Sri Lanka Institute of Information Technology

IE2062 - Web Security

Final Assignment

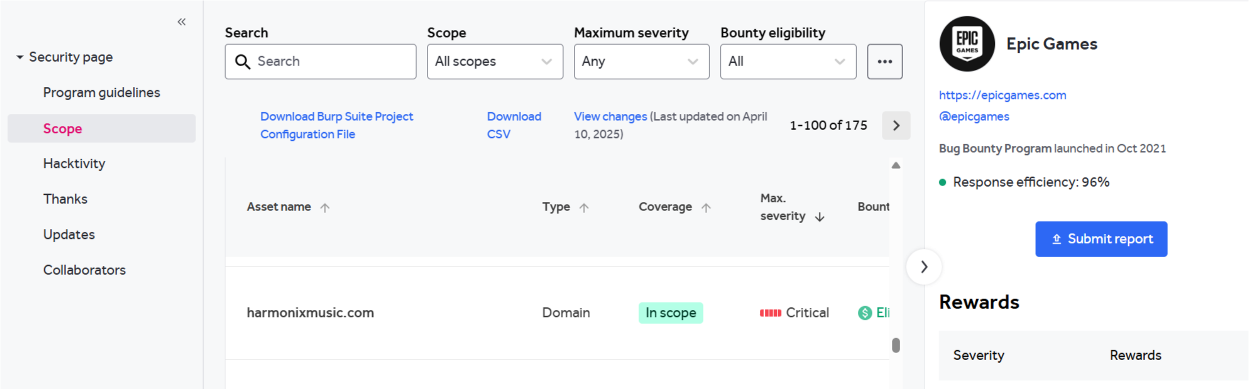
Bug Bounty Report 02

Name: Peiris W.S.S.N

Registration Number: IT23227286

Contents

1. Introduction



Search: Search

Scope: All scopes

Maximum severity: Any

Bounty eligibility: All

View changes (Last updated on April 10, 2025)

1-100 of 175

Asset name	Type	Coverage	Max. severity	Bount
harmonixmusic.com	Domain	In scope	Critical	Eli

