

# SECURITY ASSESSMENT

Submitted to: Application Development Team  
Security Analyst: George Ghira

Date of Testing: **February 2025**  
Date of Report Delivery: February 2025

# Table of Contents

Security Engagement Summary	2
Engagement Overview	2
Scope	2
Risk Analysis	2
Recommendations	2
Significant Vulnerabilities Summary	4
High-Risk Vulnerabilities	4
Medium-Risk Vulnerabilities	4
Low-Risk Vulnerabilities	4
Significant Vulnerability Details	4
Appendix A: Security Analysis Methodology	6
Assessment Tools Selection	6
Reconnaissance	7
Scanning	11
Exploitation	12

# Security Engagement Summary

## Engagement Overview

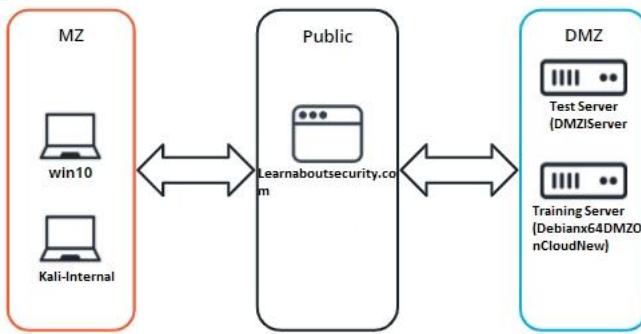
The engagement has been conducted in order to determine the security posture of PJ Bank's virtual environment and to highlight any security risks associated with the infrastructure in scope.

## Scope

The following devices are in scope of the assessment:

S. No.	Asset Information	Hostname	IP Address
1	Public web server	Learnaboutsecurity.com	
2	Employee Workstation	Win10	10.1.2.4
3	Debian Server in DMZ	DMZiServer	10.1.0.7
4	Web App Server in DMZ	Debianx64DMZOnCloudNew	10.1.0.11

PROJECT NETWORK DIAGRAM



## Risk Analysis

<Considering the significant vulnerabilities identified, the overall security risk of the virtual machine tested during the engagement is <**DEFINE SEVERITY HERE** as Low Moderate or High>.

- **High** – severe or catastrophic impact
- **Moderate** – Serious impact
- **Low** – limited impact

>

## Recommendations

<Complete this section with recommendations based on major vulnerabilities discovered and/or exploited. The vulnerabilities highlighted in this report should be remediated as soon as possible>

- <Make non-technical and high level recommendations for an executive team to review. The recommendations should include things that executive-level directors, board members, and if provided to the public, someone non-technical can understand.

For example: The company should implement a policy that enforces multi-factor authentication. The security analysts determined that account passwords could be guessed and access to the network was gained remotely. Implementing multi-factor authentication would have prevented the analyst from gaining access to the network in this manner.>

# Significant Vulnerabilities Summary

Significant vulnerabilities identified during the vulnerability assessment and validation are summarized below. While additional vulnerabilities may be present, these are considered significant and warrant resolution.

## High-Risk Vulnerabilities

<Add the vulnerabilities here, if there are no vulnerabilities in this category, remove the category>

## Medium-Risk Vulnerabilities

<Add the vulnerabilities here, if there are no vulnerabilities in this category, remove the category>

## Low-Risk Vulnerabilities

<Add the vulnerabilities here, if there are no vulnerabilities in this category, remove the category>

# Significant Vulnerability Details

*Details about the significant vulnerabilities you listed above are provided below.*

---

<For each vulnerability, make sure to:

- Identify the risk priority
  - Describe the vulnerability
  - Provide a screenshot that is centered, bordered, and has a caption
  - Add a Discussion section under the screenshot>
- 

Example of a vulnerability finding:

### HIGH-RISK Vulnerability

The student found that both the LibSSH and Elasticsearch packages contained vulnerabilities directly associated with the lack of patching.

```
Starting Nmap 7.60 ( https://nmap.org ) at 2020-08-11 04:34 MDT
Nmap scan report for 10.1.1.227
Host is up, received conn-refused (0.0069s latency).
Not shown: 997 closed ports
Reason: 997 conn-refused
PORT      STATE SERVICE REASON  VERSION
22/tcp    open  ssh      syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (
| ssh-hostkey:
|   2048 8a:b5:3b:3c:6e:5f:a0:58:19:59:64:c4:34:b9:ff:c8 (RSA)
|   256 ee:cb:19:01:e1:d7:15:58:d2:72:17:11:ea:84:4c:d7 (ECDSA)
|   256 5b:03:e7:5d:ff:14:87:b3:77:40:da:e2:bf:43:1f:29 (EdDSA)
2222/tcp  open  ssh      syn-ack (protocol 2.0)
| fingerprint-strings:
|   NULL:
|_  SSH-2.0-libssh 0.8.1
```

