Sri Lanka Institute of Information Technology

IE2062 - Web Security

Final Assignment

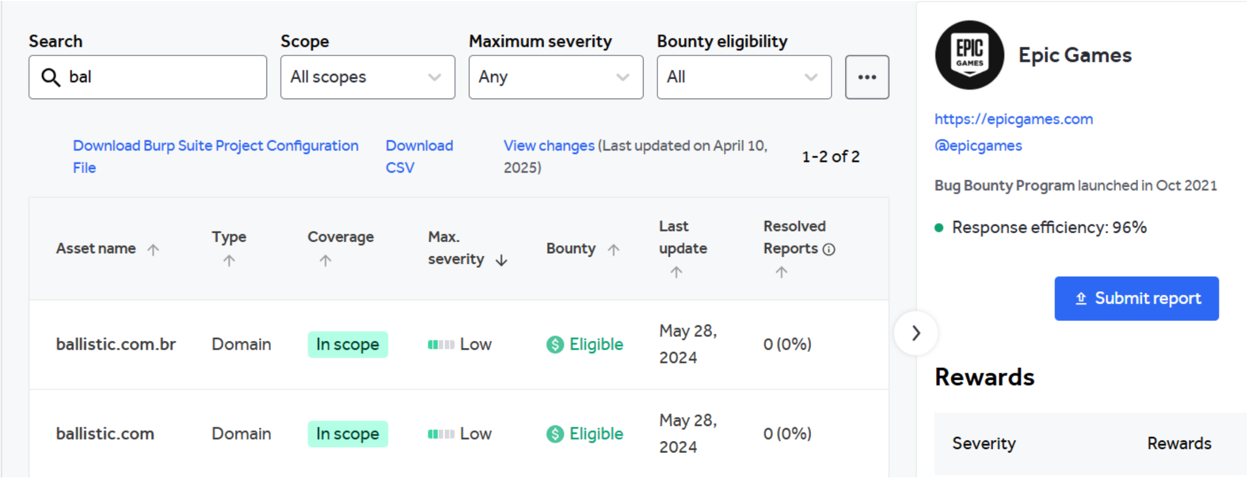
Bug Bounty Report 06

Name: Peiris W.S.S.N

Registration Number: IT23227286

Contents

1. Introduction



Search: bal

Scope: All scopes

Maximum severity: Any

Bounty eligibility: All

Download Burp Suite Project Configuration File | Download CSV | View changes (Last updated on April 10, 2025) | 1-2 of 2

Asset name ↑	Type ↑	Coverage ↑	Max. severity ↓	Bounty ↑	Last update ↑	Resolved Reports ⓘ ↑
ballistic.com.br	Domain	In scope	Low	Eligible	May 28, 2024	0 (0%)
ballistic.com	Domain	In scope	Low	Eligible	May 28, 2024	0 (0%)

