Sri Lanka Institute of Information Technology

Web Security – IE2062

Topic: Bug Bounty Report 7

Y2S2.WE.CS

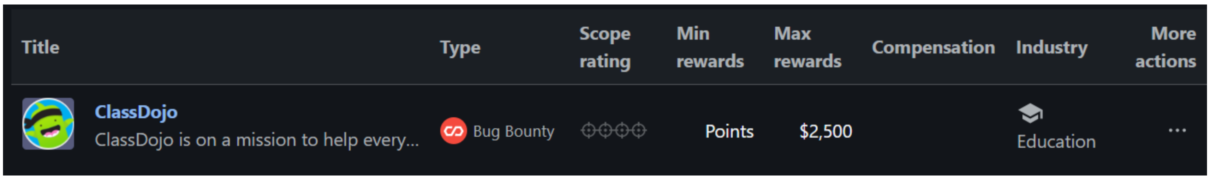
Name: S.D.W.Gunaratne

(IT23241978)

Table of Content

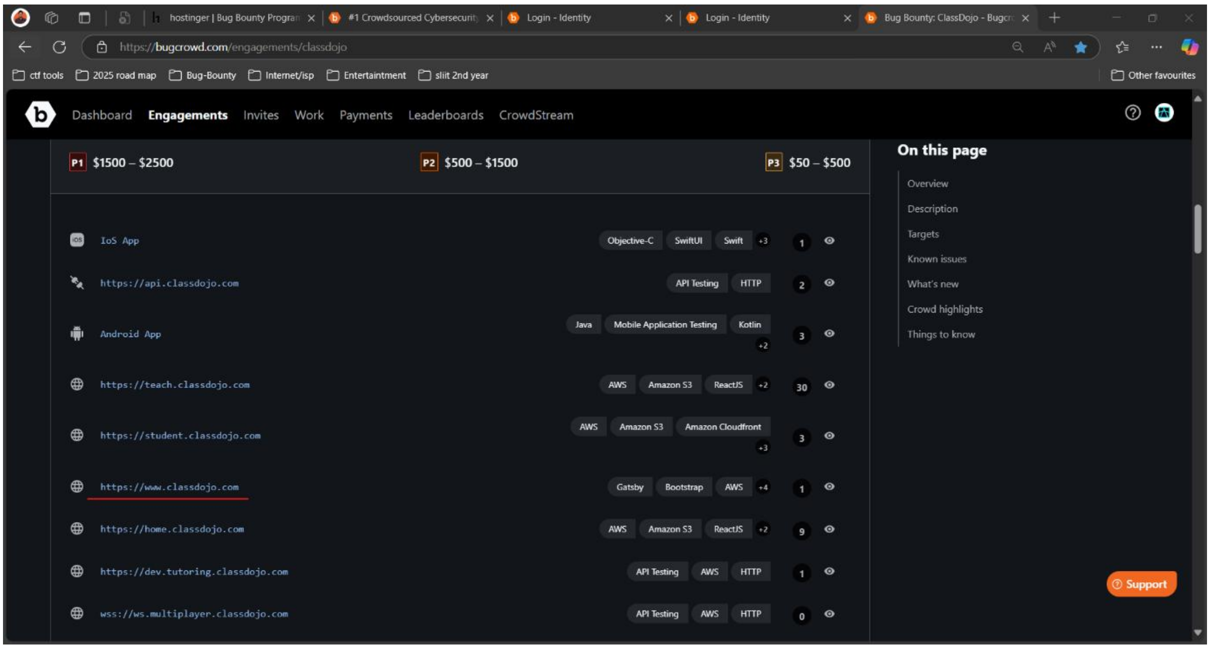
How I started?

1. Once I search from Bug crowd, I saw the classdojo bug bounty program.



Title	Type	Scope rating	Min rewards	Max rewards	Compensation	Industry	More actions
ClassDojo ClassDojo is on a mission to help every...	Bug Bounty		Points	$2,500		Education	⋯

