Sri Lanka Institute of Information Technology

Web Security – IE2062

Topic: Bug Bounty Report 6

Y2S2.WE.CS

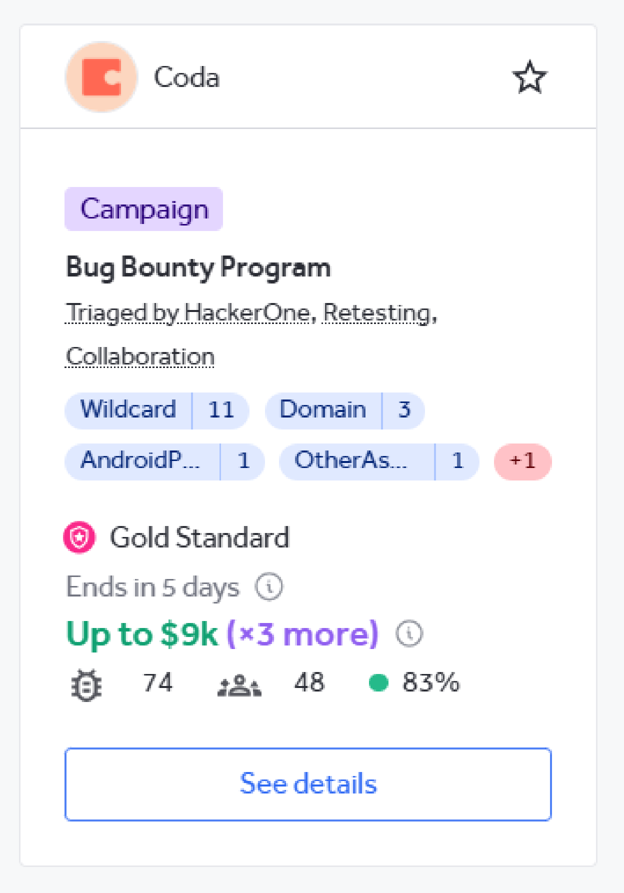
Name: S.D.W.Gunaratne

(IT23241978)

Table of Content

How I started?