Example of a machine with LibSSH Missing Software Patches

Discussion:

<In your discussion, be sure to mention:

- Vulnerabilities were discovered <in what? why?>
  - Are there any links available to discuss?
-

# Appendix A: Security Analysis Methodology

The methodology the analyst used for the vulnerability assessment is provided below.

## Assessment Tools Selection

Noting the scope of the engagement was focused on a web application, the security analyst chose relevant web-application security analyst tools. The analyst created a Kali Virtual Machine which had many included tools. Tools used during this engagement included:

- Kali Operating System
  - <https://www.kali.org/>
  - Description
- Python Environment
  - <https://www.python.org/>
  - Description
- Nmap
  - <https://nmap.org/>
  - Description
- Others
  - Link
  - Description

---

### Example:

#### Description of what/why you did

- Command used

```
ehnd2-vm login: ehnd2-stu
Password:
Last login: Tue Aug 11 22:33:31 UTC 2020 on tty1
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-112-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

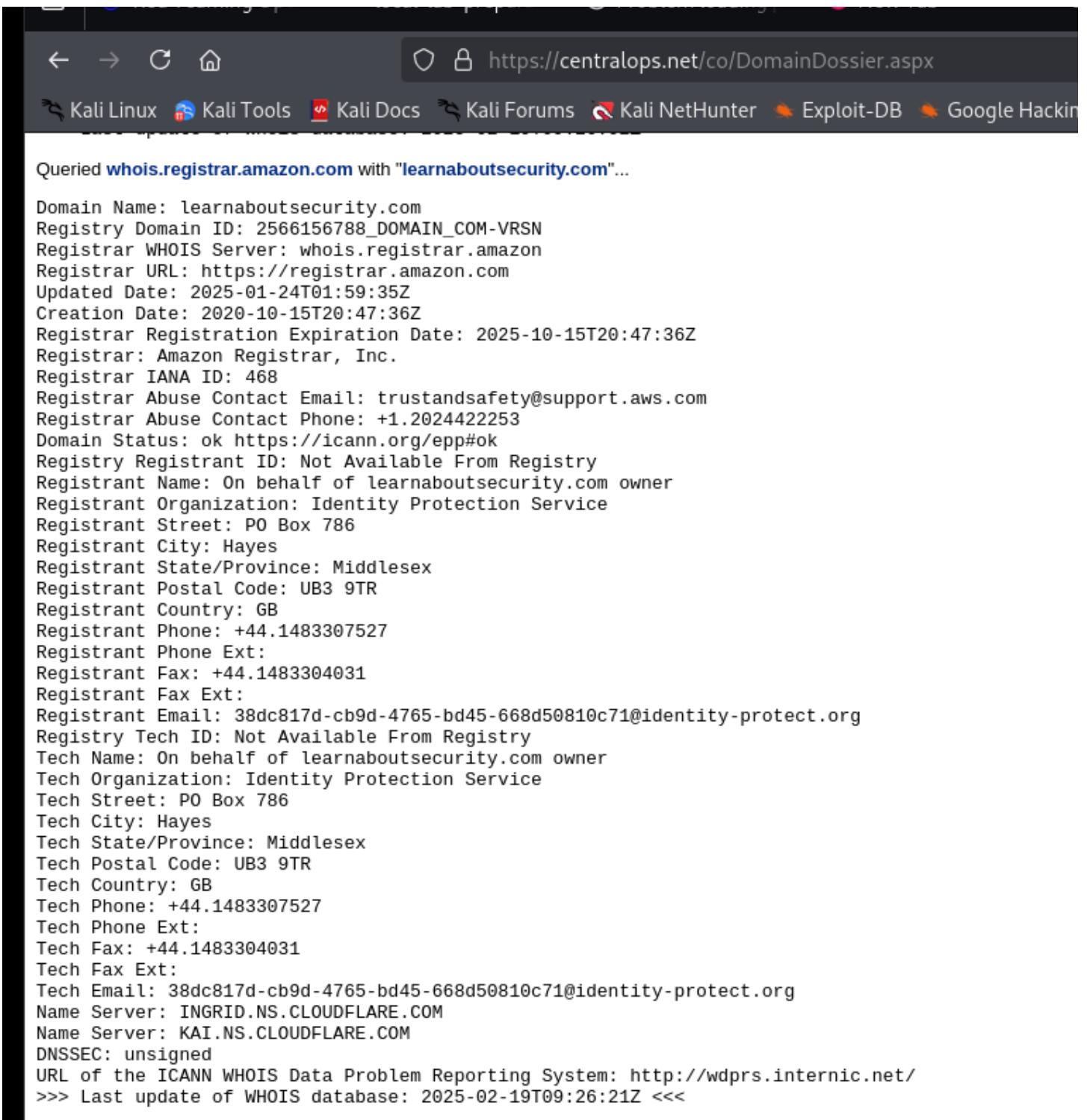
 System information as of Tue Aug 11 22:36:57 UTC 2020

 System load:  0.28           Users logged in:          0
 Usage of /:   67.9% of 7.81GB IP address for ens33:      10.1.1.228
 Memory usage: 25%
 Swap usage:   0%
 Processes:    190            IP address for docker0:  172.17.0.1
                                         IP address for br-0cce8a152264: 172.19.0.1
                                         IP address for br-914151e561c2: 172.18.0.1
```

