Sri Lanka Institute of Information Technology

Year 2 semester 2

IT23360600
G. P. I. Perera

SLIIT KANDY UNI

BUG BOUNTY REPORT 1

Web Security – IE2062

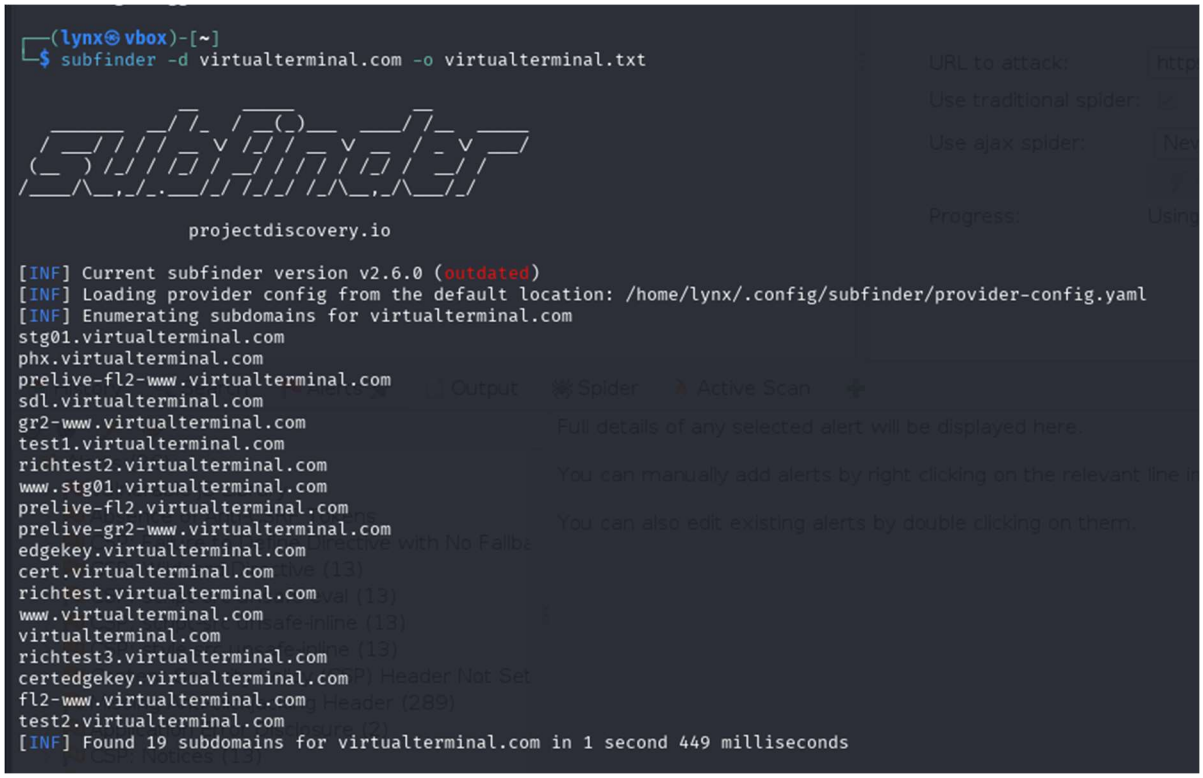
B.Sc. (Hons) in information Technology Specializing in Cyber Security

