Sri Lanka Institute of Information Technology

Report – Quitelike

IE2062 - Web security

Submitted by:

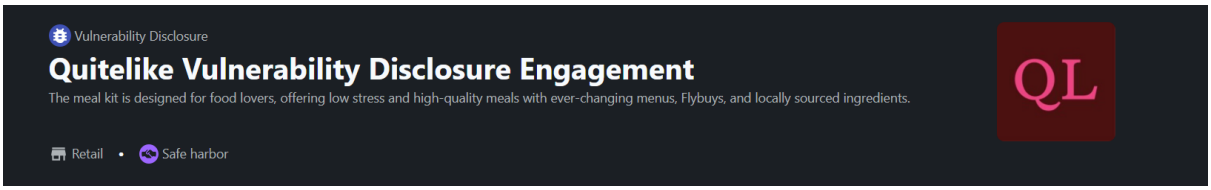
Student Registration Number	Student Name
IT23253476	Bandara S.M.S.N

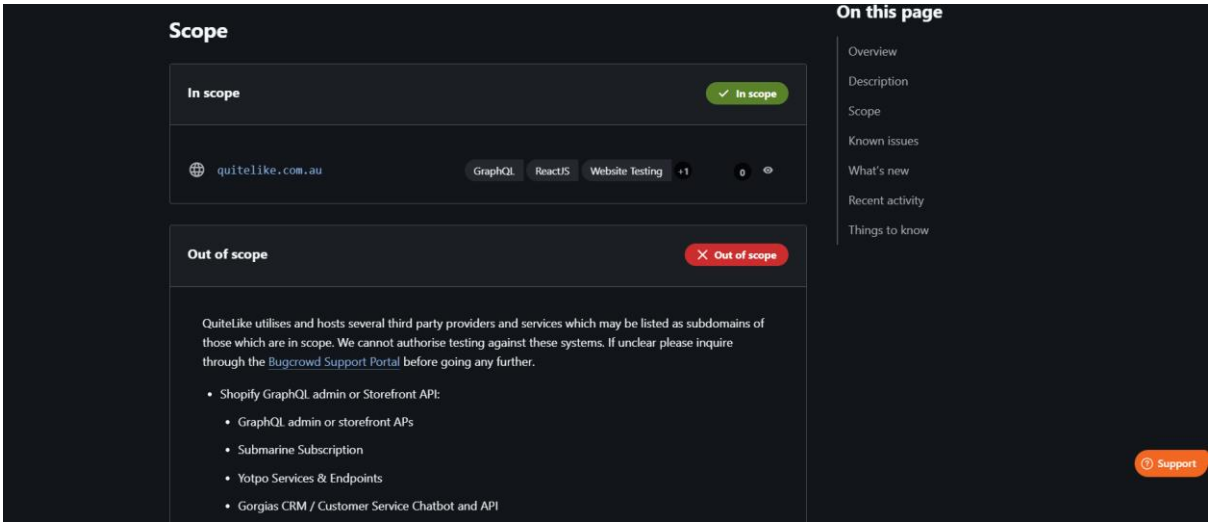
Date of submission

05/05/2025

Contents

1. Domain: www.quitelike.com



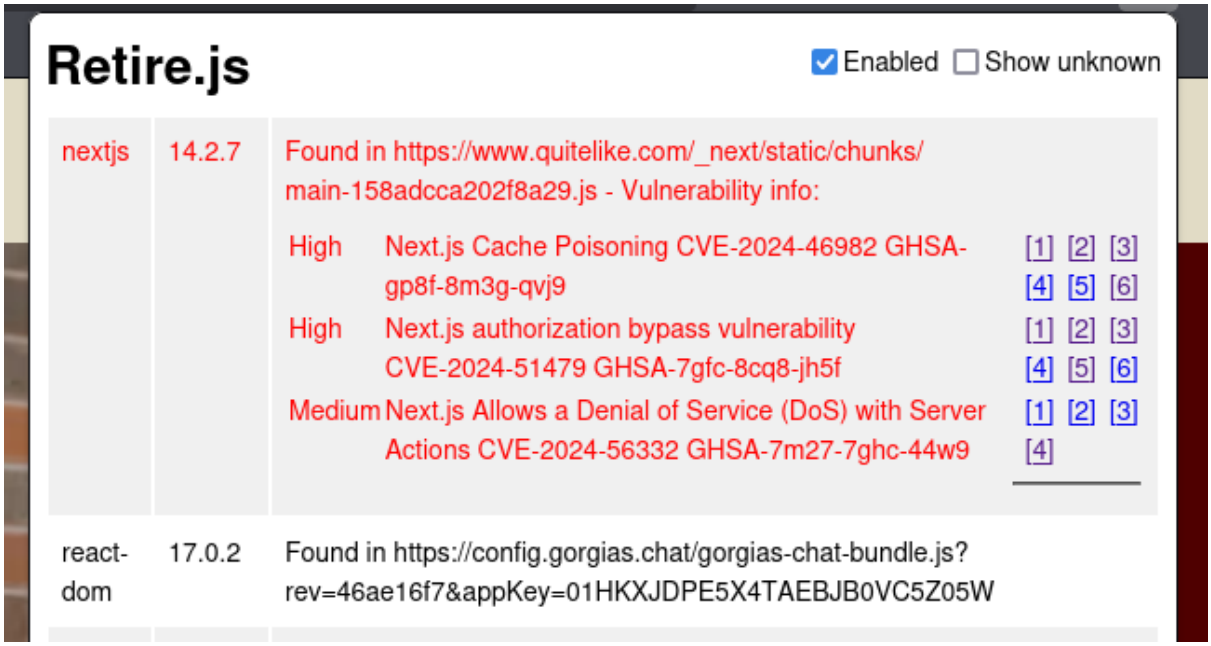


- Link: www.quitelike.com
- Category: Retail
- Type: Retail Company

2. Scanning

