

Sri Lanka Institute of Information Technology



Bug Bounty Report - 06

Module: IE2062

Web Security

Year 2, Semester 2

Aazaf Ritha. J – IT23151710

B.Sc. (Hons) in Information Technology

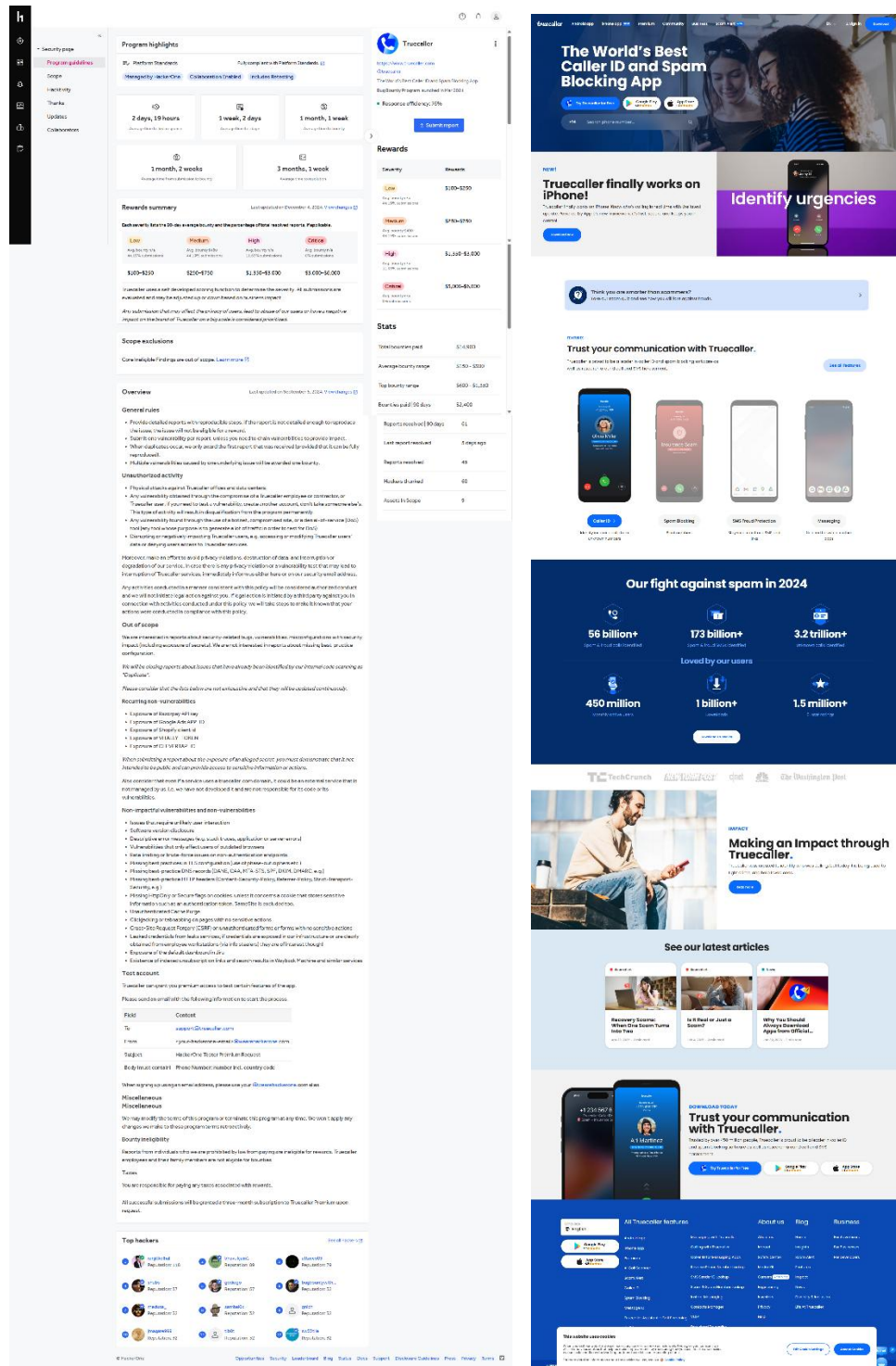
Specialized in Cyber Security

Table of Contents

Introduction	3
Vulnerability Title	4
Description.....	5
Affected Component.....	6
Impact Assessment	7
Steps to Reproduce.....	8
Proof of Concept (Screenshots)	9
Proposed Mitigation or Fix.....	11
Conclusion.....	12

Introduction

This report outlines a Vulnerable JS Library discovered on Truecaller's public website (<https://www.truecaller.com>) as part of the HackerOne bug bounty program. The issues were confirmed through both manual testing and automated scanning. This document provides technical details, clear reproduction steps, proof-of-concept evidence, and practical mitigation recommendations.



