

Vulnerability Discovery

Vulnerability Discovery

Table of Contents

1.	Executive Summary	3
2.	Methodology	4
2.1.	Tools utilized	5
2.2.	Findings.....	6
■	Vulnerability 1 Title - No Content Security Policy (CSP) Header.....	6
■	Description	6
■	Vulnerability Discovery	7
■	Severity Rating.....	7
■	Proof of Concept (PoC).....	8
■	Exploitation	9
■	Impact.....	10
■	Remediation	10
■	Vulnerability 2 Title – PII Disclosure.....	11
■	Description	12
■	Vulnerability Discovery	12
■	Severity Rating.....	12
■	Proof of Concept (PoC).....	13
■	Exploitation	14
■	Impact.....	15
■	Remediation	15
■	Vulnerability 3 Title - Vulnerable JS Library.....	16
■	Description	17
■	Vulnerability Discovery	17
■	Severity Rating.....	17
■	Proof of Concept (PoC).....	18
■	Exploitation	20
■	Impact.....	21
■	Remediation	21
3.	Conclusions and Reflections	22
3.1.	What you learned from the process.....	22
3.2.	Challenges faced	22

1. Executive Summary

This report presents the vulnerability assessment of three websites, Tide (financial services application) SoundCloud (global music-sharing website) and Bullish (crypto-trading website). The main goal of the analysis was to verify whether there would be any loopholes in these websites which might put users or their data, as well any other projects by the company itself at risk.

The analysis revealed three major vulnerabilities. The first was that Tide had no Content Security Policy (CSP) header. A CSP is a feature that allows to block loading of any malware website. if it does not exist hackers can manipulate the user interface or run unauthorized scripts which will then result to data breaches or get stolen.

The second vulnerability which was found was Personally Identifiable Information (PII) on SoundCloud. PII disclosures happen when personal information, such as banking information or names, is inadvertently available on the site. The disclosures have the potential to allow malicious users to utilize personal information to stage targeted attacks or violate privacy.

The third threat found in Bullish was the incorporation of an insecure JavaScript library in its installation. Old or insecure libraries can grant hackers access to a site, interfere with its proper functioning, or even steal users' information. It is used for cryptocurrency trading, such an attack can have serious monetary implications.

The methodology adopted considers potential implications, well established proof of concept which contains evidence, and utilized industry-accepted tools. All vulnerabilities were rated for severity, and remediation has been recommended to minimize the risk.

The findings indicate the necessity of continuous upgrade, proper privacy policies, and up-to-date security. Though the vulnerabilities are of numerous different types, they all lead us to the same point high-profile and reputed sites are at risk if there is no continuous scanning and updating of the security. Such issues being solved in a timely manner will enhance the users' confidence, safeguard individual data, and ensure that the long-term success of these websites is sustained.

2. Methodology

vulnerability assessment was done with manual tools to ensure that the findings were valid and evidence based. Analysis went ahead with target websites Tide, SoundCloud, and Bullish in relation to how critical they were to finance services, music sharing, and cryptocurrency trading. The websites were chosen because they had many customers, and it was crucial to ensure users trust and safety in their services.

Tools like Burp Suite and OWASP ZAP were used both for vulnerability scanning, and browser developer tools were used to scan headers, JavaScript libraries. Manual validation was performed to check results and prevent miss-information, and first impressions were obtained using OWASP ZAP.

For each vulnerability, the discovery process was as below in a formal manner: initial reconnaissance, detection of vulnerabilities, verification, and documentation. After detecting a likely issue, it was examined in depth to determine its root cause, potential steps for exploiting it, and threat to the system. Proof of Concept (PoC) was developed to prove the vulnerabilities with evidence without causing any harm to the targeted systems.

All findings were documented in a standardized style, including description, discovery technique, severity rating, exploitation methods, possible impact, and remediation. This systematic process ensured that all findings were uniform and provided actionable information.

2.1. Tools utilized

➤ Browser Developer Tools

Built-in function in web browsers, these tools let you inspect what a website sends and shows in real time (page source code, network traffic, and response headers). Used to quickly check missing headers (like CSP), view loaded scripts, and confirm what data is sent or received, helpful for fast and visual validation.

➤ OWASP ZAP

An automated scanner and a manual scanner designed for web application security testing. It is to crawl the sites and find issues automatically, providing initial findings that were then reviewed manually to remove errors.

➤ Burp Suite

A web security toolkit used to intercept, modify, and replay web traffic between the browser and server. Used manual testing, validating vulnerabilities and capturing evidence without harming the services.