Screenshot of <COMMAND> and results

## Reconnaissance

<Provide a screenshot from the OSINT tool, and a description of the findings>



Queried [whois.registrar.amazon.com](https://whois.registrar.amazon.com) with "learnaboutsecurity.com"...

```
Domain Name: learnaboutsecurity.com
Registry Domain ID: 2566156788_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrar.amazon
Registrar URL: https://registrar.amazon.com
Updated Date: 2025-01-24T01:59:35Z
Creation Date: 2020-10-15T20:47:36Z
Registrar Registration Expiration Date: 2025-10-15T20:47:36Z
Registrar: Amazon Registrar, Inc.
Registrar IANA ID: 468
Registrar Abuse Contact Email: trustandsafety@support.aws.com
Registrar Abuse Contact Phone: +1.2024422253
Domain Status: ok https://icann.org/epp#ok
Registry Registrant ID: Not Available From Registry
Registrant Name: On behalf of learnaboutsecurity.com owner
Registrant Organization: Identity Protection Service
Registrant Street: PO Box 786
Registrant City: Hayes
Registrant State/Province: Middlesex
Registrant Postal Code: UB3 9TR
Registrant Country: GB
Registrant Phone: +44.1483307527
Registrant Phone Ext:
Registrant Fax: +44.1483304031
Registrant Fax Ext:
Registrant Email: 38dc817d-cb9d-4765-bd45-668d50810c71@identity-protect.org
Registry Tech ID: Not Available From Registry
Tech Name: On behalf of learnaboutsecurity.com owner
Tech Organization: Identity Protection Service
Tech Street: PO Box 786
Tech City: Hayes
Tech State/Province: Middlesex
Tech Postal Code: UB3 9TR
Tech Country: GB
Tech Phone: +44.1483307527
Tech Phone Ext:
Tech Fax: +44.1483304031
Tech Fax Ext:
Tech Email: 38dc817d-cb9d-4765-bd45-668d50810c71@identity-protect.org
Name Server: INGRID.NS.CLOUDFLARE.COM
Name Server: KAI.NS.CLOUDFLARE.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2025-02-19T09:26:21Z <<<
```