1. Once I search from hacker one, I saw a coda.io bug bounty program.



Coda

Campaign

Bug Bounty Program

Triaged by HackerOne, Retesting, Collaboration

Wildcard 11 | Domain 3 | AndroidP... 1 | OtherAs... 1 | +1

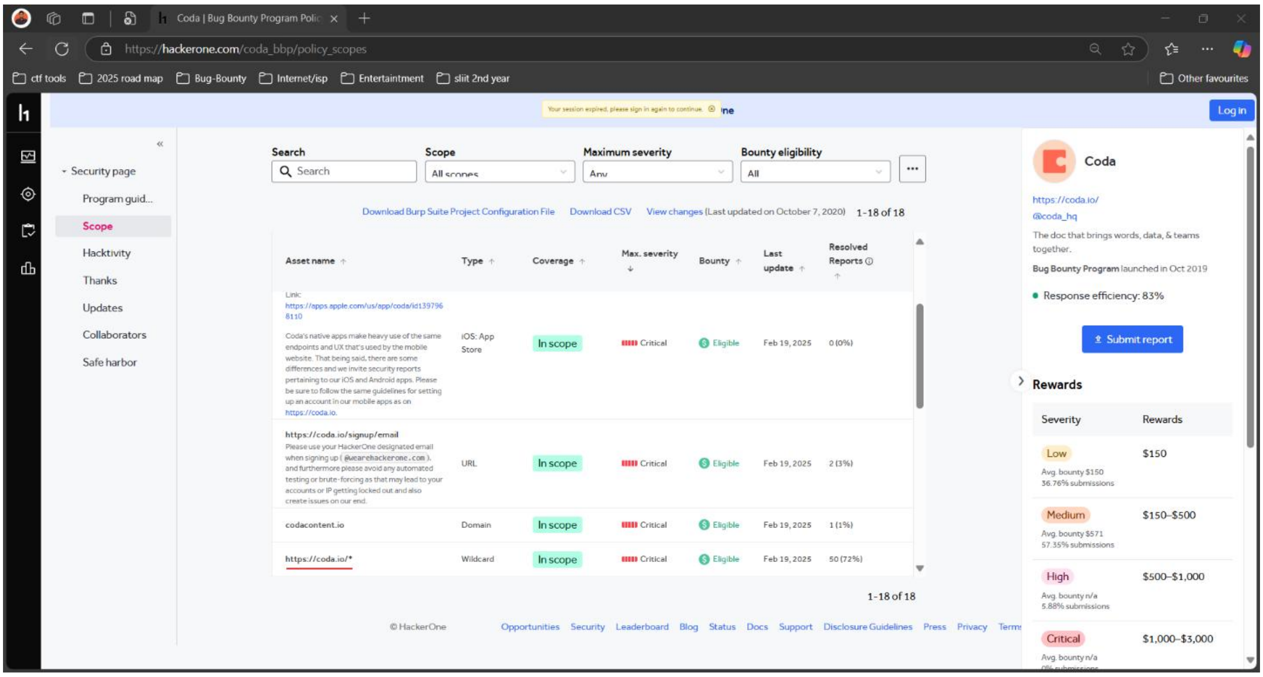
Gold Standard

Ends in 5 days

Up to $9k (×3 more)

74 48 ● 83%

2. Then, I discovered allowed domains scope, so that I choose https://coda.io .



Your session expired, please sign in again to continue.

Search: Search | Scope: All scopes | Maximum severity: Any | Bounty eligibility: All

Download Burp Suite Project Configuration File   Download CSV   View changes (Last updated on October 7, 2020)   1-18 of 18

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
Link: https://apps.apple.com/us/app/coda/id1397968110 Coda's native apps make heavy use of the same endpoints and UX that's used by the mobile website. That being said, there are some differences and we invite security reports pertaining to our iOS and Android apps. Please be sure to follow the same guidelines for setting up an account in our mobile apps as on https://coda.io.	iOS: App Store	In scope	Critical	Eligible	Feb 19, 2025	0 (0%)
https://coda.io/signup/email Please use your HackerOne designated email when signing up (@wearehackerone.com), and furthermore please avoid any automated testing or brute-forcing as that may lead to your accounts or IP getting locked out and also create issues on our end.	URL	In scope	Critical	Eligible	Feb 19, 2025	2 (3%)
codacontent.io	Domain	In scope	Critical	Eligible	Feb 19, 2025	1 (1%)
https://coda.io/*	Wildcard	In scope	Critical	Eligible	Feb 19, 2025	50 (72%)

1-18 of 18

© HackerOne   Opportunities   Security   Leaderboard   Blog   Status   Docs   Support   Disclosure Guidelines   Press   Privacy   Terms

Coda

https://coda.io/

@coda_hq

The doc that brings words, data, & teams together.