➤ Kali Basic Commands (e.g., curl)

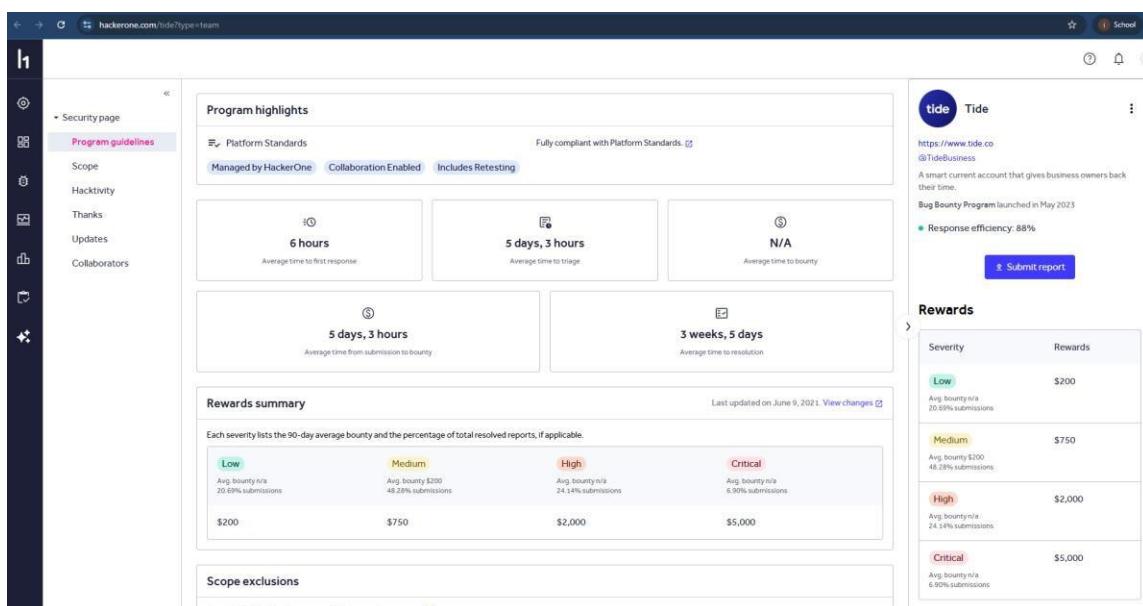
Simple command line tools available in Kali Linux, curl is used to perform HTTP requests and quickly view raw responses. Useful for reproducing and documenting vulnerabilities. For example, showing a missing header or exposed data.

Vulnerability Discovery

2.2. Findings

▪ Vulnerability 1 Title - No Content Security Policy (CSP) Header

Content Security Policy Header not set is a vulnerability found in <https://www.tide.co/> as a bug bounty program hosted in HackerOne site. It is a finance web application, so security plays a major role.



The screenshot shows the Tide bug bounty program page on the HackerOne platform. The left sidebar includes links for Security page, Program guidelines (which is selected), Scope, Hacktivity, Thanks, Updates, and Collaborators. The main content area has a header "Program highlights" with a note about being fully compliant with Platform Standards. Below this are four time-related metrics: "6 hours" (Average time to first response), "5 days, 3 hours" (Average time to triage), "N/A" (Average time to bounty), and "5 days, 3 hours" (Average time from submission to bounty). A "Rewards summary" section shows reward levels for Low, Medium, High, and Critical vulnerabilities. The "Rewards" table lists the following details:

Severity	Rewards
Low	\$200 Avg. bounty n/a 20.69% submissions
Medium	\$750 Avg. bounty \$200 48.28% submissions
High	\$2,000 Avg. bounty n/a 24.14% submissions
Critical	\$5,000 Avg. bounty n/a 6.90% submissions

▪ Description

Content Security Policy (CSP) is a security feature used in websites to specify the permitted content sources in a web page. No Content Security Policy is a vulnerability found in the site (<https://www.tide.co/>)

The browser receives no proper guidance what is safe to run on it without a CSP header. This increases the risk of execution of malicious scripts or malicious third-party content

This vulnerability relates to OWASP Top 10 – A05:2021 (Security Misconfiguration), since failing to set security headers is a classic misconfiguration. A07:2021 (Identification and Authentication Failures) is less accurate due to the lack of CSP paired with weak session management or user-controlled input that allows credential/session compromise. For example if a malicious script is injected through query parameters to form fields, no policy is there to block the execution of payloads.

Vulnerability Discovery

- **Vulnerability Discovery**

- By Inspecting the Site

Step 1 - Open the browser and navigate to the <https://www.tide.co/> site.

Step 2 – Press F12 to **Inspect** the page and it pops the network tab and refresh by pressing CTRL +R

Step 3 – under **Response Headers**, check for Content-Security-Policy header or Content-Security-Policy-Report-Only header.

- By OWASP ZAP

Step 1 – Start OWASP ZAP and enter the URL - <https://www.tide.co/>

Step 2 – after completing the scan navigate to the **Alerts**, by analyzing it Content-Security-Policy header is missing.

- By Basic Kali Commands

Step 1 – In a terminal type the **curl -I https://www.tide.co/** (it sends requests to the URL and shows only headers.

