Sri Lanka Institute of Information Technology

IE2062 - Web Security

Final Assignment

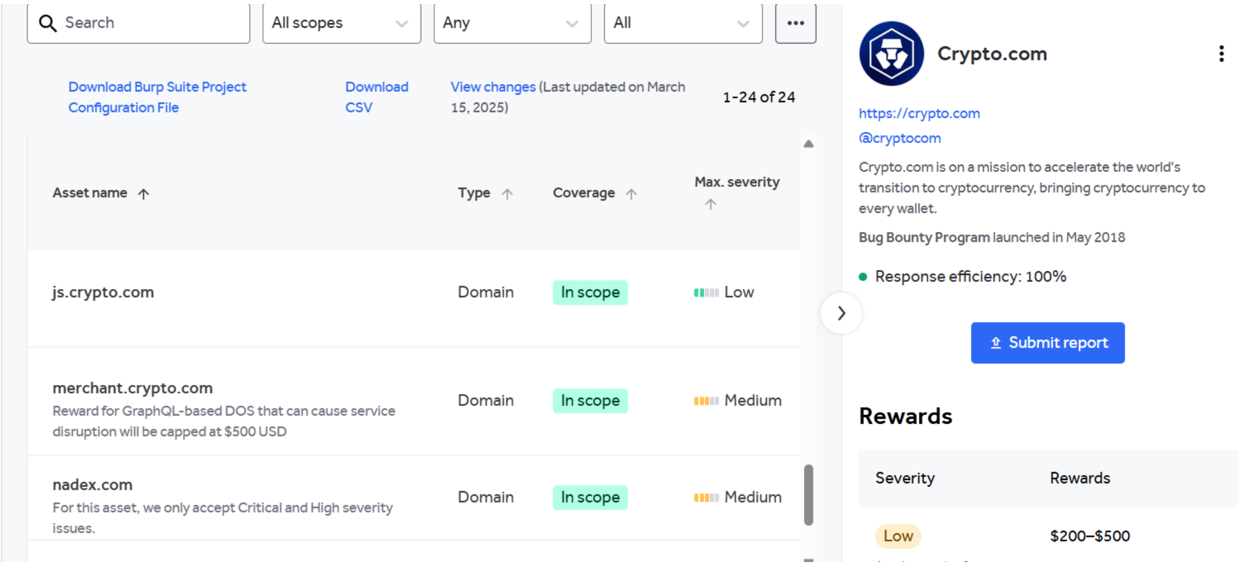
Bug Bounty Report 09

Name: Peiris W.S.S.N

Registration Number: IT23227286

Contents

1. Introduction



Search | All scopes | Any | All | ...

Download Burp Suite Project Configuration File | Download CSV | View changes (Last updated on March 15, 2025) | 1-24 of 24

Asset name ↑	Type ↑	Coverage ↑	Max. severity ↑
js.crypto.com	Domain	In scope	Low
merchant.crypto.com Reward for GraphQL-based DOS that can cause service disruption will be capped at $500 USD	Domain	In scope	Medium
nadex.com For this asset, we only accept Critical and High severity issues.	Domain	In scope	Medium

Crypto.com

https://crypto.com

@cryptocom

Crypto.com is on a mission to accelerate the world's transition to cryptocurrency, bringing cryptocurrency to every wallet.