Bug Bounty Program launched in Oct 2019

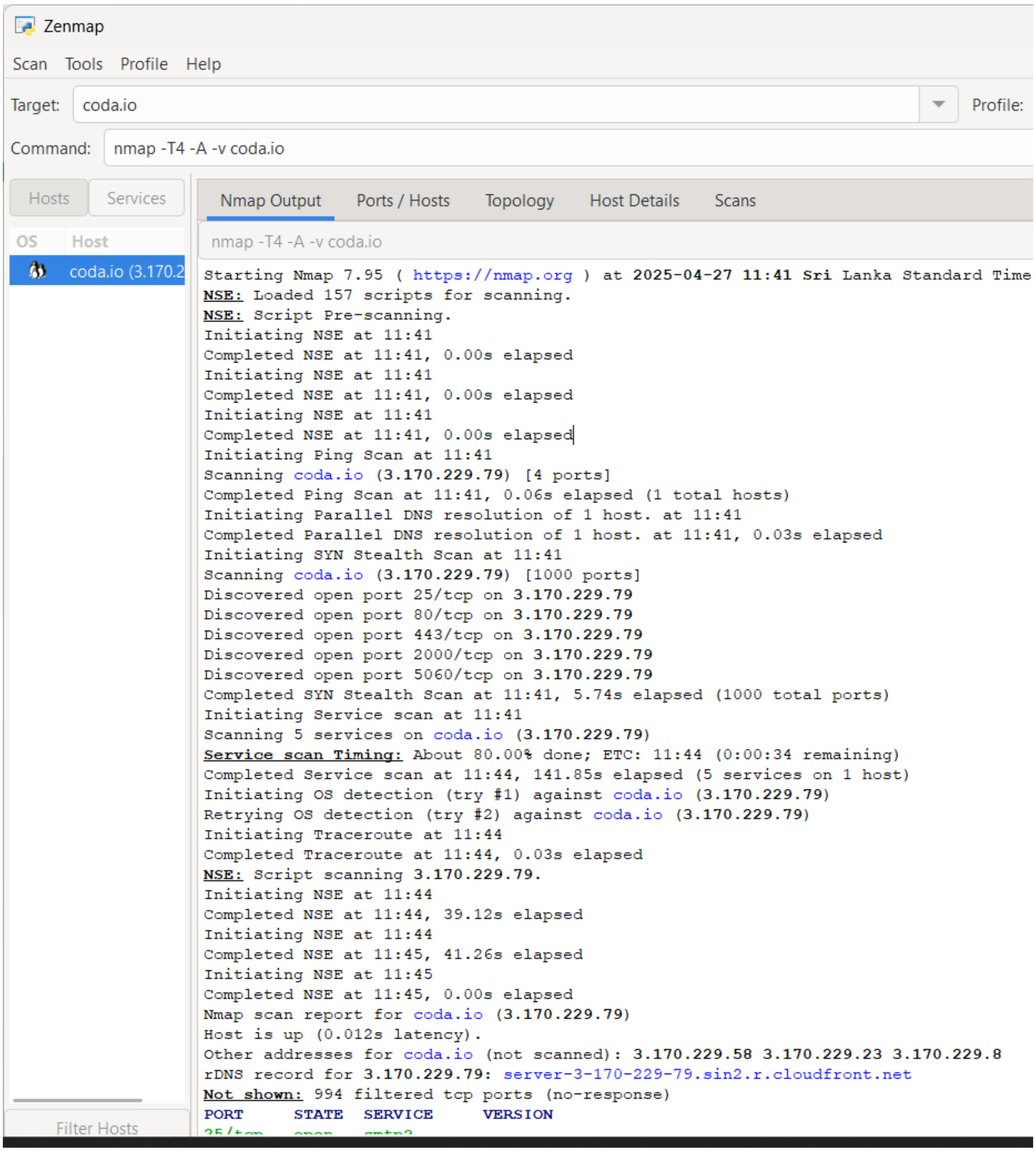
● Response efficiency: 83%

Rewards

Severity	Rewards
Low Avg. bounty $150 36.76% submissions	$150
Medium Avg. bounty $571 57.35% submissions	$150–$500
High Avg. bounty n/a 5.88% submissions	$500–$1,000
Critical Avg. bounty n/a 0% submissions	$1,000–$3,000

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.

