**Sri Lanka Institute of Information Technology**

**IE2062 - Web Security**

**Final Assignment**

**Bug Bounty Report 01**

**Name:** Peiris W.S.S.N

**Registration Number:** IT23227286

Contents

[1. Introduction 3](#_Toc196580830)

[2. Reconnaissance 4](#_Toc196580831)

[3. Vulnerability 6](#_Toc196580832)

[4. Vulnerability description 6](#_Toc196580833)

[5. Affected Components 7](#_Toc196580834)

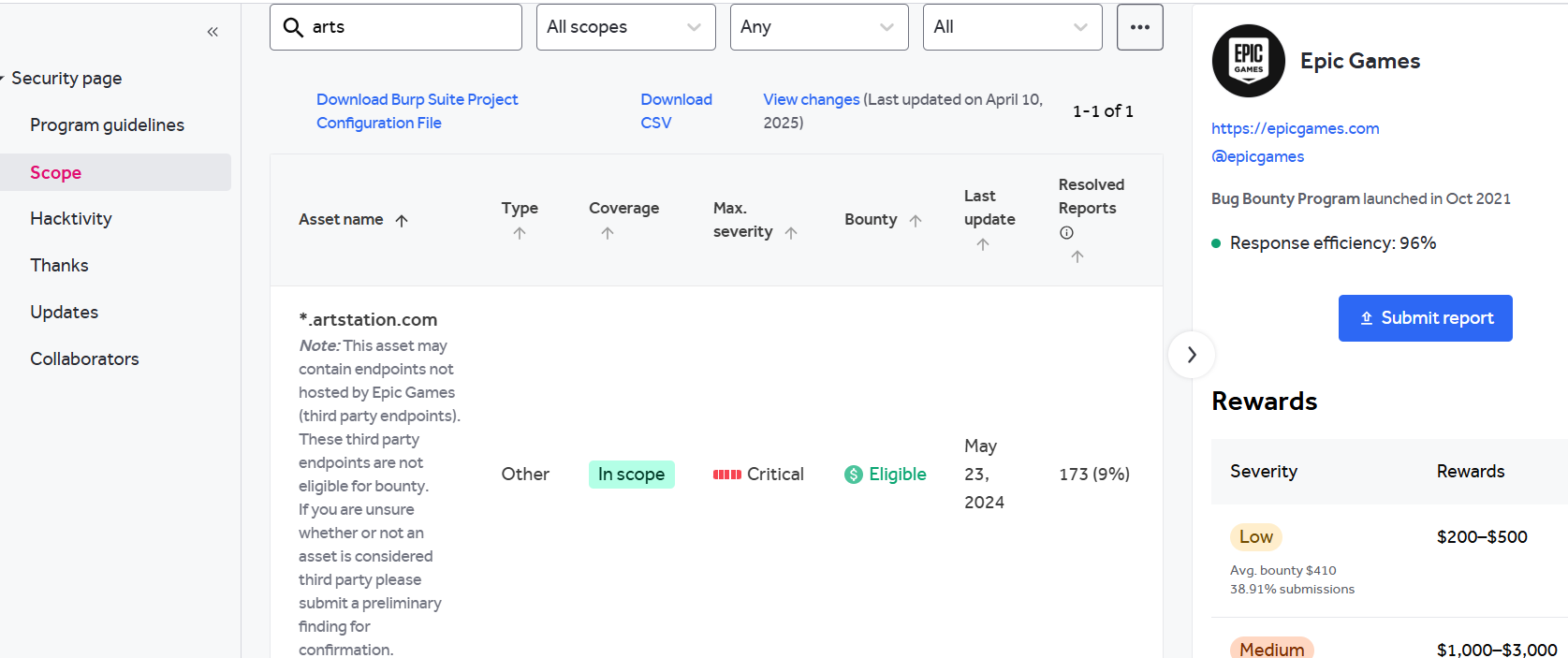
[6. Impact Assessment 7](#_Toc196580835)

[7. Steps to reproduce 8](#_Toc196580836)

[8. Proof of concept 8](#_Toc196580837)

[9. Proposed mitigation or fix 9](#_Toc196580838)

# Introduction



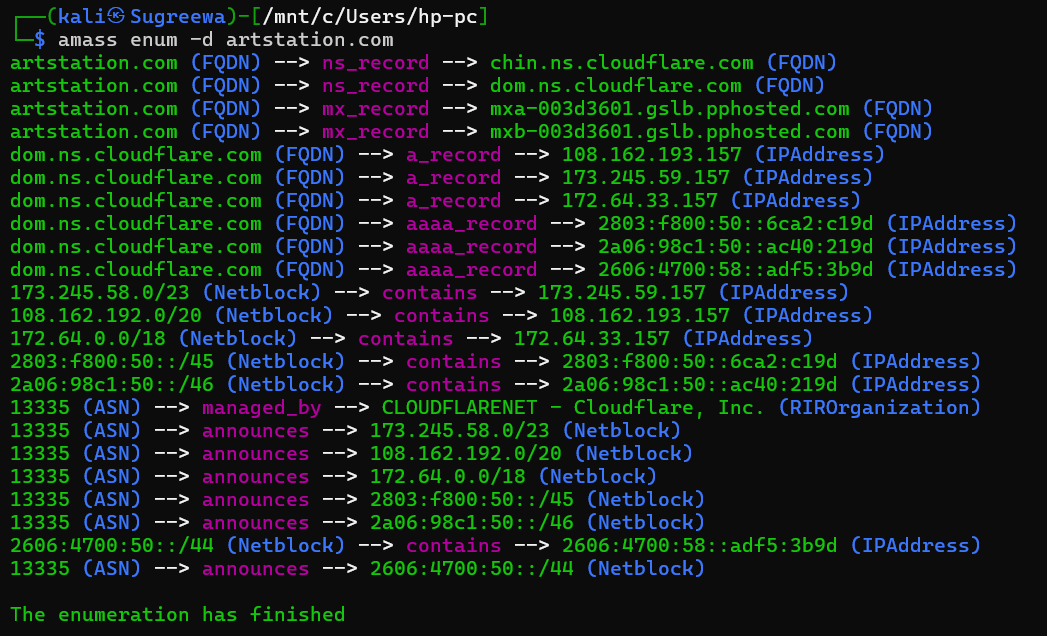
**Website:** <https://artstation.com>

**Subdomain:** <https://help.artstation.com>

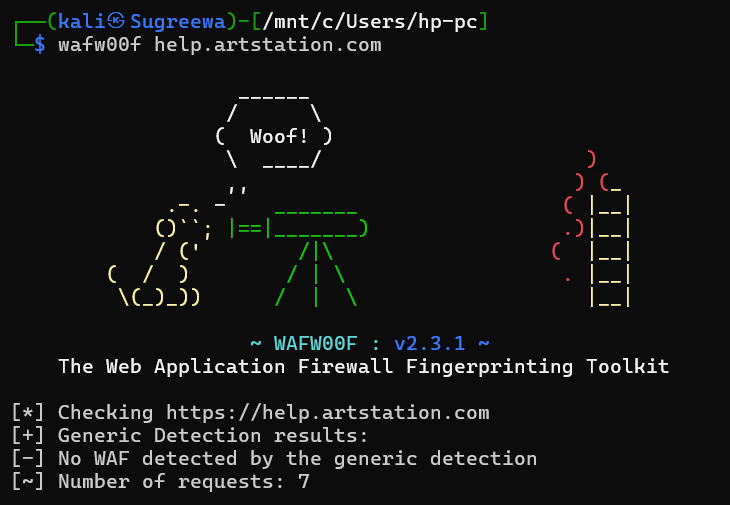
**Listed by:** Epic Games

# Reconnaissance

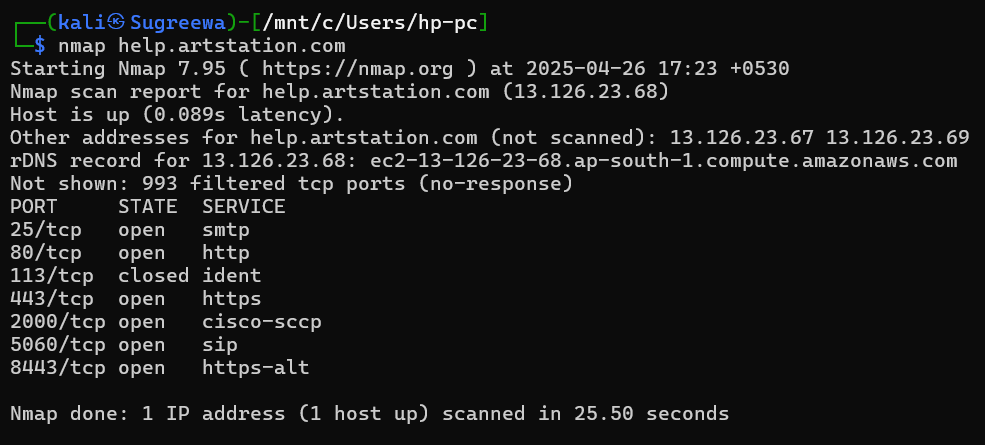
* **Subdomain enumeration using Amass**

****

* **Firewall Detection**

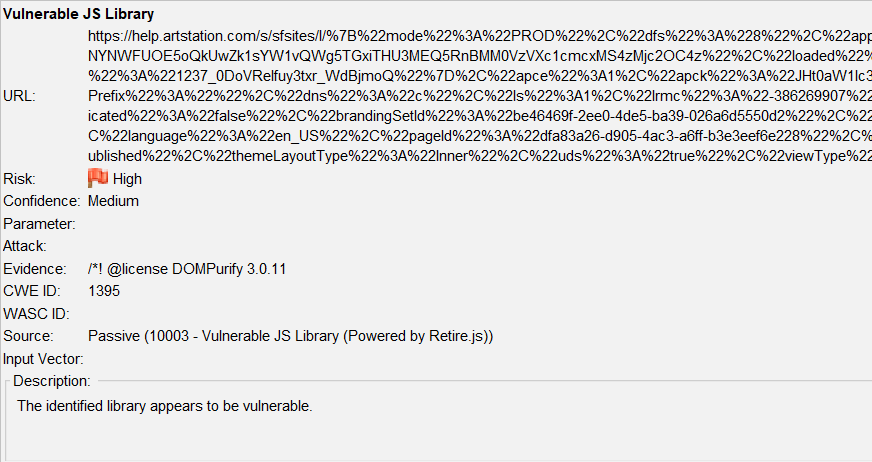
****

* **Nmap Scan**

****

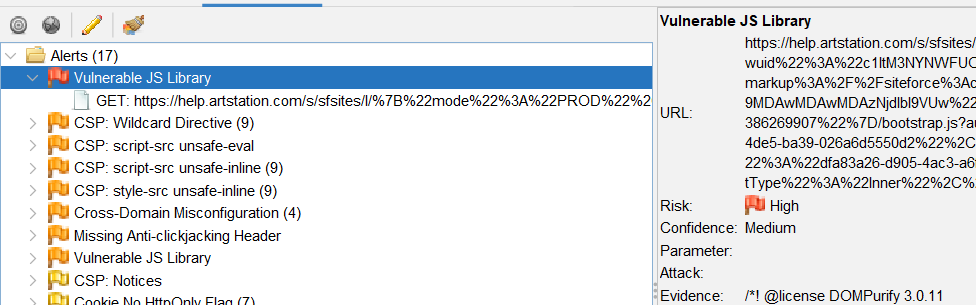
# Vulnerability

* **Vulnerable JS Library**

****

# Vulnerability description

The identified JavaScript library appears to be vulnerable. Based on the version detected (DOMPurify 3.0.11), there are known security issues which may expose the application to risks such as insufficient sanitization, potentially leading to Cross-Site Scripting (XSS) vulnerabilities.