Epic Games

https://epicgames.com

@epicgames

Bug Bounty Program launched in Oct 2021

● Response efficiency: 96%

Submit report

Rewards

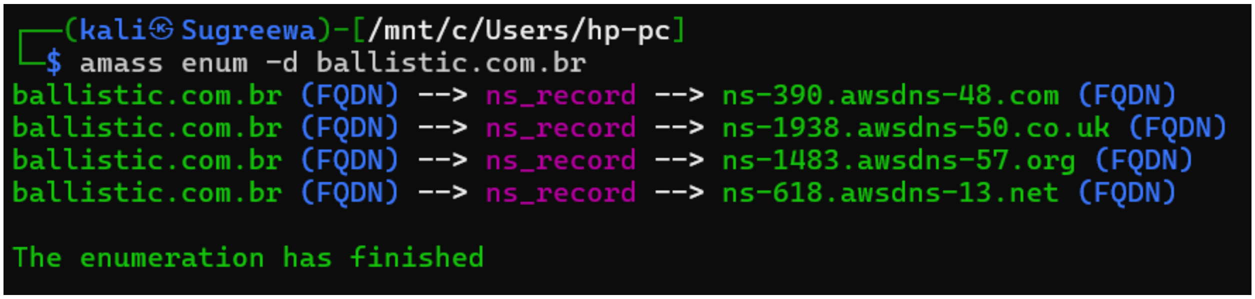
Severity	Rewards

Website: https://ballistic.com.br/

Listed by: Epic Games

2. Reconnaissance

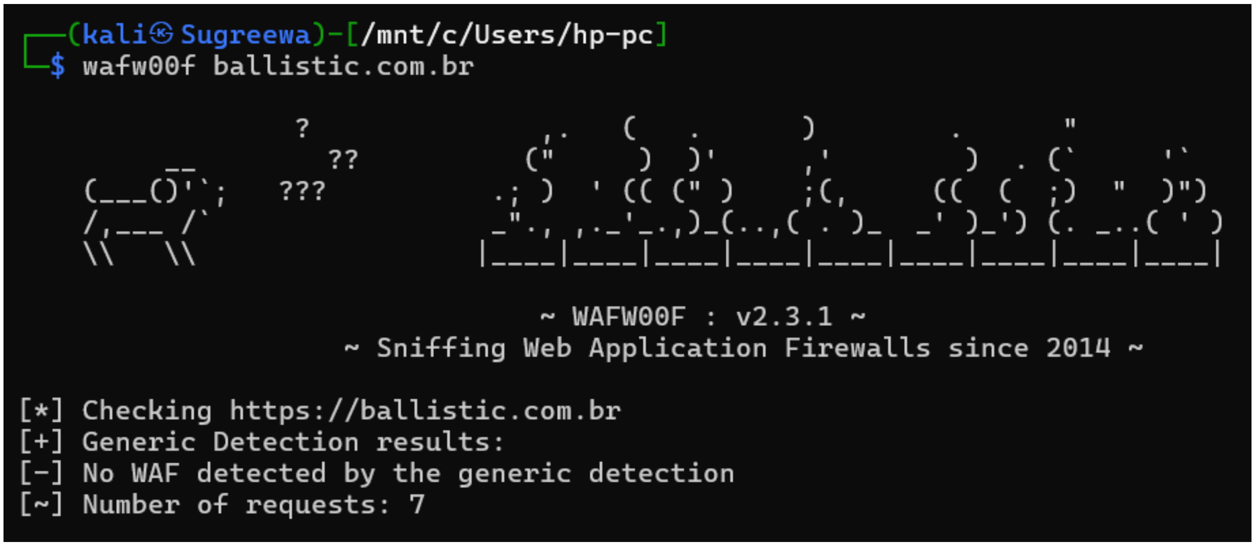
- **Subdomain enumeration using Amass**



```
┌──(kali㉿Sugreewa)-[/mnt/c/Users/hp-pc]
└─$ amass enum -d ballistic.com.br
ballistic.com.br (FQDN) --> ns_record --> ns-390.awsdns-48.com (FQDN)
ballistic.com.br (FQDN) --> ns_record --> ns-1938.awsdns-50.co.uk (FQDN)
ballistic.com.br (FQDN) --> ns_record --> ns-1483.awsdns-57.org (FQDN)
ballistic.com.br (FQDN) --> ns_record --> ns-618.awsdns-13.net (FQDN)

The enumeration has finished
```

- **Firewall Detection**



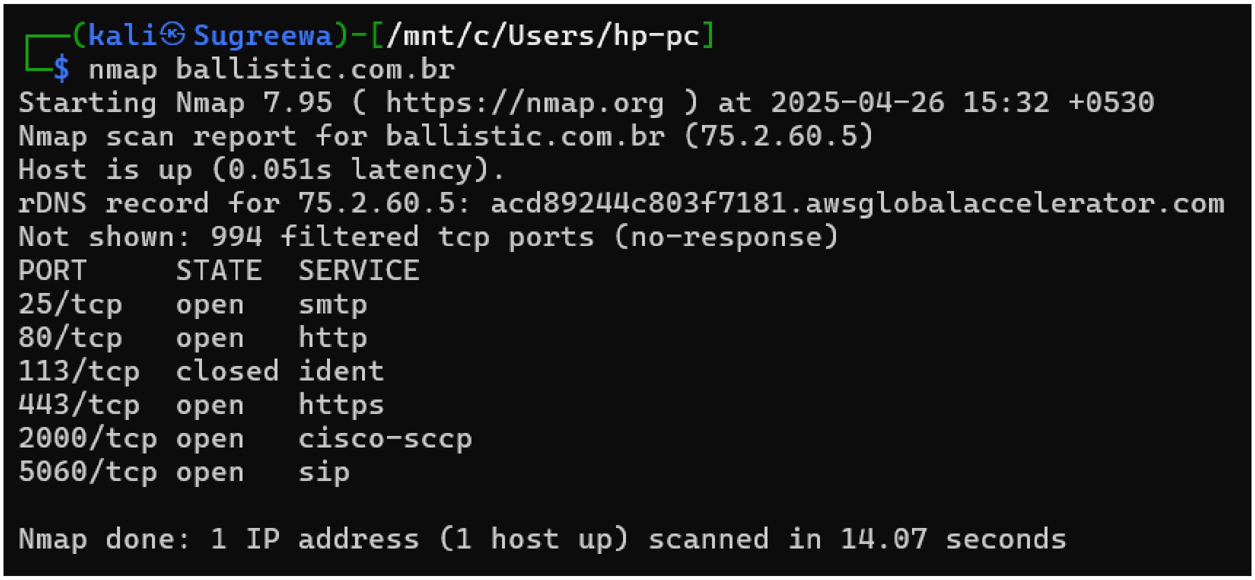
```
┌──(kali㉿Sugreewa)-[/mnt/c/Users/hp-pc]
└─$ wafw00f ballistic.com.br

                 ?              ,.   (   .      )        .      "
         __     ??          ("     )  )'     ,'        )  . (`     '`
    (___()'`;   ???          .; )  ' (( (" )    ;(,     ((  (  ;)  "  )")
    /,___ /`                 _"., ,._'_.,)_(..,( . )_  _' )_') (. _..( ' )
    \\   \\                 |____|____|____|____|____|____|____|____|____|

                                ~ WAFW00F : v2.3.1 ~
                    ~ Sniffing Web Application Firewalls since 2014 ~

[*] Checking https://ballistic.com.br
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7
```

