context to investigate
- Test against both benign and simulated attack traffic
- Detect at least two attack patterns (e.g. port scan, brute force)
- Tune detection to minimize false positives
- Alert in near-real-time, not only in a batch report
- Document detection logic and its limitations

Focus: Traffic analysis, intrusion detection logic and false-positive-aware tuning.

03 Secure Secrets & Password Vault

Build a vault that stores credentials and secrets with real cryptographic protection, not just a database column.

REQUIREMENTS

- Encrypt secrets at rest with a proper cipher
- Master-password or key-derivation-based unlock
- Full audit log of who accessed what and when
- Protection against common attack vectors (timing, brute force)
- Never store or log secrets in plaintext
- Fine-grained access policies per secret
- Secure secret rotation / update flow
- Document the threat model and its limits

Focus: Applied cryptography, access control and audit logging done properly.

04 Web Application Penetration Test & Remediation Report

Perform a structured penetration test against a deliberately vulnerable application and document your findings professionally.

REQUIREMENTS

- Follow a real methodology (recon, enumeration, exploitation, reporting)
- Chain findings where realistic (e.g. XSS leading to session theft)
- Rate severity and business impact per finding
- Test only against an authorized target (DVWA/Juice Shop/your own app)
- Identify and exploit at least three distinct vulnerabilities
- Document exact reproduction steps for each finding
- Recommend concrete remediation per finding
- Deliver a professional written report

Focus: End-to-end penetration testing methodology and professional security reporting.

05 Phishing & Email Security Analyzer

Build a tool that analyzes emails and URLs for phishing indicators and scores the risk.

REQUIREMENTS

- Parse email headers for spoofing indicators
- Analyze links for typosquatting or redirect chains
- Explain which signals drove the score
- Measure false positive / false negative rate
- Check SPF/DKIM/DMARC alignment
- Score overall phishing risk, not just flag yes/no
- Test against a set of known-good and known-phishing samples
- Document detection limitations honestly

Focus: Email authentication analysis, URL inspection and explainable risk scoring.

06 Security Log Monitoring & Alerting Dashboard

Build a SIEM-style dashboard that aggregates security-relevant logs and surfaces suspicious patterns.

REQUIREMENTS

- Ingest logs from at least two distinct sources
- Detect patterns indicating compromise (e.g. repeated failed logins)
- Alert on high-severity patterns with clear context
- Support querying/filtering historical events
- Normalize logs into a consistent event format
- Correlate related events across sources
- Visualize event volume and trends over time
- Document what each alert rule is designed to catch

Focus: Log aggregation, correlation and security-focused alerting design.

FINAL STEP

Ready to Submit?

Verify everything below before you send your work in.

SUBMISSION

- [ ] GitHub repository
- [ ] Written assessment report
- [ ] README describing scope and methodology
- [ ] Submission form completed
- [ ] LinkedIn post where required

REMEDIATION

- [ ] Concrete fix recommended per issue
- [ ] Remediation prioritized by severity
- [ ] Report is professional and readable

SCOPE & ETHICS

- [ ] Testing scoped to authorized targets only
- [ ] No real sensitive data exposed in evidence
- [ ] Legal/ethical boundaries respected

FINDINGS

- [ ] Each finding documented clearly
- [ ] Severity rated for each issue
- [ ] Evidence included for each finding

Important. Complete any 2 projects. Every project must be tested only against authorized systems — this is a hard requirement, not a suggestion.

Submission Form

Submit your repository, live link and screenshots here.

https://forms.gle/vxL5JE8cvRXXfDBv8

internStudio

LEARN · BUILD · GROW

www.internstudio.in

team.internstudio@gmail.com