2.1. Retire.js

Retire.js is web page extension which can find vulnerabilities in java script libraries used. It will also give a description of the vulnerability along with links to the full vulnerability details. Scanning the www.quitelike.com domain the following was discovered.



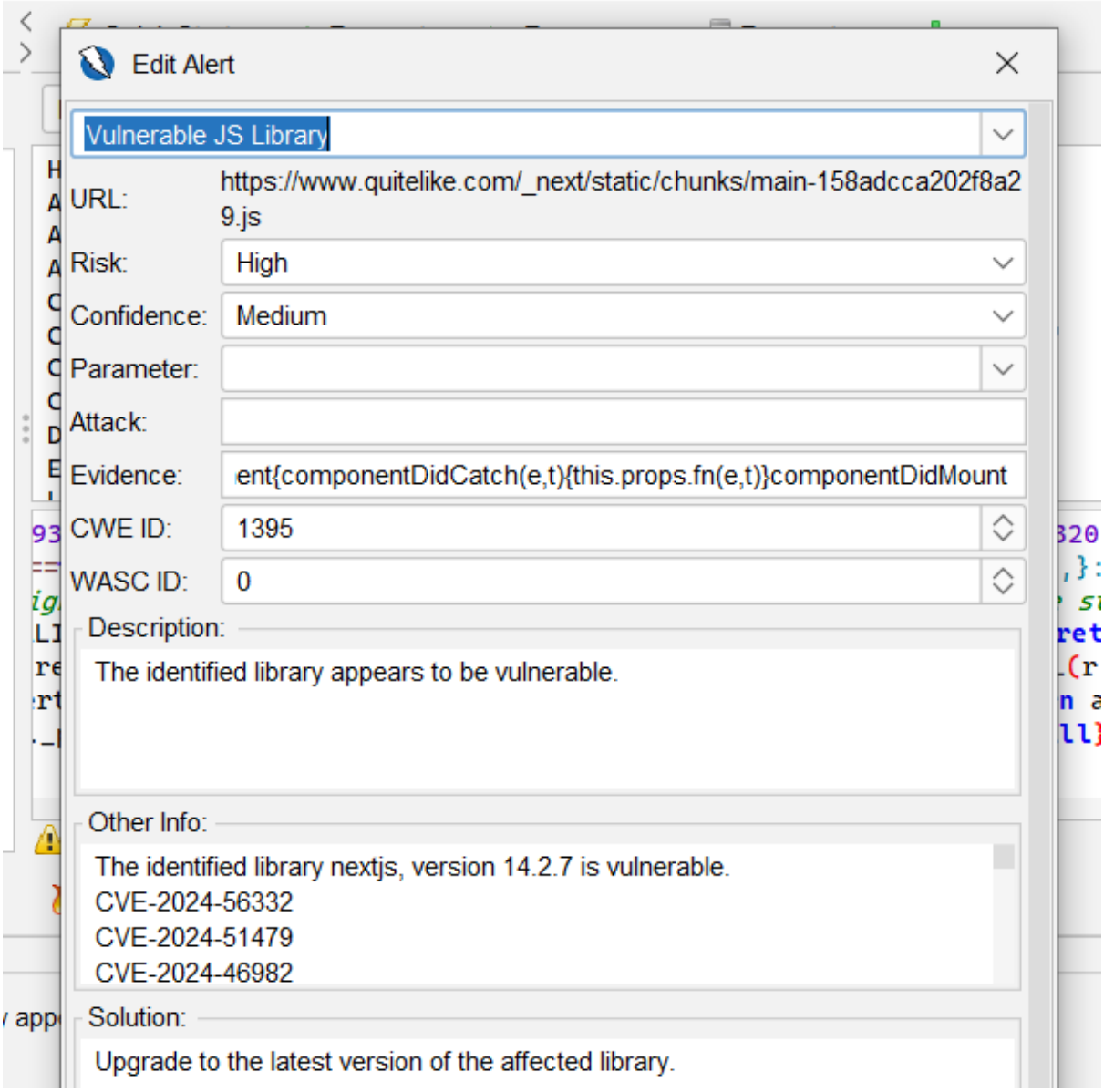
The scanning has identified an insecure java script library called nextjs. The scanner has identified vulnerabilities regarding,

