Sri Lanka Institute of Information Technology

Year 2 semester 2

IT23360600
G. P. I. Perera

SLIIT KANDY UNI

BUG BOUNTY REPORT 5

Web Security – IE2062

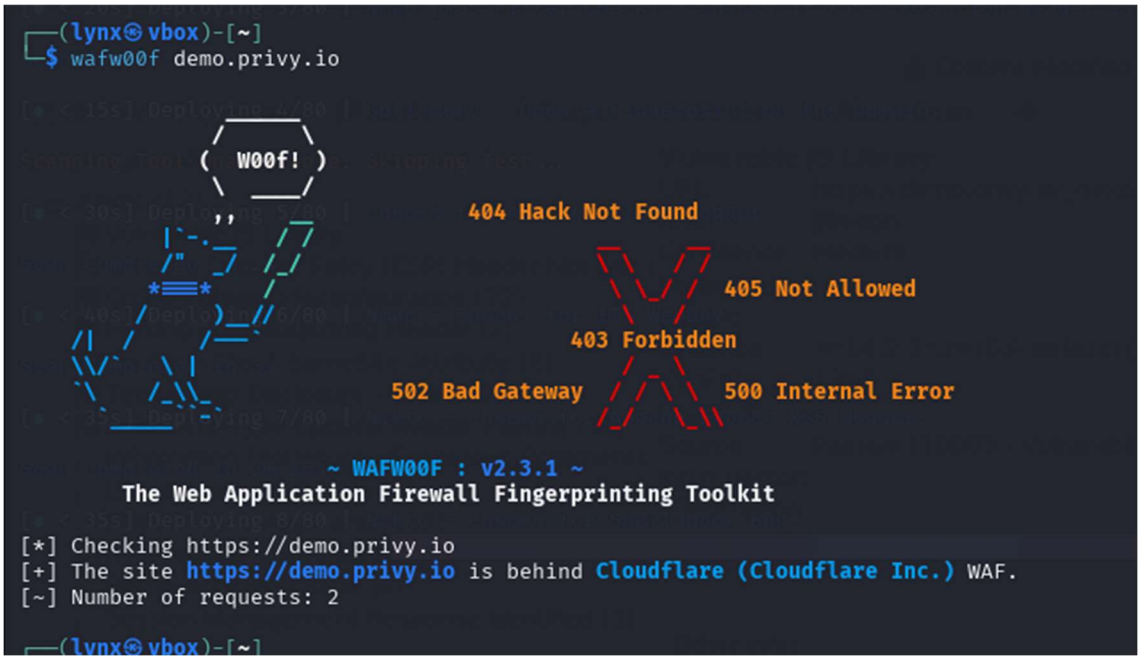
B.Sc. (Hons) in information Technology Specializing in Cyber Security

1. Requirement gathering and analysis

Selected sub domain	demo.privy.io
Hakerone URL	https://hackerone.com/
IP address	104.18.20.237/104.18.21.237

