**Sri Lanka Institute of Information Technology**

**IE2062 - Web Security**

**Final Assignment**

**Bug Bounty Report 02**

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

**Registration Number:** IT23227286

Contents

[1. Introduction 3](#_Toc196580172)

[2. Reconnaissance 4](#_Toc196580173)

[3. Vulnerability 6](#_Toc196580174)

[4. Vulnerability description 6](#_Toc196580175)

[5. Affected Components 7](#_Toc196580176)

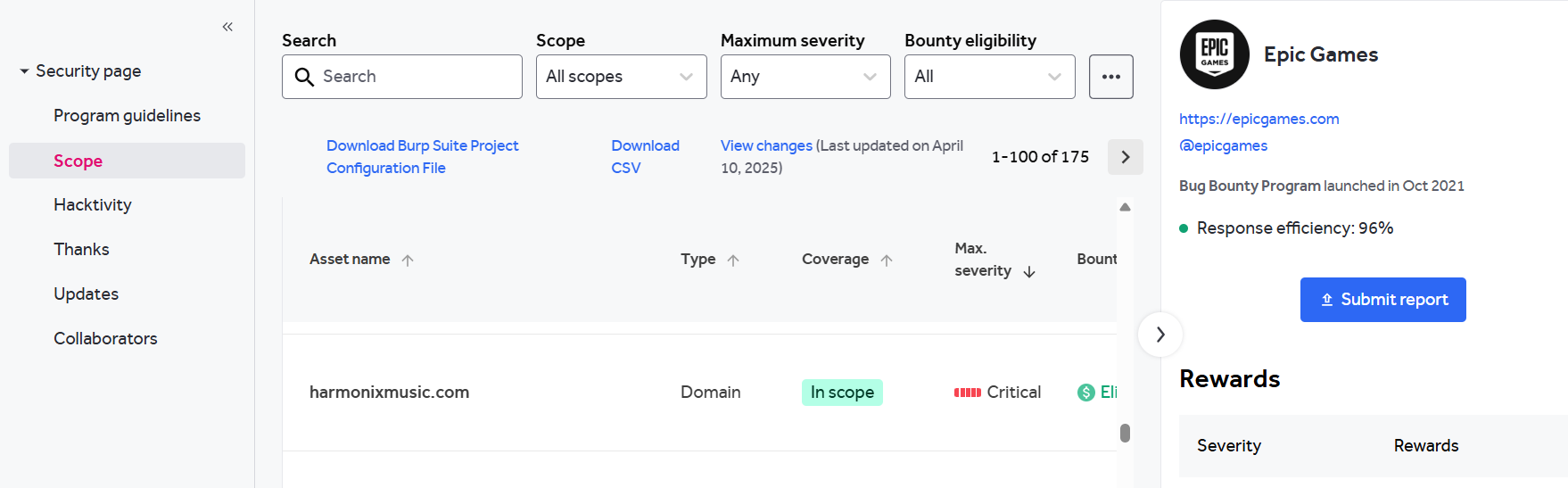
[6. Impact Assessment 7](#_Toc196580177)

[7. Steps to reproduce 8](#_Toc196580178)

[8. Proof of concept 9](#_Toc196580179)

[9. Proposed mitigation or fix 9](#_Toc196580180)