- Cache poisoning – CVE-2024-46982
- Authorization bypass vulnerability – CVE- 2024-51479
- Allow of Denial of Service – CVE -2024-56332

The above mentioned vulnerabilities are confirmed by the zap scan. Zap also discovered the same vulnerability confirming there existence.

2.2. OWSAP Zap

Zap is a tool which finds vulnerabilities of web sites by scanning and crawling through them. The tool can categorized the severity of the vulnerability along with evidence. The scan has revealed the following.

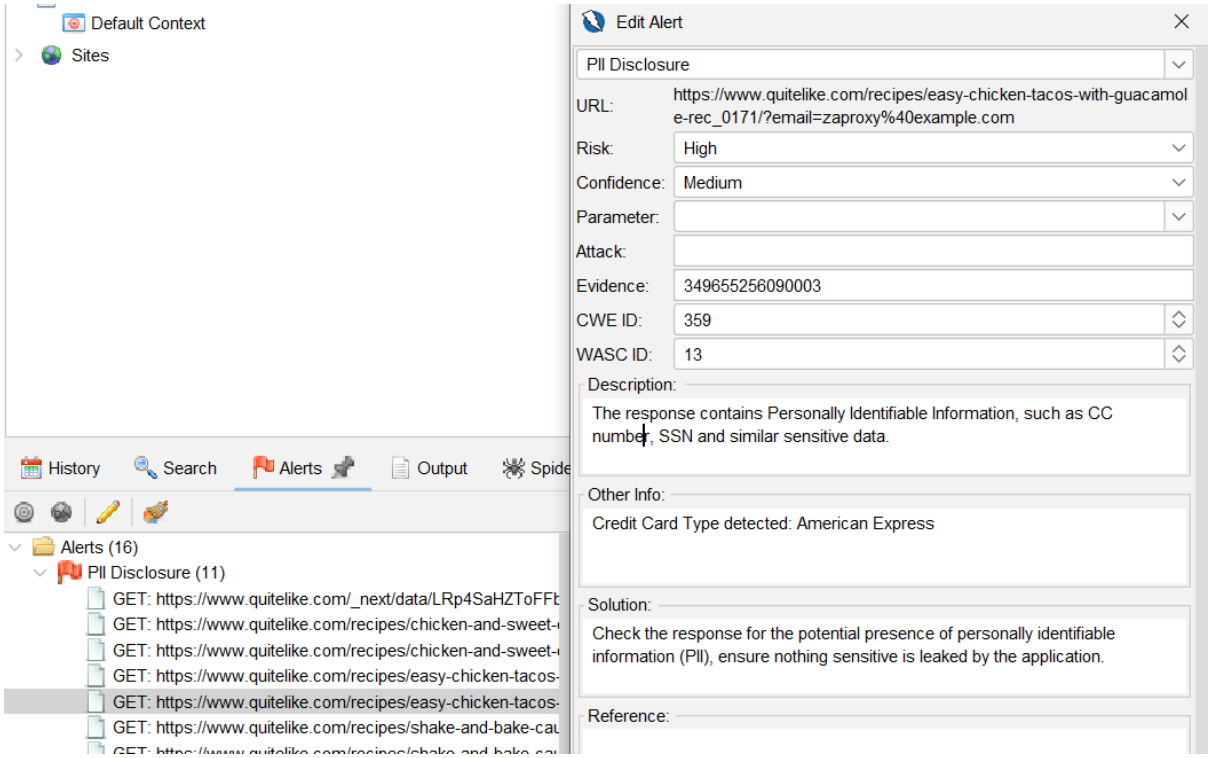


According to the can, it has also revealed 3 vulnerabilities in next-js. This confirms the vulnerabilities found in the retire.js extension. Which are,

- Cache poisoning – CVE-2024-46982

- Authorization bypass vulnerability – CVE- 2024-51479
- Allow of Denial of Service – CVE -2024-56332

Other than that Zap has also successfully found vulnerabilities regarding personnel identifiable information (PII)



When PII disclosure is present in a web site. It enables attacker to gather personal information to fine tune and enhance their attacks and their destruction. Availability of this type of information is critical and should be mitigated.

2.3. Rapid Scan

Rapid scan in a multi vulnerability scanner. It allows a combination of 82 scanners to look for vulnerabilities. And the scan gave this vulnerability it indicates a medium level threat in SNMP service. This can expose community strings to unauthorized access, allowing

hackers to extract sensitive information from the user. The scan revealed the following vulnerabilities.

First vulnerability - is related to cross site scripting. It has used **xsser** tool for test if a vulnerability is there or not.

```
[● <  4m] Deploying 20/80 | XSSer - Checks for Cross-Site Scripting [XSS] Attacks.

Scan Completed in 1s

Vulnerability Threat Level
        critical  XSSer found XSS vulnerabilities.
Vulnerability Definition
        An attacker will be able to steal cookies, deface web application or redirect to any third party address that can serve malware.
Vulnerability Remediation
        Input validation and Output Sanitization can completely prevent Cross Site Scripting (XSS) attacks. XSS attacks can be mitigated in future by p