The image shows a screenshot of the Truecaller website, specifically the bug bounty program page. The page is divided into several sections:

- Program highlights:** Includes a sidebar with navigation links (Home, Scope, Security, Thanks, Updates, Collaborators) and a main content area with program details. The program is titled "Truecaller Open Source Project" and is part of the "HackerOne Bug Bounty Program". It offers a reward of up to \$10,000 for a "Critical" vulnerability.
- Rewards:** A table showing the reward structure based on the severity of the vulnerability. The table has columns for "Severity", "Reward", and "Status".
- Scope:** A section detailing the scope of the program, including the types of vulnerabilities accepted and the exclusions.
- Overview:** A section providing an overview of the program, including the number of reports received, the number of vulnerabilities discovered, and the total amount paid.
- Our fight against spam in 2024:** A section highlighting Truecaller's achievements in fighting spam, including the number of spam calls blocked and the number of users who have benefited.
- See our latest articles:** A section featuring a list of recent articles, including "Making an Impact through Truecaller" and "Why You Should Always Download Apps from Official Sources".
- Top hackers:** A section listing the top hackers who have discovered vulnerabilities in Truecaller, including their names, the number of reports they have submitted, and the total amount they have earned.

Vulnerability Title

Title – Vulnerable JS Library

Risk Level- High

Domain – <https://www.truecaller.com>

Description

Vulnerable JavaScript Library issue was identified on True caller's public website (<https://www.truecaller.com>) in the `/year-in-calling-2021/js/webflow.js` bundle. The site is loading **moment.js v2.22.2**, a version known to contain critical flaws (CVE-2022-31129, CVE-2022-24785) that allow prototype pollution and client-side code execution.

This vulnerability stems from the inclusion of an **outdated third-party component** without validation or isolation and falls under **OWASP Top 10 – A06:2021 (Vulnerable and Outdated Components)** and **A05:2021 (Security Misconfiguration)**. By relying on a library release with publicly documented exploits, the application exposes its users to unnecessary risk.

If an attacker can manipulate data passed to the vulnerable `moment()` functions—either via crafted JSON payloads or reflected input in the page—they may trigger prototype pollution, escalate privileges within the JavaScript context, or execute arbitrary scripts in the victim's browser. This can lead to session hijacking, theft of sensitive information (tokens, PII), or forced actions on protected endpoints under the user's authority.

Affected Component

/year-in-calling-2021/js/webflow.js - Includes the vulnerable moment.js v2.22.2 library, exposing its known prototype-pollution flaws.

Global JavaScript Bundles - Any front-end bundle that imports or re-uses moment.js without version checks inherits the same vulnerabilities.

Third-Party CDN References - References to moment.js@2.22.2 served via external CDNs load the affected version across all pages that include it.

Impact Assessment

Client-Side Prototype Pollution: An attacker supplying crafted data to the vulnerable `moment.js` functions can manipulate object prototypes, potentially altering application logic or bypassing security checks in the browser.

Arbitrary Code Execution: Exploiting prototype pollution may allow injection of malicious scripts that execute in the context of the user's session, leading to full compromise of the client environment.

Data Exfiltration: Malicious code executed via the vulnerable library can read sensitive information such as authentication tokens, user preferences, or PII and send it to an attacker-controlled server.

Session Hijacking: Injected scripts can steal session cookies or local storage tokens, enabling the attacker to hijack the user's authenticated session.

Phishing & UI Manipulation: An attacker could modify the page's DOM or inject fake UI elements (e.g., login prompts), tricking users into revealing credentials or other sensitive data.

Reputation & Trust Damage: Successful exploitation undermines user confidence in the application's security posture and may lead to regulatory scrutiny if personal data is exposed.

Steps to Reproduce

Step 01: Locate the Vulnerable Bundle

1. Configure your browser to proxy through Burp (or ZAP) and open DevTools.
2. In Burp → Proxy → HTTP history (filter “JS”), reload the page at:
`https://www.truecaller.com/year-in-calling-2021`
3. Identify the request for `/year-in-calling-2021/js/webflow.js`.