1. Requirement gathering and analysis

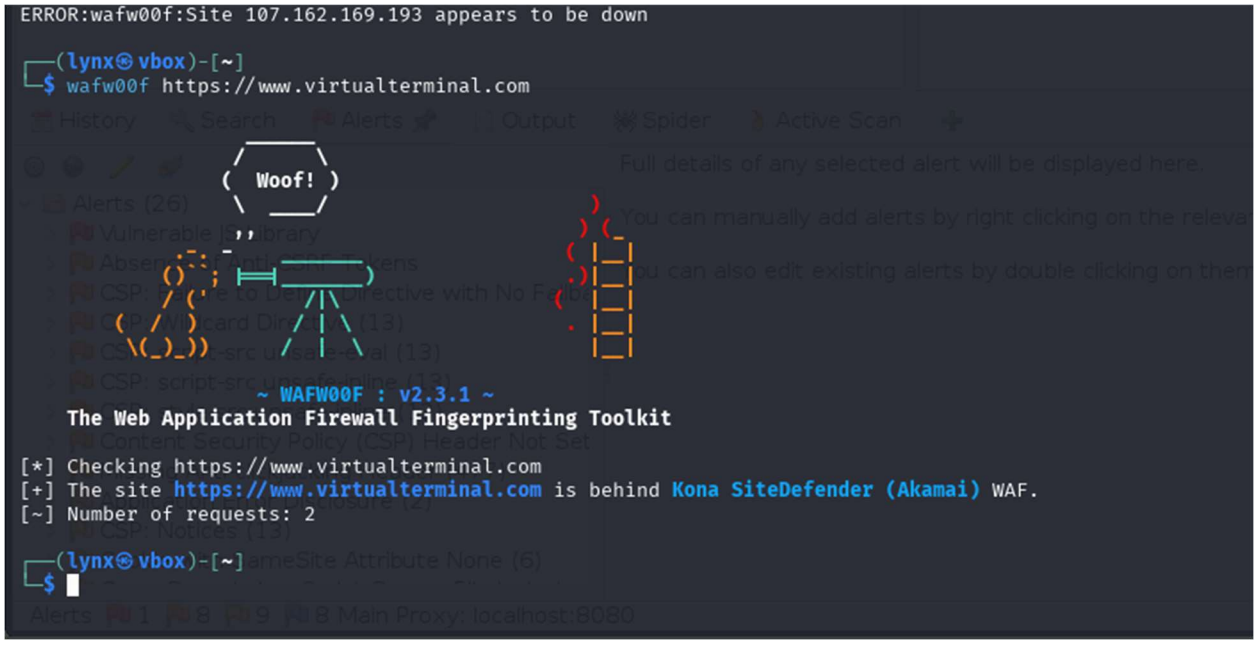
Selected sub domain	virtualterminal.com
Hakerone URL	https://hackerone.com/worldpay?type=team
IP address	107.162.169.193

Subdomain list

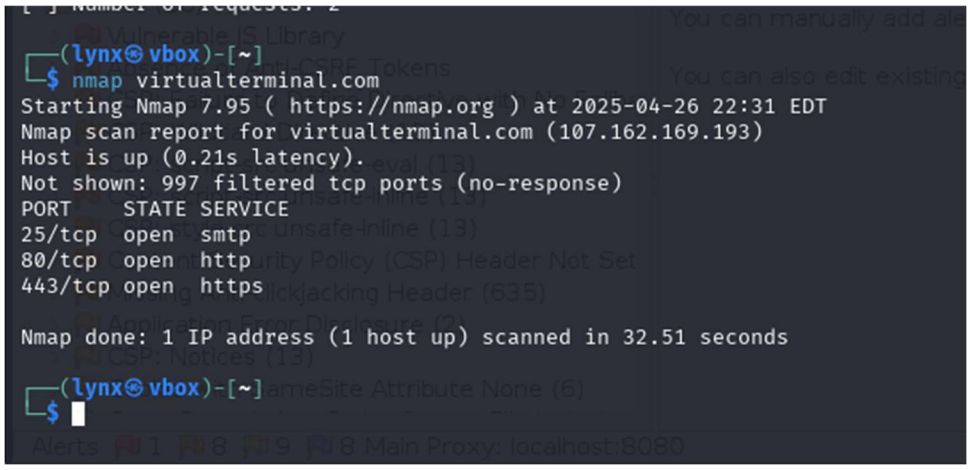
- stg01.virtualterminal.com
- phx.virtualterminal.com
- prelive-fl2-www.virtualterminal.com
- sdl.virtualterminal.com
- gr2-www.virtualterminal.com
- test1.virtualterminal.com
- richtest2.virtualterminal.com
- www.stg01.virtualterminal.com
- prelive-fl2.virtualterminal.com
- prelive-gr2-www.virtualterminal.com
- edgekey.virtualterminal.com
- cert.virtualterminal.com
- richtest.virtualterminal.com
- www.virtualterminal.com
- virtualterminal.com
- richtest3.virtualterminal.com
- certedgekey.virtualterminal.com
- fl2-www.virtualterminal.com
- test2.virtualterminal.com