2. Then, I discovered full main domain allowed for scope, so that I choose https://www.classdojo.com .



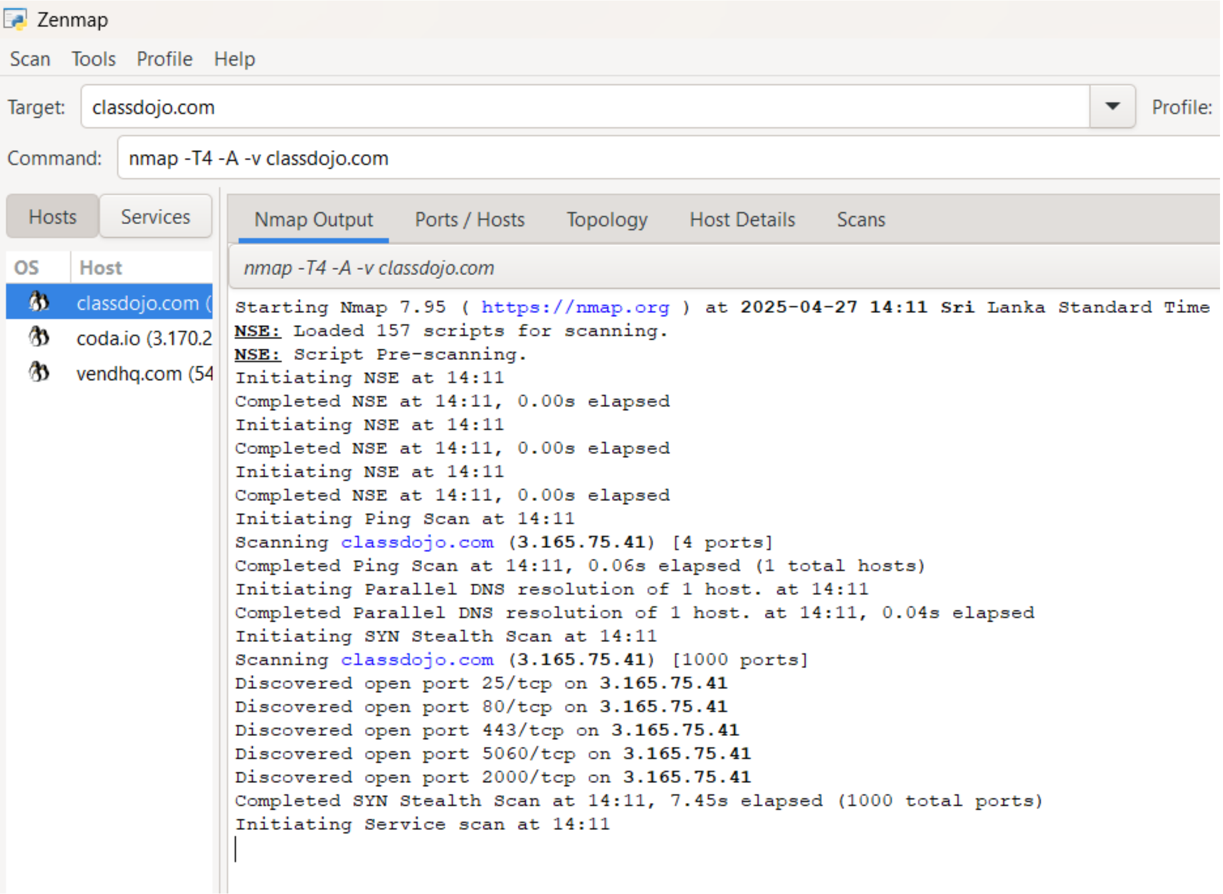
https://bugcrowd.com/engagements/classdojo

P1 $1500 – $2500 P2 $500 – $1500 P3 $50 – $500

IoS App	Objective-C, SwiftUI, Swift, +3	1	
https://api.classdojo.com	API Testing, HTTP	2	
Android App	Java, Mobile Application Testing, Kotlin, +2	3	
https://teach.classdojo.com	AWS, Amazon S3, ReactJS, +2	30	
https://student.classdojo.com	AWS, Amazon S3, Amazon Cloudfront, +3	3	
https://www.classdojo.com	Gatsby, Bootstrap, AWS, +4	1	
https://home.classdojo.com	AWS, Amazon S3, ReactJS, +2	9	
https://dev.tutoring.classdojo.com	API Testing, AWS, HTTP	1	
wss://ws.multiplayer.classdojo.com	API Testing, AWS, HTTP	0	