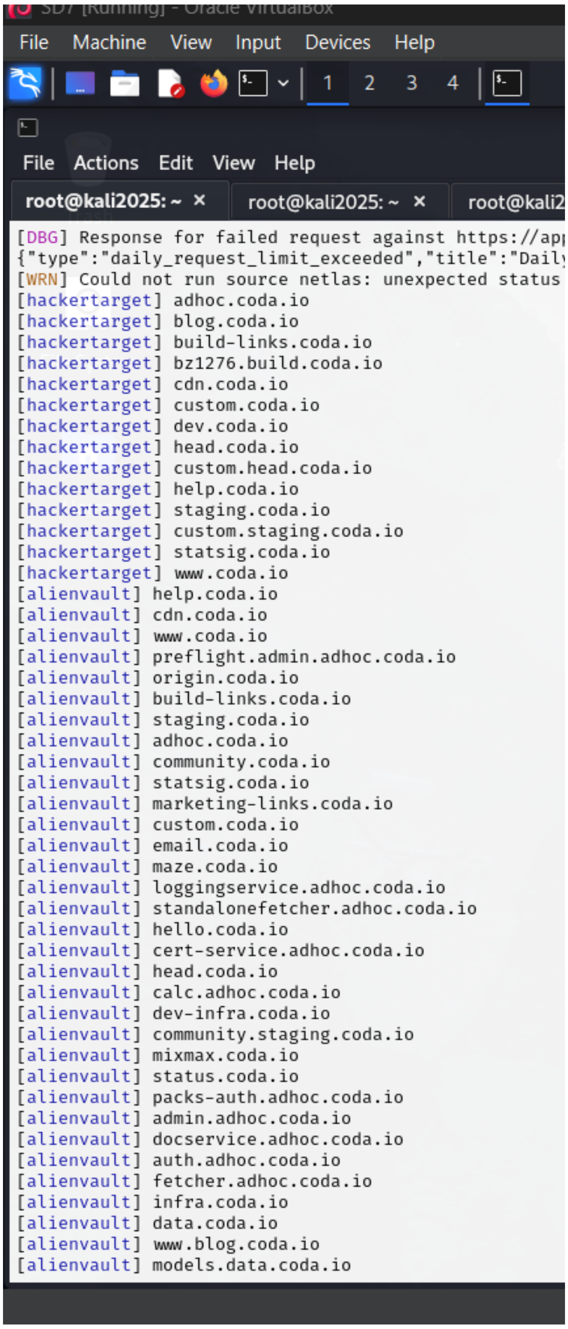


Target: coda.io

Command: nmap -T4 -A -v coda.io

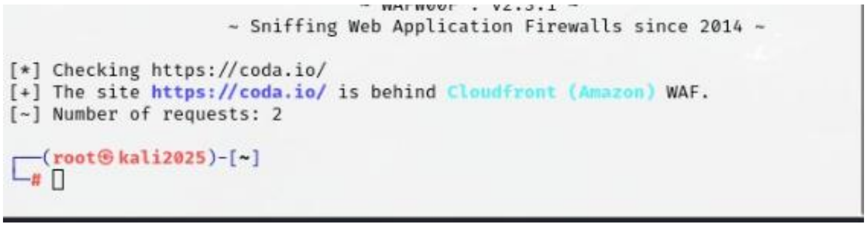
```
nmap -T4 -A -v coda.io
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-27 11:41 Sri Lanka Standard Time
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 11:41
Completed NSE at 11:41, 0.00s elapsed
Initiating NSE at 11:41
Completed NSE at 11:41, 0.00s elapsed
Initiating NSE at 11:41
Completed NSE at 11:41, 0.00s elapsed
Initiating Ping Scan at 11:41
Scanning coda.io (3.170.229.79) [4 ports]
Completed Ping Scan at 11:41, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:41
Completed Parallel DNS resolution of 1 host. at 11:41, 0.03s elapsed
Initiating SYN Stealth Scan at 11:41
Scanning coda.io (3.170.229.79) [1000 ports]
Discovered open port 25/tcp on 3.170.229.79
Discovered open port 80/tcp on 3.170.229.79
Discovered open port 443/tcp on 3.170.229.79
Discovered open port 2000/tcp on 3.170.229.79
Discovered open port 5060/tcp on 3.170.229.79
Completed SYN Stealth Scan at 11:41, 5.74s elapsed (1000 total ports)
Initiating Service scan at 11:41
Scanning 5 services on coda.io (3.170.229.79)
Service scan Timing: About 80.00% done; ETC: 11:44 (0:00:34 remaining)
Completed Service scan at 11:44, 141.85s elapsed (5 services on 1 host)
Initiating OS detection (try #1) against coda.io (3.170.229.79)
Retrying OS detection (try #2) against coda.io (3.170.229.79)
Initiating Traceroute at 11:44
Completed Traceroute at 11:44, 0.03s elapsed
NSE: Script scanning 3.170.229.79.
Initiating NSE at 11:44
Completed NSE at 11:44, 39.12s elapsed
Initiating NSE at 11:44
Completed NSE at 11:45, 41.26s elapsed
Initiating NSE at 11:45
Completed NSE at 11:45, 0.00s elapsed
Nmap scan report for coda.io (3.170.229.79)
Host is up (0.012s latency).
Other addresses for coda.io (not scanned): 3.170.229.58 3.170.229.23 3.170.229.8
rDNS record for 3.170.229.79: server-3-170-229-79.sin2.r.cloudfront.net
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE  SERVICE    VERSION
25/tcp    open   smtp?
```

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



```
[DBG] Response for failed request against https://app
{"type":"daily_request_limit_exceeded","title":"Daily
[WRN] Could not run source netlas: unexpected status
[hackertarget] adhoc.coda.io
[hackertarget] blog.coda.io
[hackertarget] build-links.coda.io
[hackertarget] bz1276.build.coda.io
[hackertarget] cdn.coda.io
[hackertarget] custom.coda.io
[hackertarget] dev.coda.io
[hackertarget] head.coda.io
[hackertarget] custom.head.coda.io
[hackertarget] help.coda.io
[hackertarget] staging.coda.io
[hackertarget] custom.staging.coda.io
[hackertarget] statsig.coda.io
[hackertarget] www.coda.io
[alienvault] help.coda.io
[alienvault] cdn.coda.io
[alienvault] www.coda.io
[alienvault] preflight.admin.adhoc.coda.io
[alienvault] origin.coda.io
[alienvault] build-links.coda.io
[alienvault] staging.coda.io
[alienvault] adhoc.coda.io
[alienvault] community.coda.io
[alienvault] statsig.coda.io
[alienvault] marketing-links.coda.io
[alienvault] custom.coda.io
[alienvault] email.coda.io
[alienvault] maze.coda.io
[alienvault] loggingservice.adhoc.coda.io
[alienvault] standalonefetcher.adhoc.coda.io
[alienvault] hello.coda.io
[alienvault] cert-service.adhoc.coda.io
[alienvault] head.coda.io
[alienvault] calc.adhoc.coda.io
[alienvault] dev-infra.coda.io
[alienvault] community.staging.coda.io
[alienvault] mixmax.coda.io
[alienvault] status.coda.io
[alienvault] packs-auth.adhoc.coda.io
[alienvault] admin.adhoc.coda.io
[alienvault] docservice.adhoc.coda.io
[alienvault] auth.adhoc.coda.io
[alienvault] fetcher.adhoc.coda.io
[alienvault] infra.coda.io
[alienvault] data.coda.io
[alienvault] www.blog.coda.io
[alienvault] models.data.coda.io
```