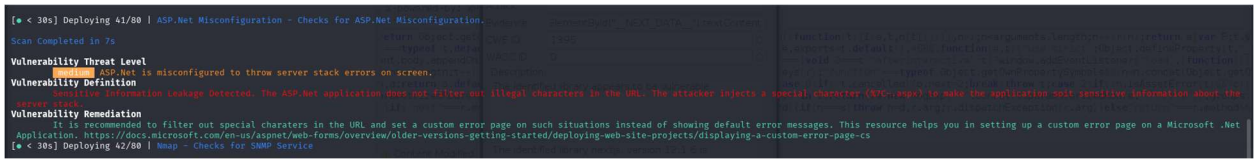
Firewall detection:

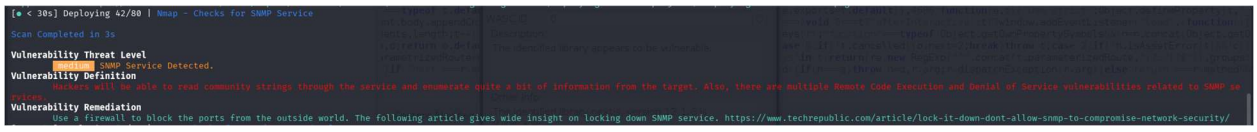


Nmap scan:



RapidScan result: detected vulnerabilities





```
Use a firewall to block the ports from the outside world. The following article gives wide insight on locking down SNMP service. https://www.techrepublic.com/article/lock-it-down-dont-allow-snmp-to-compromise-network-security/
[● <  4m] Deploying 43/80 | LBD - Checks for DNS/HTTP Load Balancers.

Scan Completed in 3m 22s

Vulnerability Threat Level
        low  No DNS/HTTP based Load Balancers Found.
Vulnerability Definition
        Not directly to do with security risks, however attackers may use this unavailability of load balancers as an advantage to leverage a denial of service attack on certain services or on the whole application itself.
Vulnerability Remediation
        Load-Balancers are highly encouraged for any web application. They improve performance times as well as data availability on during times of server outage. To know more information on load balancers and setup, check this resource. https://www.digitalocean.com/community/tutorials/what-is-load-balancing
[● <  9m] Deploying 44/80 | Uniscan - Stress Tests the Domain.
```

```
[● < 75m] Deploying 60/80 | Fierce Subdomains Bruter - Brute Forces Subdomain Discovery.

Scan Completed in 15m 53s

Vulnerability Threat Level
        medium  Found Subdomains with Fierce.
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 with 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 the tech stack. Complex naming practices also help in reducing the attack surface as attackers find hard to perform subdomain bruteforcing through dictionaries and wordlists.
[● < 35s] Deploying 61/80 | Nikto - Checks for Apache Expect XSS Header.
```

