# Security Engineer Intern task

# Pinewheel.ai

# Ronit Gupta

**Command:** sudo apt update && apt install {necessary tools}

**Output :**

- terminal gets updated to latest version in order to run desired commands

**Reason:** most of the tools were not found

**command:** nmap -Pn testing.pinewheel.ai

**output:**

- Ports 80 (HTTP) and 443 (HTTPS) are open.

**reason:** Identifying open services and potential attack vectors.

**Command:** wafw00f https://testing.pinewheel.ai

**Output:**

- Amazon Cloudfront WAF is enabled

**Reason:** to check wether the server is prone to web based attacks such SQLi

**Command:** nslookup testing.pinewheel.ai

**Output:**

- testing.pinwheel.ai is using the IP address “172.31.0.2” which is a private IP address used by AWS

**Reason:** trying to find the IP address

**Command:** whatweb testing.pinewheel.ai

**Output:**

- “http://” gets redirected to “https://” Cloudfront rejects the request

Reason: trying to identifying framework and service details

**Command:** sqlmap -u "https://testing.pinewheel.ai/login?username=admin&password=123" --dbs --batch

**Output:**

- site is protected by AWS WAF

**Reason**: to extract database number

**Command:** curl -I https://testing.pinewheel.ai

**Output:**

- Website is running next.js
- security headers are missing

**Reason:** identifying missing security headers

**Command:** git clone --depth 1 https://github.com/drwetter/testssl.sh.git

**Output:**

- installing testsshl.sh

**Reason:** used for checking SSL/TLS configuration, and to check for security weaknesses

**Command:** ./testssl.sh https://testing.pinewheel.ai

**Output:**

- TLS 1.2 and TLS 1.3 are enabled
- Site is using AEAD cipher which not only encrypts data but verifies its authenticity and integrity
- Certificate issued by Amazon and valid till 2026
- **Http compression is enabled which can be exploited for breach attacks**
- **RSA 2048 key is used**
- Application-Layer Protocol Negotiation (ALPN) is supported

**Reason:** identifying weak encryption, misconfiguration, and vulnerabilities in SSL/TLS settings

**Command:** nikto -h https://testing.pinewheel.ai

**Output:**

- HTTP Strict Transport Security (HSTS) is missing
- which can result in Man in the middle Attack.
- X-Frame-option header is missing.
- /Robot.txt exposes /api/
- Content encoding is set “deflate” which is vulnerable to breach attacks

**Reason:** scanning for security misconfiguration and vulnerabilities