Step 02: Confirm the Moment.js Version

1. Right-click the webflow.js entry → Send to Repeater.
2. In Repeater’s Response pane (Raw view), search for:

`<= 2.22.2`

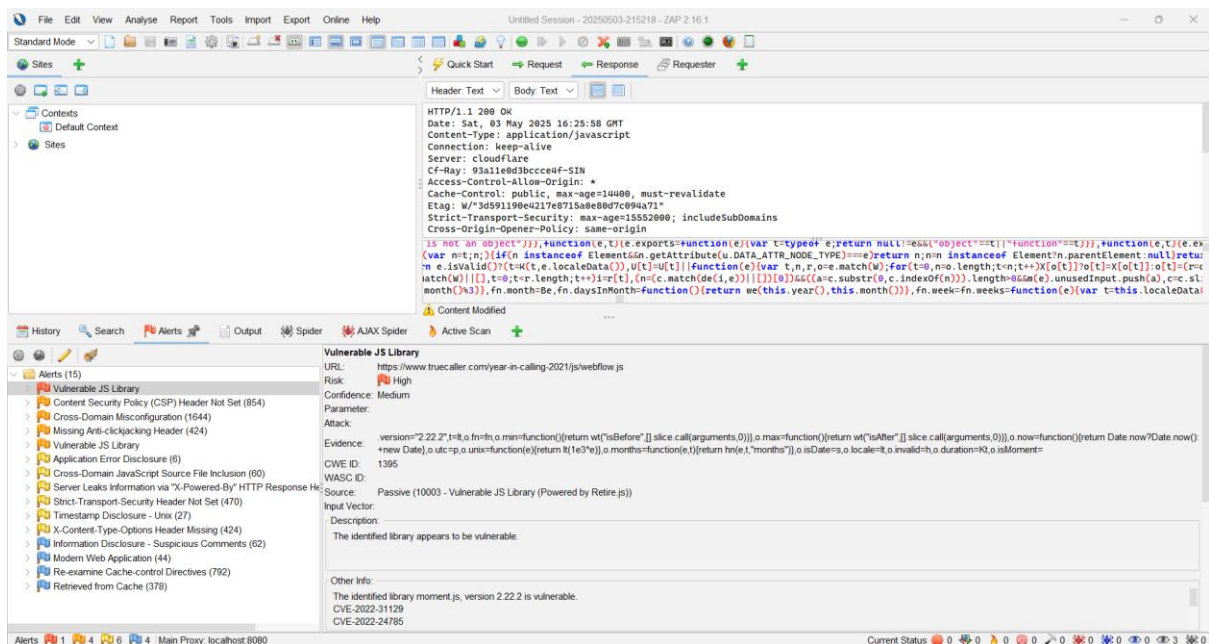
This confirms that Moment.js v2.22.2 (or less) is bundled.

Proof of Concept (Screenshots)

Subfinder

```
ar@Kali2024: ~  
File Actions Edit View Help  
$ subfinder -d truecaller.com -o subfinder.txt  
  
projectdiscovery.io  
[INF] Current subfinder version v2.6.0 (outdated)  
[INF] Loading provider config from /home/ar/.config/subfinder/provider-config.yaml  
[INF] Enumerating subdomains for truecaller.com  
truecaller.com  
notifications-gateway-se1.truecaller.com  
search-warnings-noneu.truecaller.com  
opt-out-noneu.truecaller.com  
topspammers-noneu.truecaller.com  
notifications5.truecaller.com  
cloud-telephony-v2-noneu.truecaller.com  
survey-noneu.truecaller.com  
business-priority-media-noneu-tmp.truecaller.com  
tagging5.truecaller.com  
phonebook5-noneu.truecaller.com  
corporate.truecaller.com  
images-override-eu.truecaller.com  
rv-e0-1513.truecaller.com  
invite3.truecaller.com  
loans.truecaller.com  
account-eu.truecaller.com  
feature-flags-eu.truecaller.com  
www.blog.truecaller.com  
webapp.truecaller.com  
contact-upload4-noneu.truecaller.com  
callmeback.truecaller.com  
tagging5-noneu.truecaller.com  
messenger-se1.truecaller.com  
images-se1.truecaller.com  
priority.truecaller.com  
ads-segment-profile-noneu.truecaller.com  
telecom-operator-data-noneu.truecaller.com  
se-st-egw2.truecaller.com  
o3.email.truecaller.com  
app.truecaller.com  
tagging-assets-eu.truecaller.com  
edge-locations5-noneu.truecaller.com  
outline-noneu.truecaller.com  
callkit-media.truecaller.com  
device-safety-eu.truecaller.com  
push-callerid-eu.truecaller.com  
  
userapps.truecaller.com  
[INF] Found 235 subdomains for truecaller.com in 10 seconds 91 milliseconds  
(ar@Kali2024)-[~]  
$
```