- **Severity Rating**

Risk level – Medium

Domain - <https://www.tide.co/>

OWASP Top 10 – A05:2021 (Security Misconfiguration)

Vulnerability Discovery

▪ Proof of Concept (PoC)

- By Inspecting the Site

Name	Headers	Preview	Response	Initiator	Timing	Cookies
www.tide.co				[2b064/00:b812:1e1]443		
IQdR27epKQ5E30wyrRT-RIR-...	Referer Policy					strict-origin-when-cross-origin
index.html?templateId=54196...						
index.html?templateId=54196...	Cache-Control				public, max-age=1800	
IQdR27epKQ5E30wyrRT-RIR-...	CF-Cache-Status				DYNAMIC	
sw_iframe.html?origin=https%...	CF-Ray				980ee64a0cb7a8f8-SIN	
IQdR27epKQ5E30wyrRT-RIR-...	Date				Thu, 18 Sep 2025 06:48:47 GMT	
	Etag				*af9183a2299ad1d57b346218d266793*	
	Last-Modified				Wed, 17 Sep 2025 12:34:50 GMT	
	Referrer-Policy				strict-origin-when-cross-origin	
	Server				cloudflare	
	Strict-Transport-Security				max-age=31536000; includeSubDomains; preload	
	Vary				Origin	
	Via				1.1 2ba0f5c1608b7148404c7fd295985ea.cloudfront.net (CloudFront)	
	X-Amz-Cf-Id				7REaq8OEeBdLSBF_BNRjLbxzCYNbkW07JEXObXgXeOkPwArSS3w==	
	X-Amz-Cf-Pop				LHR5D-P2	
	X-Amz-Server-Side-Encryption				AES256	
	X-Amz-Version-Id				J9fGerjT1K5ZkOF6dSaKnF_DbRejRMM	
	X-Cache				Miss from cloudfront	
	X-Content-Type-Options				nosniff	
	X-Frame-Options				ALLOW-FROM https://unclient-demo.web.app	
	X-Headers-Script-Version				0.0.5	
	X-Xss-Protection				1; mode=block	

Below is a basic example of Content Security policy

Content-Security-Policy: default-src 'self'; script-src 'self' https://asset.google.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:;

According to the above image, CSP header is missing.

- By OWASP ZAP

Content Security Policy (CSP) Header Not Set

URL: https://www.tide.co/

Risk: Medium

Confidence: High

Parameter:

Attack:

Evidence:

CWE ID: 693

WASC ID: 15

Source: Passive (10038 - Content Security Policy (CSP) Header Not Set)

Alert Reference: 10038-1

Input Vector:

Description:

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content such as Java applets, ActiveX, audio and video files.

Other Info:

Solution:

Above image confirms that CSP header is missing in the site <https://www.tide.co/>. The scan classified it as a medium risk issue.

Vulnerability Discovery

- By Basic Kali Commands

```
(kali㉿kali)-[~]
$ curl -I https://www.tide.co

HTTP/2 200
date: Wed, 17 Sep 2025 19:24:32 GMT
content-type: text/html
cf-ray: 980afbf9e324cccd-CMB
accept-ranges: bytes
cache-control: public, max-age=1800
last-modified: Wed, 17 Sep 2025 12:34:50 GMT
referrer-policy: strict-origin-when-cross-origin
strict-transport-security: max-age=31536000; includeSubDomains; preload
vary: Origin
via: 1.1 ce8f85a4dd9437febbc40094aa7d575a.cloudfront.net (CloudFront)
x-amz-cf-id: vIyzwySiSUE4v4Sodt94HtluF0ycgv4KCHwXpZCAoren14By2Ii7ow==
x-amz-cf-pop: LHR50-P2
x-amz-server-side-encryption: AES256
x-amz-version-id: J9fGerj.T1K5ZkOF6dSaKNF_DbReJRMM
x-cache: Miss from cloudfront
x-content-type-options: nosniff
x-frame-options: ALLOW-FROM https://uniclient-demo.web.app
x-headers-script-version: 0.0.5
x-xss-protection: 1; mode=block
cf-cache-status: DYNAMIC
set-cookie: _cfuvid=_Icdpx4reY7kCS7yKsGFpwYcNAvLvHouYjSyPg5phtQ-1758137072856-0.0.1.1-604800000; path=/; domain=.tide.co; HttpOnly; Secure; SameSite=None
server: cloudflare
```

By using the code `curl -I https://www.tide.co`, headers in the site and be identified. The above Screenshot again reveals CSP header is missing.

- **Exploitation**

Step 1 - An attacker identifies the NO CSP Header Vulnerability in <https://www.tide.co>

Step 2 – Attacker Creates a Malicious iframe to redirect to another site.

Example-

```
<iframe src="http://spy.com" width="500" height="500"></iframe>
```

Step 3 – Embed the iframe in site.

Step 4 – Exploit triggers because no CSP header to block inline scripts.

▪ Impact

Absence of a CSP header increases the risk of client-side attacks, without CSP header browser has no restrictions on the permitted sources. Which means it is easy for an attacker to inject malicious codes.

- Data theft – cookie stores the sensitive user data which can be exfiltrated from the browser.
- Clickjacking – without “*frame-ancestors*”, attackers can embed an *iframe* and trick users.
- Compliance Risks – vulnerabilities can lead to data breaches which could affect a user’s trust towards the site.

▪ Remediation

- Implement a CSP header – only allow content from trusted sources and restrict malicious scripts. An example of a CSP Header,

Content-Security-Policy: default-src 'self';

- Prevent clickjacking to avoid attackers tricking users to perform particular tasks. An example to avoid clickjacking,

frame-ancestors 'none';

- Use report-only mode – It identifies blocked content before enforcing the policy.