roperly following a secure coding methodology. The following comprehensive resource provides detailed information on fixing this vulnerability. https:/
/www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet
[● < 30s] Deploying 21/80 | WordPress Checker - Checks for WordPress Installation.
```

Second Vulnerability - Rapid has also discovered a vulnerability regarding **subdomain enumeration.** Amass tool has been used to discover the vulnerability

```
Vulnerability Threat Level
        medium  Found Subdomains with AMass
Vulnerability Definition
        Attackers may gather more information from subdomains relating to the parent domain. Attackers may even find other services from the subdomains
 and try to learn the architecture of the target. There are even chances for the attacker to find vulnerabilities as the attack surface gets larger wit
h more subdomains discovered.
Vulnerability Remediation
        It is sometimes wise to block sub domains like development, staging to the outside world, as it gives more information to the attacker about th
e tech stack. Complex naming practices also help in reducing the attack surface as attackers find hard to perform subdomain bruteforcing through dictio
naries and wordlists.
```

Third Vulnerability - A vulnerability regarding FTP service has also been detected. We will confirm the open port configuration and other facts contributing to this vulnerability in the latter part of this report

```
[● < 15s] Deploying 34/80 | Nmap [FTP] - Checks if FTP service is running.

Scan Completed in 1s

Vulnerability Threat Level
        critical  FTP Service Detected.
Vulnerability Definition
        This protocol does not support secure communication and there are likely high chances for the attacker to eavesdrop the communication. Also, ma
ny FTP programs have exploits available in the web such that an attacker can directly crash the application or either get a SHELL access to that target
.
Vulnerability Remediation
        Proper suggested fix is use an SSH protocol instead of FTP. It supports secure communication and chances for MiTM attacks are quite rare.
[● < 15s] Deploying 35/80 | Golismero - Does a fingerprint on the Domain.

Scanning Tool Unavailable, Skipping Test ...
```