Epic Games

https://epicgames.com

@epicgames

Bug Bounty Program launched in Oct 2021

● Response efficiency: 96%

Rewards

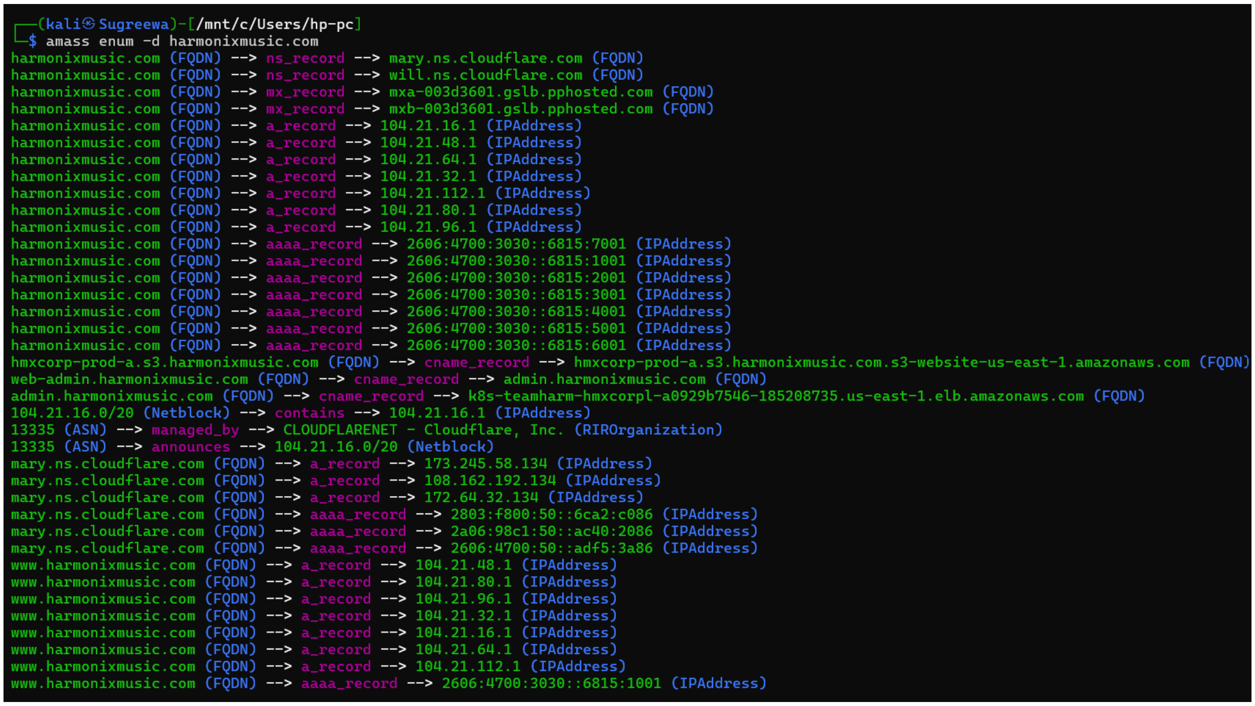
Severity	Rewards

Website: https://www.harmonixmusic.com/

Listed by: Epic Games

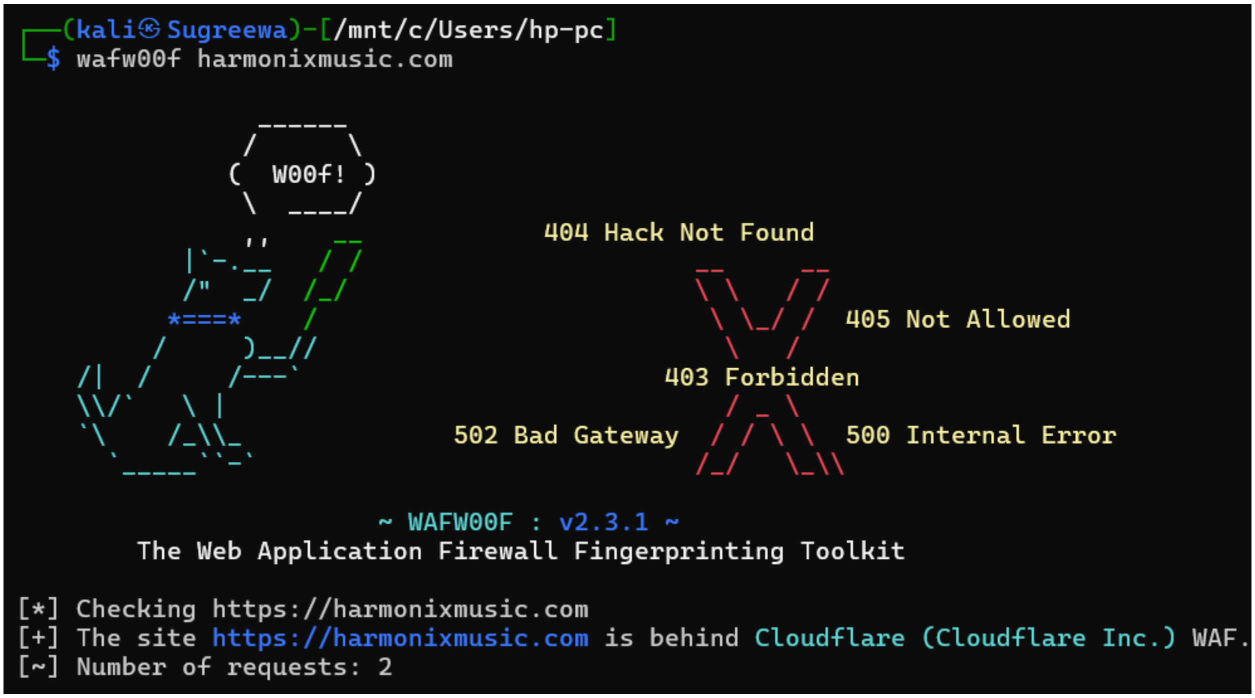
2. Reconnaissance

- **Subdomain enumeration using Amass**



```
┌──(kali㉿Sugreewa)-[/mnt/c/Users/hp-pc]
└─$ amass enum -d harmonixmusic.com
harmonixmusic.com (FQDN) --> ns_record --> mary.ns.cloudflare.com (FQDN)
harmonixmusic.com (FQDN) --> ns_record --> will.ns.cloudflare.com (FQDN)
harmonixmusic.com (FQDN) --> mx_record --> mxa-003d3601.gslb.pphosted.com (FQDN)
harmonixmusic.com (FQDN) --> mx_record --> mxb-003d3601.gslb.pphosted.com (FQDN)
harmonixmusic.com (FQDN) --> a_record --> 104.21.16.1 (IPAddress)
harmonixmusic.com (FQDN) --> a_record --> 104.21.48.1 (IPAddress)
harmonixmusic.com (FQDN) --> a_record --> 104.21.64.1 (IPAddress)
harmonixmusic.com (FQDN) --> a_record --> 104.21.32.1 (IPAddress)
harmonixmusic.com (FQDN) --> a_record --> 104.21.112.1 (IPAddress)
harmonixmusic.com (FQDN) --> a_record --> 104.21.80.1 (IPAddress)
harmonixmusic.com (FQDN) --> a_record --> 104.21.96.1 (IPAddress)
harmonixmusic.com (FQDN) --> aaaa_record --> 2606:4700:3030::6815:7001 (IPAddress)
harmonixmusic.com (FQDN) --> aaaa_record --> 2606:4700:3030::6815:1001 (IPAddress)
harmonixmusic.com (FQDN) --> aaaa_record --> 2606:4700:3030::6815:2001 (IPAddress)
harmonixmusic.com (FQDN) --> aaaa_record --> 2606:4700:3030::6815:3001 (IPAddress)
harmonixmusic.com (FQDN) --> aaaa_record --> 2606:4700:3030::6815:4001 (IPAddress)
harmonixmusic.com (FQDN) --> aaaa_record --> 2606:4700:3030::6815:5001 (IPAddress)
