IN-DEPTH PENTEST /
SECURITY AUDIT

22/02/2025

# Security Engineer Intern Task

PINEWHEEL.AI

**PREPARED BY :**

Shriram Mahadeo Hage

# 1. Introduction

This penetration test was conducted to assess the security posture of testing.pinewheel.ai. The test involved identifying vulnerabilities in both pre-authentication and post-authentication phases using a combination of manual and automated tools in Kali Linux.

# 2. Scope of Testing

- Target URL: https://testing.pinewheel.ai
- Testing Methods: Black-box, Grey-box
- Tools Used: Kali Linux (Nmap, Burp Suite, SQLmap, etc.)
- Areas Tested:
  - Pre-authentication vulnerabilities
  - Post-authentication vulnerabilities
  - API security
  - Web application security (SQL Injection, XSS, SSRF, SSTI, Prompt Injection, RCE, etc.)

# 3. Execution.

## 3.1 Subdomain & Directory Enumeration

command: sublist3r -d testing.pinewheel.ai
output: Not a satisfactory response.
reason: "Identifying subdomains for further testing."
Onlinetool output-

| Host | Subdomain |
|---|---|
| pinewheel.ai | india.pinewheel.ai |
| pinewheel.ai | docs.pinewheel.ai |
| pinewheel.ai | local.pinewheel.ai |
| pinewheel.ai | testing.pinewheel.ai |
| pinewheel.ai | terminal.pinewheel.ai |
| pinewheel.ai | blog-staging.pinewheel.ai |
| pinewheel.ai | www.pinewheel.ai |
| pinewheel.ai | vercel.pinewheel.ai |

command: gobuster dir -u https://testing.pinewheel.ai -w /usr/share/wordlists/dirb/common.txt
output:

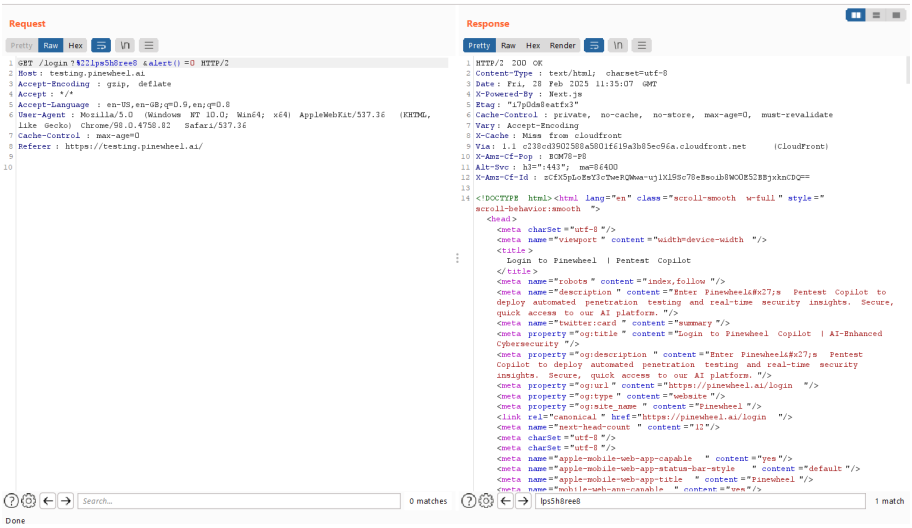

reason: "Discovering hidden directories."

## 3.2. Suspicious HTTP Request and Response Analysis

**Test Request:**

GET /login?8221ps5h8ree8&alert()=0 HTTP/2
Host: testing.pinewheel.ai
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US, en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, Chrome/98.0.4758.82 Safari/537.36)
Cache-Control: max-age=0
Referer: https://testing.pinewheel.ai/

**Observations:**




- The request included a **query string parameter (8221ps5h8ree8&alert()=0)**.
- No significant security warning or error message was triggered in the response.