- **Nmap Scan**

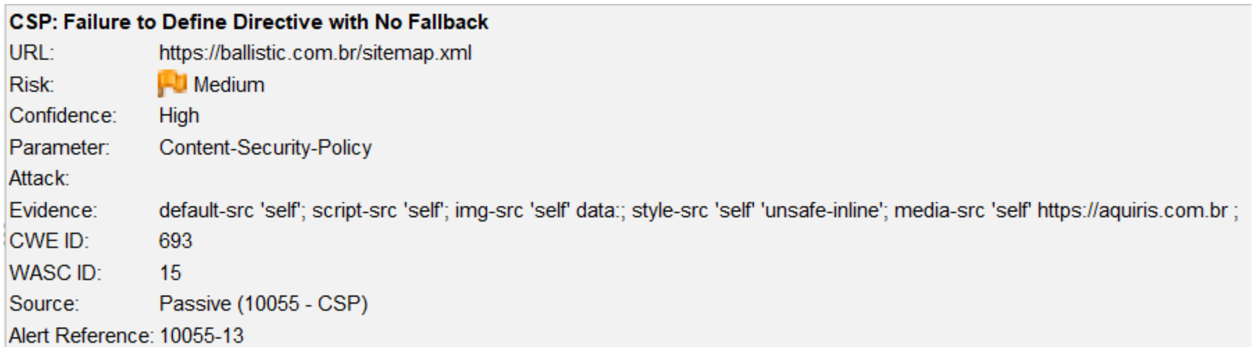


```
┌──(kali㉿Sugreewa)-[/mnt/c/Users/hp-pc]
└─$ nmap ballistic.com.br
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-26 15:32 +0530
Nmap scan report for ballistic.com.br (75.2.60.5)
Host is up (0.051s latency).
rDNS record for 75.2.60.5: acd89244c803f7181.awsglobalaccelerator.com
Not shown: 994 filtered 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

Nmap done: 1 IP address (1 host up) scanned in 14.07 seconds
```

3. Vulnerability

- **CSP: Failure to Define Directive with No Fallback**



CSP: Failure to Define Directive with No Fallback

URL:	https://ballistic.com.br/sitemap.xml
Risk:	Medium
Confidence:	High
Parameter:	Content-Security-Policy
Attack:	
Evidence:	default-src 'self'; script-src 'self'; img-src 'self' data:; style-src 'self' 'unsafe-inline'; media-src 'self' https://aquiris.com.br ;
CWE ID:	693
WASC ID:	15
Source:	Passive (10055 - CSP)
Alert Reference:	10055-13

4. Vulnerability description

The Content Security Policy fails to define one of the directives that has no fallback. Missing/excluding them is the same as allowing anything.