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.

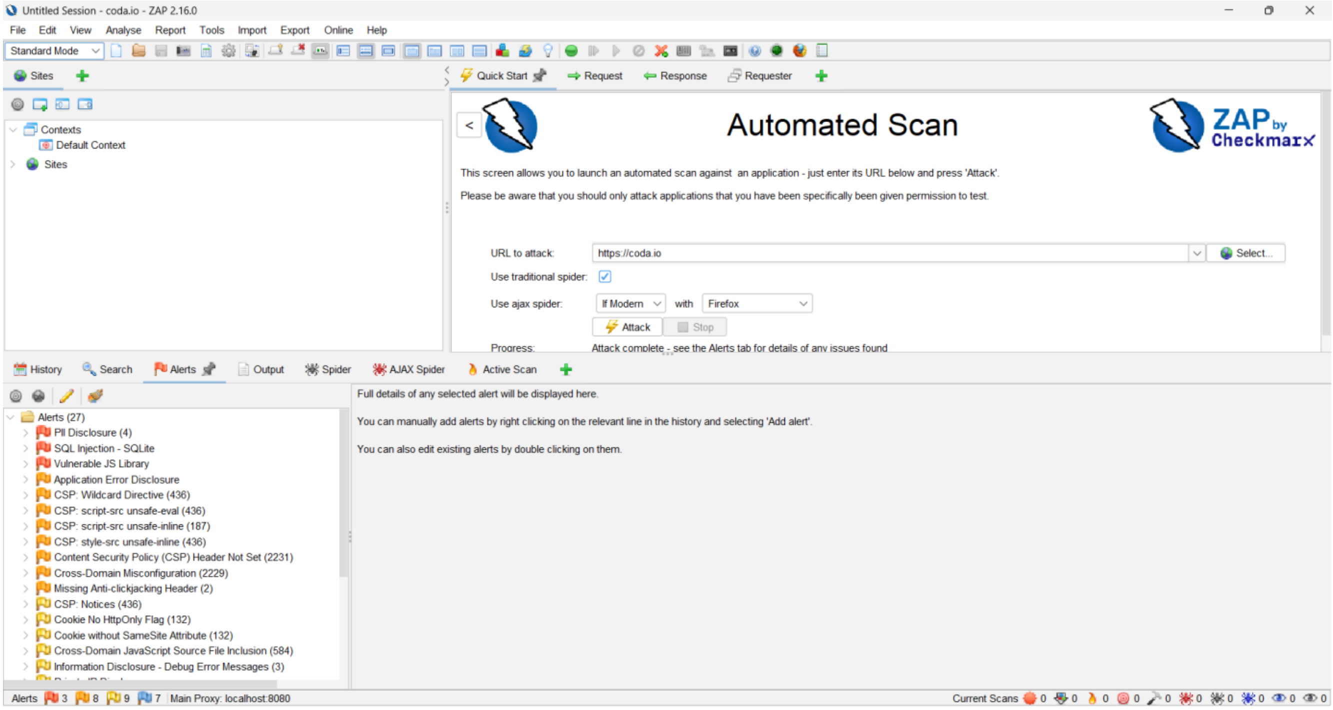


```
                        ~ WAFW00F : v2.3.1 ~
            ~ Sniffing Web Application Firewalls since 2014 ~

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

┌──(root㉿kali2025)-[~]
└─# 
```