3. I use several methods/tools to do penetration testing.

4. First, I used Nmap. It helps me to find what are the open ports, Identify the web technologies such as webservers.



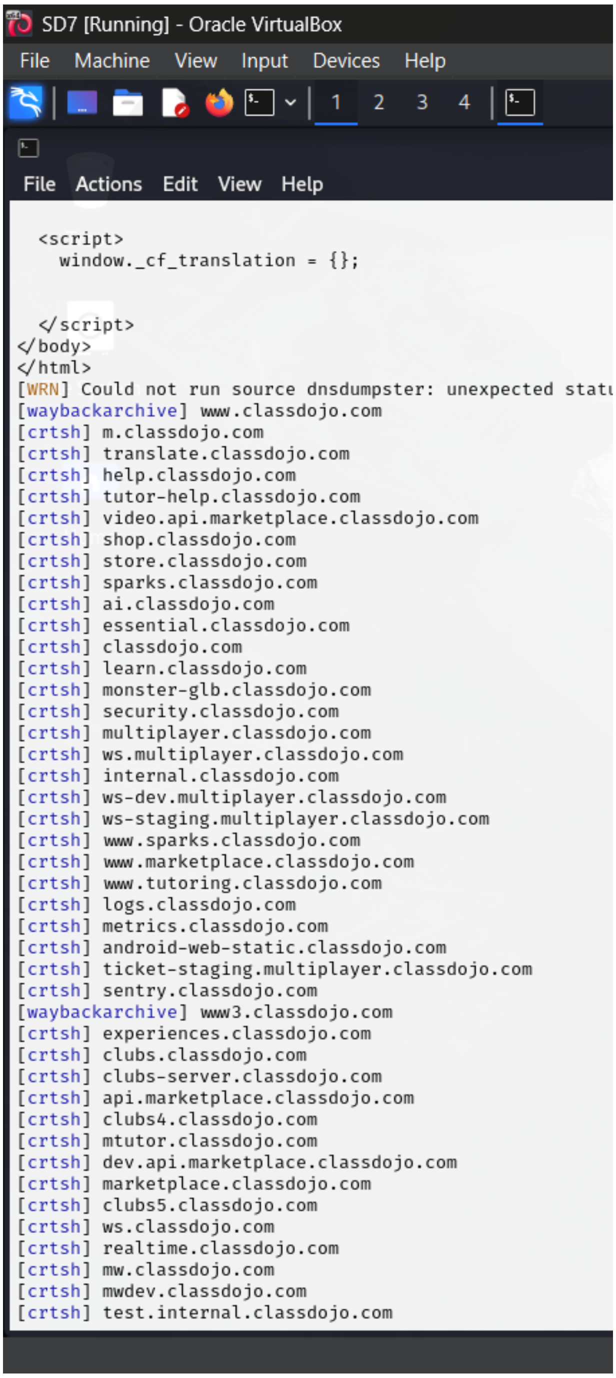
Target: classdojo.com

Command: nmap -T4 -A -v classdojo.com

nmap -T4 -A -v classdojo.com

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-27 14:11 Sri Lanka Standard Time
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:11
Completed NSE at 14:11, 0.00s elapsed
Initiating NSE at 14:11
Completed NSE at 14:11, 0.00s elapsed
Initiating NSE at 14:11
Completed NSE at 14:11, 0.00s elapsed
Initiating Ping Scan at 14:11
Scanning classdojo.com (3.165.75.41) [4 ports]
Completed Ping Scan at 14:11, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:11
Completed Parallel DNS resolution of 1 host. at 14:11, 0.04s elapsed
Initiating SYN Stealth Scan at 14:11
Scanning classdojo.com (3.165.75.41) [1000 ports]
Discovered open port 25/tcp on 3.165.75.41
Discovered open port 80/tcp on 3.165.75.41
Discovered open port 443/tcp on 3.165.75.41
Discovered open port 5060/tcp on 3.165.75.41
Discovered open port 2000/tcp on 3.165.75.41
Completed SYN Stealth Scan at 14:11, 7.45s elapsed (1000 total ports)
Initiating Service scan at 14:11
```

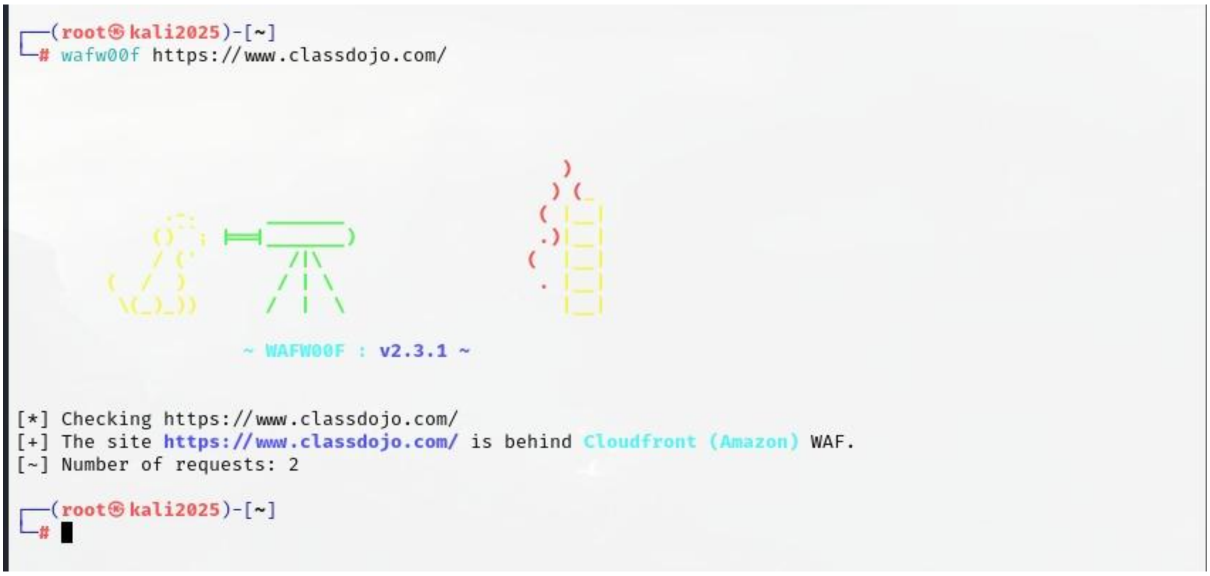
5. Secondly, I used Subfider tool to find hidden or forgotten web asserts. Because hidden web assert can have poor security, unpatched vulnerabilities.


SD7 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
File Actions Edit View Help

