

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
Hackerone URL	https://hackerone.com/
IP address	104.18.20.237/104.18.21.237

Subdomain list

[illegible]

Firewall detection:

```
(lynx@vbox)-[~]
$ wafw00f demo.privv.io

[* < 15s] Deploying 4/80 | 404 Hack Not Found
Scanning Tool: ( W00f! )
[* < 30s] Deploying 6/80 | 405 Not Allowed
[* < 40s] Deploying 8/80 | 403 Forbidden
[* < 50s] Deploying 7/80 | 502 Bad Gateway
[* < 55s] Deploying 7/80 | 500 Internal Error

~ WAFW00F : v2.3.1 ~
The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://demo.privv.io
[+] The site https://demo.privv.io is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2

(lynx@vbox)-[~]
```

Nmap scan:

```
(lynx@vbox)-[~]
$ nmap demo.privv.io
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-27 07:46 EDT
Nmap scan report for demo.privv.io (104.18.20.237)
Host is up (0.28s latency).
Other addresses for demo.privv.io (not scanned): 104.18.21.237 2606:4700::6812:14ed 2606:4700::6812:15ed
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
443/tcp   open  https
8080/tcp   open  http-proxy
8443/tcp   open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 37.40 seconds
```

Scan result from OWASP ZAP:

The screenshot shows the OWASP ZAP Automated Scan interface. The top section is titled "Automated Scan" and includes a description: "This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'. Please be aware that you should only attack applications that you have been specifically given permission to test." The URL to attack is set to "http://demo.privy.io". The spider is set to "Firefox" and the attack is set to "Never". The progress bar shows "Manually stopped".

The bottom section displays the scan results. The first result is "Vulnerable JS Library" with a URL of "https://demo.privy.io/_next/static/chunks/main-4c56f415151e0ab9.js". The risk is "High", confidence is "Medium", and the parameter is "Attack". The evidence is "14.2.3", and the CWE ID is "1395". The WASC ID is "0". The description is "The identified library appears to be vulnerable." The other info is "The identified library nextjs, version 14.2.3 is vulnerable. CVE-2024-47831 CVE-2024-56332 CVE-2024-51479".

The screenshot shows the "Edit Alert" dialog box for the "Vulnerable JS Library" alert. The dialog box contains the following information:

- URL: https://demo.privy.io/_next/static/chunks/main-4c56f415151e0ab9.js
- Risk: High
- Confidence: Medium
- Parameter: Attack
- Evidence: .call(e),X=!1;class \$ extends y.default.Component{componentDidCatch(e,t){this.props.fn(e,t)}componentDidMount
- CWE ID: 1395
- WASC ID: 0
- Description: The identified library appears to be vulnerable.
- Other Info: The identified library nextjs, version 14.2.3 is vulnerable. CVE-2024-47831 CVE-2024-56332 CVE-2024-51479
- Solution: Upgrade to the latest version of the affected library.
- Reference: https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/

The dialog box has "Cancel" and "Save" buttons at the bottom right.

Retire.js result:

Retire.js

☒ Enabled ☐ Show unknown

nextjs	14.2.3	Found in https://demo.privy.io/_next/static/chunks/main-4c56f415151e0ab9.js - Vulnerability info: Medium Denial of Service condition in Next.js image optimization CVE-2024-47831 GHSA-g77x-44xx-532m High Next.js Cache Poisoning CVE-2024-46982 GHSA-gp8f-8m3g-qvj9 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	<div><div>1</div><div>2</div><div>3</div></div> <div><div>4</div><div>5</div></div> <div><div>1</div><div>2</div><div>3</div></div> <div><div>4</div><div>5</div><div>6</div></div> <div><div>1</div><div>2</div><div>3</div></div> <div><div>4</div><div>5</div><div>6</div></div> <div><div>1</div><div>2</div><div>3</div></div> <div><div>4</div></div>
nextjs	15.2.4	Found in https://auth.privy.io/_next/static/chunks/main-2559e22e1fb0facd.js	
react-dom	18.2.0	Found in https://demo.privy.io/_next/static/chunks/framework-ff7f418116f76b2d.js	
react-dom	18.3.1	Found in https://auth.privy.io/_next/static/chunks/framework-346393ae8ff8fb73.js	
ua-parser-js	1.0.35	Found in https://demo.privy.io/_next/static/chunks/pages/_app-a81044de31c191c6.js	

Save

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:

Open 2

Needs more information

Pending bounty

Pending disclosure

Pending retests

All 4

Draft 1

Favorites

Search all reports

Show filters

Show: 25

Sort: Latest activity

#3114523 Vulnerable JS library

To: Privy (Bounty) • \$100 None

#3114161 Script Served From Malicious Domain (polyfill)

To: Zurich Insurance • \$500 Medium

Add your collaborators if you collaborated on the report. Learn more about collaboration [here](#).

#3114523

Vulnerable JS library

ADD HACKER SUMMARY

TIMELINE · EXPORT

lynxjr2002 submitted a report to Privy (Bounty). [\(Edit information\)](#)

a few seconds ago

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:

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

5. 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>

Reply:



andrewmohawk-privy Privy (Bounty) staff posted a comment.

3 days ago

Hi,

Please can you demonstrate any vulnerabilities within these libraries, we regularly review and validate any audit findings in our libraries and if they are applicable will resolve them promptly. However its totally possible that we missed something and welcome any findings that are validated!

Regards,
Andrew MacPherson
Principal Security Engineer