harmonixmusic.com (FQDN) --> aaaa_record --> 2606:4700:3030::6815:6001 (IPAddress)
hmxcorp-prod-a.s3.harmonixmusic.com (FQDN) --> cname_record --> hmxcorp-prod-a.s3.harmonixmusic.com.s3-website-us-east-1.amazonaws.com (FQDN)
web-admin.harmonixmusic.com (FQDN) --> cname_record --> admin.harmonixmusic.com (FQDN)
admin.harmonixmusic.com (FQDN) --> cname_record --> k8s-teamharm-hmxcorpl-a0929b7546-185208735.us-east-1.elb.amazonaws.com (FQDN)
104.21.16.0/20 (Netblock) --> contains --> 104.21.16.1 (IPAddress)
13335 (ASN) --> managed_by --> CLOUDFLARENET - Cloudflare, Inc. (RIROrganization)
13335 (ASN) --> announces --> 104.21.16.0/20 (Netblock)
mary.ns.cloudflare.com (FQDN) --> a_record --> 173.245.58.134 (IPAddress)
mary.ns.cloudflare.com (FQDN) --> a_record --> 108.162.192.134 (IPAddress)
mary.ns.cloudflare.com (FQDN) --> a_record --> 172.64.32.134 (IPAddress)
mary.ns.cloudflare.com (FQDN) --> aaaa_record --> 2803:f800:50::6ca2:c086 (IPAddress)
mary.ns.cloudflare.com (FQDN) --> aaaa_record --> 2a06:98c1:50::ac40:2086 (IPAddress)
mary.ns.cloudflare.com (FQDN) --> aaaa_record --> 2606:4700:50::adf5:3a86 (IPAddress)
www.harmonixmusic.com (FQDN) --> a_record --> 104.21.48.1 (IPAddress)
www.harmonixmusic.com (FQDN) --> a_record --> 104.21.80.1 (IPAddress)
www.harmonixmusic.com (FQDN) --> a_record --> 104.21.96.1 (IPAddress)
www.harmonixmusic.com (FQDN) --> a_record --> 104.21.32.1 (IPAddress)
www.harmonixmusic.com (FQDN) --> a_record --> 104.21.16.1 (IPAddress)
www.harmonixmusic.com (FQDN) --> a_record --> 104.21.64.1 (IPAddress)
www.harmonixmusic.com (FQDN) --> a_record --> 104.21.112.1 (IPAddress)
www.harmonixmusic.com (FQDN) --> aaaa_record --> 2606:4700:3030::6815:1001 (IPAddress)
```