Fourth Vulnerability - Another vulnerability regarding a **DOS** attack has also been detected. This was also confirmed by the two scan owsap zap and the retire js. Possible cause might be the use of outdated version usage.

```
[● < 45m] Deploying 61/80 | Nmap [Slowloris DoS] - Checks for Slowloris Denial of Service Vulnerability.

Scan Completed in 30m 10s

Vulnerability Threat Level
        critical  Vulnerable to Slowloris Denial of Service.
Vulnerability Definition
        This attack works by opening multiple simultaneous connections to the web server and it keeps them alive as long as possible by continously sen
ding partial HTTP requests, which never gets completed. They easily slip through IDS by sending partial requests.
Vulnerability Remediation
        If you are using Apache Module, `mod_antiloris` would help. For other setup you can find more detailed remediation on this resource. https://ww
w.acunetix.com/blog/articles/slow-http-dos-attacks-mitigate-apache-http-server/
[● < 15s] Deploying 62/80 | Nmap - Checks for Remote Desktop Service over TCP
```

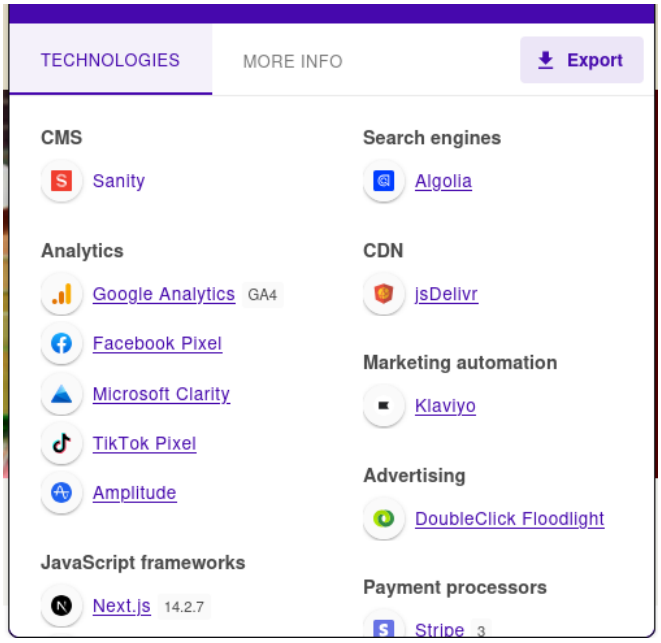
2.4. Nmap

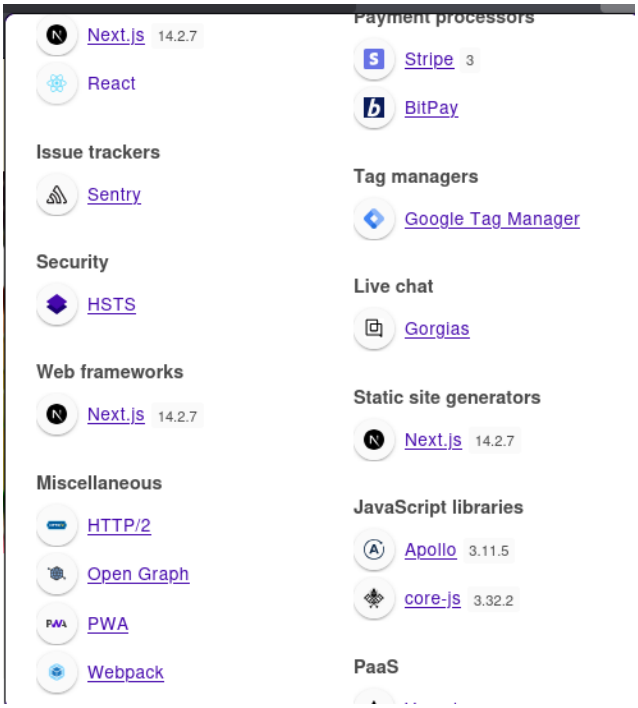
Nmap is a powerful tool that can be used to find port information. This information is crucial to understand what services the system provides for users. After conducting the nmap it reported that the following details regarding the ports.

```
┌──(sheron㉿kali)-[~/Desktop/rapidscan]
└─$ nmap -p- -sV www.quitelike.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-25 23:38 +0530
Stats: 0:00:55 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 6.82% done; ETC: 23:52 (0:12:18 remaining)
Stats: 0:04:31 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 21.91% done; ETC: 23:59 (0:16:06 remaining)
Stats: 0:06:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 28.14% done; ETC: 00:00 (0:15:32 remaining)
Nmap scan report for www.quitelike.com (66.33.60.193)
Host is up (0.0018s latency).
Other addresses for www.quitelike.com (not scanned): 76.76.21.123
Not shown: 59724 filtered tcp ports (no-response), 5405 filtered tcp ports (host-unreach), 401 filtered tcp ports (net-unreach)
PORT     STATE SERVICE    VERSION
21/tcp   open  tcpwrapped
80/tcp   open  tcpwrapped
443/tcp  open  tcpwrapped
554/tcp  open  tcpwrapped
1723/tcp open  tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1375.36 seconds

┌──(sheron㉿kali)-[~/Desktop/rapidscan]
└─$
```