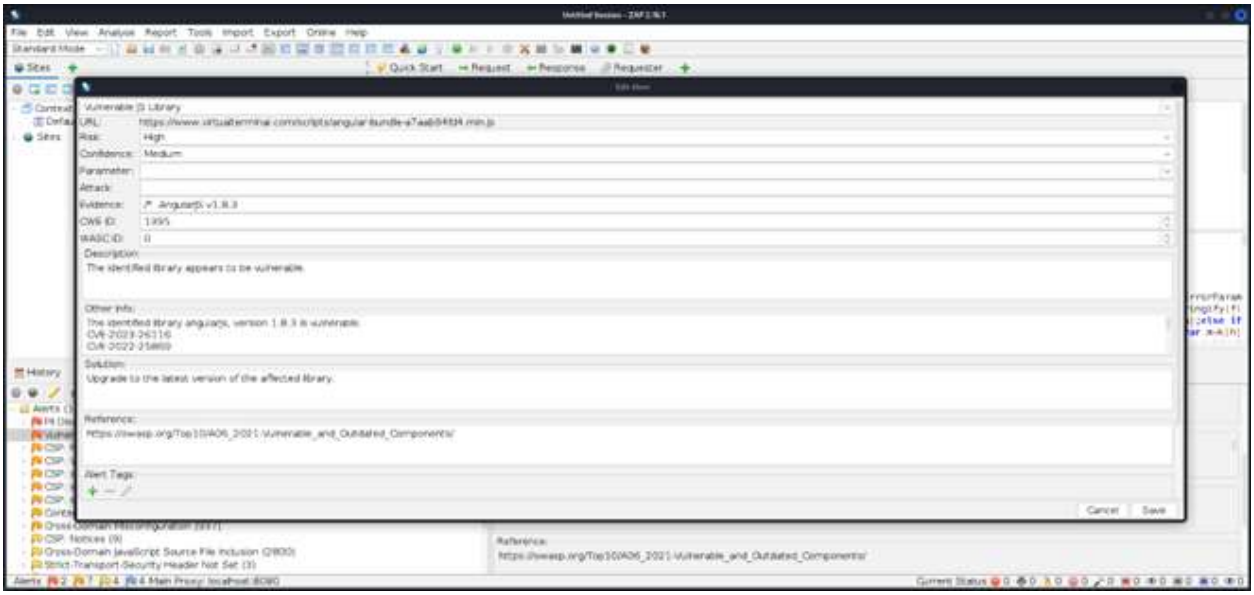
```
[● <  3m] Deploying 69/80 | WhatWeb - Checks for X-XSS Protection Header

Scan Completed in 6m

Vulnerability Threat Level
        medium  X-XSS Protection is not Present
Vulnerability Definition
        As the target is lacking this header, older browsers will be prone to Reflected XSS attacks.
Vulnerability Remediation
        Modern browsers does not face any issues with this vulnerability (missing headers). However, older browsers are strongly recommended to be upgraded.
[● <  8m] Deploying 70/80 | Uniscan - Checks for LFI, RFI and RCE.
```

```
[● < 15s] Deploying 74/80 | Nmap - Checks for Remote Desktop Service over UDP

Scan Completed in 3s

Vulnerability Threat Level
        high  RDP Server Detected over UDP.
Vulnerability Definition
        Attackers may launch remote exploits to either crash the service or tools like ncrack to try brute-forcing the password on the target.
Vulnerability Remediation
        It is recommended to block the service to outside world and made the service accessible only through the a set of allowed IPs only really neccessary. The following resource provides insights on the risks and as well as the steps to block the service. https://www.perspectiverisk.com/remote-desktop-service-vulnerabilities/
[● < 45s] Deploying 75/80 | DNSEnum - Attempts Zone Transfer.
```

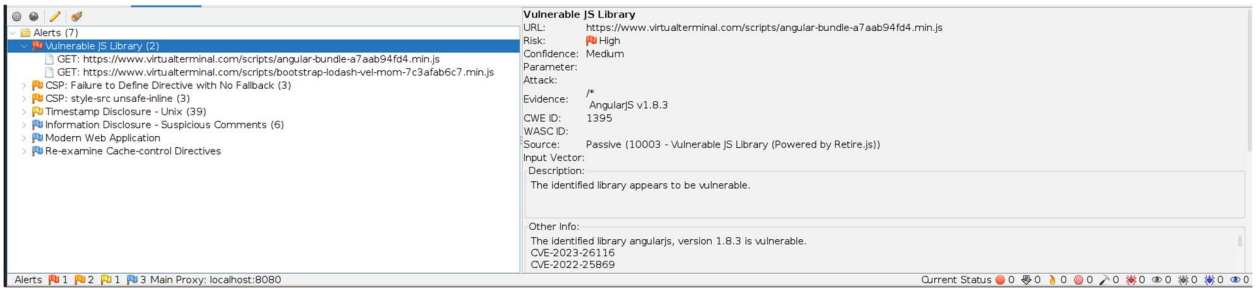
```
Scanning Tool Unavailable. Skipping Test ...

[ Preliminary Scan Phase Completed. ]


[ Report Generation Phase Initiated. ]
        Complete Vulnerability Report for virtualterminal.com named rs.vul.virtualterminal.com.2025-04-27 is available under the same directory RapidScan resides.
        Total Number of Vulnerability Checks       : 80
        Total Number of Vulnerability Checks Skipped: 23
        Total Number of Vulnerabilities Detected   : 11
        Total Time Elapsed for the Scan            : 1h 26m 34s


        For Debugging Purposes, You can view the complete output generated by all the tools named rs.dbg.virtualterminal.com.2025-04-27 under the same directory.
[ Report Generation Phase Completed. ]
```

Active scan result from OWASP ZAP:

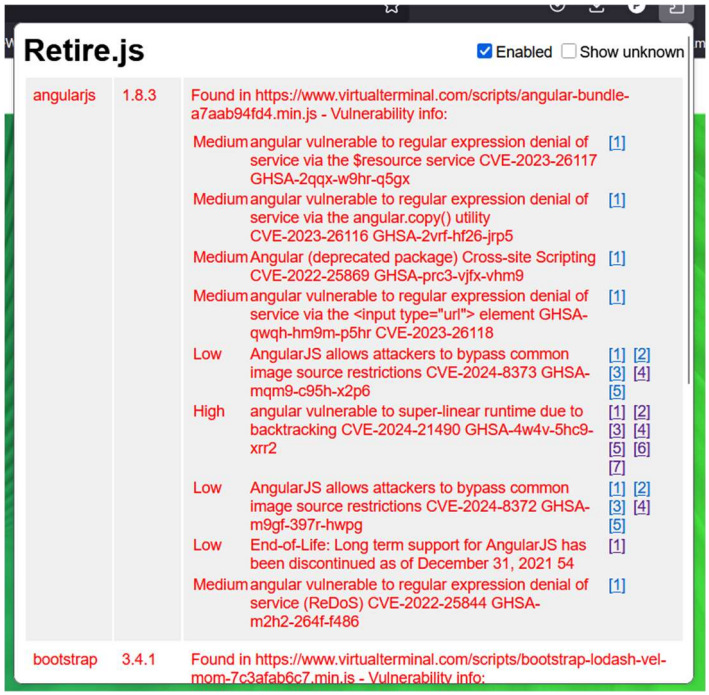
High threat vulnerability found

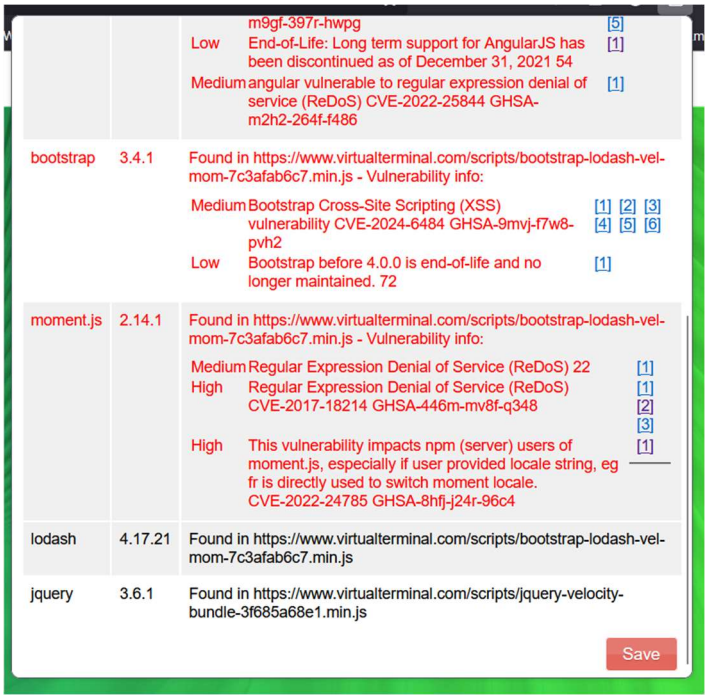


Other vulnerabilities:



Retire.js result:





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 Worldplay VDP Domain, **www.virtualterminal.com** two vulnerable js libraries were found. That contains outdated libraries with ReDos and locale handling vulnerabilities.

1. https://www.virtualterminal.com/scripts/angular-bundle-a7aab94fd4.min.js
2. https://www.virtualterminal.com/scripts/bootstrap-lodash-vel-mom-7c3afab6c7.min.js

The full exploitation was not possible since full testing of the website could not be performed manually as access is restricted to registered users, and I did not have valid login credentials to proceed past the authentication step since the vdp was not provided with sample credentials.

Observation:

The angularjs library found in https://www.virtualterminal.com/scripts/angular-bundle-a7aab94fd4.min.js was an outdated version that contained a high threat level CVE-2024-21490 GHSA-4w4v-5hc9-xrr2 vulnerability that contains a known **ReDos** vulnerability that has super-linear runtime due to backtracking. This means the time it takes to process a certain task grows very quickly with input size and when regex engines use backtracking to try every possible match path if the regex pattern is complex and input is specially crafted, the engine may spend a huge amount of time finding a possible match path resulting in a DOS attack. This attack could lead to:

- Freeze the frontend by triggering expensive regex operations.
- Exploit web applications that rely on Angular's parsing mechanisms.