- **Firewall Detection**



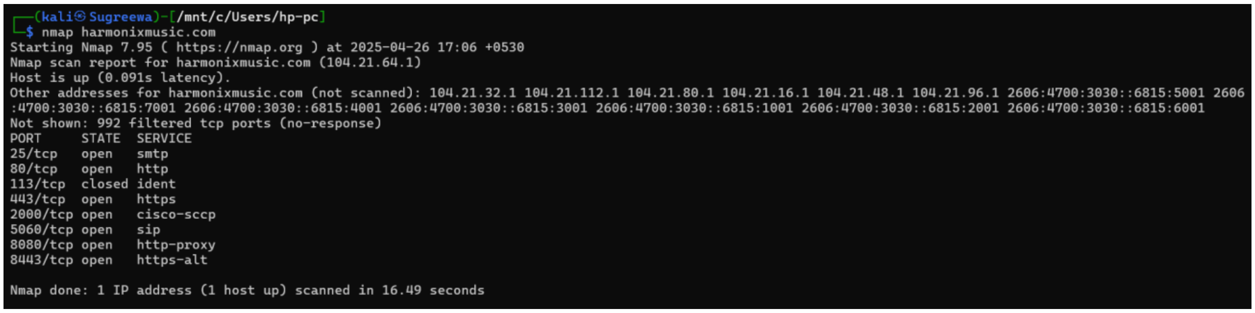
```
┌──(kali㉿Sugreewa)-[/mnt/c/Users/hp-pc]
└─$ wafw00f harmonixmusic.com

                ______
               /      \
              (  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://harmonixmusic.com
[+] The site https://harmonixmusic.com is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2
```

- **Nmap Scan**

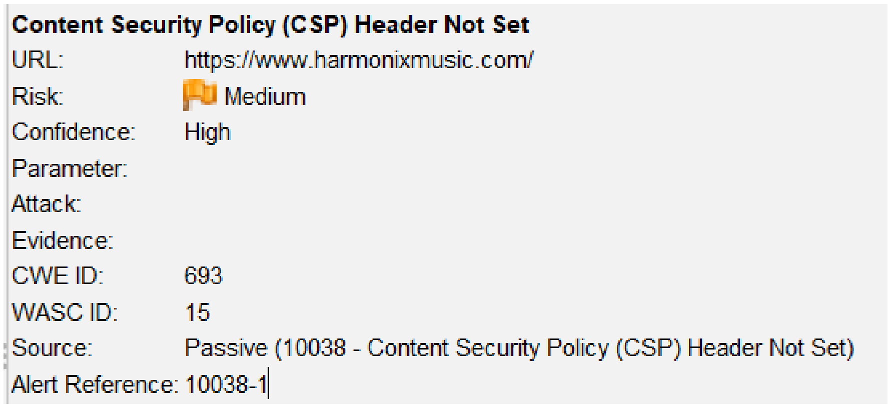


```
┌──(kali㉿Sugreewa)-[/mnt/c/Users/hp-pc]
└─$ nmap harmonixmusic.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-26 17:06 +0530
Nmap scan report for harmonixmusic.com (104.21.64.1)
Host is up (0.091s latency).
Other addresses for harmonixmusic.com (not scanned): 104.21.32.1 104.21.112.1 104.21.80.1 104.21.16.1 104.21.48.1 104.21.96.1 2606:4700:3030::6815:5001 2606
:4700:3030::6815:7001 2606:4700:3030::6815:4001 2606:4700:3030::6815:3001 2606:4700:3030::6815:1001 2606:4700:3030::6815:2001 2606:4700:3030::6815:6001
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 16.49 seconds
```

3. Vulnerability

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



Content Security Policy (CSP) Header Not Set

URL:	https://www.harmonixmusic.com/
Risk:	Medium
Confidence:	High
Parameter:	
Attack:	
Evidence:	
CWE ID:	693
WASC ID:	15
Source:	Passive (10038 - Content Security Policy (CSP) Header Not Set)
Alert Reference:	10038-1

4. 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.

5. Affected Components

- **Component:** HTTP Response Headers
- **Header Missing:** Content-Security-Policy
- **Affected Endpoints:** http://www.harmonixmusic.com/DropMixManiaRules/, http://www.harmonixmusic.com/DropMixPAXEastRules etc.