Bug Bounty Program launched in May 2018

● Response efficiency: 100%

Submit report

Rewards

Severity	Rewards
Low	$200–$500

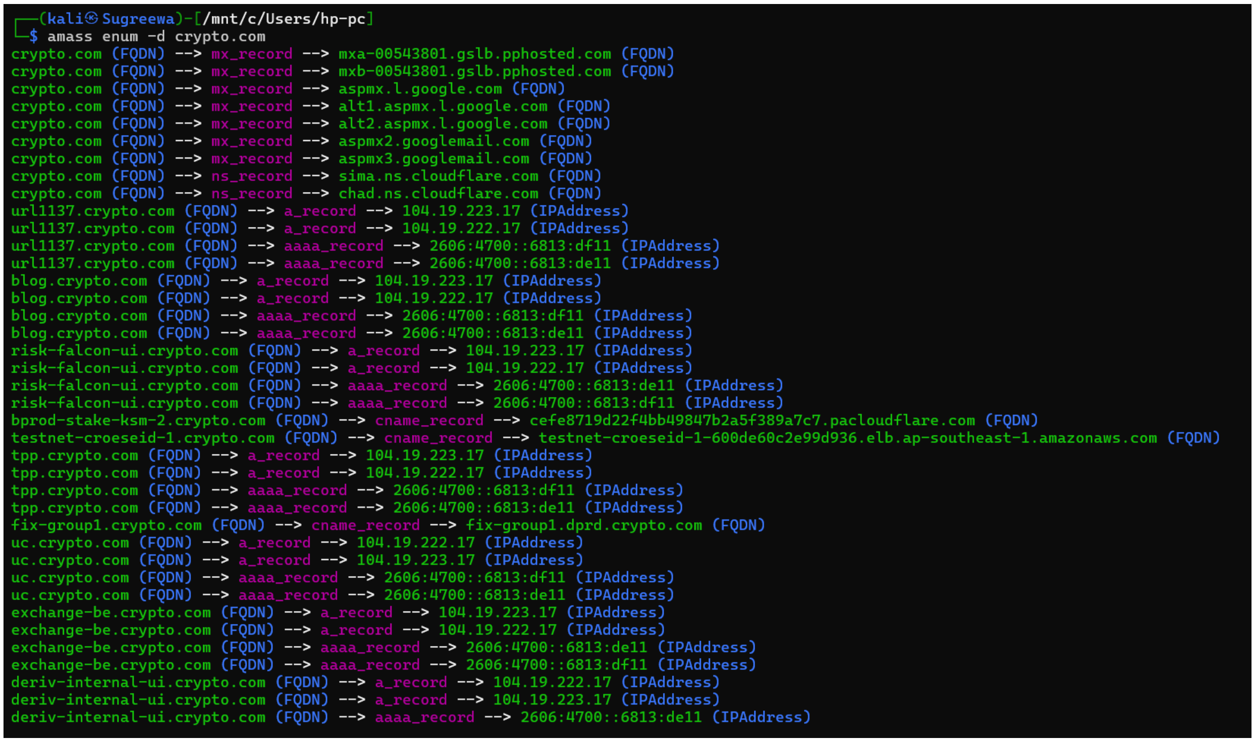
Website: https://crypto.com/

Sub-domain: https://merchant.crypto.com/users/sign_in

Listed by: Crypto.com

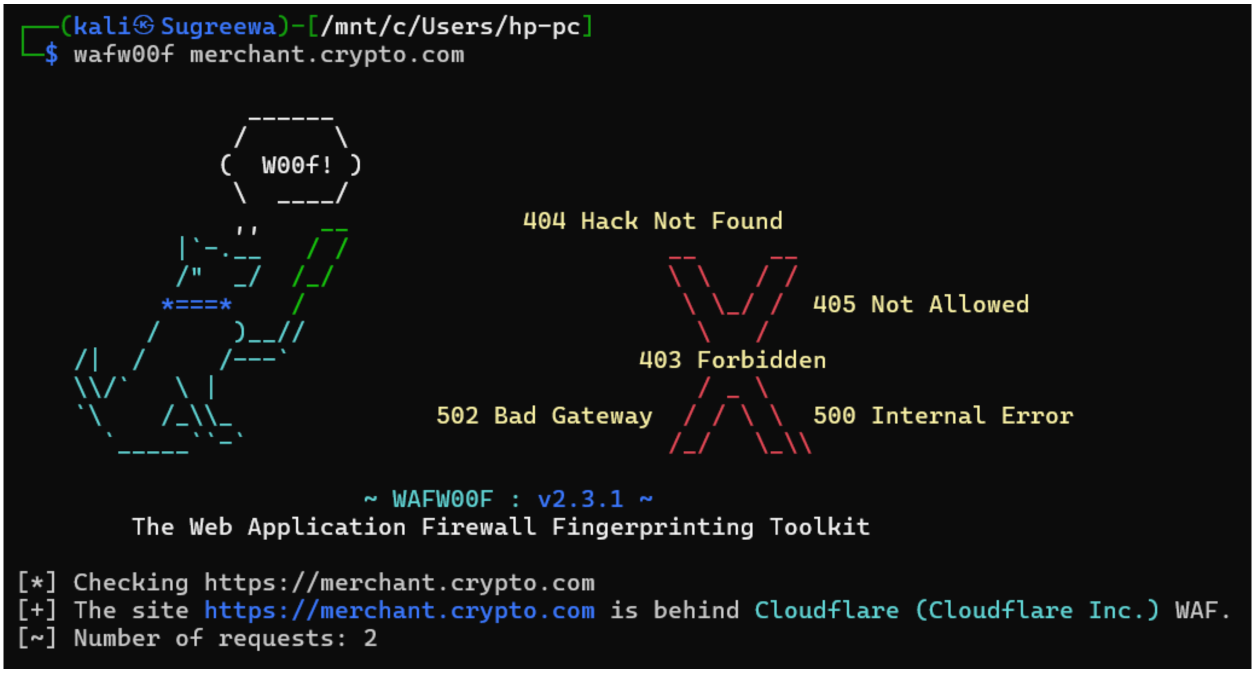
2. Reconnaissance

- **Subdomain enumeration using Amass**



```
┌──(kali㉿Sugreewa)-[/mnt/c/Users/hp-pc]
└─$ amass enum -d crypto.com
crypto.com (FQDN) --> mx_record --> mxa-00543801.gslb.pphosted.com (FQDN)
crypto.com (FQDN) --> mx_record --> mxb-00543801.gslb.pphosted.com (FQDN)
crypto.com (FQDN) --> mx_record --> aspmx.l.google.com (FQDN)
crypto.com (FQDN) --> mx_record --> alt1.aspmx.l.google.com (FQDN)
crypto.com (FQDN) --> mx_record --> alt2.aspmx.l.google.com (FQDN)
crypto.com (FQDN) --> mx_record --> aspmx2.googlemail.com (FQDN)
crypto.com (FQDN) --> mx_record --> aspmx3.googlemail.com (FQDN)
crypto.com (FQDN) --> ns_record --> sima.ns.cloudflare.com (FQDN)
crypto.com (FQDN) --> ns_record --> chad.ns.cloudflare.com (FQDN)
url1137.crypto.com (FQDN) --> a_record --> 104.19.223.17 (IPAddress)
url1137.crypto.com (FQDN) --> a_record --> 104.19.222.17 (IPAddress)
url1137.crypto.com (FQDN) --> aaaa_record --> 2606:4700::6813:df11 (IPAddress)
url1137.crypto.com (FQDN) --> aaaa_record --> 2606:4700::6813:de11 (IPAddress)
blog.crypto.com (FQDN) --> a_record --> 104.19.223.17 (IPAddress)
blog.crypto.com (FQDN) --> a_record --> 104.19.222.17 (IPAddress)
blog.crypto.com (FQDN) --> aaaa_record --> 2606:4700::6813:df11 (IPAddress)
blog.crypto.com (FQDN) --> aaaa_record --> 2606:4700::6813:de11 (IPAddress)
risk-falcon-ui.crypto.com (FQDN) --> a_record --> 104.19.223.17 (IPAddress)
