**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 3](#_Toc196574238)

[2. Reconnaissance 4](#_Toc196574239)

[3. Vulnerability 5](#_Toc196574240)

[4. Vulnerability description 5](#_Toc196574241)

[5. Affected Components 6](#_Toc196574242)

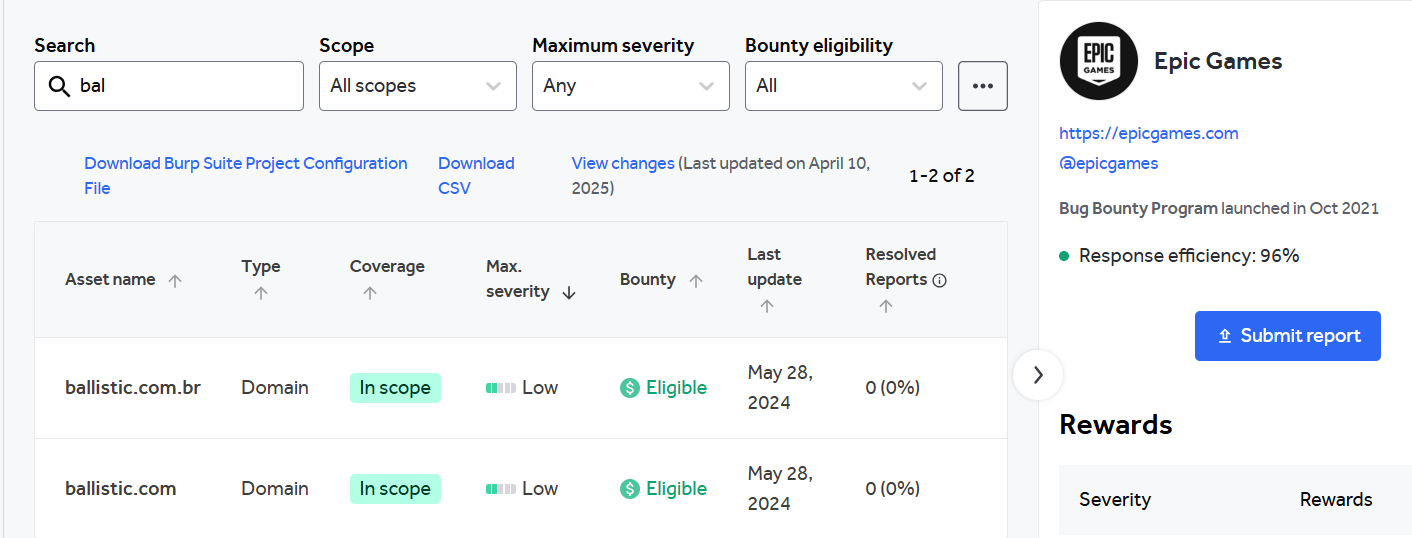
[6. Impact Assessment 6](#_Toc196574243)

[7. Steps to reproduce 7](#_Toc196574244)

[8. Proof of concept 7](#_Toc196574245)

[9. Proposed mitigation or fix 7](#_Toc196574246)

