



**Sri Lanka Institute of Information Technology**

**IE2062 - Web Security**

**Final Assignment**

**Bug Bounty Report 08**

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

**Registration Number:** IT23227286

## Contents

1. Introduction.....	3
2. Reconnaissance .....	4
3. Vulnerability .....	6
4. Vulnerability description.....	6
5. Affected Components .....	7
6. Impact Assessment.....	7
7. Steps to reproduce.....	8
8. Proof of concept.....	9
9. Proposed mitigation or fix .....	9

# 1. Introduction

If you are unsure of whether a report would be in-scope, you can either email us at [hackerone@crypto.com](mailto:hackerone@crypto.com) or submit your report here anyway.

Search

Scope

All scopes

Maximum severity

Any

Bounty eligibility

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 ↓
web.crypto.com	Domain	In scope	Critical
*.crypto.com We will consider all vulnerability reports against assets in Crypto.com's control. Severity might be limited for certain assets based on business impact.	Wildcard	In scope	Critical
com.monaco.mobile	iOS: App Store	In scope	High

[@crypto.com](https://crypto.com)  
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 Avg. bounty \$428 37.87% submissions	\$200-\$500
Medium Avg. bounty \$2,424	\$500-\$5,000

**Website:** <https://web.crypto.com/login>

**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.pac.cloudflare.com (FQDN)
testnet-croeseid-1.crypto.com (FQDN) --> cname_record --> testnet-croeseid-1-608de60c2e99d936.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 web.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://web.crypto.com
[+] The site https://web.crypto.com is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2

```

- Nmap Scan