```
  <script>
    window._cf_translation = {};


  </script>
</body>
</html>
[WRN] Could not run source dnsdumpster: unexpected statu
[waybackarchive] www.classdojo.com
[crtsh] m.classdojo.com
[crtsh] translate.classdojo.com
[crtsh] help.classdojo.com
[crtsh] tutor-help.classdojo.com
[crtsh] video.api.marketplace.classdojo.com
[crtsh] shop.classdojo.com
[crtsh] store.classdojo.com
[crtsh] sparks.classdojo.com
[crtsh] ai.classdojo.com
[crtsh] essential.classdojo.com
[crtsh] classdojo.com
[crtsh] learn.classdojo.com
[crtsh] monster-glb.classdojo.com
[crtsh] security.classdojo.com
[crtsh] multiplayer.classdojo.com
[crtsh] ws.multiplayer.classdojo.com
[crtsh] internal.classdojo.com
[crtsh] ws-dev.multiplayer.classdojo.com
[crtsh] ws-staging.multiplayer.classdojo.com
[crtsh] www.sparks.classdojo.com
[crtsh] www.marketplace.classdojo.com
[crtsh] www.tutoring.classdojo.com
[crtsh] logs.classdojo.com
[crtsh] metrics.classdojo.com
[crtsh] android-web-static.classdojo.com
[crtsh] ticket-staging.multiplayer.classdojo.com
[crtsh] sentry.classdojo.com
[waybackarchive] www3.classdojo.com
[crtsh] experiences.classdojo.com
[crtsh] clubs.classdojo.com
[crtsh] clubs-server.classdojo.com
[crtsh] api.marketplace.classdojo.com
[crtsh] clubs4.classdojo.com
[crtsh] mtutor.classdojo.com
[crtsh] dev.api.marketplace.classdojo.com
[crtsh] marketplace.classdojo.com
[crtsh] clubs5.classdojo.com
[crtsh] ws.classdojo.com
[crtsh] realtime.classdojo.com
[crtsh] mw.classdojo.com
[crtsh] mwdev.classdojo.com
[crtsh] test.internal.classdojo.com
```

6. Thirdly, I used Wafwoof tool to find website is protected by a WAF (web application firewall). Because if WAF is active, so pen tester do their test without blocked, and they can do their testing with bypass WAF.



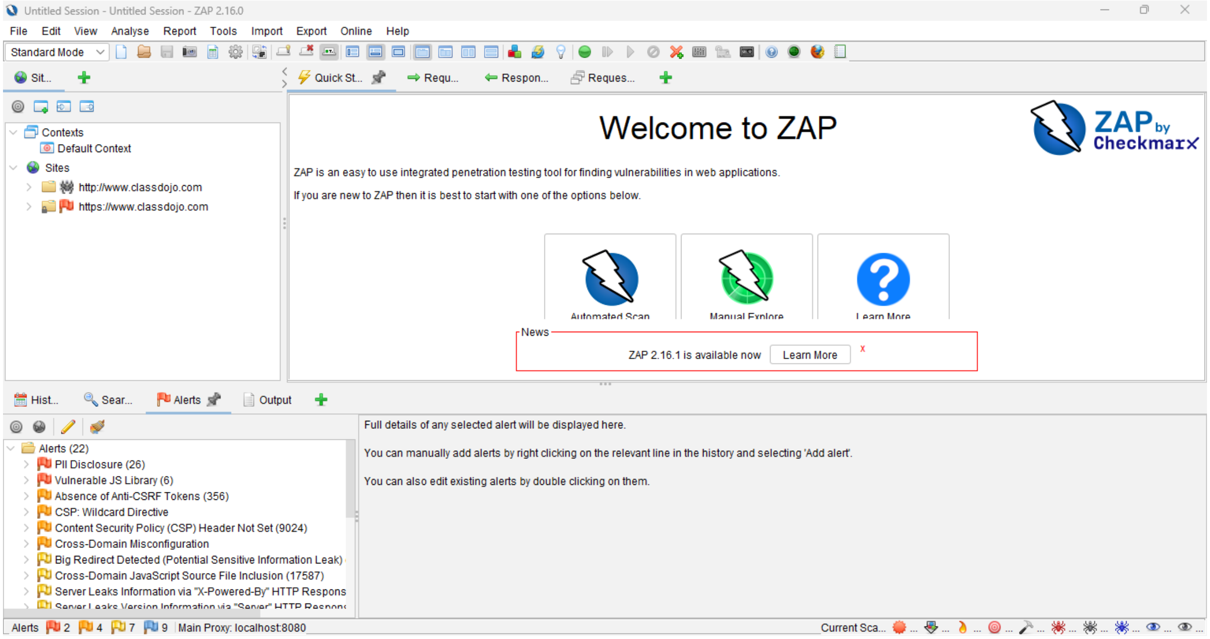
```
┌──(root㉿kali2025)-[~]
└─# wafw00f https://www.classdojo.com/