- The application responded with HTTP/2 200 OK, which might indicate **input handling without proper validation.**
- X-Powered-By: Next.js in the response header indicates the backend framework.
- The presence of X-Cache Miss from cloudfront suggests **CloudFront is being used as a CDN.**

**Potential Risks:**

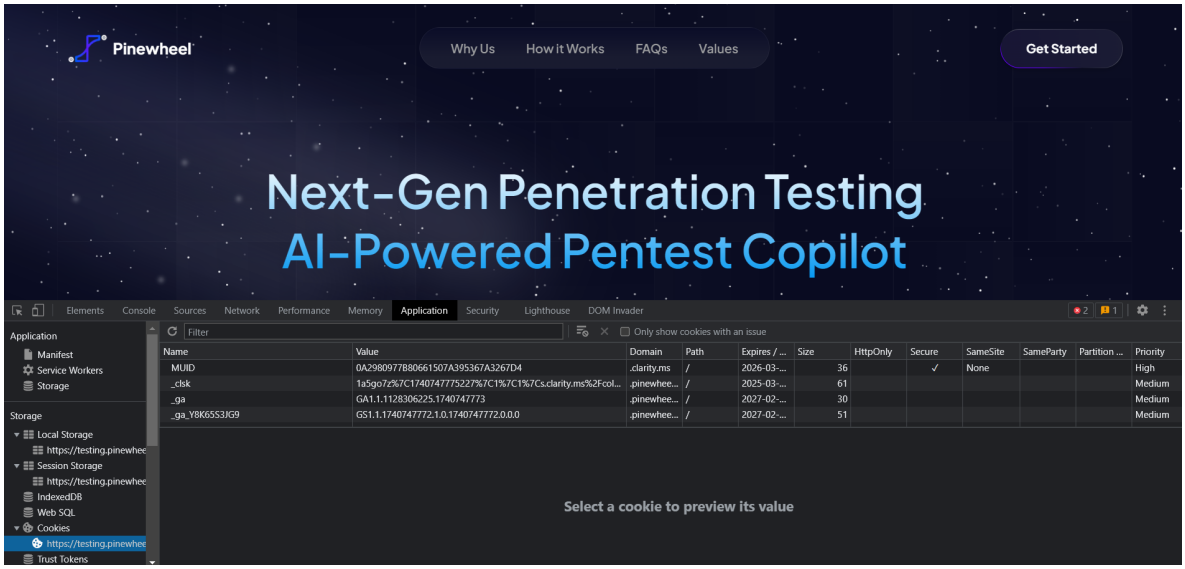
- If the alert() function was meant to execute JavaScript, this could indicate **a potential XSS vulnerability.**
- Lack of explicit error messages reduces the risk of **information disclosure**, but further testing is needed to confirm input validation.

**Recommendations:**

- Implement **strict input validation** to prevent potential **XSS attacks.**
- Sanitize and escape special characters in user input fields.
- Use **Content Security Policy (CSP)** headers to mitigate JavaScript injection.
- Implement proper logging and monitoring to detect unusual query patterns.

## 3.3. Cookie and Storage Analysis

**Observations: HTTP and secure flag not set properly**




- The application sets multiple cookies, including _clsk, _ga, and _ga_Y8K65S3JG9.
- The cookies have various expiration dates ranging from **2025 to 2027**.

- SameSite=None is present, which may allow **cross-site tracking** if not handled properly.
- Some cookies are marked as **Secure**, but HttpOnly is not set for all, increasing risk of client-side access.