```
(kali@Sugreewa)-[/mnt/c/Users/hp-pc]
$ nmap web.crypto.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-26 15:04 +0530
Nmap scan report for web.crypto.com (104.19.223.17)
Host is up (0.019s latency).
Other addresses for web.crypto.com (not scanned): 104.19.222.17 2606:4700::6813:df11 2606:4700::6813:de11
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 5.32 seconds
```

### 3. Vulnerability

- **CSP: Wildcard Directive**

#### **CSP: Wildcard Directive**

URL: <https://web.crypt0.com/login>  
Risk: 🟡 Medium  
Confidence: High  
Parameter: content-security-policy  
Attack:  
Evidence: frame-ancestors 'self'; upgrade-insecure-requests|  
CWE ID: 693  
WASC ID: 15  
Source: Passive (10055 - CSP)  
Alert Reference: 10055-4

### 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

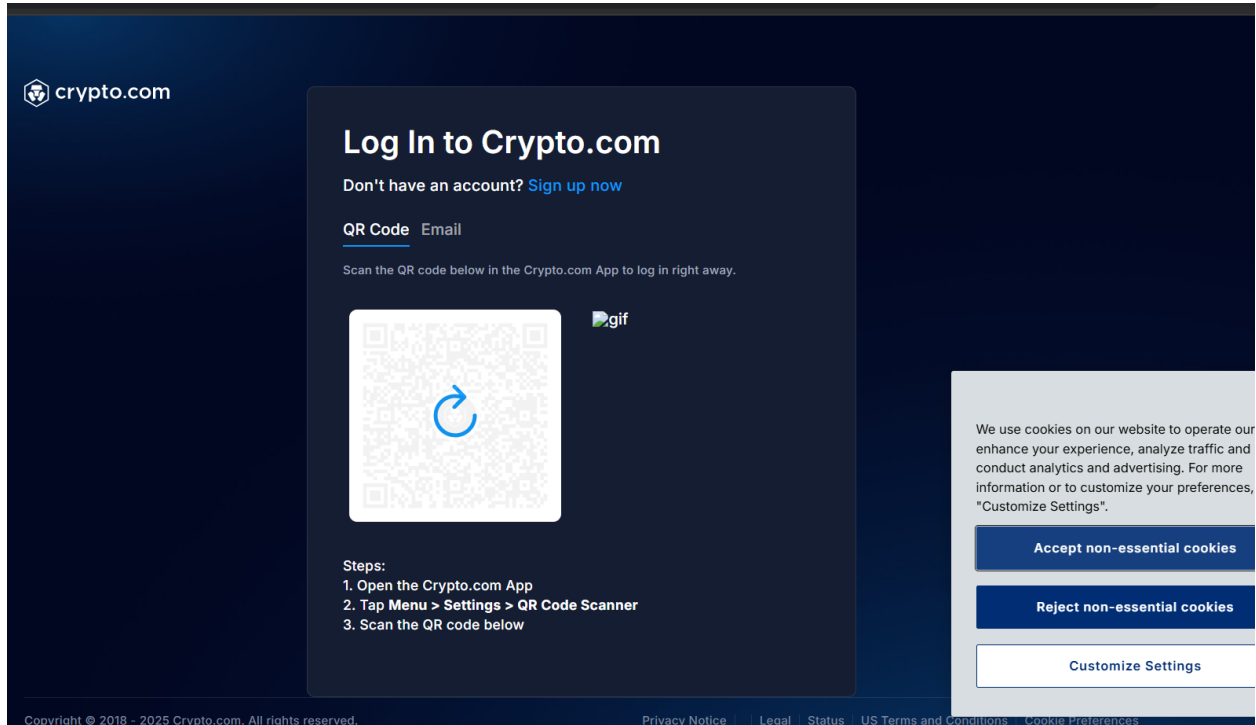
- **Component:** HTTP Response Header → Content-Security-Policy
- **Current Policy:**
  - frame-ancestors 'self'; upgrade-insecure-requests;
- **Missing or Overly Broad Directives:**
  - Script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
- **Impacted Pages:** All pages where this CSP header is applied.

## 6. Impact Assessment

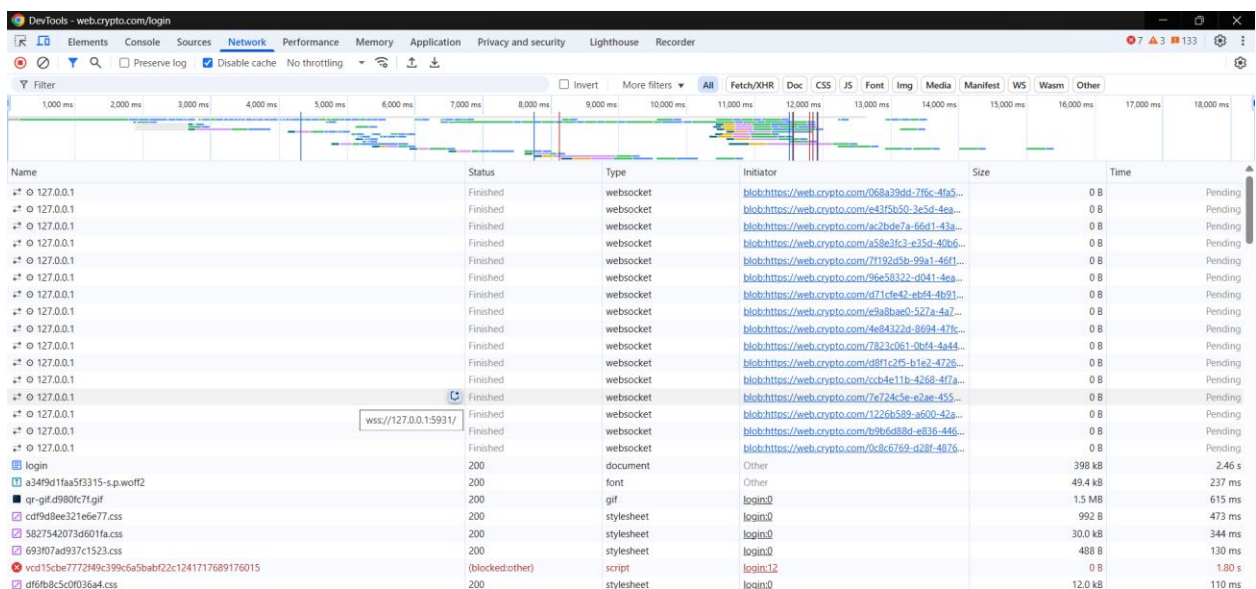
- **Risk Level:** Medium
- **Potential Impacts:**
  - Insufficient restriction on where resources can be loaded from
  - Allows injection or execution of malicious scripts, styles, or media from untrusted sources
  - Reduced protection against XSS and malicious third-party content
  - Increases exposure to client-side attacks and data leaks

## 7. Steps to reproduce

- Open the affected site in a browser.



- Open Developer Tools → Network tab → Reload the page.





- Inspect the Content-Security-Policy response header.

🌐 127.0.0.1	LT-Cache-Status:	DYNAMIC
login	Cf-Ray:	9397ecef8dc05132-CMB
a34f9d1faa5f3315-s.p.woff2	Content-Encoding:	br
qr-gif.d980fc7f.gif	Content-Security-Policy:	frame-ancestors 'self'; upgrade-insecure-requests; ✎
cdf9d8ee321e6e77.css	Content-Type:	text/html; charset=utf-8
5827542073d601fa.css	Date:	Fri, 02 May 2025 13:39:36 GMT
693f07ad937c1523.css	Link:	<https://web-static.crypto.com/_next/static/media/a34f9d1faa5f3315-s.p.woff2>; rel=preload; as=font; crossorigin=""
vcd15cbe7772f49c399c6a5...	Referrer-Policy:	strict-origin-when-cross-origin
df6fb8c5c0f036a4.css	Server:	cloudflare
	Server-Timing:	cfCacheStatus;desc="DYNAMIC"

- Confirm the presence of a **limited or incomplete CSP** (e.g., frame-ancestors 'self' only).
- Note the absence or wildcards (\*) in key directives like script-src, style-src, etc.

## 8. Proof of concept