6. Impact Assessment

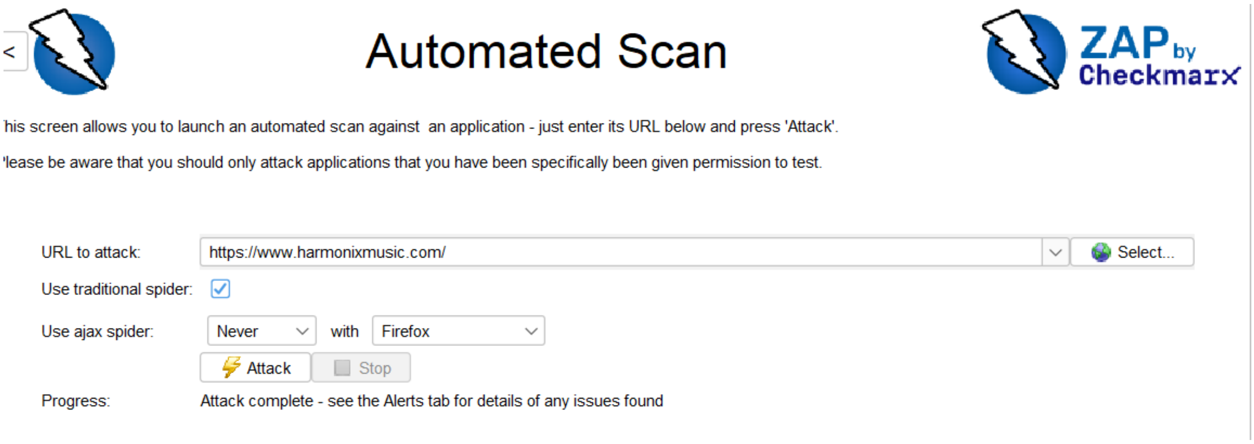
Risk Level: Medium

Possible Impacts:

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

7. Steps to reproduce

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



Automated Scan

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

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

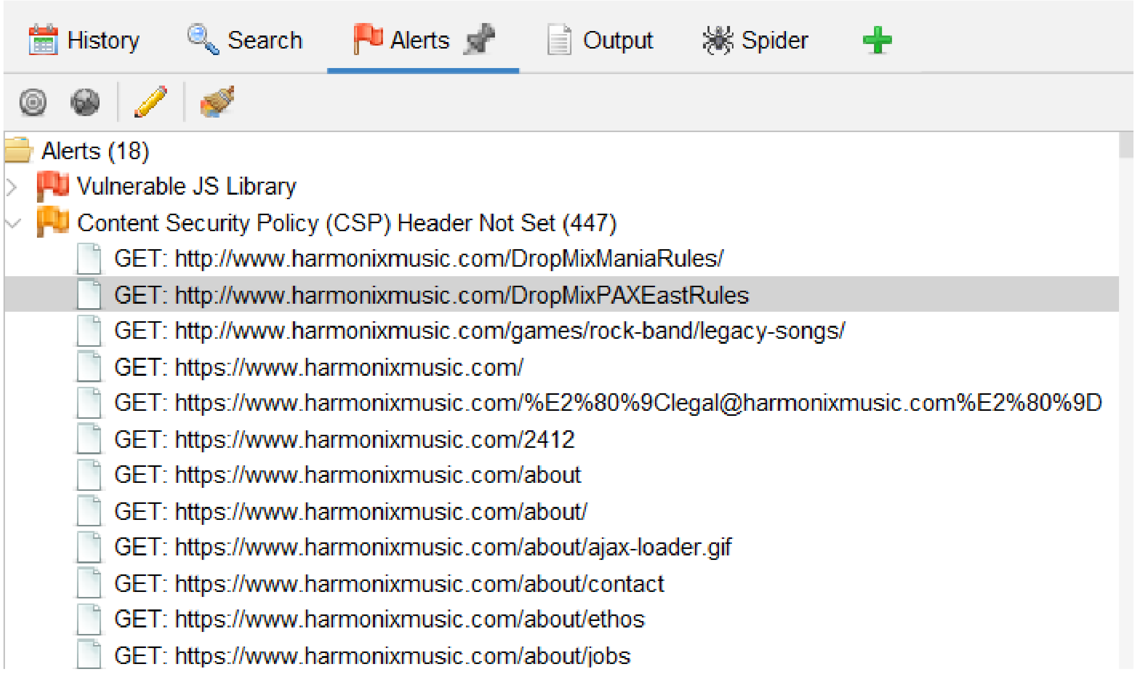
URL to attack: https://www.harmonixmusic.com/

Use traditional spider: ☑

Use ajax spider: Never with Firefox

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

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



Alerts (18)