The moment.js found in https://www.virtualterminal.com/scripts/bootstrap-lodash-vel-mom-7c3afab6c7.min.js contained two high threat level known vulnerabilities CVE-2017-18214 GHSA-446m-mv8f-q348 that contains **ReDos** vulnerability and a **locale handling vulnerability** in Moment.js – CVE-2022-24785 / GHSA-8hfj-j24r-96c4 that affects moment.js that affects if the server-side app uses moment.js and directly yses a user provided locale string to switch the locale like `moment.locale(userInput);`

Then an attacker could input a **malicious or invalid string**, which could lead to:

- Unexpected behavior
- Loading of unintended locale files
- Potential **path traversal or code execution** depending on how locales are loaded

Conclusion/ Inference:

The identified vulnerabilities - Angular super-linear runtime issue (CVE-2024-21490), the Regular Expression Denial of Service in JavaScript regex engines (CVE-2017-18214), and the unsafe locale handling in Moment.js (CVE-2022-24785) highlight critical risks posed by insecure or outdated js libraries and improper input handling.

These vulnerabilities expose DOS, unexpected behavior, improper use of library features.

3. Affected Components:

1. https://www.virtualterminal.com/scripts/angular-bundle-a7aab94fd4.min.js
2. https://www.virtualterminal.com/scripts/bootstrap-lodash-vel-mom-7c3afab6c7.min.js
3. https://www.virtualterminal.com/scripts/bootstrap-lodash-vel-mom-7c3afab6c7.min.js

4. Impact Assessment:

OWASP analysis:

Risk level	High
Confidence	Medium

Other information:

1. The identified library moment.js, version 2.14.1 is vulnerable.

- CVE-2017-18214
- CVE-2022-24785
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-18214
- https://security.snyk.io/vuln/npm:moment:20170905
- https://security.snyk.io/vuln/npm:moment:20161019
- https://github.com/moment/moment/security/advisories/GHSA-8hfj-j24r-96c4
- https://github.com/moment/moment/issues/4163

2. The identified library angularjs, version 1.8.3 is vulnerable.

- CVE-2023-26116
- CVE-2022-25869
- CVE-2022-25844
- CVE-2024-21490
- CVE-2024-8373
- CVE-2024-8372
- CVE-2023-26117
- CVE-2023-26118

- https://github.com/advisories/GHSA-2vrf-hf26-jrp5
- https://github.com/advisories/GHSA-mqm9-c95h-x2p6
- https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-6241746
- https://nvd.nist.gov/vuln/detail/CVE-2024-21490
- https://codepen.io/herodevs/full/bGPQgMp/8da9ce87e99403ee13a295c305ebfa0b
- https://nvd.nist.gov/vuln/detail/CVE-2024-8373
- https://github.com/advisories/GHSA-4w4v-5hc9-xrr2
- https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-6241747
- https://nvd.nist.gov/vuln/detail/CVE-2024-8372
- https://security.snyk.io/vuln/SNYK-JS-ANGULAR-6091113
- https://github.com/angular/angular.js
- https://github.com/advisories/GHSA-qwqh-hm9m-p5hr
- https://github.com/advisories/GHSA-m2h2-264f-f486
- https://github.com/advisories/GHSA-prc3-vjfx-vhm9
- https://github.com/advisories/GHSA-m9gf-397r-hwpg
- https://codepen.io/herodevs/full/xxoQRNL/0072e627abe03e9cda373bc75b4c1017
- https://www.herodevs.com/vulnerability-directory/cve-2024-8373
- https://github.com/advisories/GHSA-2qqx-w9hr-q5gx
- https://docs.angularjs.org/misc/version-support-status
- https://www.herodevs.com/vulnerability-directory/cve-2024-8372
- https://stackblitz.com/edit/angularjs-vulnerability-ng-srcset-redos

Retire.js analysis

1. Found in https://www.virtualterminal.com/scripts/angular-bundle-a7aab94fd4.min.js - Vulnerability info
   Library – angular.js version 1.8.3

