**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](#_Toc197105960)

[2. Reconnaissance 4](#_Toc197105961)

[3. Vulnerability 6](#_Toc197105962)

[4. Vulnerability description 6](#_Toc197105963)

[5. Affected Components 7](#_Toc197105964)

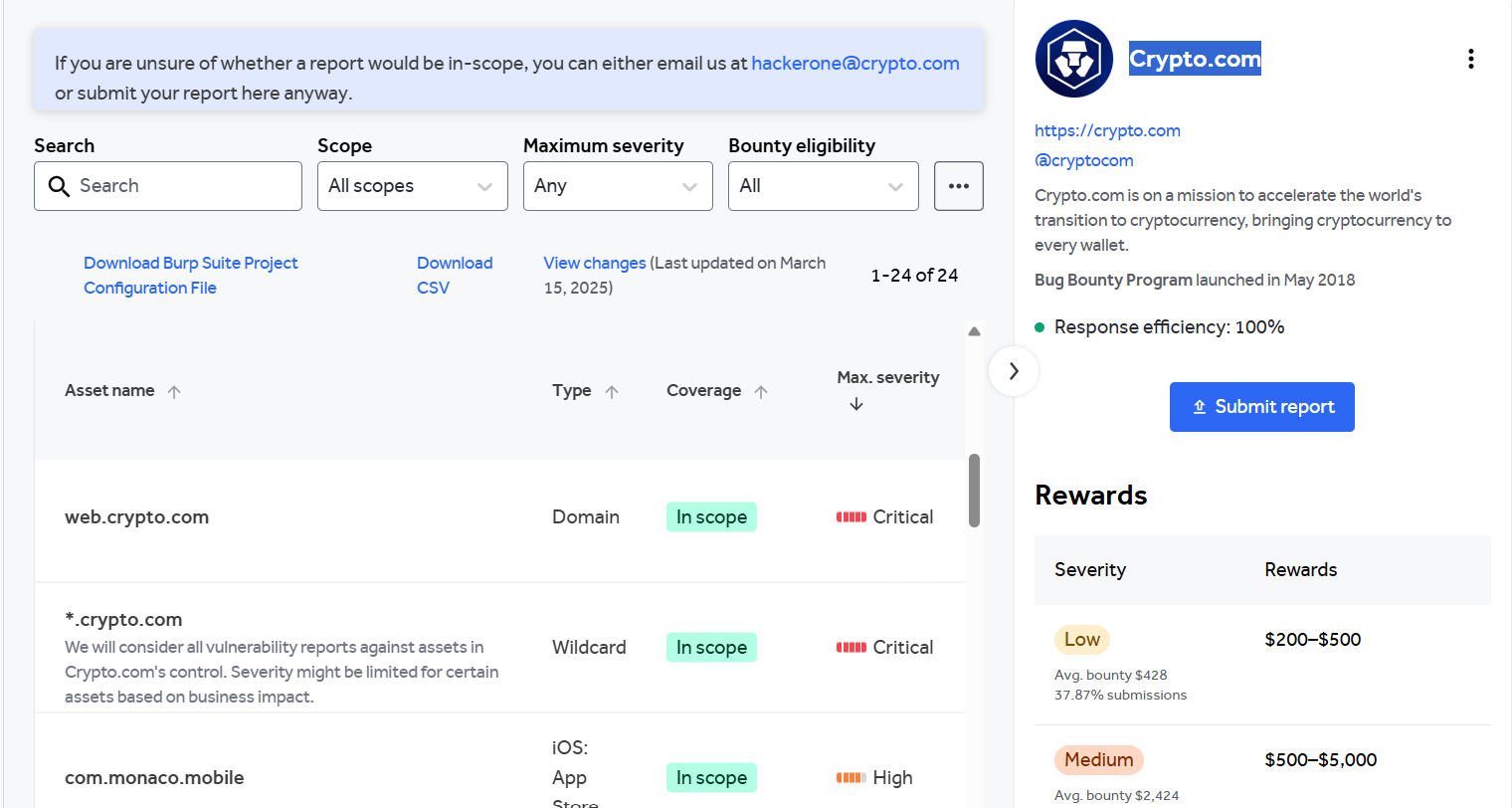
[6. Impact Assessment 7](#_Toc197105965)

[7. Steps to reproduce 8](#_Toc197105966)

[8. Proof of concept 9](#_Toc197105967)

[9. Proposed mitigation or fix 9](#_Toc197105968)