risk-falcon-ui.crypto.com (FQDN) --> a_record --> 104.19.222.17 (IPAddress)
risk-falcon-ui.crypto.com (FQDN) --> aaaa_record --> 2606:4700::6813:de11 (IPAddress)
risk-falcon-ui.crypto.com (FQDN) --> aaaa_record --> 2606:4700::6813:df11 (IPAddress)
bprod-stake-ksm-2.crypto.com (FQDN) --> cname_record --> cefe8719d22f4bb49847b2a5f389a7c7.pacloudflare.com (FQDN)
testnet-croeseid-1.crypto.com (FQDN) --> cname_record --> testnet-croeseid-1-600de60c2e99d936.elb.ap-southeast-1.amazonaws.com (FQDN)
tpp.crypto.com (FQDN) --> a_record --> 104.19.223.17 (IPAddress)
tpp.crypto.com (FQDN) --> a_record --> 104.19.222.17 (IPAddress)
tpp.crypto.com (FQDN) --> aaaa_record --> 2606:4700::6813:df11 (IPAddress)
tpp.crypto.com (FQDN) --> aaaa_record --> 2606:4700::6813:de11 (IPAddress)
fix-group1.crypto.com (FQDN) --> cname_record --> fix-group1.dprd.crypto.com (FQDN)
uc.crypto.com (FQDN) --> a_record --> 104.19.222.17 (IPAddress)
uc.crypto.com (FQDN) --> a_record --> 104.19.223.17 (IPAddress)
uc.crypto.com (FQDN) --> aaaa_record --> 2606:4700::6813:df11 (IPAddress)
uc.crypto.com (FQDN) --> aaaa_record --> 2606:4700::6813:de11 (IPAddress)
exchange-be.crypto.com (FQDN) --> a_record --> 104.19.223.17 (IPAddress)
exchange-be.crypto.com (FQDN) --> a_record --> 104.19.222.17 (IPAddress)
exchange-be.crypto.com (FQDN) --> aaaa_record --> 2606:4700::6813:de11 (IPAddress)
exchange-be.crypto.com (FQDN) --> aaaa_record --> 2606:4700::6813:df11 (IPAddress)
deriv-internal-ui.crypto.com (FQDN) --> a_record --> 104.19.222.17 (IPAddress)
deriv-internal-ui.crypto.com (FQDN) --> a_record --> 104.19.223.17 (IPAddress)
deriv-internal-ui.crypto.com (FQDN) --> aaaa_record --> 2606:4700::6813:de11 (IPAddress)
```