Threat level	Description
medium	angular vulnerable to regular expression denial of service via the $resource service CVE-2023-26117 GHSA-2qqx-w9hr-q5gx
medium	angular vulnerable to regular expression denial of service via the angular.copy() utility CVE-2023-26116 GHSA-2vrf-hf26-jrp5
medium	Angular (deprecated package) Cross-site Scripting CVE-2022-25869 GHSA-prc3-vjfx-vhm9
medium	angular vulnerable to regular expression denial of service via the <input type="url"> element GHSA-qwqh-hm9m-p5hr CVE-2023-26118

low	AngularJS allows attackers to bypass common image source restrictions CVE-2024-8373 GHSA-mqm9-c95h-x2p6
high	angular vulnerable to super-linear runtime due to backtracking CVE-2024-21490 GHSA-4w4v-5hc9-xrr2 1234567
low	AngularJS allows attackers to bypass common image source restrictions CVE-2024-8372 GHSA-m9gf-397r-hwpg
low	End-of-Life: Long term support for AngularJS has been discontinued as of December 31, 2021
medium	angular vulnerable to regular expression denial of service (ReDoS) CVE-2022-25844 GHSA-m2h2-264f-f486

2. Found in https://www.virtualterminal.com/scripts/bootstrap-lodash-vel-mom-7c3afab6c7.min.js - Vulnerability info:
   Library – bootstrap version 3.4.1

Threat level	Description
medium	Bootstrap Cross-Site Scripting (XSS) vulnerability CVE-2024-6484 GHSA-9mvj-f7w8-pvh2
low	Bootstrap before 4.0.0 is end-of-life and no longer maintained.

3. Found in https://www.virtualterminal.com/scripts/bootstrap-lodash-vel-mom-7c3afab6c7.min.js - Vulnerability info:
   Library – moment.js 2.14.1

Threat level	Description
medium	Regular Expression Denial of Service (ReDoS)
high	Regular Expression Denial of Service (ReDoS) CVE-2017-18214 GHSA-446m-mv8f-q348
high	This vulnerability impacts npm (server) users of moment.js, especially if user provided locale string, eg fr is directly used to switch moment locale. CVE-2022-24785 GHSA-8hfj-j24r-96c4

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)