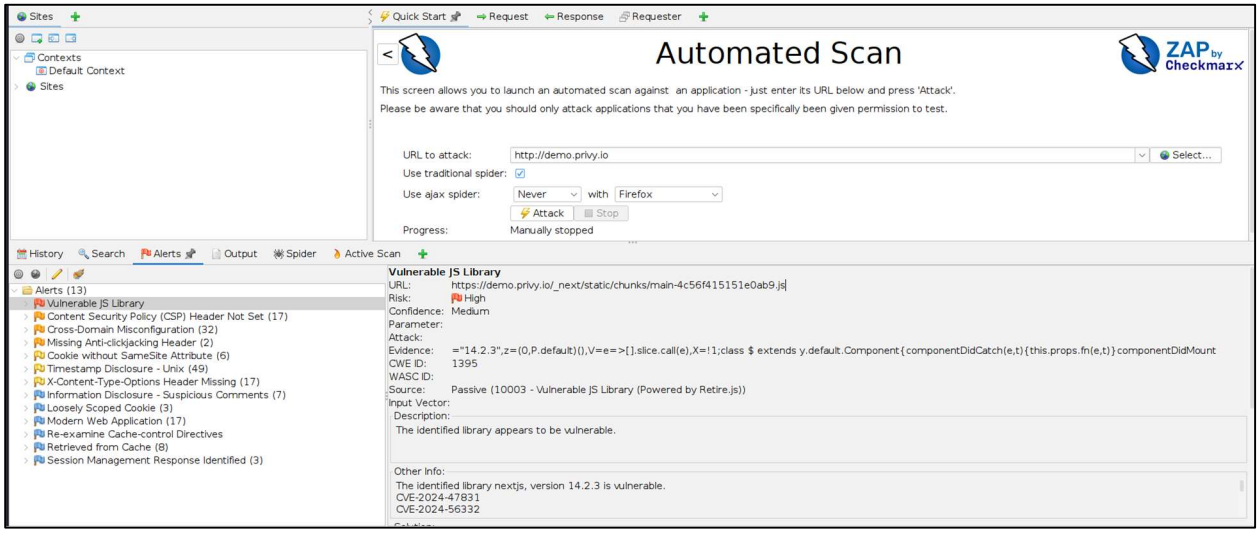
Subdomain list

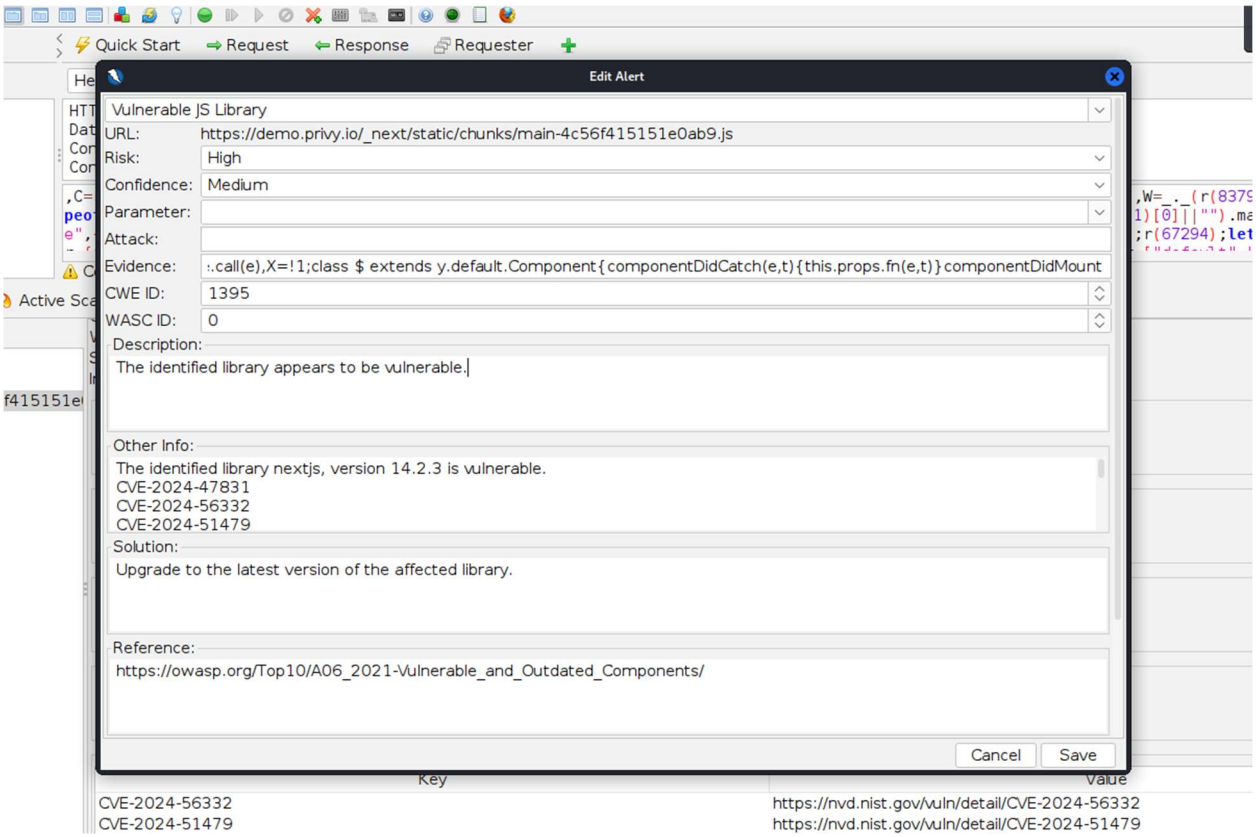
Firewall detection:



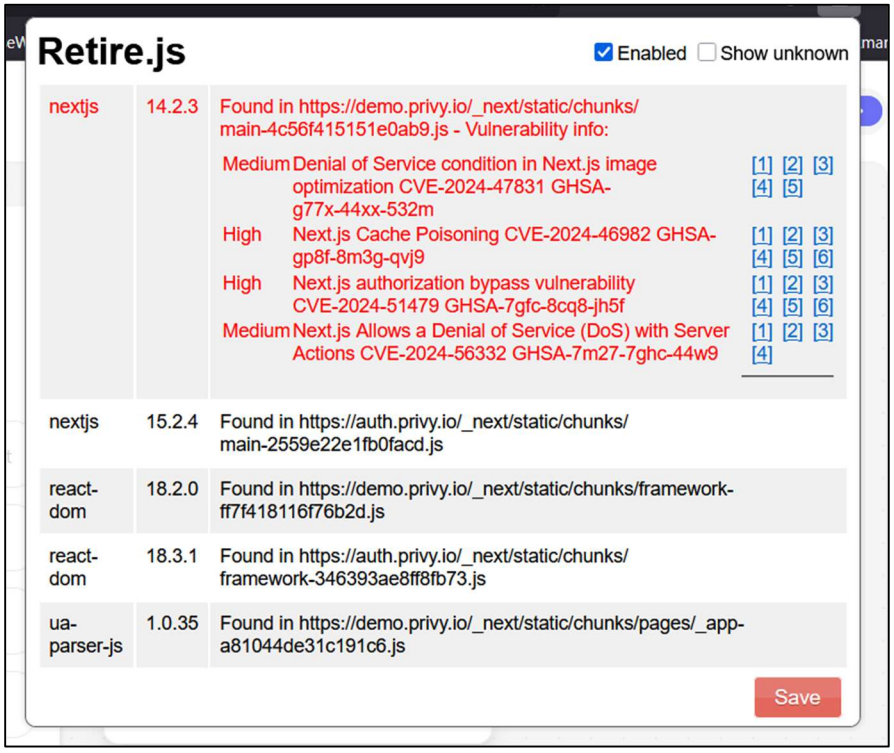
Nmap scan:

Scan result from OWASP ZAP:





Retire.js result:



2. Report Details

1. Vulnerability Title: Vulnerable JS library

2. Vulnerability Description:

Vulnerable JavaScript libraries are a major threat to the security of web applications, providing attackers with potential entry points to exploit flaws and launch harmful activities. These risks may lead to sensitive data leaks, session hijacking, or even the injection of malicious scripts. Frequently encountered vulnerabilities include Cross-Site Scripting (XSS) and SQL Injection, both of which can have serious consequences if left unaddressed.

During testing of Privy BBP Domain, **demo.privy.io** , a vulnerable js libraries were found that contains DOS in Next.js image optimization, cache poisoning and authorization bypass in Next.js and denial of service via server actions in Next.js.

Observation:

The Next.js library found in https://demo.privy.io/_next/static/chunks/main-4c56f415151e0ab9.js is an outdated version that contains two threat level vulnerabilities - CVE-2024-46982 and CVE-2024-51479 and two medium level vulnerabilities CVE-2024-56332 and CVE-2024-47831.