```
GET https://web.crypto.com/login HTTP/1.1
host: web.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: Fri, 25 Apr 2025 16:12:38 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
strict-transport-security: max-age=63072000; includeSubDomains; preload
x-dns-prefetch-control: on
x-content-type-options: nosniff
referrer-policy: strict-origin-when-cross-origin
content-security-policy: frame-ancestors 'self'; upgrade-insecure-requests;
vary: RSC, Next-Router-State-Tree, Next-Router-Prefetch, Accept-Encoding
link: <https://web-static.crypto.com/_next/static/media/a34f9d1faa5f3315-s.p.woff2>; rel=preload; as="font"; crossorigin=""
Cache-Control: private, no-cache, no-store, max-age=0, must-revalidate
cf-cache-status: DYNAMIC
Set-Cookie: __cf_bm=12XxYRgvnNjBngTq7MN5.lnwovrpvirLT5AIXYf84UQ-1745597558-1.0.1.1-xwupd6NSG7fab77wHtnSOCfFHDBM4toSAhUtMb_otyXf5EeSb7AqiE1tpzg0D2hf9QZE5aQiJ05Pp63VmyEIPNxmHmsY27MHVOxubfsQeIO8; path=/; expires=Fri, 25-Apr-25 16:42:38 GMT; domain=.crypto.com; HttpOnly; Secure; SameSite=None
Set-Cookie: _cfuvid=846uboPMTq4S8lbbIgbZ8bTBR1l9afoe1BjJ0JvPcKk-1745597558811-0.0.1.1-604800000; path=/; domain=.crypto.com; HttpOnly; Secure; SameSite=None
Server: cloudflare
CF-RAY: 935f1f849bea87ef-SIN
alt-svc: h3=":443"; ma=86400
content-length: 2039818
```

## 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.