                ~ WAFW00F : v2.3.1 ~

[*] Checking https://www.classdojo.com/
[+] The site https://www.classdojo.com/ is behind Cloudfront (Amazon) WAF.
[~] Number of requests: 2

┌──(root㉿kali2025)-[~]
└─# █
```

7.Finaly, I use OWASP zap to automatically find the vulnerabilities.



Welcome to ZAP

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

If you are new to ZAP then it is best to start with one of the options below.

ZAP 2.16.1 is available now

Alerts (22)
- PII Disclosure (26)
- Vulnerable JS Library (6)
- Absence of Anti-CSRF Tokens (356)
- CSP: Wildcard Directive
- Content Security Policy (CSP) Header Not Set (9024)
- Cross-Domain Misconfiguration
- Big Redirect Detected (Potential Sensitive Information Leak)
- Cross-Domain JavaScript Source File Inclusion (17587)
- Server Leaks Information via "X-Powered-By" HTTP Respons
- Server Leaks Version Information via "Server" HTTP Respons

Full details of any selected alert will be displayed here.

You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.

You can also edit existing alerts by double clicking on them.

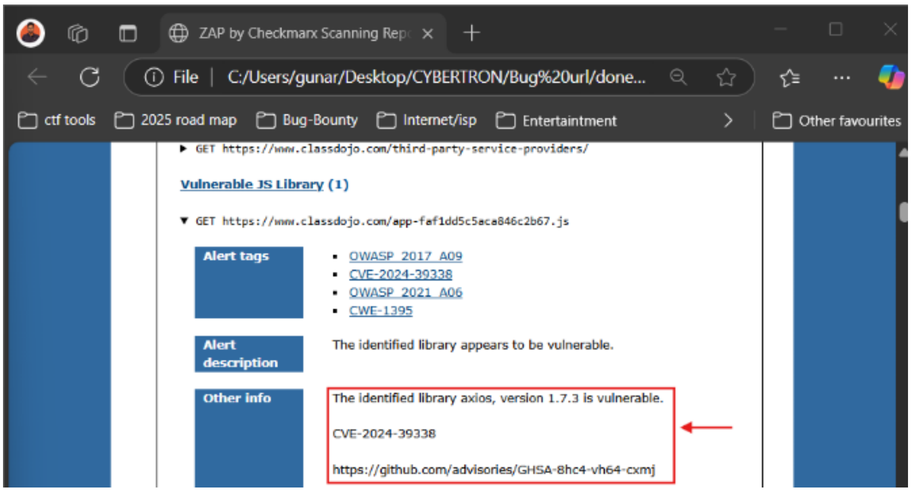
Alerts 🟥 2 🟧 4 🟨 7 🟦 9 Main Proxy: localhost:8080

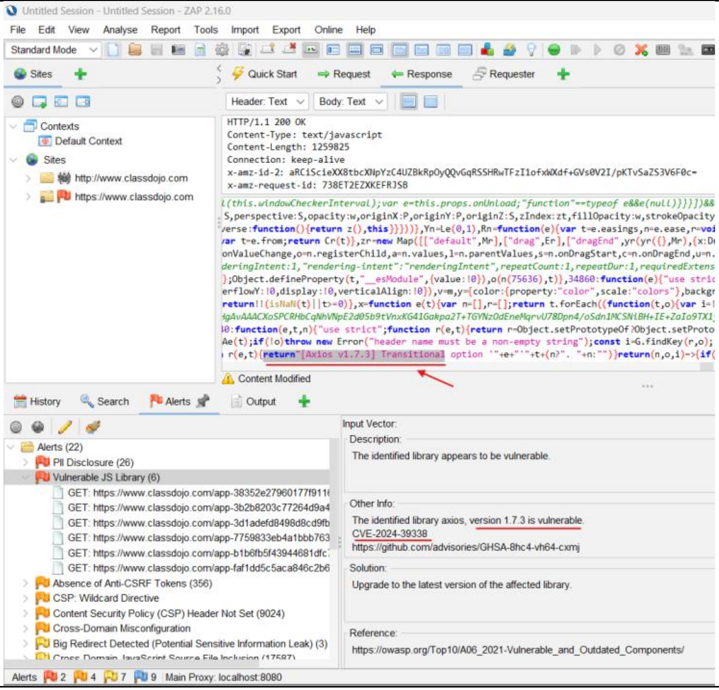
With getting these tool’s support, I found below details about vulnerability.

2) Introduction

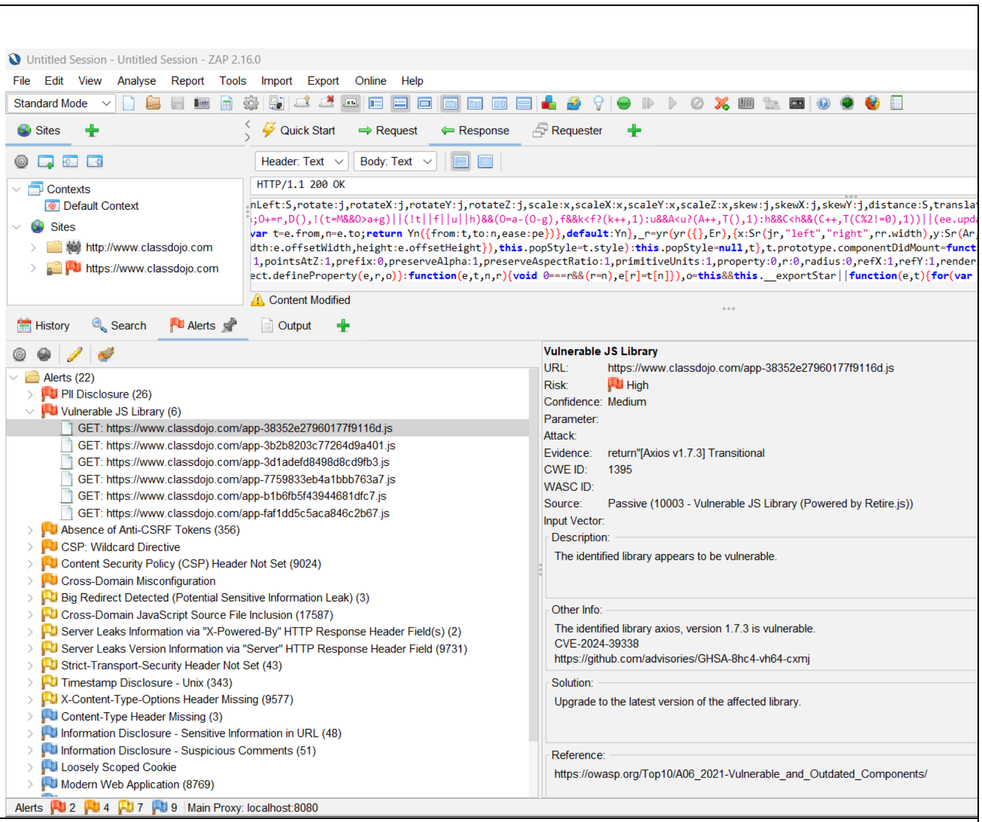
1.1 Domain	**https://www.classdojo.com** https://www.classdojo.com/third-party-service-providers/
1.2 Severity	- **High**

3) Vulnerability

3.1 Vulnerability title	Vulnerable JS Library OWASP_2021_A06 CWE-1395
3.2 Vulnerability description	The response contains Personally Identifiable Information, such as CC number, SSN and similar sensitive data.