1. Denial of Service in Next.js Image Optimization

CVE-2024-47831 | **Medium Severity**

- **Problem:**
  Next.js has an image optimization feature (next/image) that processes and resizes images.
  Attackers could abuse it by sending **very large or specially crafted images**, making the server **work too hard**, **consume memory**, or **crash**.
- **Impact:**
  Website becomes **slow**, **unavailable**, or even **crashes** — **Denial of Service** (DoS).

2. Cache Poisoning in Next.js

CVE-2024-46982 | **High Severity**

- **Problem:**
  Next.js sometimes **caches** web pages to make them load faster.
  A flaw made it possible for an attacker to **trick the server into caching** a **bad/malicious** version of a page, which would then be shown to other users.
- **Impact:**
  Users see **wrong** or even **dangerous content** — this could lead to **phishing**, **defacements**, or worse.

3. Authorization Bypass in Next.js

CVE-2024-51479 | **High Severity**

- **Problem:**
  Certain parts of a Next.js app that were supposed to be **protected** (like user-specific data or admin panels) could be accessed by **unauthorized** users.
- **Impact:**
  Attackers might be able to **view**, **edit**, or **steal** information they shouldn't have access to.

4. Denial of Service via Server Actions in Next.js

CVE-2024-56332 | **Medium Severity**

- **Problem:**
  Newer versions of Next.js use **Server Actions** (functions that run on the server when triggered by the client).
  An attacker could **abuse** these by making the server **run expensive actions repeatedly**, causing **resource exhaustion**.
- **Impact:**
  Server could become **slow** or **unavailable** — another form of **Denial of Service** (DoS).

3. Affected Components:

1. https://demo.privy.io/_next/static/chunks/main-4c56f415151e0ab9.js

4. Impact Assessment:

OWASP analysis:

Risk level	High
Confidence	Medium

Other information:

- The identified library nextjs, version 14.2.3 is vulnerable.
- CVE-2024-47831
- CVE-2024-56332
- CVE-2024-51479
- CVE-2024-46982
- https://github.com/advisories/GHSA-g77x-44xx-532m
- https://github.com/vercel/next.js/commit/7ed7f125e07ef0517a331009ed7e32691ba403d3
- https://github.com/vercel/next.js/commit/bd164d53af259c05f1ab434004bcfdd3837d7cda
- https://github.com/vercel/next.js/security/advisories/GHSA-7m27-7ghc-44w9
- https://nvd.nist.gov/vuln/detail/CVE-2024-56332
- https://github.com/advisories/GHSA-7gfc-8cq8-jh5f
- https://nvd.nist.gov/vuln/detail/CVE-2024-51479
- https://github.com/advisories/GHSA-7m27-7ghc-44w9
- https://github.com/vercel/next.js/commit/d11cbc9ff0b1aaefabcba9afe1e562e0b1fde65a
- https://github.com/vercel/next.js/commit/1c8234eb20bc8afd396b89999a00f06b61d72d7b
- https://github.com/advisories/GHSA-gp8f-8m3g-qvj9
- https://github.com/vercel/next.js/security/advisories/GHSA-7gfc-8cq8-jh5f
- https://github.com/vercel/next.js/releases/tag/v14.2.15
- https://github.com/vercel/next.js
- https://nvd.nist.gov/vuln/detail/CVE-2024-47831
- https://github.com/vercel/next.js/security/advisories/GHSA-gp8f-8m3g-qvj9
- https://nvd.nist.gov/vuln/detail/CVE-2024-46982
- https://github.com/vercel/next.js/security/advisories/GHSA-g77x-44xx-532m

Retire.js analysis

1. **Found in** https://demo.privy.io/_next/static/chunks/main-4c56f415151e0ab9.js
   Library – next.js version 14.2.3