Content-Security-Policy-Report-Only: default-src 'self'; report-uri https://tide.co.

- Analyze CSP reports and do changes if necessary to avoid any errors before enforcing it.
- Acknowledge developers to use best practices write codes with the necessary headers.

Vulnerability Discovery

▪ Vulnerability 2 Title – PII Disclosure

PII Disclosure is a vulnerability found in <https://soundcloud.com> as a bug bounty program hosted in Bugcrowd site. SoundCloud is a platform designed to share music similar to spotify.

The screenshot shows the Bugcrowd interface for a SoundCloud engagement. At the top, it says "Engagements > SoundCloud". Below that, there's a "Bug Bounty" section with the SoundCloud logo. The main summary area includes:

- Scope rating: 4 out of 4
- Testing period: Ongoing, Started at Jan 09, 2018
- Status: In progress, 09 Jan 2018 20:00 UTC

Below this, there are tabs for Details, Changelog, Announcements (14), CrowdStream, and Hall of Fame. A "Submit report" button is visible. On the right, there's a sidebar titled "On this page" with links for Overview and Description.

The screenshot shows the SoundCloud homepage. It features a large banner with the text "Discover. Get Discovered." and "Now available: Get heard by up to 100 listeners on your next upload with Artist or Artist Pro. Learn More". Below the banner, there's a search bar with the placeholder "Search for artists, bands, tracks, podcasts" and a "Get Started" button. To the right of the search bar, there are "Sign in", "Create account", and "For Artists" buttons. Further down, there's a section for trending content with the text "Hear what's trending for free in the SoundCloud community" and a "Explore trending playlists" button.

Vulnerability Discovery

▪ Description

Personally Identifiable Information (PII) Disclosure is a vulnerability found in the site <https://soundcloud.com/147calboy/calboy> where the sensitive information of an individual is exposed due to insufficient protection mechanisms. These data can include phone numbers, banking details, medical records or login details.

This vulnerability could occur due to improper server configurations, inadequate data protection or saving sensitive data in plain text. There is a high risk that these data could lead to financial frauds, identity theft, reputational damage to user and to organizations.

Credit card number of a Maestro card found in this domain, which shouldn't be exposed or included plain text in the client-side. This vulnerability maps to OWASP Top 10 - A01:2021 (Broken Access Control) and A04:2021 (Insecure Design)

▪ Vulnerability Discovery

Step 1 – Navigate to the site <https://soundcloud.com/> and find a publicly available domain in the site which can be accessed without any login credentials.

Step 2 – Start OWSAP ZAP and paste the SoundCloud URL and scan for vulnerabilities.

Step 3 - Scanning found 3 PII Disclosure, analyze the response and identify the evidence. Credit card type and bank identification number are found.

Step 4 – Analyze the evidence and verify the credit card pattern.

Step 5 – Inspect the <https://soundcloud.com/147calboy/calboy> URL and validate the evidence.

▪ Severity Rating

Risk level – High

Domain – <https://soundcloud.com/147calboy/calboy>

OWASP Top 10 - A01:2021 (Broken Access Control) and A04:2021 (Insecure Design)

Vulnerability Discovery

▪ Proof of Concept (PoC)

OWASP ZAP Scan

The screenshot shows the OWASP ZAP interface with the 'Alerts' tab selected. A single alert is displayed: 'PII Disclosure (3)'. The details pane shows:

- URL:** https://soundcloud.com/147calboy/calboy
- Risk:** High
- Confidence:** High
- Parameter:** (empty)
- Attack:** (empty)
- Evidence:** 5063413670715
- CWE ID:** 359
- WASC ID:** 13
- Source:** Passive (10062 - PII Disclosure)
- Input Vector:** (empty)
- Description:** The response contains Personally Identifiable Information, such as CC number, SSN and similar sensitive data.
- Other Info:**
 - Credit Card Type detected: Maestro
 - Bank Identification Number: 506341
 - Brand: MAESTRO
- Solution:** Check the response for the potential presence of personally identifiable information (PII), ensure nothing sensitive is leaked by the application.

At the bottom, there are buttons for Alerts (1), Main Proxy: localhost:8080, and other navigation links.