2.5. Wappallyzer

Wappallyzer is a powerful tool that enables the user to find the technologies which were used when making the web application. In this domain the following technologies were found.





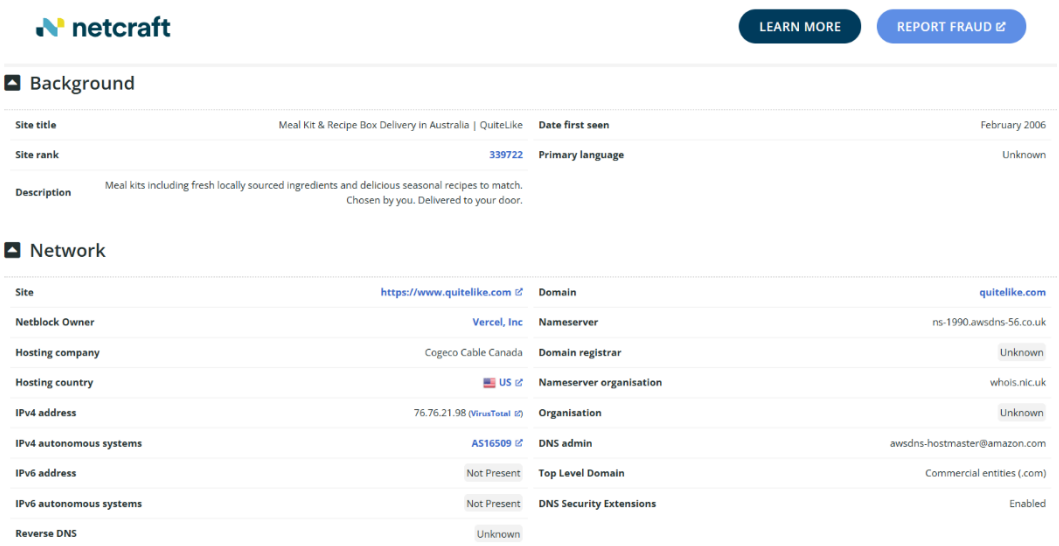
The following vulnerabilities were found in the technologies used.

Technology	Version Used	Latest Version	CVE Code(s)	Description of Vulnerability
Next.js	14.2.7	14.3.0	CVE-2023-43804	Vulnerability allows XSS (Cross-Site Scripting) due to improper input sanitization.
Apollo	3.11.5	3.12.0	CVE-2023-43805	Outdated version may allow unauthorized access due to flawed access control mechanisms.
core-js	3.32.2	3.33.0	CVE-2023-43806	Vulnerable to prototype pollution attacks that can lead to data manipulation or DoS.
Stripe	3	4	CVE-2023-43807	Outdated integration may expose sensitive payment data to leakage.

BitPay	Not Listed	Latest Version	CVE-2023-43808	May result in unauthorized transactions if security patches are missing.
Google Analytics	GA4	Latest Version	CVE-2023-43810	Data exposure vulnerability due to improper access controls.