3.3 Affected components	Library: Axios Version: 1.7.3 Vulnerability: CVE-2024-39338  ZAP by Checkmarx Scanning Rep File | C:/Users/gunar/Desktop/CYBERTRON/Bug%20url/done... ctf tools 2025 road map Bug-Bounty Internet/isp Entertaintment Other favourites ▶ GET https://www.classdojo.com/third-party-service-providers/ Vulnerable JS Library (1) ▼ GET https://www.classdojo.com/app-faf1dd5c5aca846c2b67.js Alert tags: OWASP_2017_A09, CVE-2024-39338, OWASP_2021_A06, CWE-1395 Alert description: The identified library appears to be vulnerable. Other info: The identified library axios, version 1.7.3 is vulnerable. CVE-2024-39338 https://github.com/advisories/GHSA-8hc4-vh64-cxmj (Based on generated report)

	 Untitled Session - Untitled Session - ZAP 2.16.0 File Edit View Analyse Report Tools Import Export Online Help Standard Mode Sites Quick Start Request Response Requester Header: Text Body: Text Content Modified History Search Alerts OutputContexts Default Context Sites http://www.classdojo.com https://www.classdojo.com HTTP/1.1 200 OK Content-Type: text/javascript Content-Length: 1259825 Connection: keep-alive x-amz-id-2: aRCiScieXX8tbcXNpYzC4UZBkRpOyQQvGqRSSHRwTFzI1ofxWXdf+GVs0V2I/pKTvSaZS3V6F0c= x-amz-request-id: 738ET2EZXKEFRJSB l(this.windowCheckerInterval);var e=this.props.onUnload;"function"==typeof e&&e(null)}}}])&& S,perspective:S,opacity:w,originX:P,originY:P,originZ:S,zIndex:zt,fillOpacity:w,strokeOpacity verse:function(){return z(),this}}}))},Yn=Le(0,1),Rn=function(e){var t=e.easings,n=e.ease,r=voi var t=e.from;return Cr(t)},zr=new Map([["default",Mr],["drag",Er],["dragEnd",yr(yr({},Mr),{x:Di onValueChange,o=n.registerChild,a=n.values,l=n.parentValues,s=n.onDragStart,c=n.onDragEnd,u=n. deringIntent:1,"rendering-intent":"renderingIntent",repeatCount:1,repeatDur:1,requiredExtens };Object.defineProperty(t,"__esModule",{value:!0}),o(n(75636),t)},34860:function(e){"use stric erflowY:!0,display:!0,verticalAlign:!0}),v=m,y={color:{property:"color",scale:"colors"},backgr return!!