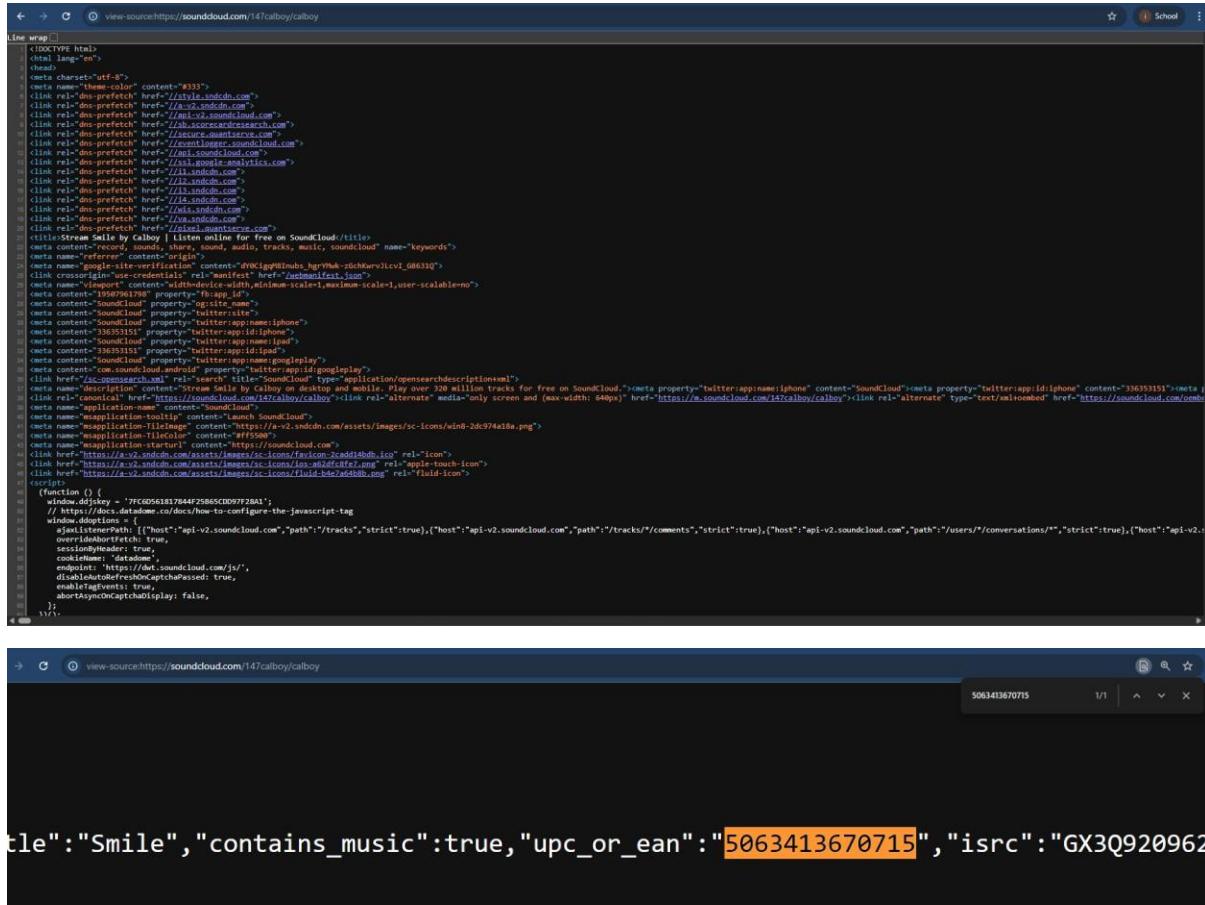
This is a detailed view of the PII Disclosure alert from the previous screenshot. It includes the following information:

- PII Disclosure**
- URL:** https://soundcloud.com/147calboy/calboy
- Risk:** High
- Confidence:** High
- Parameter:** (empty)
- Attack:** (empty)
- Evidence:** 5063413670715
- CWE ID:** 359
- WASC ID:** 13
- Source:** Passive (10062 - PII Disclosure)
- Input Vector:** (empty)
- Description:** The response contains Personally Identifiable Information, such as CC number, SSN and similar sensitive data.
- Other Info:**
 - Credit Card Type detected: Maestro
 - Bank Identification Number: 506341
 - Brand: MAESTRO
- Solution:** Check the response for the potential presence of personally identifiable information (PII), ensure nothing sensitive is leaked by the application.

Above images are the results of vulnerability scans conducted in OWASP ZAP. Scan was conducted in SoundCloud site. Results depict high level of risk in the vulnerability along with the card type and bank identification number. The vulnerability is mainly because of the insufficient server-side sanitization and should be analyzed immediately to prevent data breaches.

Mastercard Maestro is a brand of debit cards and prepaid cards owned by Mastercard.(Reference - [https://en.wikipedia.org/wiki/Maestro_\(debit_card\)](https://en.wikipedia.org/wiki/Maestro_(debit_card)))

Vulnerability Discovery



```
<meta name="description" content="Stream Smile by Calboy | Listen online for free on SoundCloud" title="Smile by Calboy | Listen online for free on SoundCloud" data-bbox="117 148 875 425"/><meta data-bbox="117 3285 875 3295" data-b
```

Vulnerability Discovery

▪ Impact

- Identity theft – An attacker can steal the personal details to open fake accounts and to make unauthorized transactions.
- Phishing attacks – attacker can use the personal data to trick the user.
- Reputational damage – exposure of personal data can cause damage to the user and the organization, which could result in loss of trust towards the organization.
- Recovery cost – After an incident organization might have to compensate the user. And pay for legal defense. Long term funds may be needed to rebuild trust of users.

▪ Remediation

- Enforcing a strong access control – Enforce principle of least privilege to limit the access of a particular content.
- Remove the leaked content – Analyze and identify the leaked content and remove it from the site.
- Encrypt and store securely – Encrypt the sensitive content and store it properly.
- Monitoring – To avoid any further data breaches enforce data loss prevention tools.
- Compliance with the standards – follow the relevant frameworks like PCI DSS (Payment Card Industry Data Security Standard) to avoid any further breaches or data loss.