- **Firewall detection**



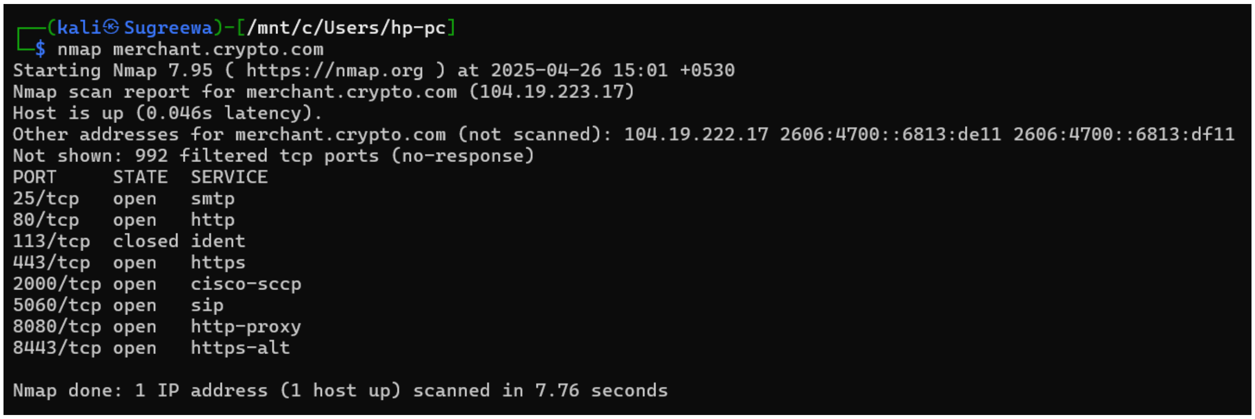
```
┌──(kali㉿Sugreewa)-[/mnt/c/Users/hp-pc]
└─$ wafw00f merchant.crypto.com

                ______
               /      \
              (  W00f! )
               \  ____/
               ,,    __            404 Hack Not Found
           |`-.__   / /                      __     __
           /"  _/  /_/                       \ \   / /
          *====*    /                          \ \_/ /  405 Not Allowed
         /     )__//                           \   /
    /|  /     /---`                        403 Forbidden
    \\/`   \ |                                 / _ \
    `\    /_\\_              502 Bad Gateway  / / \ \  500 Internal Error
      `_____``-`                             /_/   \_\\

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

[*] Checking https://merchant.crypto.com
[+] The site https://merchant.crypto.com is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2
```