Vulnerable JS Library

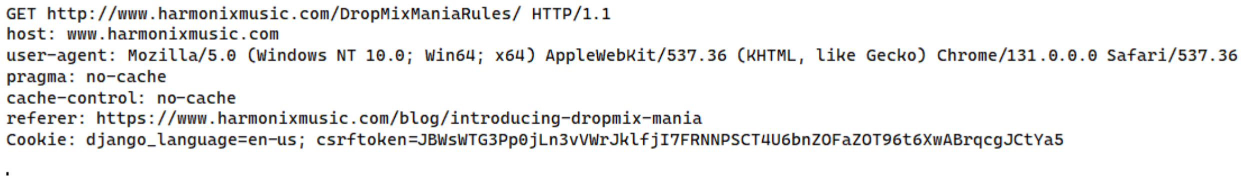
Content Security Policy (CSP) Header Not Set (447)

```
GET: http://www.harmonixmusic.com/DropMixManiaRules/
GET: http://www.harmonixmusic.com/DropMixPAXEastRules
GET: http://www.harmonixmusic.com/games/rock-band/legacy-songs/
GET: https://www.harmonixmusic.com/
GET: https://www.harmonixmusic.com/%E2%80%9Clegal@harmonixmusic.com%E2%80%9D
GET: https://www.harmonixmusic.com/2412
GET: https://www.harmonixmusic.com/about
GET: https://www.harmonixmusic.com/about/
GET: https://www.harmonixmusic.com/about/ajax-loader.gif
GET: https://www.harmonixmusic.com/about/contact
GET: https://www.harmonixmusic.com/about/ethos
GET: https://www.harmonixmusic.com/about/jobs
```

- 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.

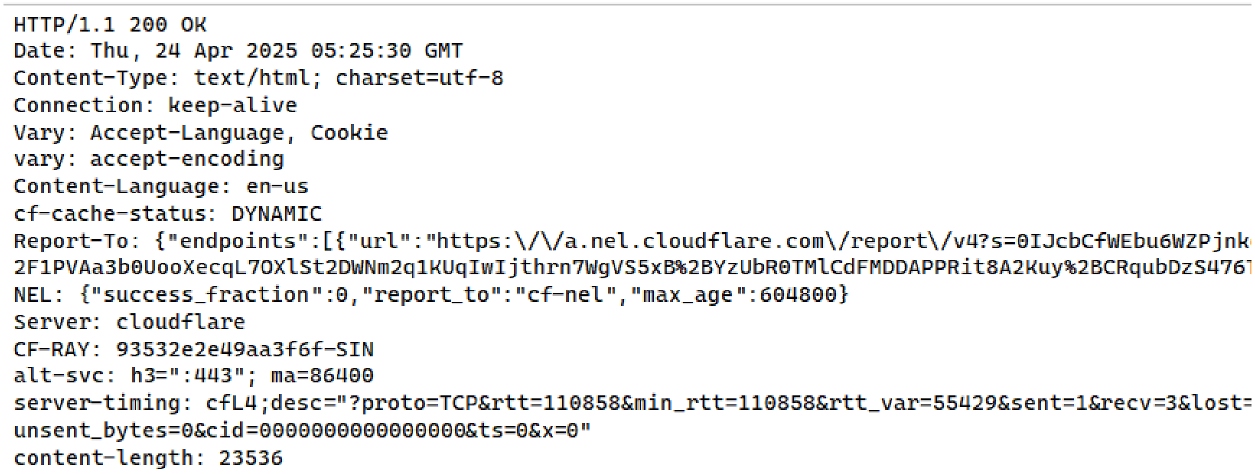
8. Proof of concept

Below is the request



```
GET http://www.harmonixmusic.com/DropMixManiaRules/ HTTP/1.1
host: www.harmonixmusic.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
referer: https://www.harmonixmusic.com/blog/introducing-dropmix-mania
Cookie: django_language=en-us; csrftoken=JBWsWTG3Pp0jLn3vVWrJklfjI7FRNNPSCT4U6bnZOFaZOT96t6XwABrqcgJCtYa5
.
```

Below is the response



```
HTTP/1.1 200 OK
Date: Thu, 24 Apr 2025 05:25:30 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Vary: Accept-Language, Cookie
vary: accept-encoding
Content-Language: en-us
cf-cache-status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?s=0IJcbCfWEbu6WZPjnk
2F1PVAa3b0UooXecqL7OXlSt2DWNm2q1KUqIwIjthrn7WgVS5xB%2BYzUbR0TMlCdFMDDAPPRit8A2Kuy%2BCRqubDzS476
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
CF-RAY: 93532e2e49aa3f6f-SIN
alt-svc: h3=":443"; ma=86400
server-timing: cfL4;desc="?proto=TCP&rtt=110858&min_rtt=110858&rtt_var=55429&sent=1&recv=3&lost=
unsent_bytes=0&cid=0000000000000000&ts=0&x=0"
content-length: 23536
```

No CSP header

9. 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