(isNaN(t)||t>=0)},x=function e(t){var n=[],r=[];return t.forEach((function(t,o){var i=! HgAvAAACXoSPCRHbCqNhVNpE2d05b9tVnxKG41Gakpa2T+TGYNzOdEneMqrvU78Dpn4/oSdn1MCSNiBH+IE+ZaIo9TX1 40:function(e,t,n){"use strict";function r(e,t){return r=Object.setPrototypeOf?Object.setProto Ae(t);if(!o)throw new Error("header name must be a non-empty string");const i=G.findKey(r,o); r(e,t){return"[Axios v1.7.3] Transitional option '"+e+"'"+t+(n?". "+n:"")}return(n,o,i)=>{if(Alerts (22) PII Disclosure (26) Vulnerable JS Library (6) GET: https://www.classdojo.com/app-38352e27960177f911 GET: https://www.classdojo.com/app-3b2b8203c77264d9a4 GET: https://www.classdojo.com/app-3d1adefd8498d8cd9fb GET: https://www.classdojo.com/app-7759833eb4a1bbb763 GET: https://www.classdojo.com/app-b1b6fb5f43944681dfc GET: https://www.classdojo.com/app-faf1dd5c5aca846c2b6 Absence of Anti-CSRF Tokens (356) CSP: Wildcard Directive Content Security Policy (CSP) Header Not Set (9024) Cross-Domain Misconfiguration Big Redirect Detected (Potential Sensitive Information Leak) (3) Cross Domain JavaScript Source File Inclusion (17587) Input Vector: Description: The identified library appears to be vulnerable. Other Info: The identified library axios, version 1.7.3 is vulnerable. CVE-2024-39338 https://github.com/advisories/GHSA-8hc4-vh64-cxmj Solution: Upgrade to the latest version of the affected library. Reference: https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/ Alerts 2 4 7 9 Main Proxy: localhost:8080
2.4 Impact assessment	It using a vulnerable version of Axios occur: * may be able to bypass expected timeout behaviour *Create logic flaws in the request/response lifecycle of the app *May even make the application susceptible to other request-based attacks.
2.5 Steps to reproduce	1. Scan the target application using OWASP ZAP. 2. Locate the JavaScript file or header referencing Axios v1.7.3. 3. Cross-reference the version with the known CVE.

2.6 Proof of concept