Vulnerability Discovery

▪ Vulnerability 3 Title - Vulnerable JS Library

Vulnerable JS Library is a vulnerability found in <https://bullish.com/> as a bug bounty program hosted in Bugcrowd site. This site is focused on crypto trading, which means security is very critical.

The screenshot shows the Bugcrowd interface for the engagement titled 'Bullish.com'. At the top, there's a navigation bar with links for 'Engagements' and 'Bug Bounty'. Below it, the engagement title 'Bullish.com' is displayed with a subtitle 'Help Secure Bullish - a new breed of exchange'. To the right is a logo featuring a stylized 'B' and 'F'. The main section includes a scope rating of '1 out of 4' (with 4 circles), a testing period status of 'Ongoing' (started at Jul 27, 2021), and a current status of 'In progress' (27 Jul 2021 18:00:00 UTC). There are buttons for 'Submit report', 'Follow', and 'Share'. Below these are tabs for 'Details', 'Changelog', 'Announcements', 'CrowdStream', and 'Hall of Fame'. A note at the bottom indicates the last update was on Sep 06, 2024, at 12:42:45 UTC.

The screenshot shows the Bullish.com homepage. The header features the 'bugcrowd' logo, 'MARKETS', 'PRODUCTS', 'AMM', 'Preview exchange', 'Log in', and 'SIGN UP' buttons. The main visual is a large monitor displaying a complex trading interface with multiple charts and data tables, accompanied by a smartphone showing a similar app. The text 'The standard for institutional crypto trading.' is prominently displayed. Below this, a subtext states: 'With tier-1 licenses and a deeply liquid global order book, Bullish offers tight spreads and low fees to institutions and advanced traders.' A 'GET STARTED' button is at the bottom.

Vulnerability Discovery

■ Description

Vulnerability java script Library is a problem found in bullish site, it is a crypto trading website where trading happens with digital assets and more secure. Bullish site loads Next.js version 12.3.4 which is vulnerable to bypass authorization (CVE-2025-29927 - <https://nvd.nist.gov/vuln/detail/CVE-2025-29927>)

This vulnerability falls under OWASP Top 10 - A06:2021 (Vulnerable and Outdated Components) and A05:2021 (Security Misconfiguration). If an attacker intercept and manipulate the data sent to vulnerable next() functions through reflected inputs trigger prototype and escalate privileges in the JavaScript context. Attackers can exploit client-side attacks like Cross-Site Scripting, data breaches and privilege escalation.

■ Vulnerability Discovery

Step 1 – Open ZAP and scan the <https://bullish.com/> site.

Step 2 – After the scan we can get the vulnerability in https://bullish.com/_next/static/chunks/main-3fd8e90ae090f348.js domain with the risk level high.

Step 3 – To confirm the vulnerability, start Burp suite and capture the request and send to the repeater.

Step 4 – check the Java Script version by searching “version” on the search bar in the response panel.

So the version “12.3.4” will appear, which is vulnerable for security misconfigurations.

■ Severity Rating

Risk level – High

Domain – https://bullish.com/_next/static/chunks/main-3fd8e90ae090f348.js

OWASP Top 10 - A06:2021 (Vulnerable and Outdated Components) and A05:2021 (Security Misconfiguration).

Vulnerability Discovery

▪ Proof of Concept (PoC)

The above screenshot show a high level of risk in the JavaScript file https://bullish.com/_next/static/chunks/main-3fd8e90ae090f348.js, which uses next.js version “12.3.4” which is vulnerable for improper authorization. The search results show two JS vulnerabilities which use next.js so by upgrading to a new version of next.js

Vulnerability Discovery

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history Match and replace Proxy settings

No proxy listeners are currently running Configure

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	List
1	https://bullish.com	GET	/_next/static/chunks/			404	4670	HTML		Page not found	✓	104.18.25.158	_cf_bm=Ddy8f...	22:21:29 21 ...	808	
2	https://bullish.com	GET	/favicon.ico			404	70363	HTML	ico		✓	104.18.25.158			22:22:25 21 ...	808
3	https://bullish.com	GET	/_next/static/			404	4379	HTML		Page not found	✓	104.18.25.158			22:22:31 21 ...	808
4	https://bullish.com	GET	/_next/static/			404	4364	HTML		Page not found	✓	104.18.25.158			22:23:15 21 ...	808
5	https://bullish.com	GET	/_next/static/			404	4365	HTML		Page not found	✓	104.18.25.158			22:23:18 21 ...	808
6	https://bullish.com	GET	/_next/static/chunks/main-3fd8e90...			200	114934	script	js		✓	104.18.25.158			22:23:21 21 ...	808
7	https://bullish.com	GET	/_next/static/chunks/main			404	4365	HTML		Page not found	✓	104.18.25.158			22:23:31 21 ...	808
8	https://bullish.com	GET	/_next/static/chunks/main-3fd8e90...			200	114932	script	js		✓	104.18.25.158			22:23:37 21 ...	808
9	https://bullish.com	GET	/_next/static/chunks/main-3fd8e90...			200	114936	script	js		✓	104.18.25.158			22:23:48 21 ...	808
10	https://bullish.com	GET	/_next/static/chunks/main-3fd8e90...			200	114932	script	js		✓	104.18.25.158			22:24:03 21 ...	808
11	https://bullish.com	GET	/favicon.ico			404	70357	HTML	ico		✓	104.18.25.158			22:24:04 21 ...	808