Threat level	Description
medium	Denial of Service condition in Next.js image optimization CVE-2024-47831 GHSA-g77x-44xx-532m
High	Denial of Service condition in Next.js image optimization CVE-2024-47831 GHSA-g77x-44xx-532m
High	Next.js authorization bypass vulnerability CVE-2024-51479 GHSA-7gfc-8cq8-jh5f
Medium	Next.js Allows a Denial of Service (DoS) with Server Actions CVE-2024-56332 GHSA-7m27-7ghc-44w9

CVE-xxxx-xxxxx - Common Vulnerabilities and Exposures (Universal identifier for security vulnerability)

GHSA – xxxx-xxxxxxx - GitHub Security Advisory (GitHub's record of security issues specifically for GitHub-hosted projects)

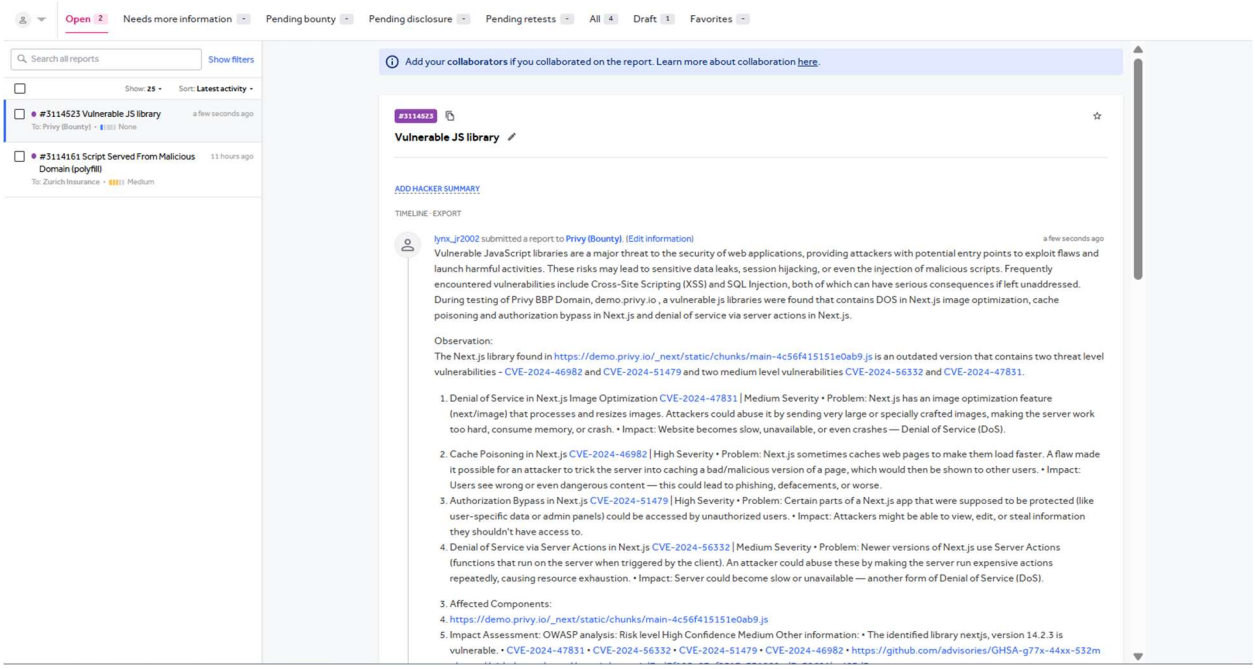
5. Steps to reproduce –

- **On owasp zap –**
  Start the application, input target URL and run an automated scan.
  Observe alerts.
- **Retire.js -**
  Add the firefox extension - retire,js to the browser and enable it. When you search the vulnerable web applications, the extension shows vulnerable libraries in the website.

6. Proposed mitigation or fix

- Regularly **audit and update dependencies**
- Avoid using user input directly in sensitive operations (e.g., setting locales)
- Use secure coding practices, including **input validation**, **regex optimization**, and **dependency scanning** with tools like **Snyk**, **Retire.js**, and **npm audit**.

7. Submission:



Reply: