Sri Lanka Institute of Information Technology

IE2062 - Web Security

Final Assignment

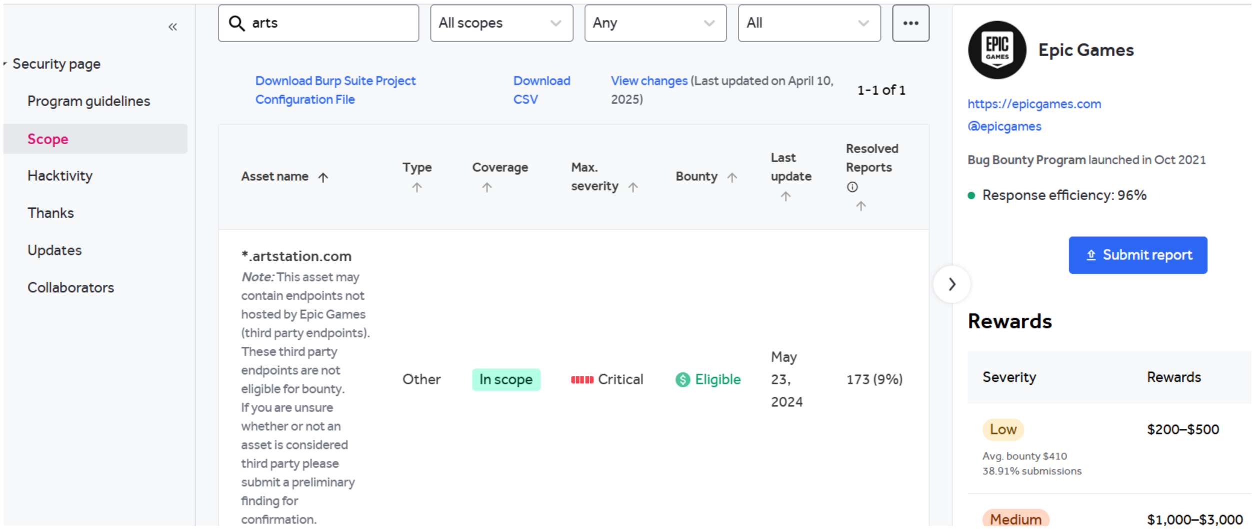
Bug Bounty Report 01

Name: Peiris W.S.S.N

Registration Number: IT23227286

Contents

1. Introduction



Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports ⓘ
*.artstation.com *Note:* This asset may contain endpoints not hosted by Epic Games (third party endpoints). These third party endpoints are not eligible for bounty. If you are unsure whether or not an asset is considered third party please submit a preliminary finding for confirmation.	Other	In scope	Critical	Eligible	May 23, 2024	173 (9%)

Epic Games

https://epicgames.com
@epicgames

Bug Bounty Program launched in Oct 2021

● Response efficiency: 96%

Rewards

Severity	Rewards
Low Avg. bounty $410 38.91% submissions	$200–$500
Medium	$1,000–$3,000

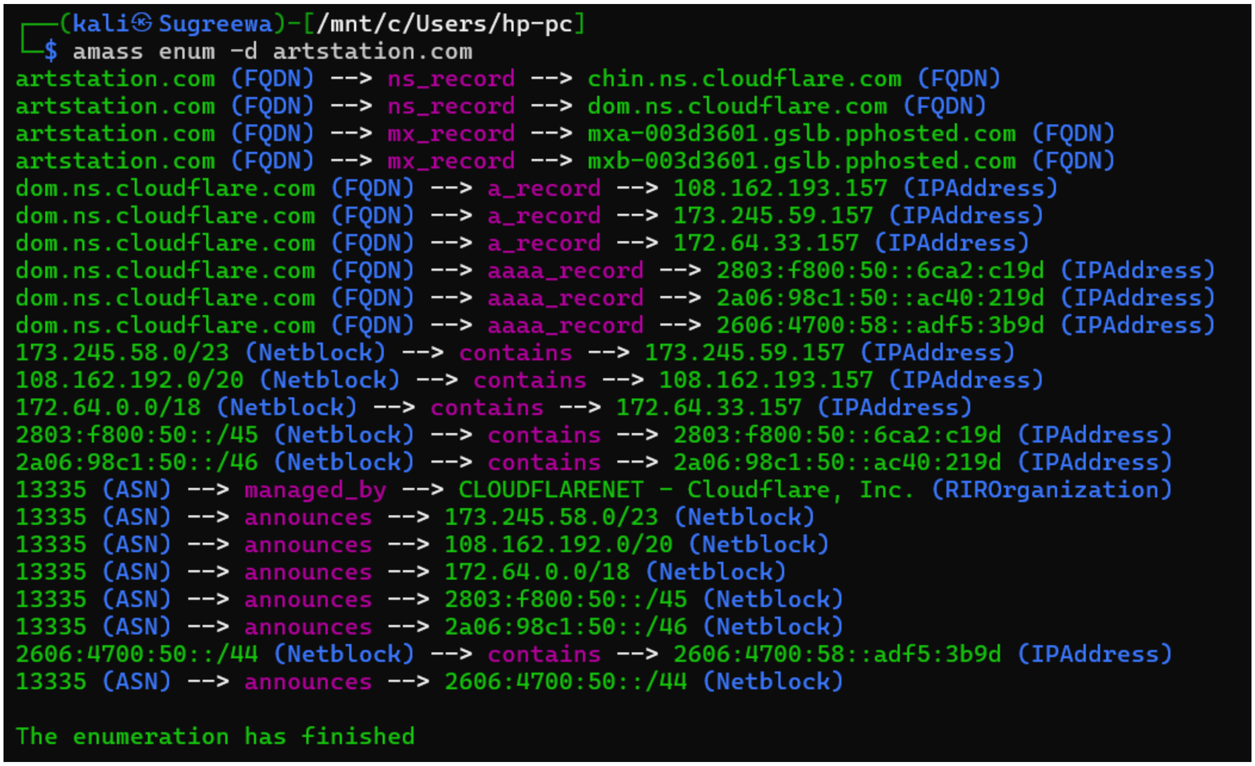
Website: https://artstation.com

Subdomain: https://help.artstation.com

Listed by: Epic Games

2. Reconnaissance

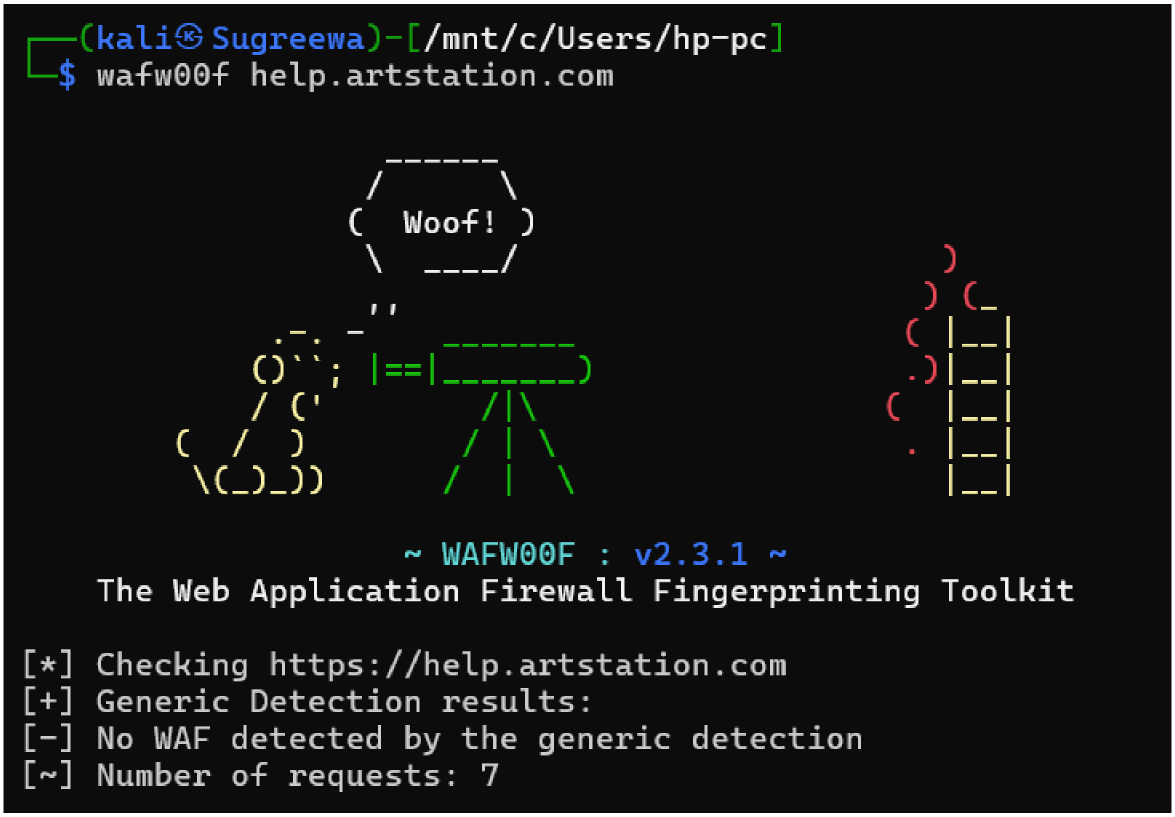
- **Subdomain enumeration using Amass**



```
┌──(kali㉿Sugreewa)-[/mnt/c/Users/hp-pc]
└─$ amass enum -d artstation.com
artstation.com (FQDN) --> ns_record --> chin.ns.cloudflare.com (FQDN)
artstation.com (FQDN) --> ns_record --> dom.ns.cloudflare.com (FQDN)
artstation.com (FQDN) --> mx_record --> mxa-003d3601.gslb.pphosted.com (FQDN)
artstation.com (FQDN) --> mx_record --> mxb-003d3601.gslb.pphosted.com (FQDN)
dom.ns.cloudflare.com (FQDN) --> a_record --> 108.162.193.157 (IPAddress)
dom.ns.cloudflare.com (FQDN) --> a_record --> 173.245.59.157 (IPAddress)
dom.ns.cloudflare.com (FQDN) --> a_record --> 172.64.33.157 (IPAddress)
dom.ns.cloudflare.com (FQDN) --> aaaa_record --> 2803:f800:50::6ca2:c19d (IPAddress)
dom.ns.cloudflare.com (FQDN) --> aaaa_record --> 2a06:98c1:50::ac40:219d (IPAddress)
dom.ns.cloudflare.com (FQDN) --> aaaa_record --> 2606:4700:58::adf5:3b9d (IPAddress)
173.245.58.0/23 (Netblock) --> contains --> 173.245.59.157 (IPAddress)
108.162.192.0/20 (Netblock) --> contains --> 108.162.193.157 (IPAddress)
172.64.0.0/18 (Netblock) --> contains --> 172.64.33.157 (IPAddress)
2803:f800:50::/45 (Netblock) --> contains --> 2803:f800:50::6ca2:c19d (IPAddress)
2a06:98c1:50::/46 (Netblock) --> contains --> 2a06:98c1:50::ac40:219d (IPAddress)
13335 (ASN) --> managed_by --> CLOUDFLARENET - Cloudflare, Inc. (RIROrganization)
13335 (ASN) --> announces --> 173.245.58.0/23 (Netblock)
13335 (ASN) --> announces --> 108.162.192.0/20 (Netblock)
13335 (ASN) --> announces --> 172.64.0.0/18 (Netblock)
13335 (ASN) --> announces --> 2803:f800:50::/45 (Netblock)
13335 (ASN) --> announces --> 2a06:98c1:50::/46 (Netblock)
2606:4700:50::/44 (Netblock) --> contains --> 2606:4700:58::adf5:3b9d (IPAddress)
13335 (ASN) --> announces --> 2606:4700:50::/44 (Netblock)

The enumeration has finished
```