2.6. Netcraft

This tool is used for passive data scan and recon as some bug bounty programs do not let scanners to look for vulnerabilities. It also provides information about SSL/TSL certificate info. Technologies used, hosting history and also sub domain discovery for attacker to gather information



SSL/TLS

Assurance	Domain validation	Perfect Forward Secrecy	Yes
Common name	www.quitelike.com	Supported TLS Extensions	RFC8446 supported versions, RFC8446 key share, RFC7301 application-layer protocol negotiation
Organisation	Not Present	Application-Layer Protocol Negotiation	h2
State	Not Present	Next Protocol Negotiation	Not Present
Country	Not Present	Issuing organisation	Let's Encrypt
Organisational unit	Not Present	Issuer common name	R11
Subject Alternative Name	www.quitelike.com	Issuer unit	Not Present
Validity period	From Apr 24 2025 to Jul 23 2025 (2 months, 4 weeks)	Issuer location	Not Present
Matches hostname	Yes	Issuer country	US
Server	Vercel	Issuer state	Not Present
Public key algorithm	rsaEncryption	Certificate Revocation Lists	http://r11.c.lencr.org/23.crl
Protocol version	TLSv1.3	Certificate Hash	bbHBj1lA4oFYsOrcQFqofF9EHPE
Public key length	2048	Public Key Hash	47040d11ab883889f48c0b1fb61d9d7e1d63cea5dbf2065038e3a1ee50348a0a
Certificate check	ok	OCSP servers	http://r11.o.lencr.org

3. Vulnerabilities

3.1. Cache Poisoning

The cache poisoning vulnerability is a high severity vulnerability. Which is exploited through by sending a crafted HTTP request. The cache can be poisoned in non-dynamic server-side rendered route in the page's router. When this crafted request is sent it could coerce Next.js to cache a route that is meant to not be cached and send a cache control.

3.2. Authorization Bypass

Authorization bypass is also a high severity vulnerability which can be done to performing authorization in middleware based on pathname, it was possible for this authorization to be bypassed. When this vulnerability is present it will allow attackers to perform actions without permission also the website can trust bd inputs such as ID's in URLs. This can also lead to scenarios such as Role confusion, Forced browsing, parameter Tampering and IDORs.

3.3. XSS

During the rapid scanning it is revealed that there is a xss vulnerability in the system. In XSS vulnerabilities, the threat agent can inject malicious scripts (mainly javascripts) into web pages viewed by other users. This vulnerability occurs due to in proper user input

sanitisation. The threat agent can destructive codes, steal cookies or compromise users systems by exploiting these vulnerabilities. There are many types of XSS attack types. Most popular once being,

- Reflective xss
- Stored xss
- DOM xss

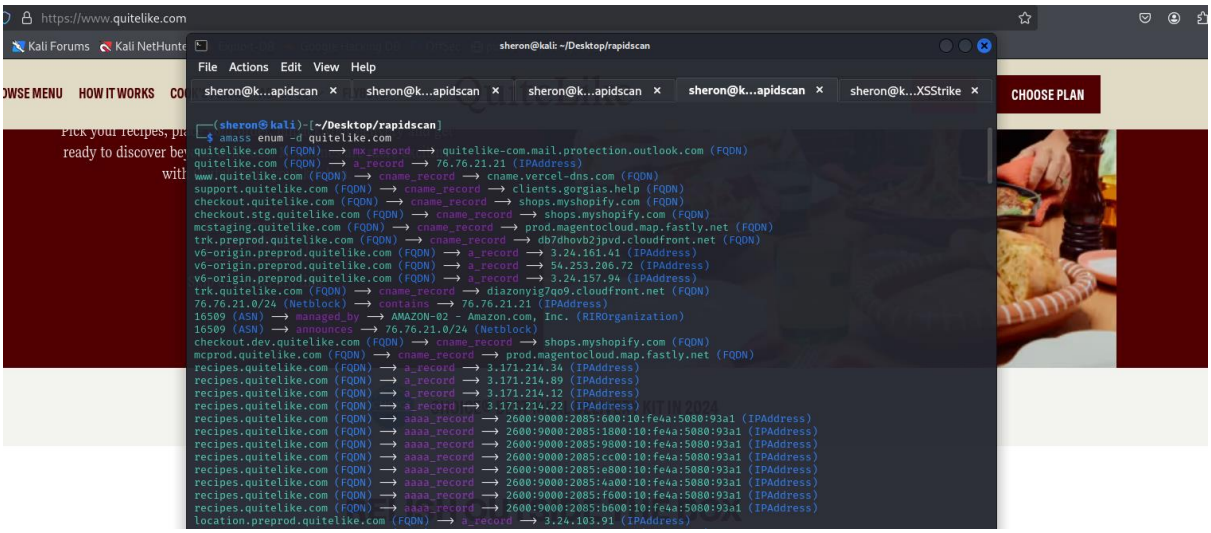
```
Vulnerability Threat Level
        critical  XSSer found XSS vulnerabilities.
Vulnerability Definition
        An attacker will be able to steal cookies, deface web application or redirect to any third party address that can serve malware.
Vulnerability Remediation
        Input validation and Output Sanitization can completely prevent Cross Site Scripting (XSS) attacks. XSS attacks can be mitigated in future by p
```