- **Nmap Scan**

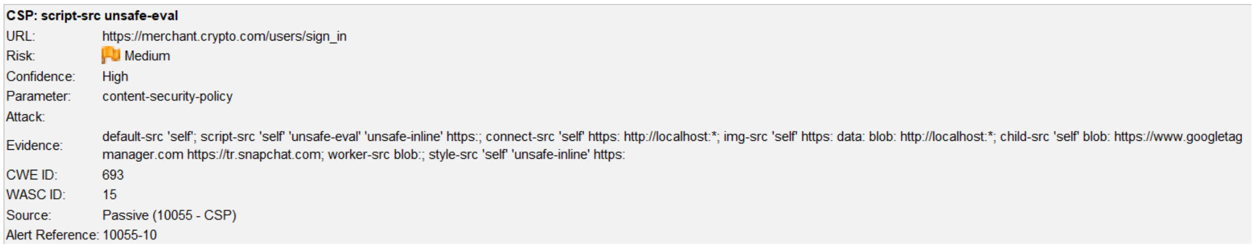


```
┌──(kali㉿Sugreewa)-[/mnt/c/Users/hp-pc]
└─$ nmap merchant.crypto.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-26 15:01 +0530
Nmap scan report for merchant.crypto.com (104.19.223.17)
Host is up (0.046s latency).
Other addresses for merchant.crypto.com (not scanned): 104.19.222.17 2606:4700::6813:de11 2606:4700::6813:df11
Not shown: 992 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
8080/tcp open   http-proxy
8443/tcp open   https-alt

Nmap done: 1 IP address (1 host up) scanned in 7.76 seconds
```

3. Vulnerability

- **CSP: script-src unsafe-eval**



CSP: script-src unsafe-eval

URL:	https://merchant.crypto.com/users/sign_in
Risk:	Medium
Confidence:	High
Parameter:	content-security-policy
Attack:	
Evidence:	default-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline' https:; connect-src 'self' https: http://localhost:*; img-src 'self' https: data: blob: http://localhost:*; child-src 'self' blob: https://www.googletagmanager.com https://tr.snapchat.com; worker-src blob:; style-src 'self' 'unsafe-inline' https:
CWE ID:	693
WASC ID:	15
Source:	Passive (10055 - CSP)
Alert Reference:	10055-10

4. Vulnerability description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

5. Affected Components

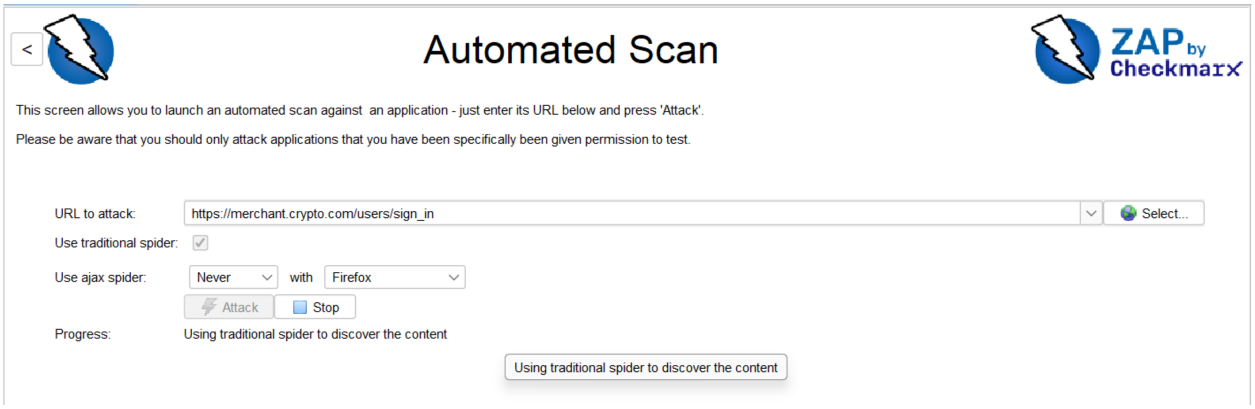
- **Component:** HTTP Response Header → Content-Security-Policy
- **Current Policy:**
  - script-src 'self' 'unsafe-eval' 'unsafe-inline' https:;
- **Directive Affected:** script-src
- **Risk Element:** Presence of 'unsafe-eval'

6. Impact Assessment

- **Risk Level:** High
- **Potential Impacts:**
  - Enables execution of injected scripts using eval()-based functions
  - Increases susceptibility to XSS, especially in apps that manipulate or parse user input dynamically
  - May allow malicious scripts to bypass filtering mechanisms
  - Violates strong CSP enforcement, failing compliance checks (e.g., PCI-DSS, OWASP)

7. Steps to reproduce

- Use browser **DevTools** or **ZAP/Burp** to inspect any page response.