5. Affected Components

- **Component:** HTTP Response Headers → Content-Security-Policy
- **Current CSP Policy:**
  - default-src 'self'; script-src 'self'; img-src 'self' data:; style-src 'self' 'unsafe-inline'; media-src 'self' https://aquiris.com.br;
- **Missing Directives:**
  - **frame-ancestors**
  - **form-action**
- **Affected Pages:** All pages serving this CSP header

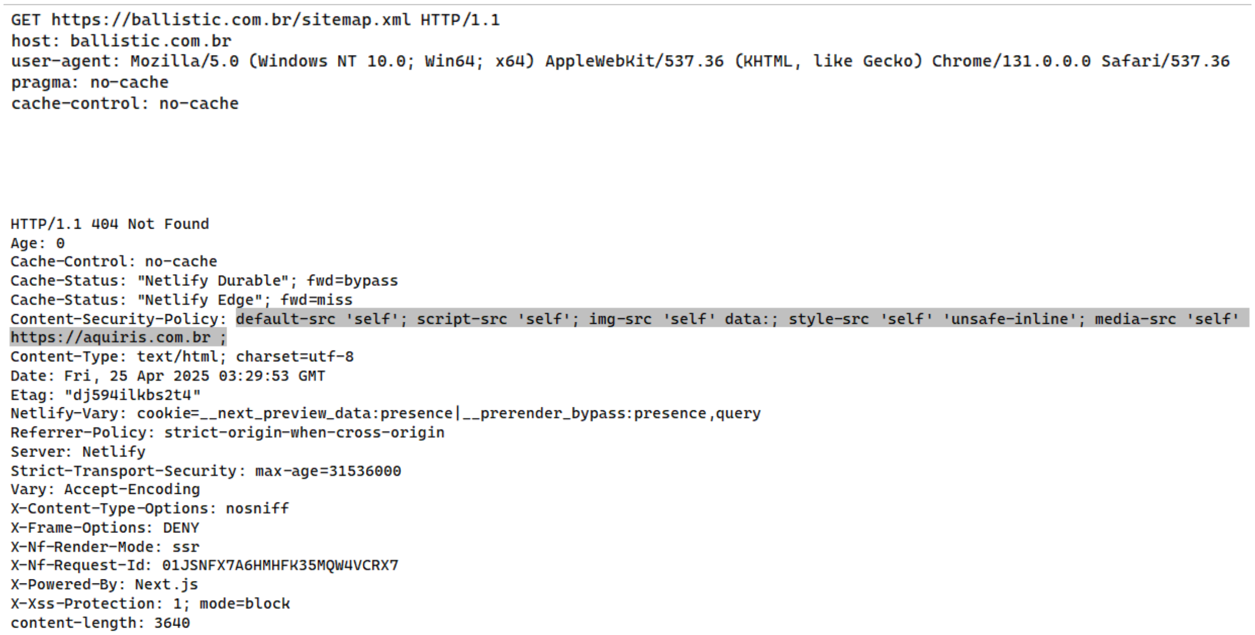
6. Impact Assessment

- **Risk Level:** Medium
- **Potential Impacts:**
  - Clickjacking (no frame-ancestors)
  - Phishing or data theft via form submission hijacking (no form-action)
  - Weakens the defense provided by CSP, making it ineffective against several types of UI-based or injection attacks

7. Steps to reproduce

- Open the affected site in a browser or intercept its HTTP response using DevTools or a proxy tool like ZAP/Burp.
- Check the Content-Security-Policy header.
- Look for the absence of:
    - frame-ancestors
    - form-action
- Verify that no fallback to default-src occurs for these directives.

8. Proof of concept



```
GET https://ballistic.com.br/sitemap.xml HTTP/1.1
host: ballistic.com.br
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/1.1 404 Not Found
Age: 0
Cache-Control: no-cache
Cache-Status: "Netlify Durable"; fwd=bypass
Cache-Status: "Netlify Edge"; fwd=miss
Content-Security-Policy: default-src 'self'; script-src 'self'; img-src 'self' data:; style-src 'self' 'unsafe-inline'; media-src 'self'
https://aquiris.com.br ;
Content-Type: text/html; charset=utf-8
Date: Fri, 25 Apr 2025 03:29:53 GMT
Etag: "dj594ilkbs2t4"
Netlify-Vary: cookie=__next_preview_data:presence|__prerender_bypass:presence,query
Referrer-Policy: strict-origin-when-cross-origin
Server: Netlify
Strict-Transport-Security: max-age=31536000
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-Nf-Render-Mode: ssr
X-Nf-Request-Id: 01JSNFX7A6HMHFK35MQW4VCRX7
X-Powered-By: Next.js
X-Xss-Protection: 1; mode=block
content-length: 3640
```

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.