**Sri Lanka Institute of Information Technology**

**IE2062 - Web Security**

**Final Assignment**

**Bug Bounty Report 05**

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

**Registration Number:** IT23227286

Contents

[1. Introduction 3](#_Toc197102641)

[2. Reconnaissance 4](#_Toc197102642)

[3. Vulnerability 5](#_Toc197102643)

[4. Vulnerability description 5](#_Toc197102644)

[5. Affected Components 6](#_Toc197102645)

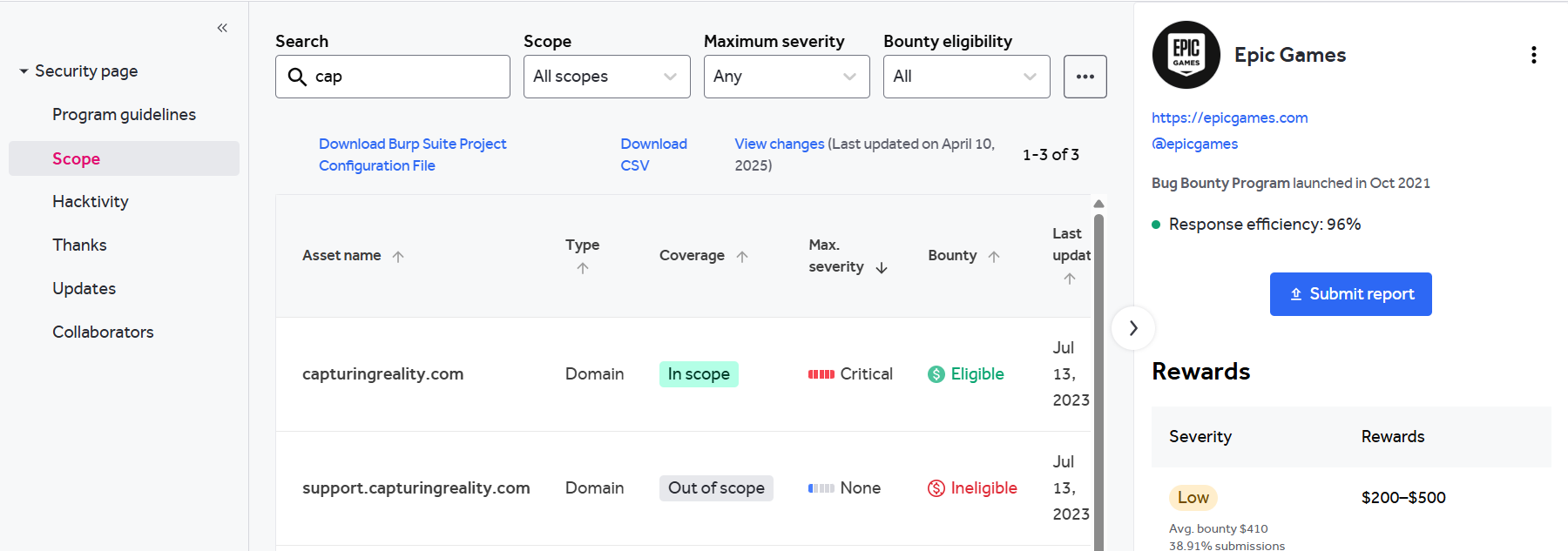
[6. Impact Assessment 6](#_Toc197102646)

[7. Steps to reproduce 7](#_Toc197102647)

[8. Proof of concept 8](#_Toc197102648)

[9. Proposed mitigation or fix 8](#_Toc197102649)