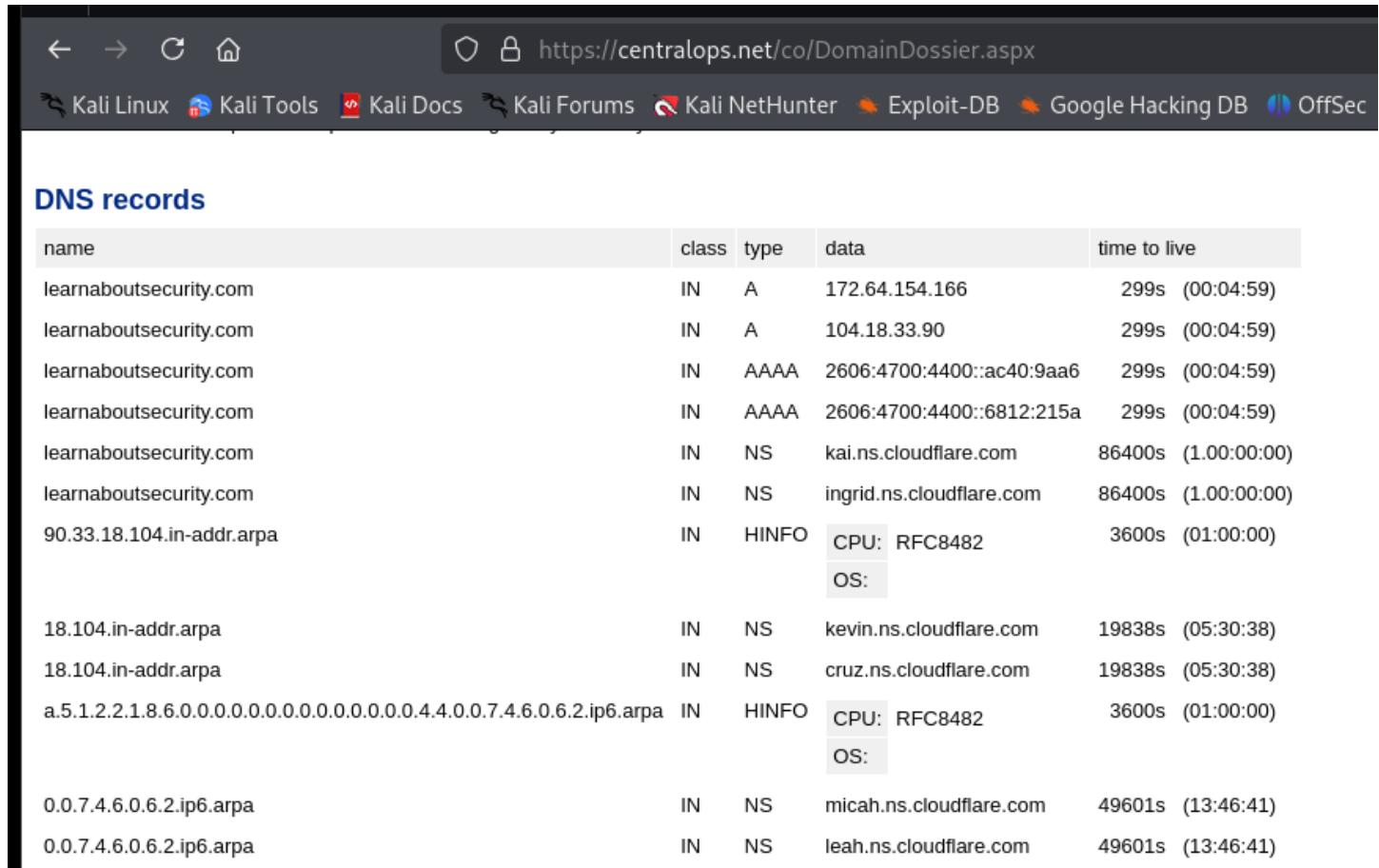
This means the domain is registered through Amazon, privacy-protected, and uses Cloudflare for DNS management.

Name server ((INGRID.NS.CLOUDFLARE.COM, KAI.NS.CLOUDFLARE.COM), which suggests security measures like DDoS protection and CDN services.

DNSSEC (Domain Name System Security Extensions) is not enabled, meaning DNS spoofing or cache poisoning attacks could be a concern.

Another interesting fact, expiration date of the site, which could be used by malicious actors to revindicate the ownership of the site before the owner and then ask a financial pay in order to transfer the ownership right.