# Introduction

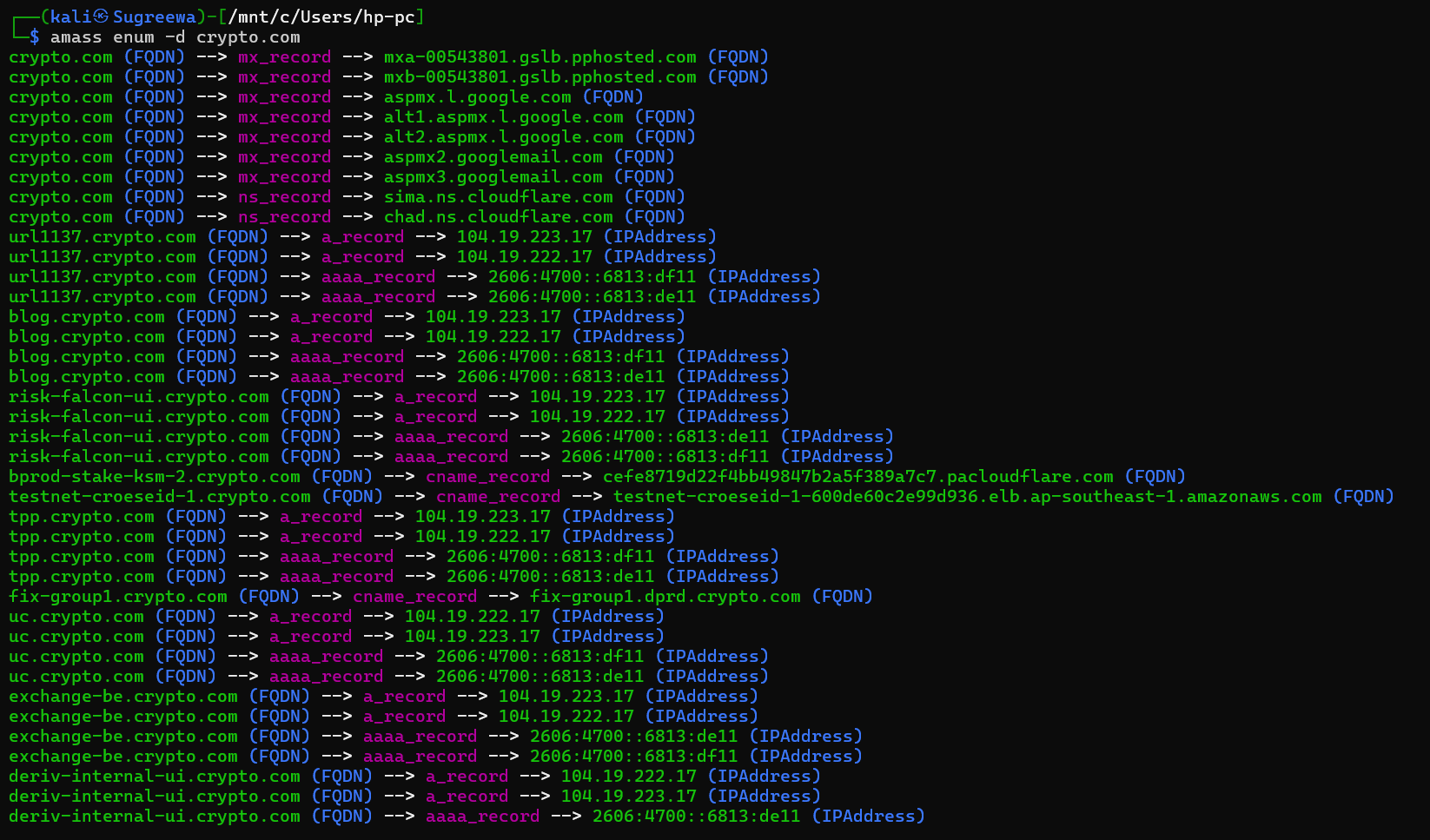


**Website:** <https://web.crypto.com/login>

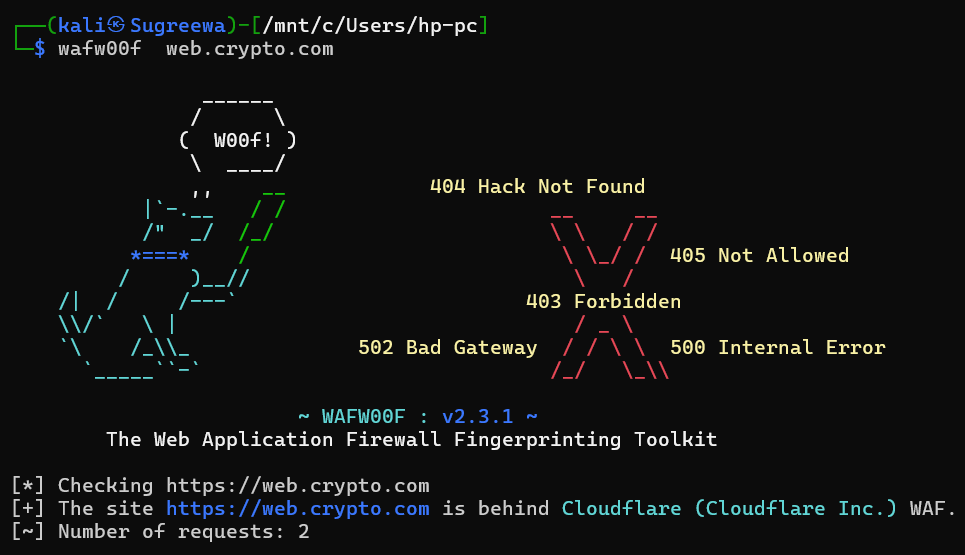
**Listed by:** Crypto.com

# Reconnaissance

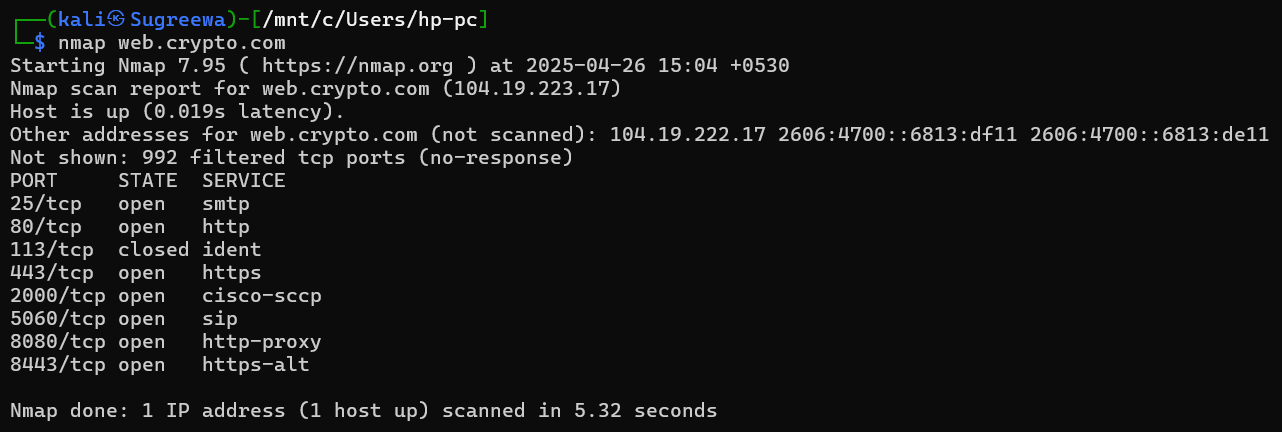
* **Subdomain enumeration using Amass**