# Introduction

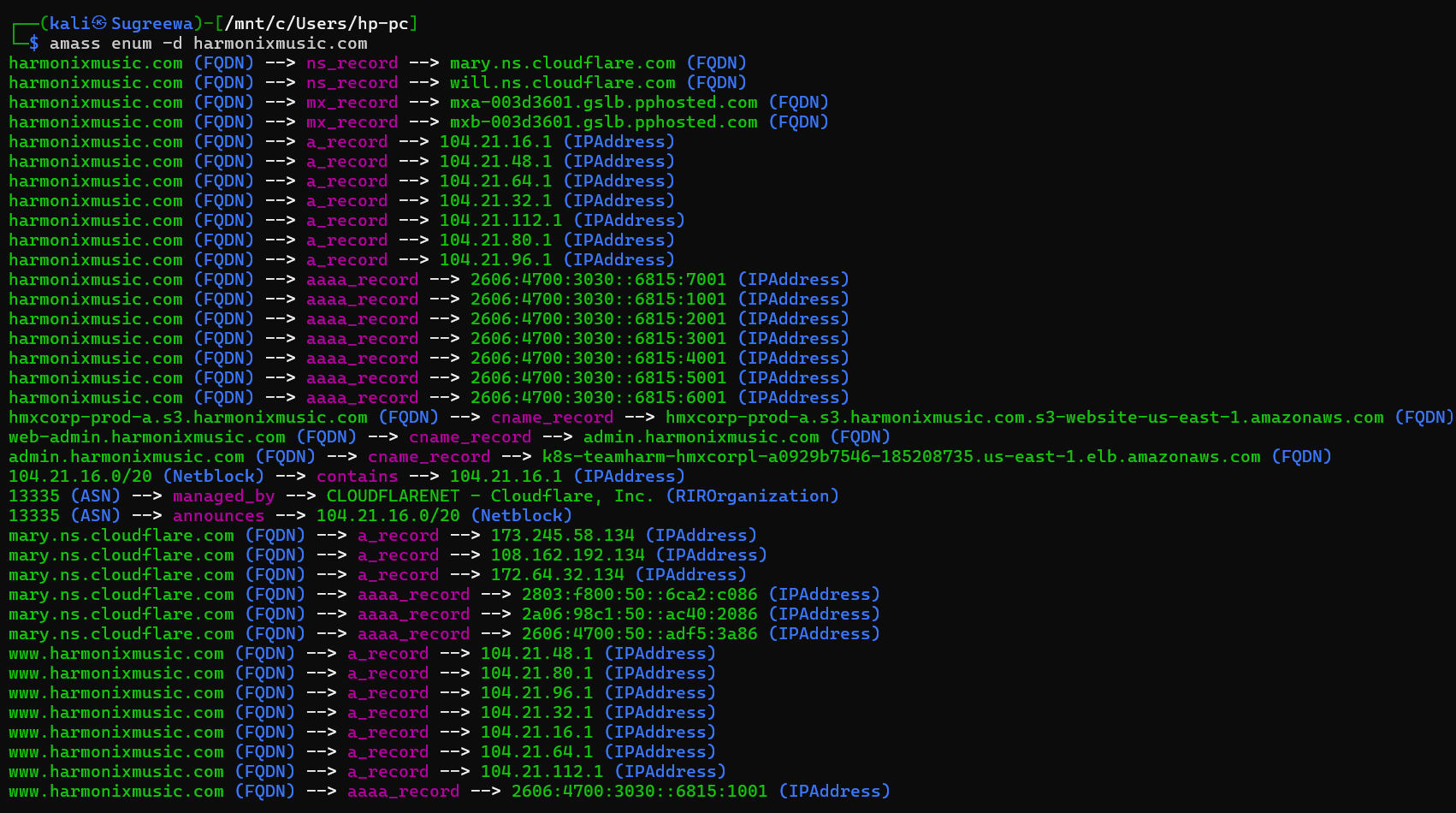


**Website:** <https://www.harmonixmusic.com/>

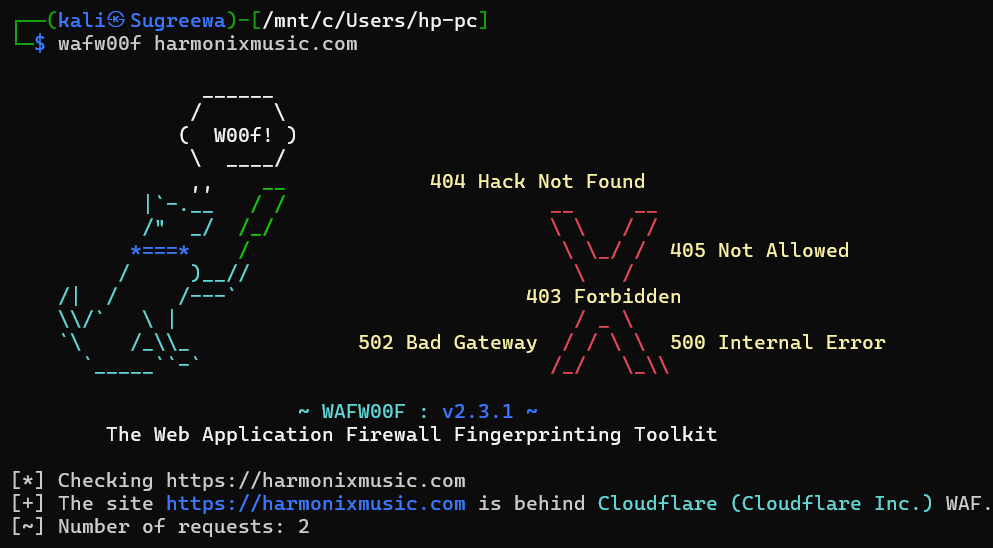
**Listed by:** Epic Games

# Reconnaissance

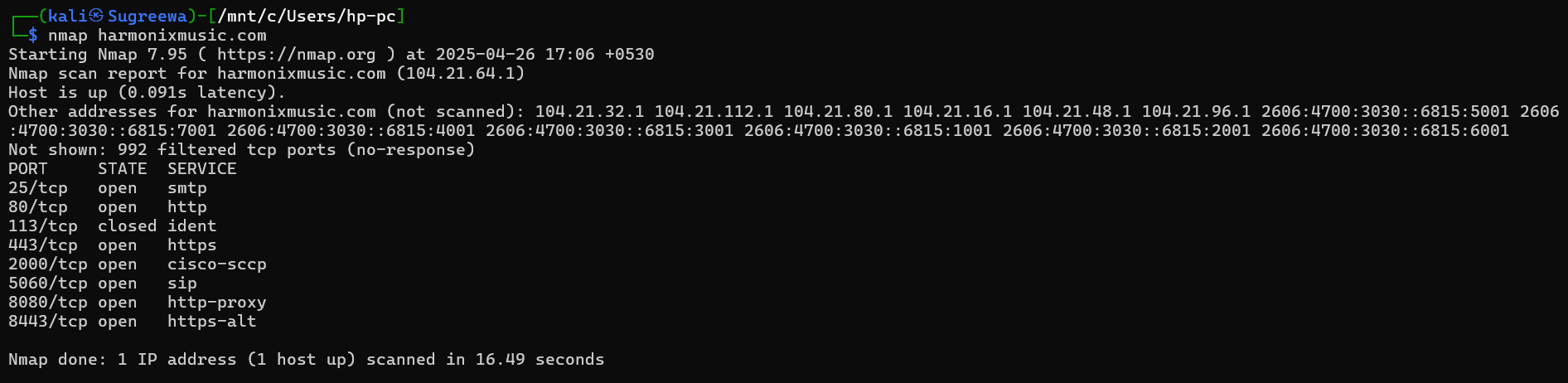
* **Subdomain enumeration using Amass**

****

* **Firewall Detection**

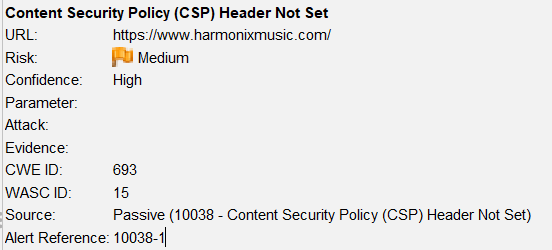
****

* **Nmap Scan**

****

# Vulnerability

* **Content Security Policy (CSP) Header Not Set**

****

# Vulnerability description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including 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 Headers
* **Header Missing:** Content-Security-Policy
* **Affected Endpoints:** <http://www.harmonixmusic.com/DropMixManiaRules/>, <http://www.harmonixmusic.com/DropMixPAXEastRules> etc.