# Introduction

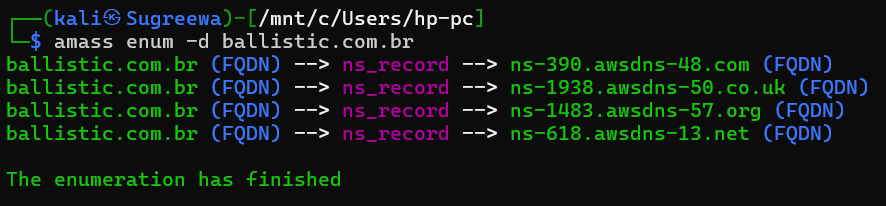


**Website:** <https://ballistic.com.br/>

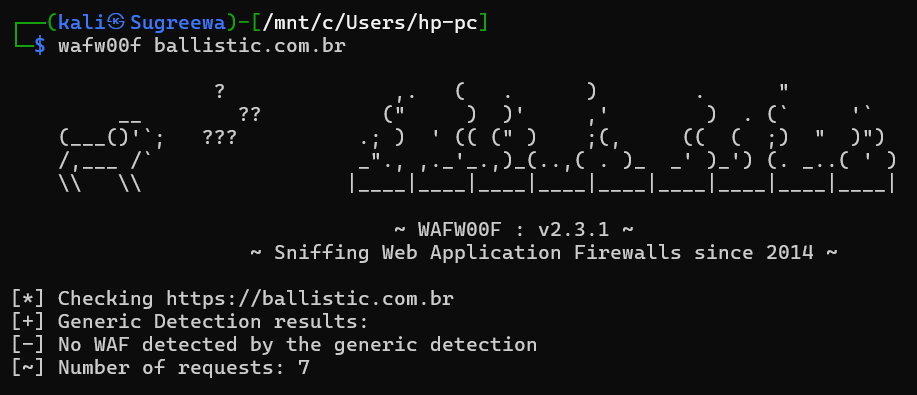
**Listed by:** Epic Games

# Reconnaissance

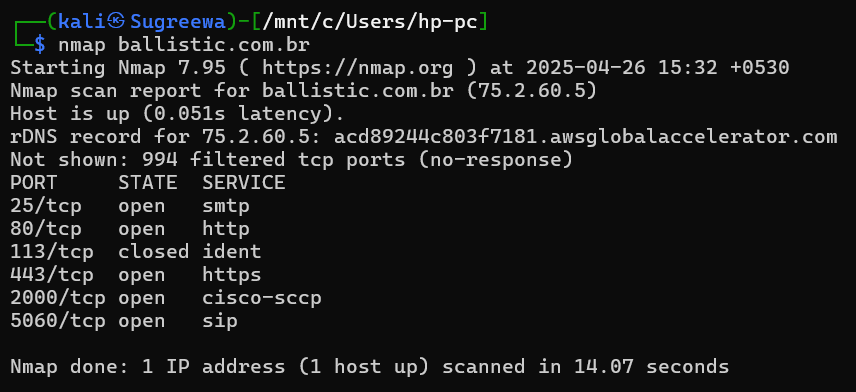
* **Subdomain enumeration using Amass**

****

* **Firewall Detection**

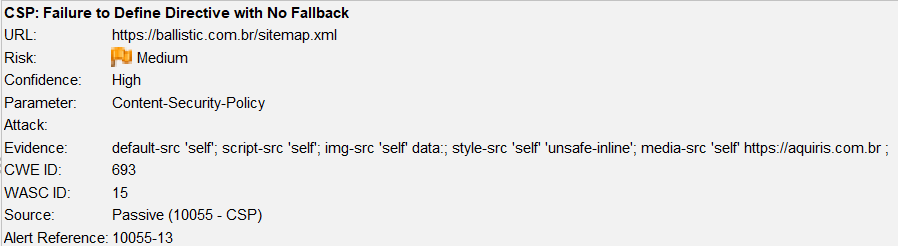
****

* **Nmap Scan**

****

# Vulnerability

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

****

# 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.

1. 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

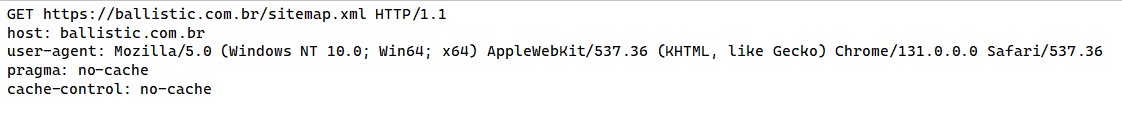
# Impact Assessment

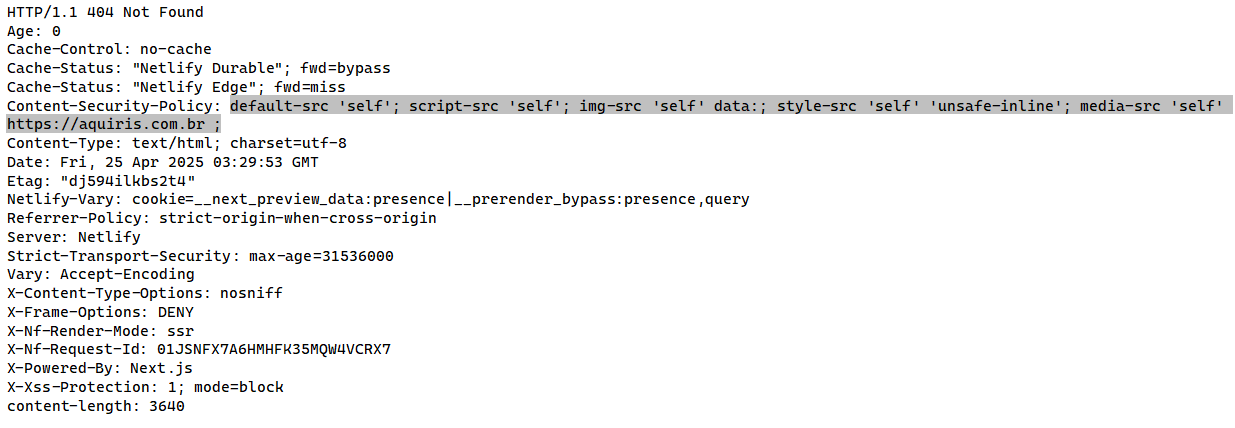
* **Risk Level:** Medium
* **Potential Impacts:**
  + Clickjacking (no frame-ancestors)
  + Phishing or data theft via form submission hijacking (no form-action)
  + Weakens the defense provided by CSP, making it ineffective against several types of UI-based or injection attacks

# 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.

# 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.