****

* **Firewall Detection**

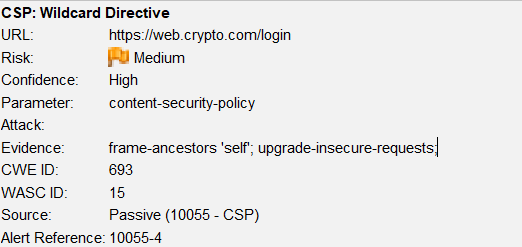
****

* **Nmap Scan**

****

# Vulnerability

* **CSP: Wildcard Directive**

****

# 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.

1. Affected Components

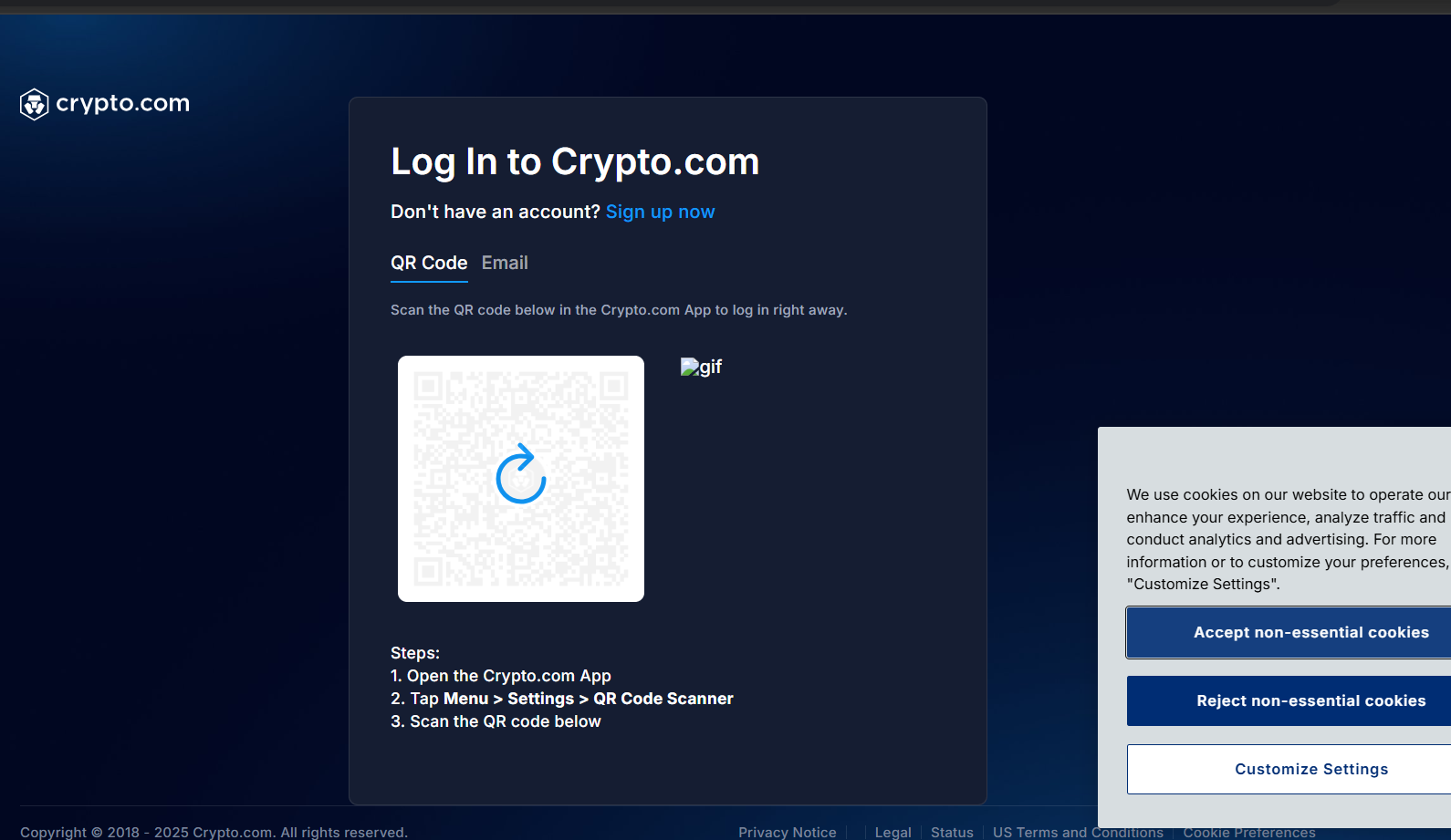
* **Component:** HTTP Response Header → Content-Security-Policy
* **Current Policy:**
  + frame-ancestors ‘self’; upgrade-insecure-requests;
* **Missing or Overly Broad Directives:**
  + Script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src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