# Impact Assessment

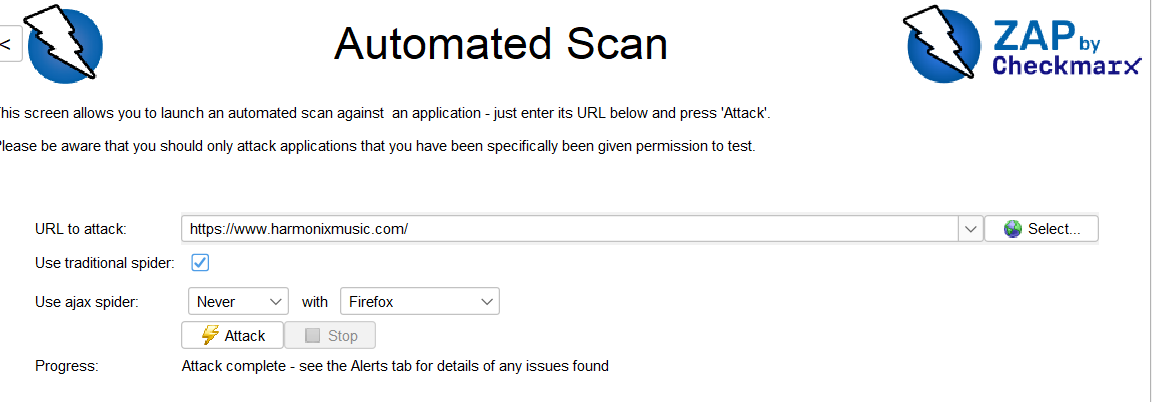
**Risk Level:** Medium

**Possible Impacts:**

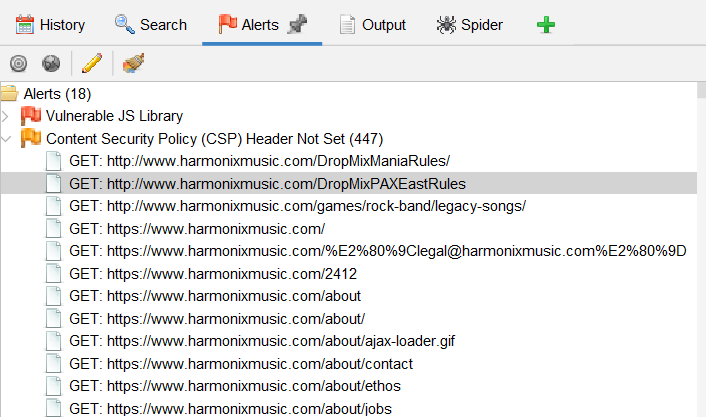
* Cross-Site Scripting (XSS) attacks
* Clickjacking
* Content injection
* Malware delivery via third-party content
* Loss of user trust and potential data breaches

# Steps to reproduce

* Open ZAP and run an active or passive scan on the target web application.



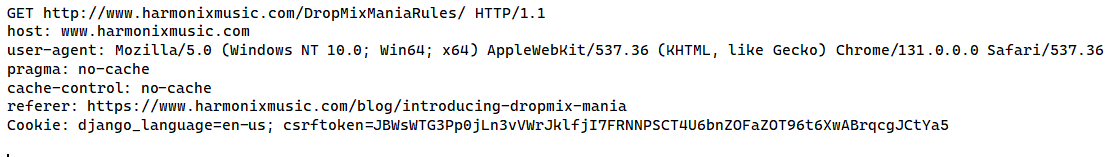
* Navigate to the **Alerts** tab in ZAP.



* Find the alert titled **"Content Security Policy (CSP) Header Not Set"**.
* Note the URLs listed where the header is missing.
* Select the page request and inspect the **Response Headers** – verify the absence of the Content-Security-Policy header.

# Proof of concept

Below is the request



Below is the response



No CSP header

# Proposed mitigation or fix

* Add a CSP header to all HTTP responses.
* If using third-party resources, update the policy
* Test with Report-Only mode before enforcing
* Use CSP tools for validation: eg: Google CSP Evaluator, [Report URI](https://report-uri.com/)