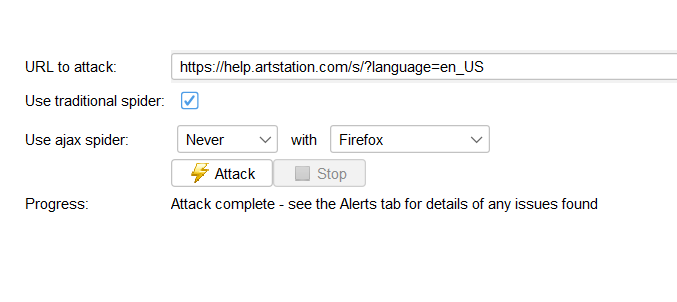
1. Affected Components

* **Library Name:** DOMPurify
* **Version:** 3.0.11
* **File Location:** [url](https://help.artstation.com/s/sfsites/l/%7B%22mode%22%3A%22PROD%22%2C%22dfs%22%3A%228%22%2C%22app%22%3A%22siteforce%3AcommunityApp%22%2C%22fwuid%22%3A%22c1ItM3NYNWFUOE5oQkUwZk1sYW1vQWg5TGxiTHU3MEQ5RnBMM0VzVXc1cmcxMS4zMjc2OC4z%22%2C%22loaded%22%3A%7B%22APPLICATION%40markup%3A%2F%2Fsiteforce%3AcommunityApp%22%3A%221237_0DoVReIfuy3txr_WdBjmoQ%22%7D%2C%22apce%22%3A1%2C%22apck%22%3A%22JHt0aW1lc3RhbXB9MDAwMDAwMDAzNjdlbl9VUw%22%2C%22mlr%22%3A1%2C%22pathPrefix%22%3A%22%22%2C%22dns%22%3A%22c%22%2C%22ls%22%3A1%2C%22lrmc%22%3A%22-386269907%22%7D/bootstrap.js?aura.attributes=%7B%22ac%22%3A%22%22%2C%22authenticated%22%3A%22false%22%2C%22brandingSetId%22%3A%22be46469f-2ee0-4de5-ba39-026a6d5550d2%22%2C%22formFactor%22%3A%22LARGE%22%2C%22isHybrid%22%3A%22false%22%2C%22language%22%3A%22en_US%22%2C%22pageId%22%3A%22dfa83a26-d905-4ac3-a6ff-b3e3eef6e228%22%2C%22publishedChangelistNum%22%3A%2268%22%2C%22schema%22%3A%22Published%22%2C%22themeLayoutType%22%3A%22Inner%22%2C%22uds%22%3A%22true%22%2C%22viewType%22%3A%22Published%22%7D)
* **Usage Context:** Likely used to sanitize HTML content from user input

# Impact Assessment

* **Prototype Pollution (CVE-2024-48910):** Attackers can manipulate the prototype chain, potentially leading to unauthorized access or modification of application behavior.
* **Mutation XSS (CVE-2024-47875):** Specially crafted input can bypass sanitization, leading to execution of malicious scripts in the user's browser.
* **Depth Check Bypass (CVE-2024-45801):** Attackers can exploit the sanitizer's depth check mechanism, leading to XSS vulnerabilities.

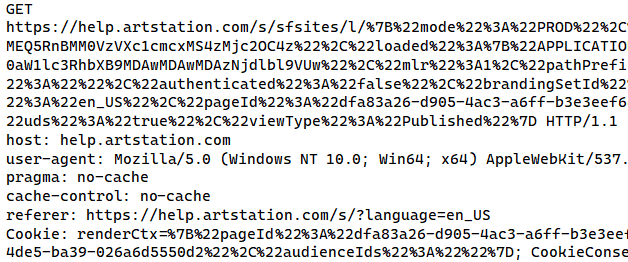
# Steps to reproduce

****

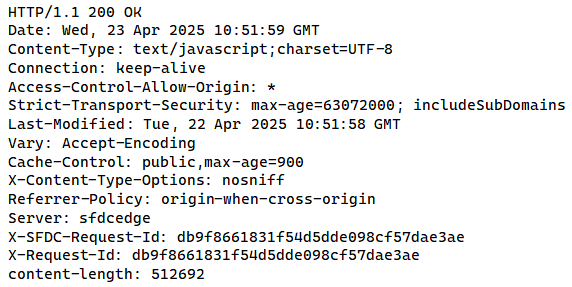
Enter the above link inside the url bar and proceed the attack. Vulnerable JS library will be shown as an high risk vulnerability.

# Proof of concept

Below is the request that made by Zap.



Below is the response made by the library



# Proposed mitigation or fix

* **Immediate Action:** Upgrade to DOMPurify version 3.1.3 or higher to mitigate these vulnerabilities.
* **Verification:** After upgrading, verify that all user inputs are properly sanitized and that no malicious scripts can be executed.
* **Monitoring:** Regularly monitor for new vulnerabilities and apply patches promptly.