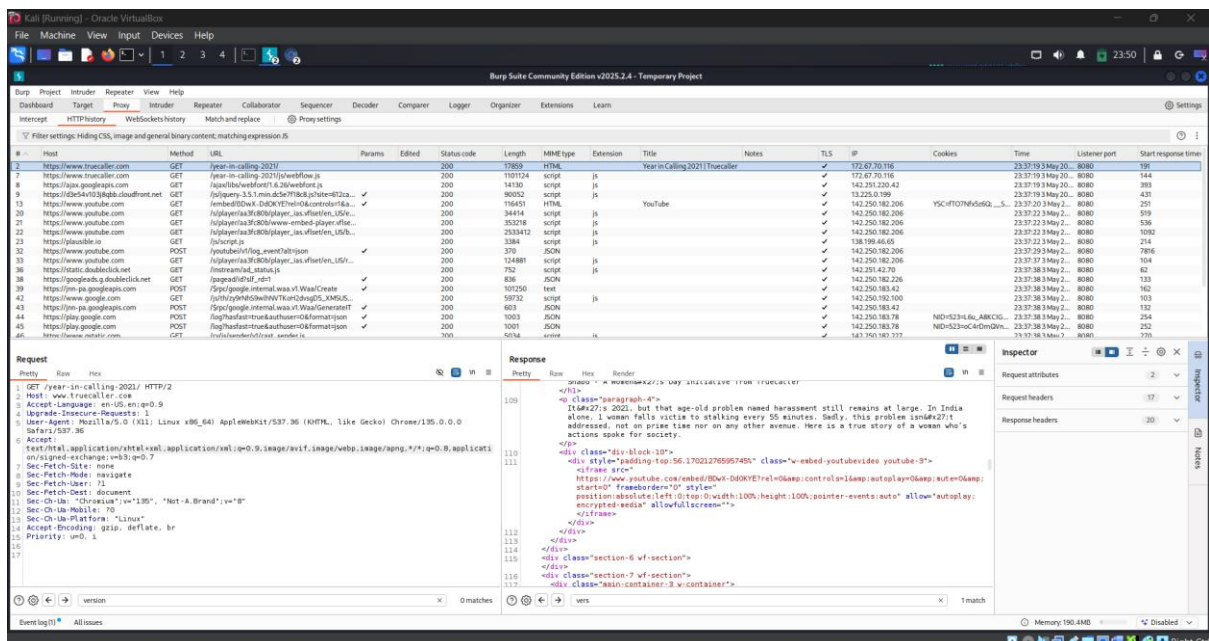
OWASP ZAP Scan



The screenshot shows the OWASP ZAP interface. The top pane displays the HTTP response for the URL `https://www.truecaller.com/year-in-calling-2021/js/webflow.js`. The response is an application/javascript file. The bottom pane shows the 'Vulnerable JS Library' alert, indicating that the library is vulnerable to a prototype-pollution attack (CVE-2022-31129, CVE-2022-24785). The alert details include the URL, risk level (High), confidence (Medium), and a description of the vulnerability.

ZAP has flagged the inclusion of **moment.js v2.22.2** in the `/year-in-calling-2021/js/webflow.js` bundle. This specific version is known to suffer from prototype-pollution flaws (CVE-2022-31129, CVE-2022-24785). An attacker who can feed crafted input into the library's parsing routines could manipulate `Object.prototype`, enabling arbitrary script execution in users' browsers. Upgrading to a non-vulnerable Moment.js release ($\geq 2.29.1$) will remove these risks.

BurpSuite



The screenshot shows the Burp Suite interface. The top pane displays the 'Proxy' tab, showing a list of intercepted requests. The bottom pane shows the 'Request' and 'Response' tabs, displaying the details of a request to `https://www.truecaller.com/year-in-calling-2021/js/webflow.js`. The response is an application/javascript file.

Proposed Mitigation or Fix

Upgrade Moment.js

- Replace v2.22.2 with a patched release ($\geq 2.29.1$) where the prototype-pollution CVEs are resolved.

Audit & Replace Outdated Libraries

- Review all third-party JS dependencies and update or swap any that are end-of-life or known vulnerable.
- Use tools like npm audit or Retire.js in your build pipeline.

Harden Input Handling

- Never pass untrusted JSON or user-controlled strings directly into date-parsing routines.
- Sanitize or validate inputs before feeding them into any library.

Enforcement Content Security Policy

- Implement a strict CSP to block unauthorized script execution, limiting the blast radius if a library is compromised.

Continuous Monitoring

- Integrate an SCA (Software Composition Analysis) to detect new vulnerabilities in your dependencies as they're disclosed.

Conclusion

The inclusion of Moment.js v2.22.2 in Truecaller's /year-in-calling-2021/js/webflow.js bundle exposes a high-risk prototype-pollution flaw (CVE-2022-31129, CVE-2022-24785), allowing an attacker to execute arbitrary code in users' browsers. Upgrading to a patched Moment.js release ($\geq 2.29.1$), auditing all third-party dependencies, and strengthening input validation and CSP policies will eliminate this vulnerability and significantly improve the site's client-side security posture.