- **Firewall Detection**



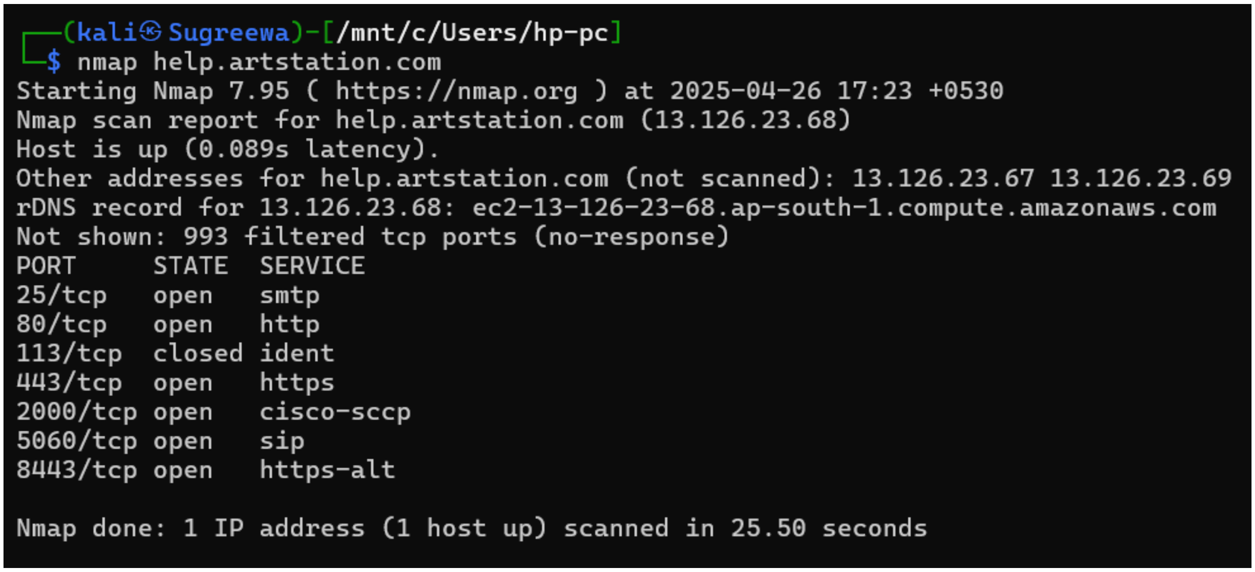
```
┌──(kali㉿Sugreewa)-[/mnt/c/Users/hp-pc]
└─$ wafw00f help.artstation.com

                   ______
                  /      \
                 (  Woof! )
                  \  ____/                      )
                   ''                         ) (_
              .-. _    ______                ( |__|
             ()``; |==|______)               .)|__|
             / ('       /|\                 (  |__|
          ( /  )       / | \                 . |__|
          \(_)_))     /  |  \                  |__|

                    ~ WAFW00F : v2.3.1 ~
    The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://help.artstation.com
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7
```