<DNS Information, including at least the names to IP mappings>



The screenshot shows a web browser window with the URL https://centralops.net/co/DomainDossier.aspx. The page displays a table of DNS records for the domain learnaboutsecurity.com. The table has columns for name, class, type, data, and time to live. The data includes both IPv4 and IPv6 addresses, along with NS records pointing to Cloudflare's name servers (kai.ns.cloudflare.com and ingrid.ns.cloudflare.com). There are also HINFO records for various IP addresses, which typically contain CPU and OS information, but here it only shows 'CPU: RFC8482' and 'OS:'.

name	class	type	data	time to live
learnaboutsecurity.com	IN	A	172.64.154.166	299s (00:04:59)
learnaboutsecurity.com	IN	A	104.18.33.90	299s (00:04:59)
learnaboutsecurity.com	IN	AAAA	2606:4700:4400::ac40:9aa6	299s (00:04:59)
learnaboutsecurity.com	IN	AAAA	2606:4700:4400::6812:215a	299s (00:04:59)
learnaboutsecurity.com	IN	NS	kai.ns.cloudflare.com	86400s (1.00:00:00)
learnaboutsecurity.com	IN	NS	ingrid.ns.cloudflare.com	86400s (1.00:00:00)
90.33.18.104.in-addr.arpa	IN	HINFO	CPU: RFC8482 OS:	3600s (01:00:00)
18.104.in-addr.arpa	IN	NS	kevin.ns.cloudflare.com	19838s (05:30:38)
18.104.in-addr.arpa	IN	NS	cruz.ns.cloudflare.com	19838s (05:30:38)
a.5.1.2.2.1.8.6.0.0.0.0.0.0.0.0.0.0.0.0.4.4.0.0.7.4.6.0.6.2.ip6.arpa	IN	HINFO	CPU: RFC8482 OS:	3600s (01:00:00)
0.0.7.4.6.0.6.2.ip6.arpa	IN	NS	micah.ns.cloudflare.com	49601s (13:46:41)
0.0.7.4.6.0.6.2.ip6.arpa	IN	NS	leah.ns.cloudflare.com	49601s (13:46:41)

These records map the domain name learnaboutsecurity.com to IP addresses: 172.64.154.166, 104.18.33.90

These records map the domain to IPv6 addresses: 2606:4700:4400::ac40:9aa6 , 2606:4700:4400::6812:215a

Name servers managing the domain's DNS: kai.ns.cloudflare.com, ingrid.ns.cloudflare.com

Host Information are not available due RFC482 standard for privacy (and security)

<Web technologies used by the website, with a screenshot of the identification >

Using Dev tools from Google Chrome we learn:

# Learn About Security

Home About

Website Search Search

The screenshot shows a browser developer tools window with several tabs open:

- Inspector**: Shows the DOM tree with nodes like `<html>`, `<head>`, and various `<link>` and `<script>` tags.
- Console**: Shows the command-line interface for running JavaScript code.
- Debugger**: A step-through debugger for JavaScript code.
- Network**: Shows network requests and responses, including files like `index.html`, `styles.css`, and `bootstrap.min.js`.
- Style Editor**: Allows editing CSS rules.
- Performance**: Tools for measuring page performance.
- Memory**: Tools for monitoring memory usage.
- Storage**: Tools for managing local storage.
- Accessibility**: Tools for accessibility analysis.
- Application**: Tools for application-specific analysis.

The **Style Editor** tab is active, displaying the CSS styles for the current page. It includes a sidebar for "Filter Styles" and a preview of the box model for a selected element.

## Use HTML for web structuring,

The screenshot shows the Network tab in the browser developer tools, displaying a timeline of network requests:

- Timeline markers: 10 ms, 20 ms, 30 ms, 40 ms, 50 ms, 60 ms, 70 ms, 80 ms, 90 ms, 100 ms.
- Request list:
  - learnaboutsecurity.com (DNS)
  - styles.9b0781bc23ea147593c7.css (CSS)
- Request details table:

Name	Headers	Preview	Response	Initiator	Timing
1 /*!					
2 * Bootstrap v5.3.3 (https://getbootstrap.com/)					
3 * Copyright 2011-2024 The Bootstrap Authors					
4 * Licensed under MIT (https://github.com/twbs/bootstrap/blob/main/LICENSE)					
5 */					