# Introduction

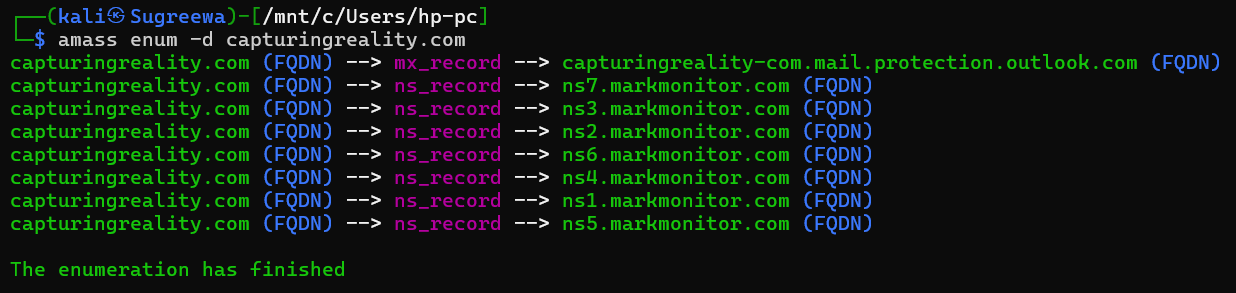


**Website:** <https://www.capturingreality.com/>

**Listed by:** Epic Games

# Reconnaissance

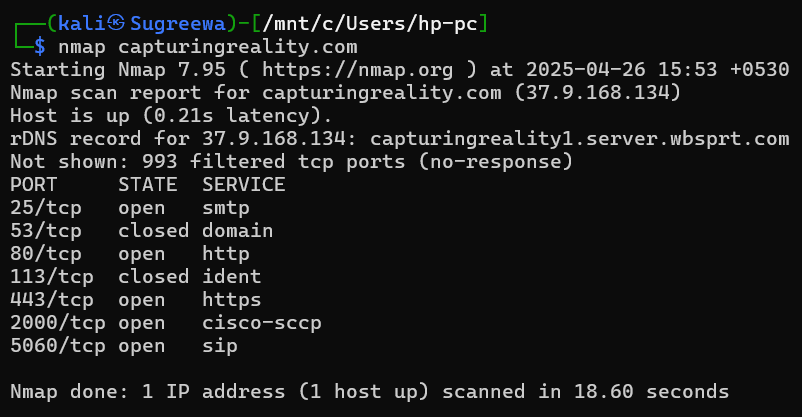
* **Subdomain enumeration using Amass**

****

* **Firewall Detection**

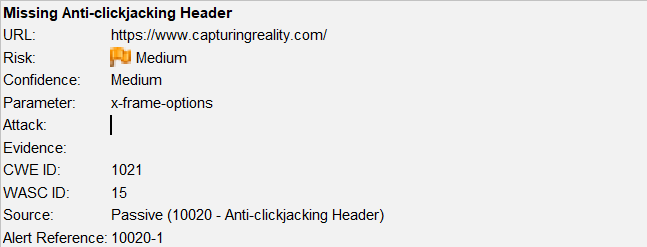
****

* **Nmap Scan**



# Vulnerability

* **Missing Anti-clickjacking Header**

****

# Vulnerability description

The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.

1. Affected Components

* **Component:** HTTP Response Headers
* **Missing Headers:**
  + X-Frame-Options
  + Content-Security-Policy with frame-ancestors directive
* **Affected Pages:** Any endpoint returning HTML content without the above headers
  + <https://www.capturingreality.com/About-Us>
  + <https://www.capturingreality.com/Archinfo-RealityCapture-Architecture>

# Impact Assessment

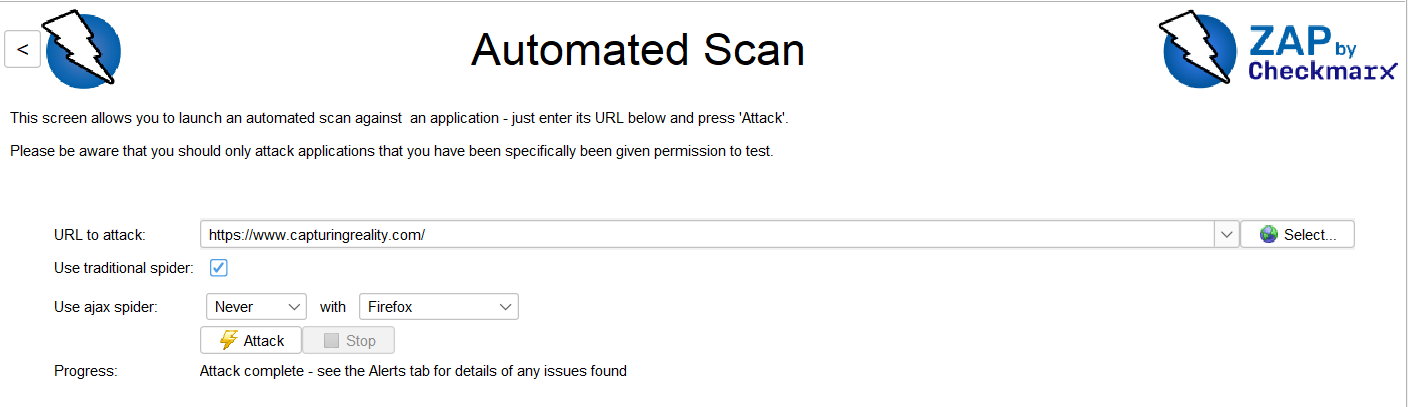
**Risk Level:** Medium

**Potential Impacts:**

* UI Redressing (Clickjacking)
* Fraudulent user actions (e.g., clicking "Transfer", "Delete", "Submit")
* Loss of user trust and security reputation
* May enable further social engineering or phishing attacks

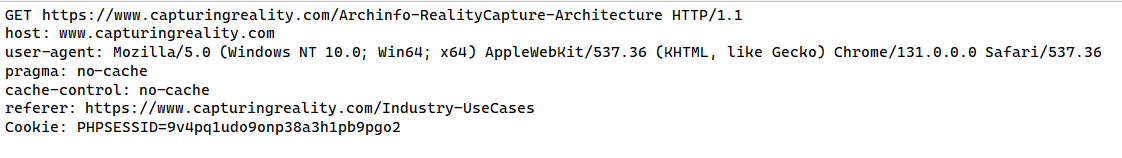
# Steps to reproduce

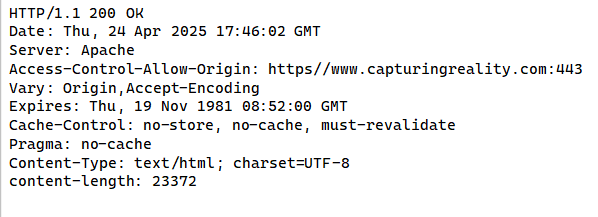
* Run a scan using OWASP ZAP or inspect HTTP responses using browser DevTools.



* Navigate to a page suspected to be vulnerable.
* Check the response headers.
* Confirm that neither:
* X-Frame-Options: DENY/SAMEORIGIN
* nor Content-Security-Policy: frame-ancestors 'none' is present.

# Proof of concept





# Proposed mitigation or fix

Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.

If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.