- **Nmap Scan**

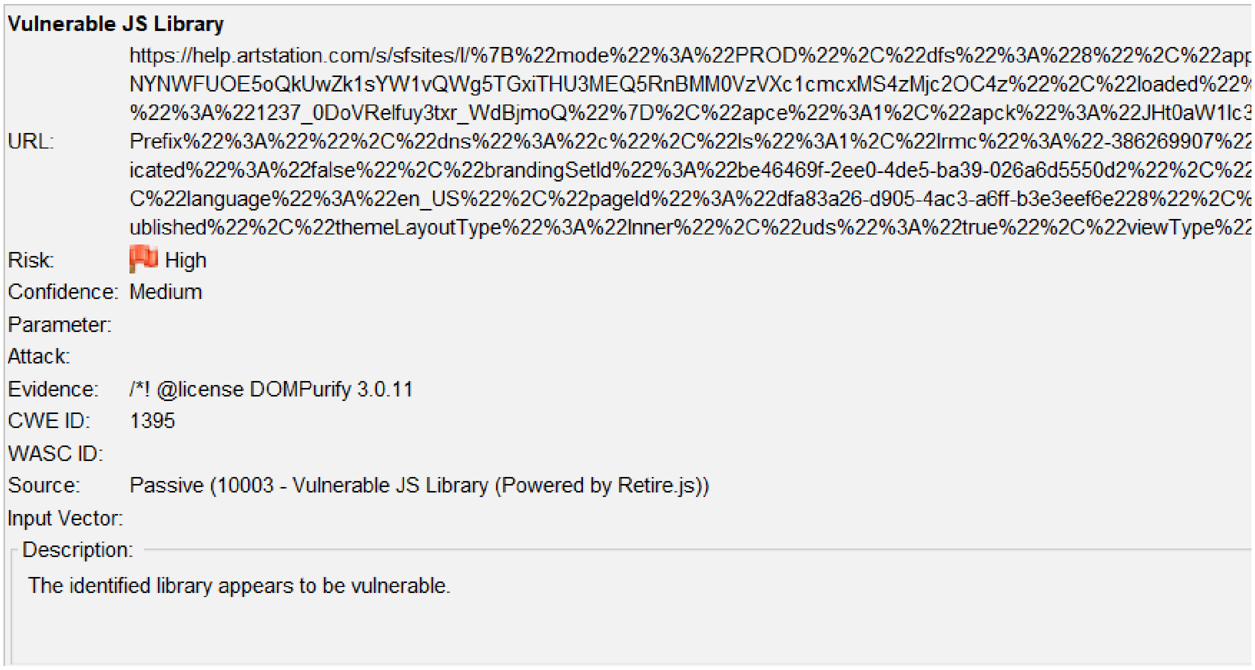


```
┌──(kali㉿Sugreewa)-[/mnt/c/Users/hp-pc]
└─$ nmap help.artstation.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-26 17:23 +0530
Nmap scan report for help.artstation.com (13.126.23.68)
Host is up (0.089s latency).
Other addresses for help.artstation.com (not scanned): 13.126.23.67 13.126.23.69
rDNS record for 13.126.23.68: ec2-13-126-23-68.ap-south-1.compute.amazonaws.com
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE  SERVICE
25/tcp   open   smtp
80/tcp   open   http
113/tcp  closed ident
443/tcp  open   https
2000/tcp open   cisco-sccp
5060/tcp open   sip
8443/tcp open   https-alt

Nmap done: 1 IP address (1 host up) scanned in 25.50 seconds
```

3. Vulnerability

- **Vulnerable JS Library**

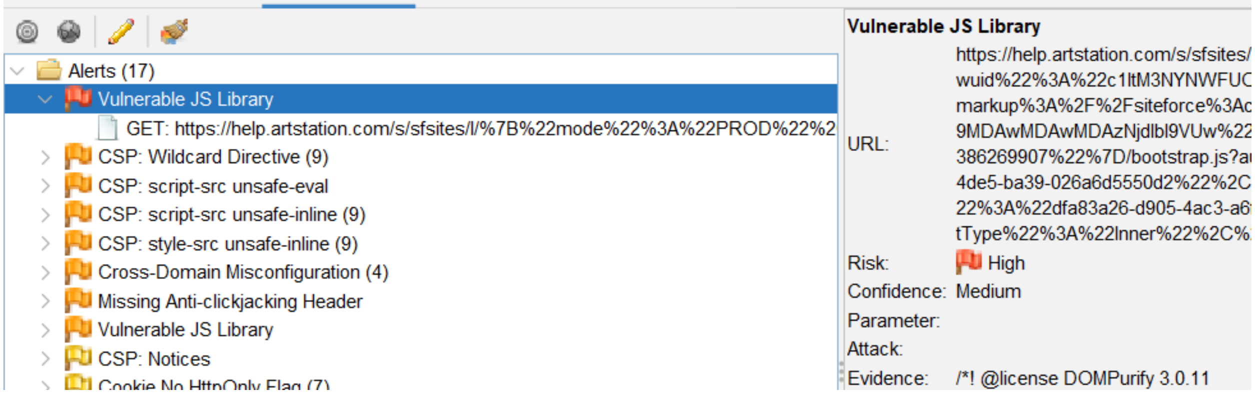


Vulnerable JS Library

```
URL:          https://help.artstation.com/s/sfsites/l/%7B%22mode%22%3A%22PROD%22%2C%22dfs%22%3A%228%22%2C%22app
              NYNWFUOE5oQkUwZk1sYW1vQWg5TGxiTHU3MEQ5RnBMM0VzVXc1cmcxMS4zMjc2OC4z%22%2C%22loaded%22
              %22%3A%221237_0DoVRelfuy3txr_WdBjmoQ%22%7D%2C%22apce%22%3A1%2C%22apck%22%3A%22JHt0aW1lc
              Prefix%22%3A%22%22%2C%22dns%22%3A%22c%22%2C%22ls%22%3A1%2C%22lrmc%22%3A%22-386269907%22
              icated%22%3A%22false%22%2C%22brandingSetId%22%3A%22be46469f-2ee0-4de5-ba39-026a6d5550d2%22%2C%22
              C%22language%22%3A%22en_US%22%2C%22pageId%22%3A%22dfa83a26-d905-4ac3-a6ff-b3e3eef6e228%22%2C%
              ublished%22%2C%22themeLayoutType%22%3A%22Inner%22%2C%22uds%22%3A%22true%22%2C%22viewType%22
Risk:         High
Confidence:   Medium
Parameter:
Attack:
Evidence:     /*! @license DOMPurify 3.0.11
CWE ID:       1395
WASC ID:
Source:       Passive (10003 - Vulnerable JS Library (Powered by Retire.js))
Input Vector:
Description:
  The identified library appears to be vulnerable.
```

4. 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.



```
Alerts (17)
  Vulnerable JS Library
    GET: https://help.artstation.com/s/sfsites/l/%7B%22mode%22%3A%22PROD%22%2
  CSP: Wildcard Directive (9)
  CSP: script-src unsafe-eval
  CSP: script-src unsafe-inline (9)
  CSP: style-src unsafe-inline (9)
  Cross-Domain Misconfiguration (4)
  Missing Anti-clickjacking Header
  Vulnerable JS Library
  CSP: Notices
  Cookie No HttpOnly Flag (7)
```

Vulnerable JS Library

```
URL:          https://help.artstation.com/s/sfsites/
              wuid%22%3A%22c1ltM3NYNWFUC
              markup%3A%2F%2Fsiteforce%3Ac
              9MDAwMDAwMDAzNjdlbl9VUw%22
              386269907%22%7D/bootstrap.js?a
              4de5-ba39-026a6d5550d2%22%2C
              22%3A%22dfa83a26-d905-4ac3-a6
              tType%22%3A%22Inner%22%2C%
Risk:         High
Confidence:   Medium
Parameter:
Attack:
Evidence:     /*! @license DOMPurify 3.0.11
```

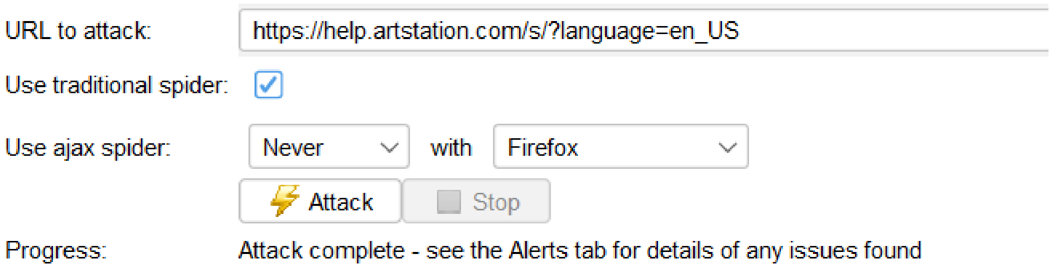
5. Affected Components

- **Library Name:** DOMPurify
- **Version:** 3.0.11
- **File Location:** url
- **Usage Context:** Likely used to sanitize HTML content from user input

6. 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.