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



Automated Scan

ZAP by Checkmarx

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: https://coda.io

Use traditional spider: ☑

Use ajax spider: If Modern with Firefox

Attack Stop

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

Alerts (27)
- PII Disclosure (4)
- SQL Injection - SQLite
- Vulnerable JS Library
- Application Error Disclosure
- CSP: Wildcard Directive (436)
- CSP: script-src unsafe-eval (436)
- CSP: script-src unsafe-inline (187)
- CSP: style-src unsafe-inline (436)
- Content Security Policy (CSP) Header Not Set (2231)
- Cross-Domain Misconfiguration (2229)
- Missing Anti-clickjacking Header (2)
- CSP: Notices (436)
- Cookie No HttpOnly Flag (132)
- Cookie without SameSite Attribute (132)
- Cross-Domain JavaScript Source File Inclusion (584)
- Information Disclosure - Debug Error Messages (3)

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 🟥 3 🟧 8 🟨 9 🟦 7 Main Proxy: localhost:8080

Current Scans 0 0 0 0 0 0 0 0 0 0

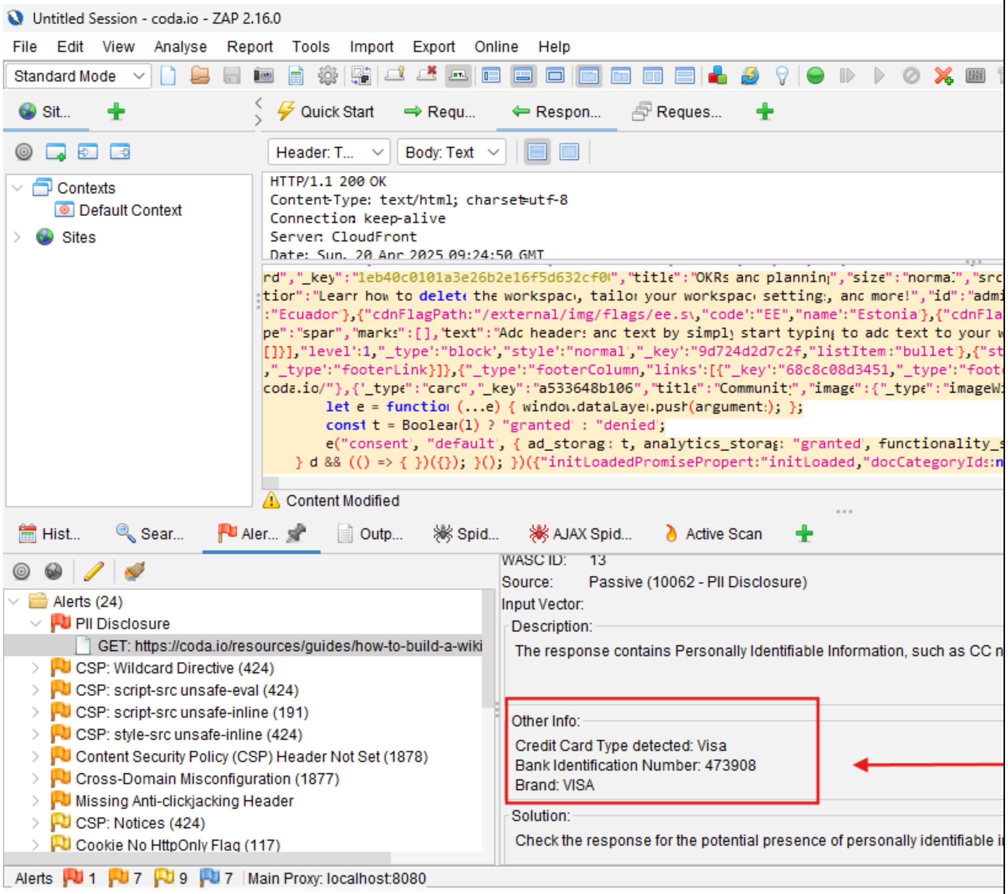
With getting these tool’s support, I found below details about vulnerability.

