



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
2. Reconnaissance	4
3. Vulnerability	5
4. Vulnerability description.....	5
5. Affected Components	6
6. Impact Assessment.....	6
7. Steps to reproduce.....	7
8. Proof of concept.....	8
9. Proposed mitigation or fix	8

1. Introduction

The screenshot displays the Epic Games Bug Bounty Program interface. On the left is a sidebar with navigation links: Security page, Program guidelines, Scope (highlighted), Hacktivity, Thanks, Updates, and Collaborators. The main content area features a search bar with 'cap' entered, and filters for Scope (All scopes), Maximum severity (Any), and Bounty eligibility (All). Below the filters, there are links to 'Download Burp Suite Project Configuration File', 'Download CSV', and 'View changes (Last updated on April 10, 2025)'. A table lists search results for 'capturingreality.com' and 'support.capturingreality.com'. The table columns are Asset name, Type, Coverage, Max. severity, Bounty, and Last update. The first result is 'capturingreality.com' (Domain, In scope, Critical, Eligible, Jul 13, 2023). The second result is 'support.capturingreality.com' (Domain, Out of scope, None, Ineligible, Jul 13, 2023). On the right, the Epic Games logo and name are shown, along with links to their website and social media. Below this, it states 'Bug Bounty Program launched in Oct 2021' and 'Response efficiency: 96%'. A 'Submit report' button is present. A 'Rewards' section shows a table with Severity (Low) and Rewards (\$200-\$500), along with average bounty and submission statistics.

Asset name	Type	Coverage	Max. severity	Bounty	Last update
capturingreality.com	Domain	In scope	Critical	Eligible	Jul 13, 2023
support.capturingreality.com	Domain	Out of scope	None	Ineligible	Jul 13, 2023

Severity	Rewards
Low	\$200-\$500

Avg. bounty \$410
38.91% submissions

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

Listed by: Epic Games

2. Reconnaissance

- Subdomain enumeration using Amass

```
(kali@Sugreewa)-[/mnt/c/Users/hp-pc]
$ amass enum -d capturingreality.com
capturingreality.com (FQDN) --> mx_record --> capturingreality-com.mail.protection.outlook.com (FQDN)
capturingreality.com (FQDN) --> ns_record --> ns7.markmonitor.com (FQDN)
capturingreality.com (FQDN) --> ns_record --> ns3.markmonitor.com (FQDN)
capturingreality.com (FQDN) --> ns_record --> ns2.markmonitor.com (FQDN)
capturingreality.com (FQDN) --> ns_record --> ns6.markmonitor.com (FQDN)
capturingreality.com (FQDN) --> ns_record --> ns4.markmonitor.com (FQDN)
capturingreality.com (FQDN) --> ns_record --> ns1.markmonitor.com (FQDN)
capturingreality.com (FQDN) --> ns_record --> ns5.markmonitor.com (FQDN)

The enumeration has finished
```

- Firewall Detection

```
(kali@Sugreewa)-[/mnt/c/Users/hp-pc]
$ wafw00f capturingreality.com

      ?
      ??
      ???
(_____)';
/,\---/\
\\      \\

      ?
      ??
      ???
      ( " ) '
      ' ( ( " )
      ; ( , ( ( ( ; ) " ) " )
      - " , , - ' - , ) - ( , , - ' ) - ' ( . - . ( ' )
      |_____|_____|_____|_____|_____|_____|_____|_____|

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

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

- **Nmap Scan**

```
(kali@Sugreewa)-[/mnt/c/Users/hp-pc]
$ nmap capturingreality.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-26 15:53 +0530
Nmap scan report for capturingreality.com (37.9.168.134)
Host is up (0.21s latency).
rDNS record for 37.9.168.134: capturingreality1.server.wbsprt.com
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
25/tcp    open  smtp
53/tcp    closed domain
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 18.60 seconds
```

3. Vulnerability

- **Missing Anti-clickjacking Header**

Missing Anti-clickjacking Header	
URL:	https://www.capturingreality.com/
Risk:	🔴 Medium
Confidence:	Medium
Parameter:	x-frame-options
Attack:	
Evidence:	
CWE ID:	1021
WASC ID:	15
Source:	Passive (10020 - Anti-clickjacking Header)
Alert Reference:	10020-1

4. 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.

5. 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>

6. Impact Assessment

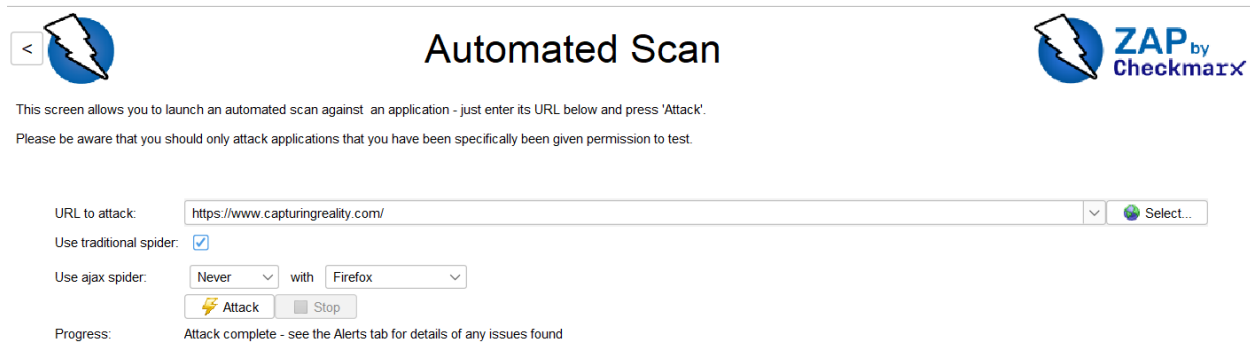
Risk Level: Medium

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

7. Steps to reproduce

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



The screenshot shows the 'Automated Scan' interface of OWASP ZAP. At the top left is a back button and a lightning bolt icon. The title 'Automated Scan' is centered. At the top right is the 'ZAP by Checkmarx' logo. Below the title, a message states: 'This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'. Please be aware that you should only attack applications that you have been specifically given permission to test.' The main form contains a 'URL to attack:' field with the value 'https://www.capturingreality.com/'. Below this are two checkboxes: 'Use traditional spider:' (checked) and 'Use ajax spider:' (unchecked). The 'Use ajax spider:' section has two dropdown menus: 'Never' and 'Firefox'. At the bottom of the form are 'Attack' and 'Stop' buttons. A progress bar at the bottom indicates 'Attack complete - see the Alerts tab for details of any issues found'.

- 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.

8. Proof of concept

```
GET https://www.capturingreality.com/Archinfo-RealityCapture-Architecture HTTP/1.1
host: www.capturingreality.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.capturingreality.com/Industry-UseCases
Cookie: PHPSESSID=9v4pq1udo9onp38a3h1pb9pgo2
```

```
HTTP/1.1 200 OK
Date: Thu, 24 Apr 2025 17:46:02 GMT
Server: Apache
Access-Control-Allow-Origin: https://www.capturingreality.com:443
Vary: Origin,Accept-Encoding
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Type: text/html; charset=UTF-8
content-length: 23372
```

9. 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.