```
HTTP/1.1 200 OK
```

```
nLeft:S,rotate:j,rotateX:j,rotateY:j,rotateZ:j,scale:x,scaleX:x,scaleY:x,scaleZ:x,skew:j,skewX:j,skewY:j,distance:S,translat
;O+=r,D(),!(t=M&&O>a+g)||(!t||f||u||h)&&(O=a-(O-g),f&&k<f?(k++,1):u&&A<u?(A++,T(),1):h&&C<h&&(C++,T(C%2!=0),1))||(ee.upda
var t=e.from,n=e.to;return Yn({from:t,to:n,ease:pe})},default:Yn},_r=yr(yr({},Er),{x:Sr(jr,"left","right",rr.width),y:Sr(Ar,
dth:e.offsetWidth,height:e.offsetHeight}),this.popStyle=t.style):this.popStyle=null,t},t.prototype.componentDidMount=funct
1,pointsAtZ:1,prefix:0,preserveAlpha:1,preserveAspectRatio:1,primitiveUnits:1,property:0,r:0,radius:0,refX:1,refY:1,render
ect.defineProperty(e,r,o)}:function(e,t,n,r){void 0===r&&(r=n),e[r]=t[n]}),o=this&&this.__exportStar||function(e,t){for(var
```

⚠ Content Modified

- Alerts (22)
  - PII Disclosure (26)
  - Vulnerable JS Library (6)
    - GET: https://www.classdojo.com/app-38352e27960177f9116d.js
    - GET: https://www.classdojo.com/app-3b2b8203c77264d9a401.js
    - GET: https://www.classdojo.com/app-3d1adefd8498d8cd9fb3.js
    - GET: https://www.classdojo.com/app-7759833eb4a1bbb763a7.js
    - GET: https://www.classdojo.com/app-b1b6fb5f43944681dfc7.js
    - GET: https://www.classdojo.com/app-faf1dd5c5aca846c2b67.js
  - Absence of Anti-CSRF Tokens (356)
  - CSP: Wildcard Directive
  - Content Security Policy (CSP) Header Not Set (9024)
  - Cross-Domain Misconfiguration
  - Big Redirect Detected (Potential Sensitive Information Leak) (3)
  - Cross-Domain JavaScript Source File Inclusion (17587)
  - Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (2)
  - Server Leaks Version Information via "Server" HTTP Response Header Field (9731)
  - Strict-Transport-Security Header Not Set (43)
  - Timestamp Disclosure - Unix (343)
  - X-Content-Type-Options Header Missing (9577)
  - Content-Type Header Missing (3)
  - Information Disclosure - Sensitive Information in URL (48)
  - Information Disclosure - Suspicious Comments (51)
  - Loosely Scoped Cookie
  - Modern Web Application (8769)

Vulnerable JS Library

URL:	https://www.classdojo.com/app-38352e27960177f9116d.js
Risk:	🟥 High
Confidence:	Medium
Parameter:	
Attack:	
Evidence:	return"[Axios v1.7.3] Transitional
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.

Other Info:

The identified library axios, version 1.7.3 is vulnerable.
CVE-2024-39338
https://github.com/advisories/GHSA-8hc4-vh64-cxmj

Solution:

Upgrade to the latest version of the affected library.

Reference:

https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/

Alerts 🟥 2 🟧 4 🟨 7 🟦 9 Main Proxy: localhost:8080

2.7 Proposed mitigation or fix

Upgrade to the latest version of the affected library. So, the current version is version 1.7.3, so we must update it.

To mitigate this type of issues, we can do audits regularly. (inter audits or third-party audits)