## Use CSS for styling (with Bootstrap v5.3.3 libraries)

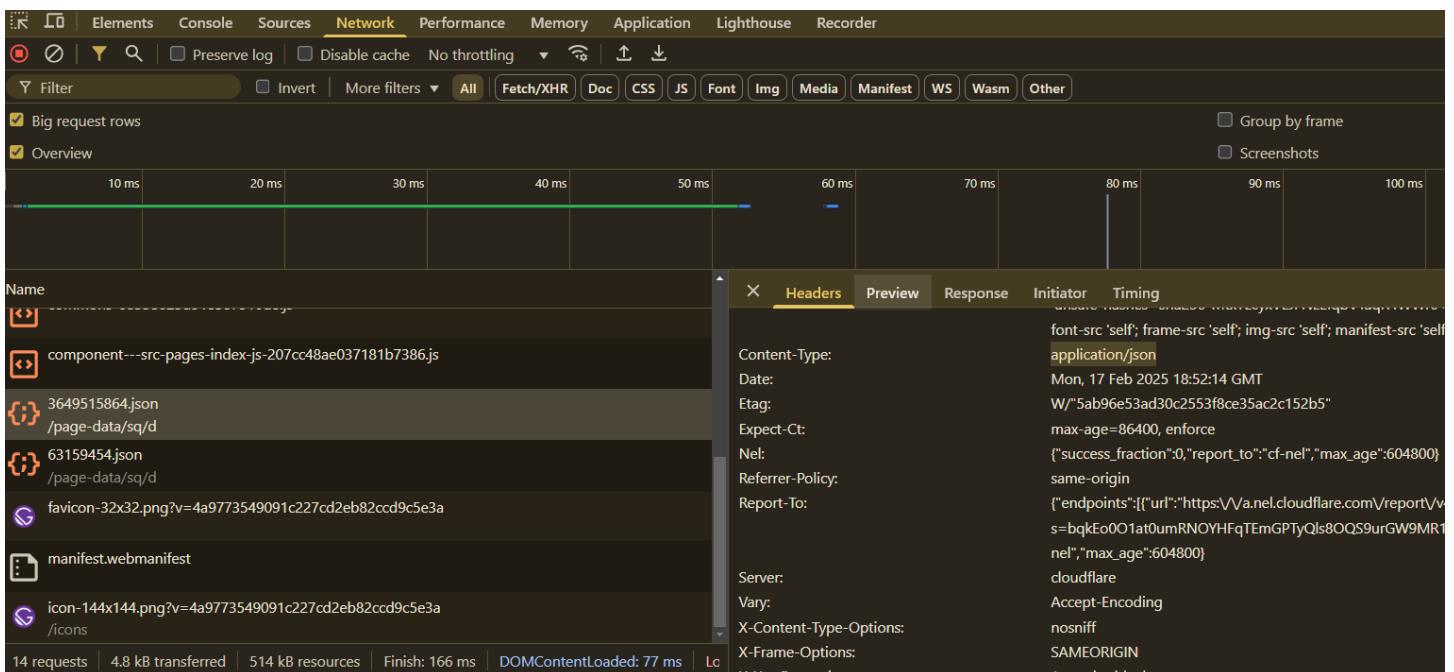
## Use JavaScript for interaction ( with react 19)

```

<!DOCTYPE html>
<html lang="en" data-react-helmet="lang"> scroll
  <head>
    <meta charset="utf-8">
    <meta http-equiv="x-ua-compatible" content="ie=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
    <meta name="generator" content="Gatsby 5.13.7"> == $0
    <meta name="theme-color" content="#20232a">

```

Use Gatsby 5.13.7 version used as a framework



Use Json to send/receive data via API.

In conclusion:

The site is React-based and likely built using Gatsby.

Uses Bootstrap for styling, meaning pre-designed UI elements.

Likely dynamically updates SEO/meta tags using React Helmet.

Variant 2:

Installed Wappalyzer as an extension and got this in less than 1 second!



TECHNOLOGIES

MORE INFO

Export

### JavaScript frameworks

[Gatsby](#) 5.13.7[React](#)

### Security

[HSTS](#)

### Miscellaneous

[HTTP/2](#)[Open Graph](#)[PWA](#)[Webpack](#)

### CDN

[Cloudflare](#)

### Static site generators

[Gatsby](#) 5.13.7[Something wrong or missing?](#)

## Scanning

&lt;Annotated screenshot and description of the nmap scans of each machine, one-by-one.&gt;

# Exploitation

<Successful exploits to gain access/ exfiltrate sensitive data>

<Exploit commands>

<Vulnerable software exploitation>

<Weak Password Cracks>

<provide the commands you used and screenshots for them, with the description as seen in the example>

---