**Recommendations:**

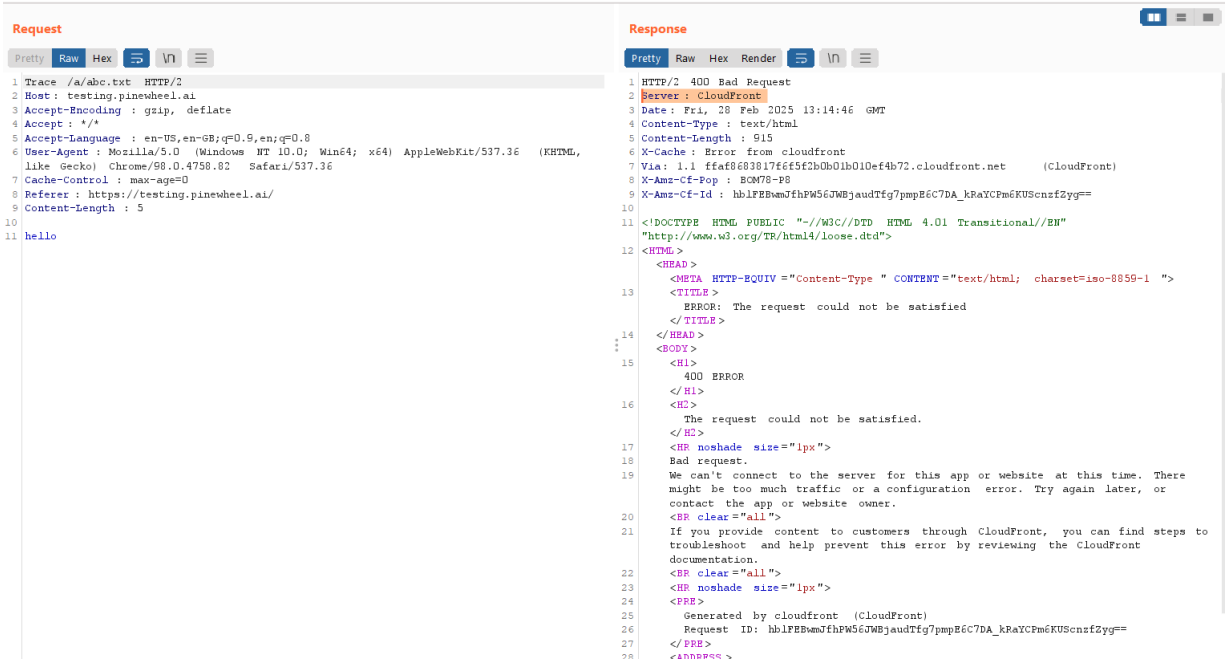
- Ensure **HttpOnly flag** is set for all sensitive cookies to prevent client-side JavaScript access.
- Restrict cookie access using **SameSite=Strict or Lax** to mitigate CSRF attacks.
- Periodically review and clean up stored cookies and local/session storage data.

## 3.4. TRACE Request Handling

**Test Request:**

TRACE /a/abc.txt HTTP/2
Host: testing.pinewheel.ai
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US, en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.82 Safari/537.36
Cache-Control: max-age=0
Referer: https://testing.pinewheel.ai/
Content-Length: 5
hello

**Observations:Server name disclosure**



- The request attempted to use the TRACE HTTP method.
- The response was HTTP/2 400 Bad Request, meaning the request was rejected.
- X-Cache: Error from cloudfront indicates that CloudFront likely blocked the request.
- TRACE method, if enabled, could be exploited for **Cross-Site Tracing (XST) attacks**.

**Recommendations:**

- **Disable the TRACE method** in web server configurations to prevent XST attacks.
- Ensure the server only allows necessary HTTP methods (GET, POST, etc.).
- Implement security headers such as X-Frame-Options and X-Content-Type-Options for additional protection.

# 4.Conclusion

- No immediate SQL Injection vulnerability was identified.
- Possible **improper input handling** in query parameters, requiring further review.
- Security mechanisms such as **CSP, input validation, and prepared statements** should be enforced to prevent potential attacks.
- Cookie security should be **strengthened** by setting appropriate flags.
- TRACE method handling should be reviewed and disabled to mitigate potential risks.

# 5.Next Steps

1. Conduct **further manual testing** to confirm input validation strength.
2. Implement **security headers** to reduce exposure to common web vulnerabilities.
3. Perform **regular security audits** and penetration testing to identify new vulnerabilities.

### Report Prepared By:

**Shriram Hage** (Security Engineer Intern)