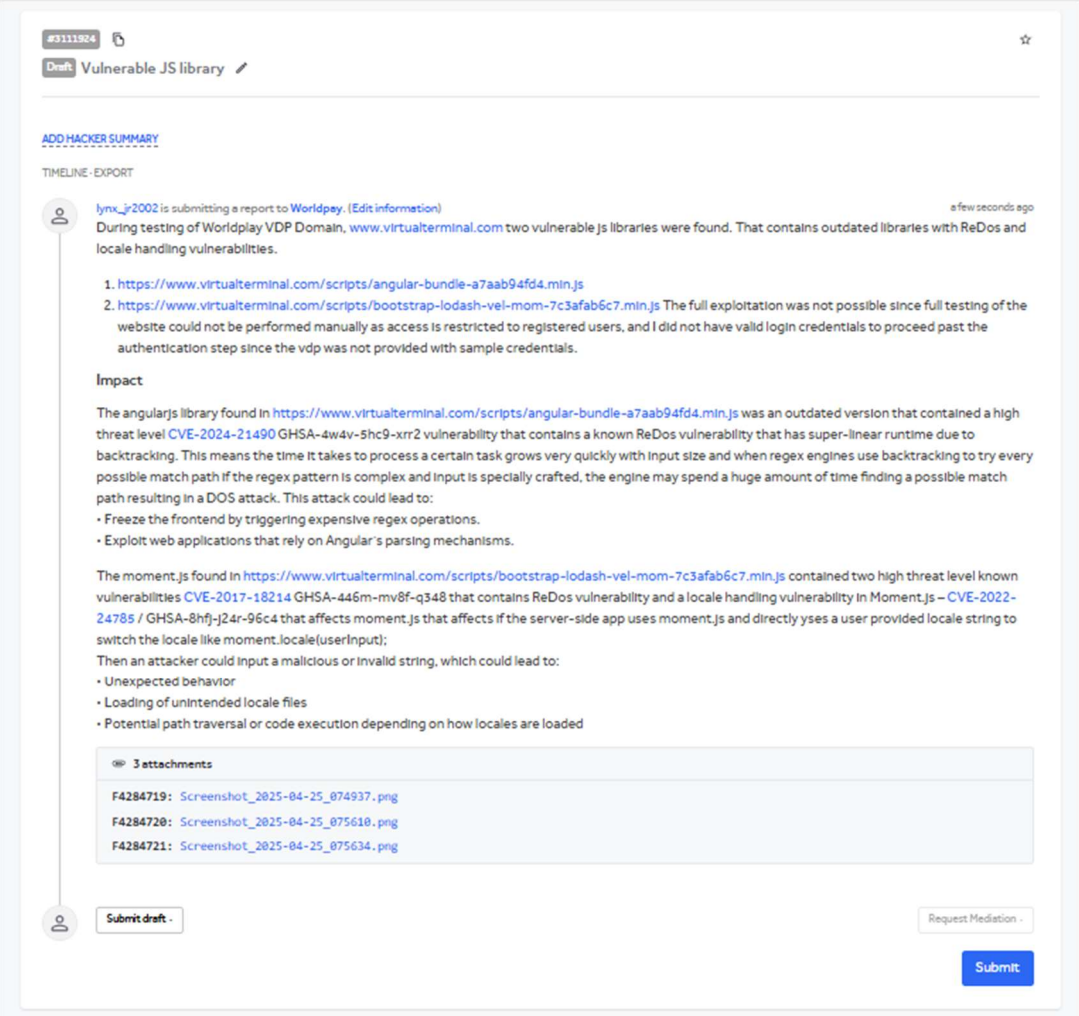
5. Steps to reproduce –

- **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**.

Submission:



#3111924

Draft Vulnerable JS library

ADD HACKER SUMMARY

TIMELINE · EXPORT

lynx_jr2002 is submitting a report to Worldpay. (Edit information) — a few seconds ago

During testing of Worldplay VDP Domain, www.virtualterminal.com two vulnerable js libraries were found. That contains outdated libraries with ReDos and locale handling vulnerabilities.

1. https://www.virtualterminal.com/scripts/angular-bundle-a7aab94fd4.min.js
2. https://www.virtualterminal.com/scripts/bootstrap-lodash-vel-mom-7c3afab6c7.min.js The full exploitation was not possible since full testing of the website could not be performed manually as access is restricted to registered users, and I did not have valid login credentials to proceed past the authentication step since the vdp was not provided with sample credentials.

Impact

The angularjs library found in https://www.virtualterminal.com/scripts/angular-bundle-a7aab94fd4.min.js was an outdated version that contained a high threat level CVE-2024-21490 GHSA-4w4v-5hc9-xrr2 vulnerability that contains a known ReDos vulnerability that has super-linear runtime due to backtracking. This means the time it takes to process a certain task grows very quickly with input size and when regex engines use backtracking to try every possible match path if the regex pattern is complex and input is specially crafted, the engine may spend a huge amount of time finding a possible match path resulting in a DOS attack. This attack could lead to:
- Freeze the frontend by triggering expensive regex operations.
- Exploit web applications that rely on Angular's parsing mechanisms.

The moment.js found in https://www.virtualterminal.com/scripts/bootstrap-lodash-vel-mom-7c3afab6c7.min.js contained two high threat level known vulnerabilities CVE-2017-18214 GHSA-446m-mv8f-q348 that contains ReDos vulnerability and a locale handling vulnerability in Moment.js – CVE-2022-24785 / GHSA-8hfj-j24r-96c4 that affects moment.js that affects if the server-side app uses moment.js and directly yses a user provided locale string to switch the locale like moment.locale(userInput);
Then an attacker could input a malicious or invalid string, which could lead to:
- Unexpected behavior
- Loading of unintended locale files
- Potential path traversal or code execution depending on how locales are loaded

3 attachments

F4284719: Screenshot_2025-04-25_074937.png
F4284720: Screenshot_2025-04-25_075610.png
F4284721: Screenshot_2025-04-25_075634.png

Submit draft · Request Mediation · Submit

Reply:

h1_analyst_akshat closed your report #3111924 Vulnerable JS library as Informative.

Hi @lynx_jr2002,

Thank you for your report!

While using an outdated software version may present potential security risks, it is important to have a working proof of concept (POC) to demonstrate the actual impact. Without a POC, it is difficult to assess whether the outdated version is exploitable and if it poses a real threat to the application.

If you can provide more details or a POC that shows how the outdated software version can be exploited to compromise the system, we'd be happy to further investigate.

As a result, we will be closing this report as informational. This closure does not impact your Signal or Reputation score. We appreciate your contributions and encourage you to continue reporting any future findings.

Kind regards,
@h1_analyst_akshat

View details on HackerOne.