Request

Pretty Raw Hex

```
1 GET /_next/static/chunks/main-3fd8e90ae090f348.js HTTP/2
2 Host: bullish.com
3 Cookie: __cf_bm=...
4 Ddy8fjkFUbzAXPnxVbKoGzROB_P113nQipGevpZkg-1758473545-1.0.1.1-QWDT
5 Bht9kspC_3hL4ui1P_pzWqY1kxNcEyKLDDmrssjZAZYNa40fHUnDrSPhy1Xw3Dc0_b
6 uxAfT_Vk2zcY7k2HUMDh_E17FJp1Up0Ih4
7 Sec-Ch-Ua: "Chromium";v="139", "Not-A-Brand";v="99"
8 Sec-Ch-Ua-Mobile: ?0
9 Sec-Ch-Ua-Platform: "Windows"
10 Accept-Language: en-US,en;q=0.9
11 Upgrade-Insecure-Requests: 1
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
14 
```

0 highlights

Response

Pretty Raw Hex Render

```
1 HTTP/2 200 OK
2 Date: Sun, 21 Sep 2025 16:53:22 GMT
3 Content-Type: application/javascript; charset=UTF-8
4 Content-Security-Policy: upgrade-insecure-requests; frame-ancestors 'self'; strict-uri-encoding none; strict-uri-reporting none; report-uri https://reporting.bullish.com/report; report-to main; report-to-id 11410dbic9cal-SIN
5 Cache-Control: no-store, no-cache, must-revalidate, max-age=0
6 Pragma: no-cache
7 Age: 66378
8 Cache-Control: public, max-age=691200
9 Cache-Status: "MetHTTP Edge"; hit
10 Etag: "5f5ce7a1c27c4a0824456442c4b959-sml-dt"
11 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
12 Vary: Accept-Encoding
13 X-Content-Type-Options: nosniff
14 X-Frame-Options: DENY
15 X-Middleware-Next: 1
16 X-Middleware-Route: /_next/static/chunks/main-3fd8e90ae090f348.js
17 
```

0 highlights

Request

Pretty Raw Hex

```
1 GET /_next/static/chunks/main-3fd8e90ae090f348.js HTTP/2
2 Host: bullish.com
3 Cookie: __cf_bm=...
4 Ddy8fjkFUbzAXPnxVbKoGzROB_P113nQipGevpZkg-1758473545-1.0.1.1-QWDT
5 Bht9kspC_3hL4ui1P_pzWqY1kxNcEyKLDDmrssjZAZYNa40fHUnDrSPhy1Xw3Dc0_b
6 uxAfT_Vk2zcY7k2HUMDh_E17FJp1Up0Ih4
7 Sec-Ch-Ua: "Chromium";v="139", "Not-A-Brand";v="99"
8 Sec-Ch-Ua-Mobile: ?0
9 Sec-Ch-Ua-Platform: "Windows"
10 Accept-Language: en-US,en;q=0.9
11 Upgrade-Insecure-Requests: 1
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
14 
```