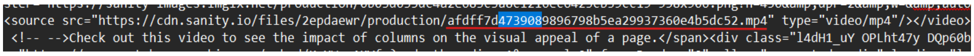
1) Introduction

1.1 Domain	**https://coda.io** https://coda.io/resources/guides/how-to-build-a-wiki
1.2 Severity	• High

2) Vulnerability

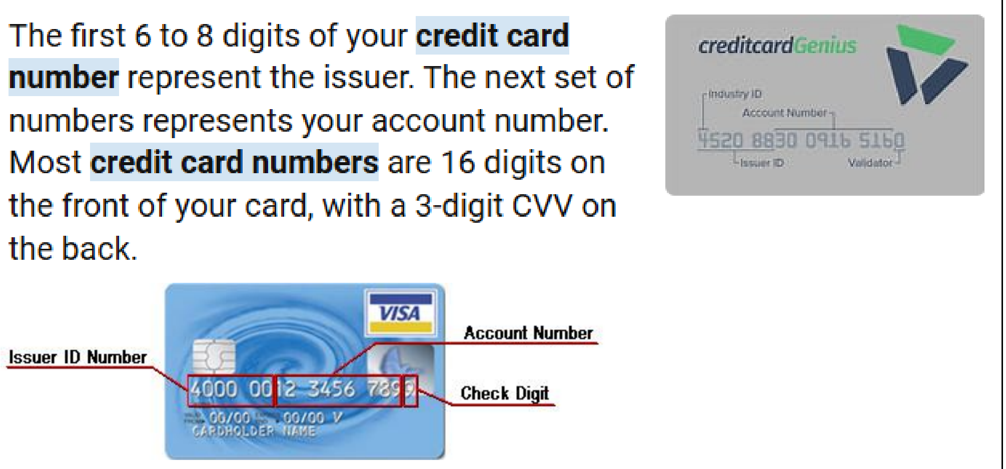
2.1 Vulnerability title	PII Disclosure CWE-359 OWASP_2021_A04
2.2 Vulnerability description	The response contains Personally Identifiable Information, such as CC number, SSN and similar sensitive data.
2.3 Affected components	vulnerability affects the API endpoint or web page that returns responses with personal user data. Like full or half credit card number. Component Type: - Server-side response handling Vulnerable Endpoint: - https://coda.io/resources/guides/how-to-build-a-wiki This found from OWASP ZAP
2.4 Impact assessment	IF it is PII disclosure is severe privacy risk. In our case this is the examples: Credit Card Type detected: Visa Bank Identification Number: 473908 Brand: VISA Category: BUSINESS Issuer: BAXTER C.U.

	 Untitled Session - coda.io - ZAP 2.16.0 HTTP/1.1 200 OK Content-Type: text/html; charset=utf-8 Connection: keep-alive Server: CloudFront Date: Sun, 20 Apr 2025 09:24:50 GMT rd","_key":"1eb40c0101a3e26b2e16f5d632cf0","title":"OKRs and planning","size":"normal","src tion":"Learn how to delete the workspace, tailor your workspace settings, and more!","id":"admi :"Ecuador"},{"cdnFlagPath":"/external/img/flags/ee.svg","code":"EE","name":"Estonia"},{"cdnFla pe":"span","marks":[],"text":"Add headers and text by simply start typing to add text to your w []}],"level":1,"_type":"block","style":"normal","_key":"9d724d2d7c2f","listItem":"bullet"},{"st ,"_type":"footerLink"}]},{"_type":"footerColumn","links":[{"_key":"68c8c08d3451","_type":"foot coda.io/"},{"_type":"card","_key":"a533648b106","title":"Community","image":{"_type":"imageWi let e = function (...e) { window.dataLayer.push(arguments); }; const t = Boolean(1) ? "granted" : "denied"; e("consent", "default", { ad_storage: t, analytics_storage: "granted", functionality_s } d && (() => { })({}); }(); })({"initLoadedPromiseProperty":"initLoaded","docCategoryIds":n Content Modified Alerts (24) PII Disclosure GET: https://coda.io/resources/guides/how-to-build-a-wiki CSP: Wildcard Directive (424) CSP: script-src unsafe-eval (424) CSP: script-src unsafe-inline (191) CSP: style-src unsafe-inline (424) Content Security Policy (CSP) Header Not Set (1878) Cross-Domain Misconfiguration (1877) Missing Anti-clickjacking Header CSP: Notices (424) Cookie No HttpOnly Flag (117) WASC ID: 13 Source: Passive (10062 - PII Disclosure) Input Vector: Description: The response contains Personally Identifiable Information, such as CC n Other Info: Credit Card Type detected: Visa Bank Identification Number: 473908 Brand: VISA Solution: Check the response for the potential presence of personally identifiable i Alerts 1 7 9 7 Main Proxy: localhost:8080 File Edit View Analyse Report Tools Import Export Online Help Standard Mode Sit... Quick Start Requ... Respon... Reques... Header: T... Body: Text Contexts Default Context Sites Hist... Sear... Aler... Outp... Spid... AJAX Spid... Active Scan