Automated Scan

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://merchant.crypto.com/users/sign_in

Use traditional spider: ☑

Use ajax spider: Never with Firefox

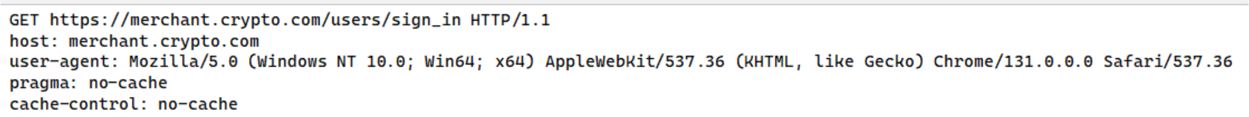
Progress: Using traditional spider to discover the content

Using traditional spider to discover the content

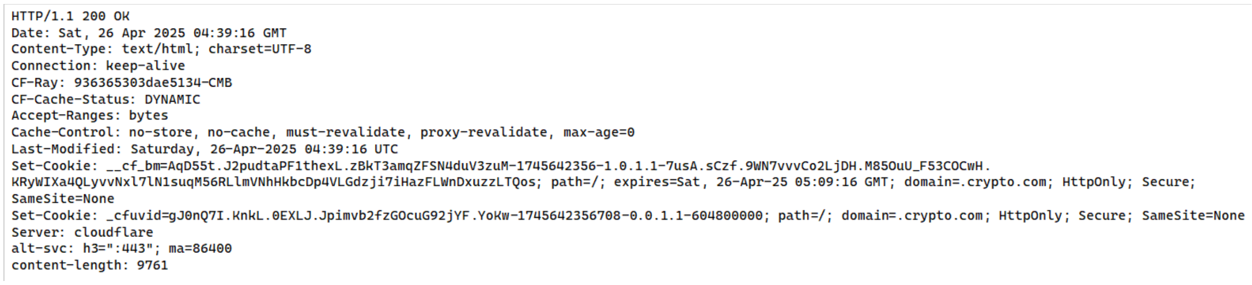
- Locate the Content-Security-Policy response header.
- Confirm the presence of:
  - script-src 'self' 'unsafe-eval' ...

- (Optional) Test usage of eval() in inline or loaded scripts and verify it executes without errors.

8. Proof of concept



```
GET https://merchant.crypto.com/users/sign_in HTTP/1.1
host: merchant.crypto.com
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
pragma: no-cache
cache-control: no-cache
```



```
HTTP/1.1 200 OK
Date: Sat, 26 Apr 2025 04:39:16 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
CF-Ray: 936365303dae5134-CMB
CF-Cache-Status: DYNAMIC
Accept-Ranges: bytes
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate, max-age=0
Last-Modified: Saturday, 26-Apr-2025 04:39:16 UTC
Set-Cookie: __cf_bm=AqD55t.J2pudtaPF1thexL.zBkT3amqZFSN4duV3zuM-1745642356-1.0.1.1-7usA.sCzf.9WN7vvvCo2LjDH.M85OuU_F53COCwH.
KRyWIXa4QLyvvNxl7lN1suqM56RLlmVNhHkbcDp4VLGdzji7iHazFLWnDxuzzLTQos; path=/; expires=Sat, 26-Apr-25 05:09:16 GMT; domain=.crypto.com; HttpOnly; Secure;
SameSite=None
Set-Cookie: _cfuvid=gJ0nQ7I.KnkL.0EXLJ.Jpimvb2fzGOcuG92jYF.YoKw-1745642356708-0.0.1.1-604800000; path=/; domain=.crypto.com; HttpOnly; Secure; SameSite=None
Server: cloudflare
alt-svc: h3=":443"; ma=86400
content-length: 9761
```

9. Proposed mitigation or fix

Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.