7. Steps to reproduce



URL to attack: https://help.artstation.com/s/?language=en_US

Use traditional spider: ☑

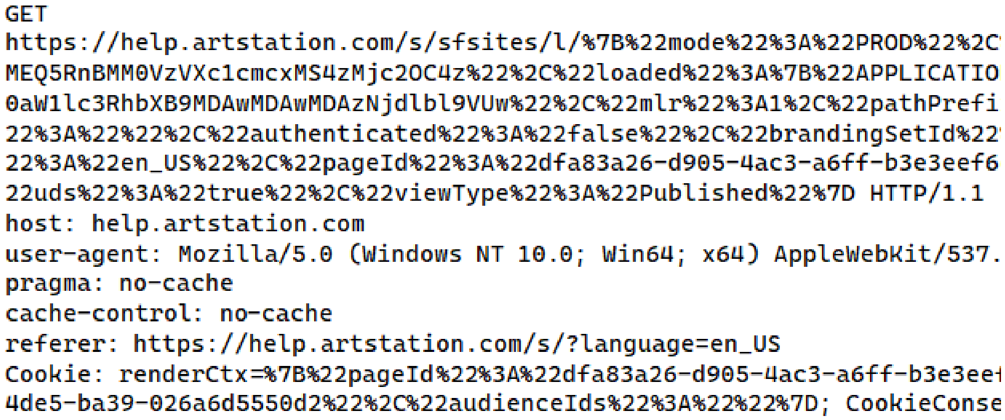
Use ajax spider: Never with Firefox

Progress: Attack complete - see the Alerts tab for details of any issues found

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

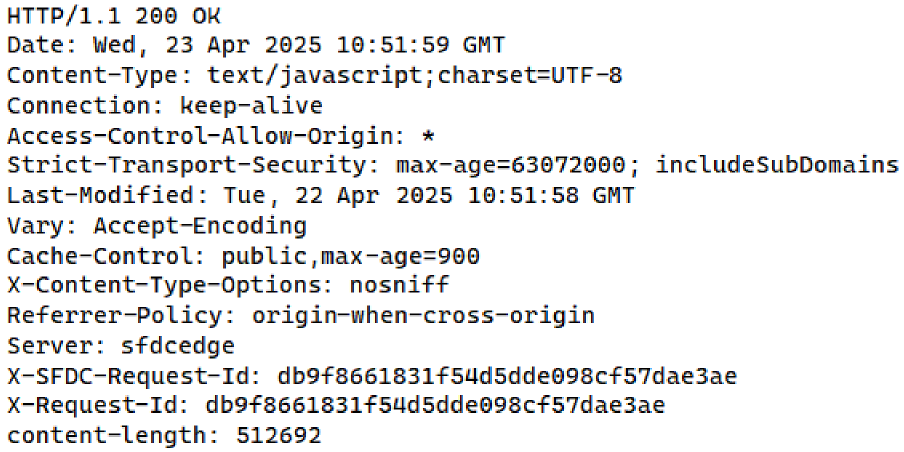
8. Proof of concept

Below is the request that made by Zap.



```
GET
https://help.artstation.com/s/sfsites/l/%7B%22mode%22%3A%22PROD%22%2C
MEQ5RnBMM0VzVXc1cmcxMS4zMjc2OC4z%22%2C%22loaded%22%3A%7B%22APPLICATIO
0aW1lc3RhbXB9MDAwMDAwMDAzNjdlbl9VUw%22%2C%22mlr%22%3A1%2C%22pathPrefi
22%3A%22%22%2C%22authenticated%22%3A%22false%22%2C%22brandingSetId%22
22%3A%22en_US%22%2C%22pageId%22%3A%22dfa83a26-d905-4ac3-a6ff-b3e3eef6
22uds%22%3A%22true%22%2C%22viewType%22%3A%22Published%22%7D HTTP/1.1
host: help.artstation.com
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.
pragma: no-cache
cache-control: no-cache
referer: https://help.artstation.com/s/?language=en_US
Cookie: renderCtx=%7B%22pageId%22%3A%22dfa83a26-d905-4ac3-a6ff-b3e3ee
4de5-ba39-026a6d5550d2%22%2C%22audienceIds%22%3A%22%22%7D; CookieConse
```

Below is the response made by the library



```
HTTP/1.1 200 OK
Date: Wed, 23 Apr 2025 10:51:59 GMT
Content-Type: text/javascript;charset=UTF-8
Connection: keep-alive
Access-Control-Allow-Origin: *
Strict-Transport-Security: max-age=63072000; includeSubDomains
Last-Modified: Tue, 22 Apr 2025 10:51:58 GMT
Vary: Accept-Encoding
Cache-Control: public,max-age=900
X-Content-Type-Options: nosniff
Referrer-Policy: origin-when-cross-origin
Server: sfdcedge
X-SFDC-Request-Id: db9f8661831f54d5dde098cf57dae3ae
X-Request-Id: db9f8661831f54d5dde098cf57dae3ae
content-length: 512692
```

9. 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.