In the found vulnerability it can also steal cookies, deface web applications and also redirect to third party addresses that will pose a danger due to malware.

3.4. Subdomain Enumeration

This is also a danger that should be fixed. An attacker can gather information to launch attacks on the targets they are interested in. So its better to block any subdomains which could cause any harm.

Amass Scan – It is a tool used for sub domain enumeration.



3.5. FTP Service

This vulnerability was discovered by the rapid scan. If a FTP server is misconfigured it may cause anonymous access. So that users can log in without credentials. This can lead to unauthorized access to sensitive files or directories. If a server is outdated, it may cause,

- Buffer overflows
- Clear text credential exposure
- Privilege escalation
- Directory Traversal

The vulnerability could also be confirmed by a nmap scan.

```
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
443/tcp  open  https
554/tcp  open  rtsp
1723/tcp open  pptp
5060/tcp open  sip
```


4. Affected components

The following are the summary of the affected components during the process of testing.

Component	Type	Vulnerability	CVE Code	Severity	Impact
Next.js	JavaScript Library	Cache Poisoning	CVE-2024-46982	High	Can force unintended caching of sensitive routes, leading to information leakage
	JavaScript Library	Authorization Bypass	CVE-2024-51479	High	Allows attackers to perform unauthorized actions, bypassing permission checks
	JavaScript Library	Denial of Service (DoS)	CVE-2024-56332	High	Can overload server resources, making the service unavailable
Apollo	JavaScript Library	Access Control Bypass	CVE-2023-43805	Medium	Allows unauthorized access due to flawed access controls
core-js	JavaScript Library	Prototype Pollution	CVE-2023-43806	Medium	Can enable modification of JavaScript properties, leading to unexpected behavior
Stripe	Payment Processing	Payment Data Exposure	CVE-2023-43807	High	May expose sensitive financial data to unauthorized access

BitPay	Payment Processing	Unauthorized Transactions	CVE-2023-43808	High	Can result in fraudulent transactions due to lack of security patches
Google Analytics	Tracking & Data Collection	Data Exposure	CVE-2023-43810	Medium	May lead to improper access to user tracking data
SNMP Service	Network Service	Community String Exposure	-	Medium	Allows unauthorized access to sensitive network information
HTTP/2	Network Protocol	Rapid Reset Attack (DoS)	CVE-2023-44487	High	Can exhaust server resources, leading to denial of service
FTP Service	Remote File Access	Unauthorized Access	-	High	Can lead to anonymous access, privilege escalation, or credential exposure
Missing CSP Header	Security Configuration	Increased XSS & Injection Risk	-	High	Can allow script injection attacks compromising user accounts

5. Mitigation

5.1. Cache poisoning and Authorization Bypass

Both the above vulnerabilities can easily be mitigated by upgrading into the latest js library and server versions. This vulnerability solely is there because of negligence for following the latest trends and versions.

5.2. XSS

This vulnerability can be fixed my implementation sanitization in both server and client side. And also the vulnerability can be fixed by implementing proper coding conventions. The rapid scanner suggested there were some coding conventions that were not followed.

5.3. FTP service

FTP related vulnerabilities can be mitigated through using firewall rules and other methods such as using ssh protocols.

5.4. Sub domain enumeration

To prevent or limit it, should reduce the attack surface. So minimizing the exposed subdomains can be done. Use firewalls to block suspicious traffic.

6. Conclusion

The web application has a multitude of vulnerabilities present. Which can be really harm full for the users using the system. Mitigating the mentioned vulnerabilities is highly recommended to prevent loss from the users and the owners