2.5 Steps to reproduce	Open the OWASP ZAP and do the scan.
	Watch for Zap's alert called PII disclosure.
	Find the respond holding the credit card number.
	Copy the entire respond to note pad, then search this 473908 (partial or full credit card number)
	
	`<source src="https://cdn.sanity.io/files/2epdaewr/production/afdff7d4739089896798b5ea29937360e4b5dc52.mp4" type="video/mp4"/></video>`
	`<!-- -->Check out this video to see the impact of columns on the visual appeal of a page.</span><div class="l4dH1_uY OPLht47y DQp60b`

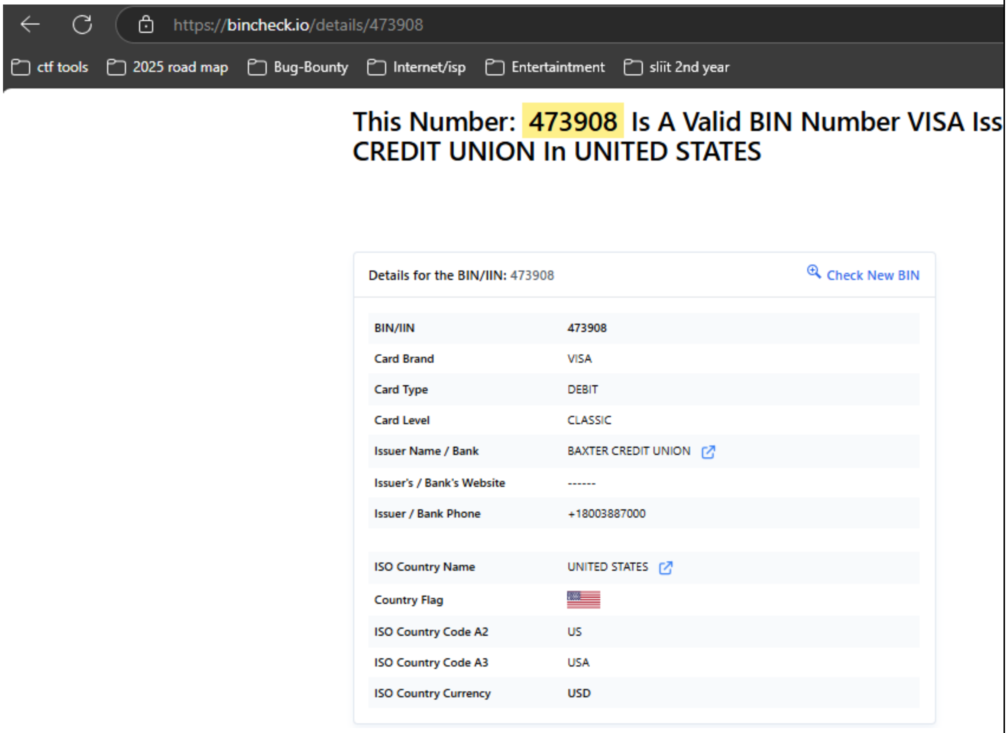
2.6 Proof of concept	The response includes a video URL with the credit card number as part of the filename https://cdn.sanity.io/files/2epdaewr/production/afdff7d4739089896798b5ea29937360e4b5dc52.mp4

prove this is VISA credit card:



The first 6 to 8 digits of your **credit card number** represent the issuer. The next set of numbers represents your account number. Most **credit card numbers** are 16 digits on the front of your card, with a 3-digit CVV on the back.

*All VISA card start with 4
and with this tool, we can identify other details - https://bincheck.io/



This Number: 473908 Is A Valid BIN Number VISA Iss
CREDIT UNION In UNITED STATES

Details for the BIN/IIN: 473908

BIN/IIN	473908
Card Brand	VISA
Card Type	DEBIT
Card Level	CLASSIC
Issuer Name / Bank	BAXTER CREDIT UNION
Issuer's / Bank's Website	------
Issuer / Bank Phone	+18003887000
ISO Country Name	UNITED STATES
Country Flag	🇺🇸
ISO Country Code A2	US
ISO Country Code A3	USA
ISO Country Currency	USD

So, if attacker know this card details, how he attacks?

1. Carding (online Fraud) – Most online platform uses card number, Expiry date and CVV, so this can be brute force by the attacker. To do that they can use Luhn algorithm to support.

*How ever this type of weakness (expose credit card detail) can violate Data protection Laws such as, GDPR, CCPA

2.7 Proposed mitigation or fix	Check the response for the potential presence of personally identifiable information (PII), ensure nothing sensitive is leaked by the application.