# Impact Assessment

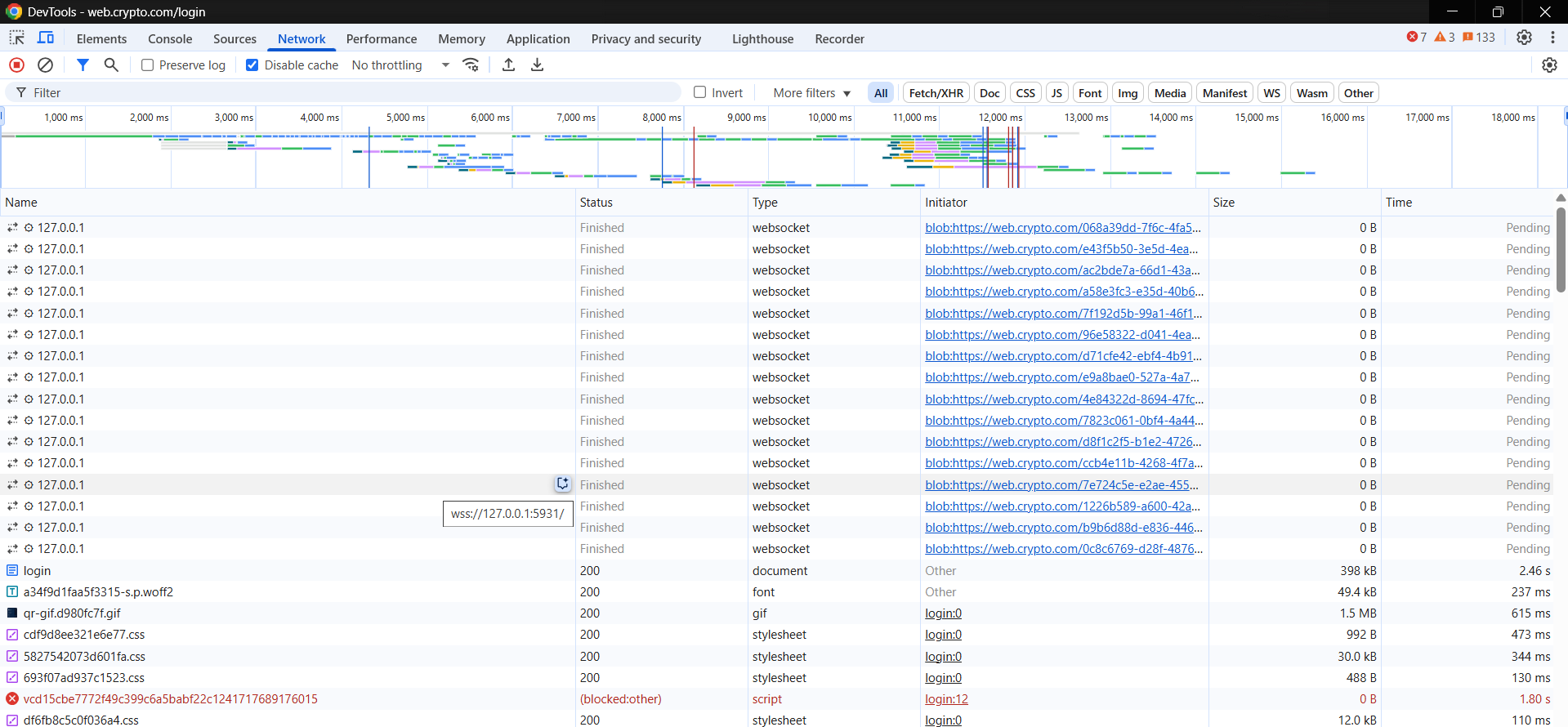
* **Risk Level:** Medium
* **Potential Impacts:**
  + Insufficient restriction on where resources can be loaded from
  + Allows injection or execution of malicious scripts, styles, or media from untrusted sources
  + Reduced protection against XSS and malicious third-party content
  + Increases exposure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

# Steps to reproduce

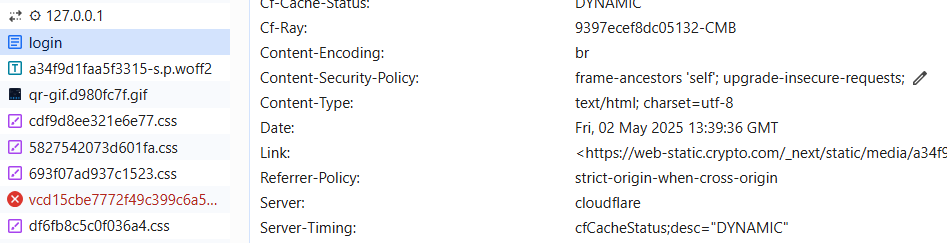
* Open the affected site in a browser.



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

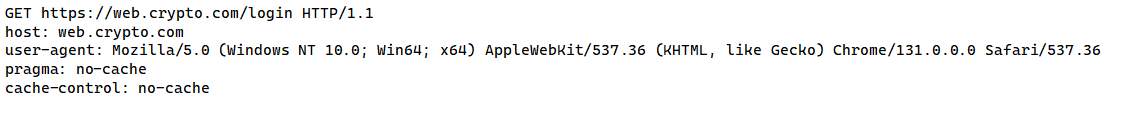


* Inspect the Content-Security-Policy response header.



* 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.

# Proof of concept





# Proposed mitigation or fix

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