7

Sec-Fetch-Site: none

Sec-Fetch-Mode: navigate

Sec-Fetch-User: ?1

Sec-Fetch-Dest: document

Accept-Encoding: gzip, deflate, br

Priority: u=0, i

Response

Pretty Raw Hex Render

```
1 // ...
2 .nonce=r====.nonce==.isEqualNode(t))return e.isEqualNode(t).t.
3 DOMAttributeNames=e,(function()=="typeof t.default||"object"===
4 typeof t.default!=null!="t.default"=="typeof t.default
5 _esModule||(Object.defineProperty(t.default,"_esModule",{}),(value:0),Object.assign(t.default,t.e.exports=t.default)),96947:function
6 (e,t){"use strict":var n=r(87794),a=r(85695),o=r(33227),i=r(88361)
7 ,u=r(85971),c=r(52715),s=r(9193);function l(e){var t=function(){}if
8 "undefined"==typeof Reflect||!Reflect.construct{return!1;if
9 Reflect.construct.sham{return!1;if("function"==typeof Proxy)return
10 !0;try{return Boolean.prototype.valueOf.call(Reflect.construct(
11 Boolean,[],(function()))),!0}catch(e){return!1}};return
12 function(){var r,n;s(e).if(t){var a=s(this).constructor;r=Reflect.
13 construct(n,arguments,a)}else r=apply(this,arguments);return c(
14 this,r)}Object.defineProperty(t,"_esModule",{}),value:{0}:0},t.
15 initialize=function(){return K.apply(this.arguments),t.emitter=t.router=t.
16 version:void 0;var f=r(60932),z=d(r(4695).Z,r(2648).Z,r(91598).Z
17 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
18 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
19 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
20 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
21 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
22 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
23 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
24 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
25 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
26 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
27 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
28 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
29 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
30 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
31 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
32 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
33 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
34 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
35 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
36 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
37 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
38 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
39 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
40 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
41 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
42 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
43 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
44 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
45 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
46 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
47 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
48 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
49 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
50 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
51 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
52 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
53 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
54 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
55 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
56 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
57 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
58 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
59 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
60 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
61 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
62 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
63 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
64 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
65 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
66 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
67 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
68 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
69 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
70 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
71 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
72 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
73 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
74 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
75 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
76 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
77 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
78 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
79 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
80 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
81 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
82 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
83 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
84 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
85 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
86 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
87 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
88 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
89 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
90 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
91 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
92 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
93 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
94 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
95 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
96 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
97 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
98 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
99 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
100 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
101 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
102 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
103 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
104 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
105 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
106 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
107 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
108 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
109 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
110 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
111 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
112 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
113 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
114 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
115 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
116 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
117 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
118 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
119 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
120 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
121 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
122 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
123 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
124 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
125 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
126 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
127 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
128 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
129 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
130 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
131 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
132 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
133 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
134 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
135 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
136 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
137 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
138 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
139 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
140 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
141 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
142 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
143 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
144 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
145 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
146 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
147 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
148 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
149 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
150 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
151 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
152 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
153 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
154 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
155 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
156 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
157 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
158 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
159 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
160 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
161 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
162 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
163 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
164 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
165 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
166 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
167 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
168 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
169 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
170 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
171 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
172 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
173 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
174 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
175 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
176 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
177 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
178 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
179 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
180 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
181 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
182 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
183 :r(40037):var h,v=h,v=r(67294)),m=r(15850),y=r(18286),g=r(30647),B
1
```

Above screenshot of Burp suite again confirms that https://bullish.com/_next/static/chunks/main-3fd8e90ae090f348.js uses next.js version “12.3.4”

Vulnerability Discovery

C [Improper Authorization](#)

`next` is a react framework.

Affected versions of this package are vulnerable to Improper Authorization due to the improper handling of the `x-middleware-subrequest` header. An attacker can bypass authorization checks by sending crafted requests containing this specific header.

`>=11.1.4 <12.3.5`

`>=13.0.0 <13.5.9`

`>=14.0.0 <14.2.25`

`>=15.0.0-rc.0 <15.2.3`

`>=15.3.0-canary.0 <15.3.0-canary.12`

How to fix Improper Authorization?

Upgrade `next` to version 12.3.5, 13.5.9, 14.2.25, 15.2.3, 15.3.0-canary.12 or higher.

Link - <https://security.snyk.io/package/npm/next/12.3.4>

According to the above site JavaScript version 12.3.4 is vulnerable due to improper authorization and an attacker can bypass the authorization.

▪ Exploitation

Step 1 – Identify the outdated or vulnerable libraries using tools like browser dev or Snyk.

Step 2 – Compare the library version with CVE listings to find vulnerabilities.

Step 3 – Create a payload.

Step 4 – Inject a malicious script to exploit the vulnerability.

Step 5 – Create a fake form to execute the malicious script.

Vulnerability Discovery

▪ Impact

- Sensitive data is exposed through cookies or forms and can be leaked.
- Session takeover - Attackers can perform unauthorized actions on behalf of users.
- Reputational damage – exposure of personal data can cause damage to the user and the organization, which could result in loss of trust towards the organization.
- Increase in number of surface attacks since multiple modules may inherit the same vulnerability due to its dependency.
- Possibility of phishing attacks – An attacker can modify the UI to inject fake logins and trick users to reveal login credentials.

▪ Remediation

- Conduct regular scans to detect vulnerabilities using manual or automated tools.
- Update the next.js library to a newly released version to avoid any outdated bugs.
- Limit third party access to scripts through principle of least privilege.
- Adapt to a well-maintained library by removing obsolete packages or unused packages.
- Maintain a dependency list with their versions and particular libraries track the package integrity.

3. **Conclusions and Reflections**

This report emphasizes critical security vulnerabilities in three platforms Tide, SoundCloud, and Bullish. The report showed that even established businesses cannot escape it, if security best practices such as security headers, data protectors for privacy, and library patching are not adhered to. All the vulnerabilities have the potential to cause harm to users, from data leakage to financial loss. The analysis confirmed the value of supplementing automated code with human checks to produce results that are accurate. Moreover, the report highlights the importances of continuous security monitoring, and proactive interventions to maintain trust, protect sensitive information, and achieve long-term resiliency against changing threats.

3.1. **What you learned from the process**

- To use manual tools and find vulnerabilities.
- Impact of vulnerability if it is not addressed.
- Proper documentation is also important to communicate with non-technical people.
- Importance of proper monitoring is a continuous responsibility of an organization.
- How different areas like music, crypto and finance have overlapping security risks.

3.2. **Challenges faced**

- Using manual tools is time consuming and difficult to discover vulnerabilities.
- Time limitations made it difficult to find vulnerabilities in depth.
- Limitation in scope of certain web applications made it difficult to find vulnerabilities.
- Inaccurate results of some tools made it difficult to figure out what is correct and wrong.
- Lack of knowledge about real-world exploitation made it challenging to understand and write how an attack is exploited.