Sri Lanka Institute of Information Technology

Individual Assignment

Bug Bounty Report

Web Security - IE2062

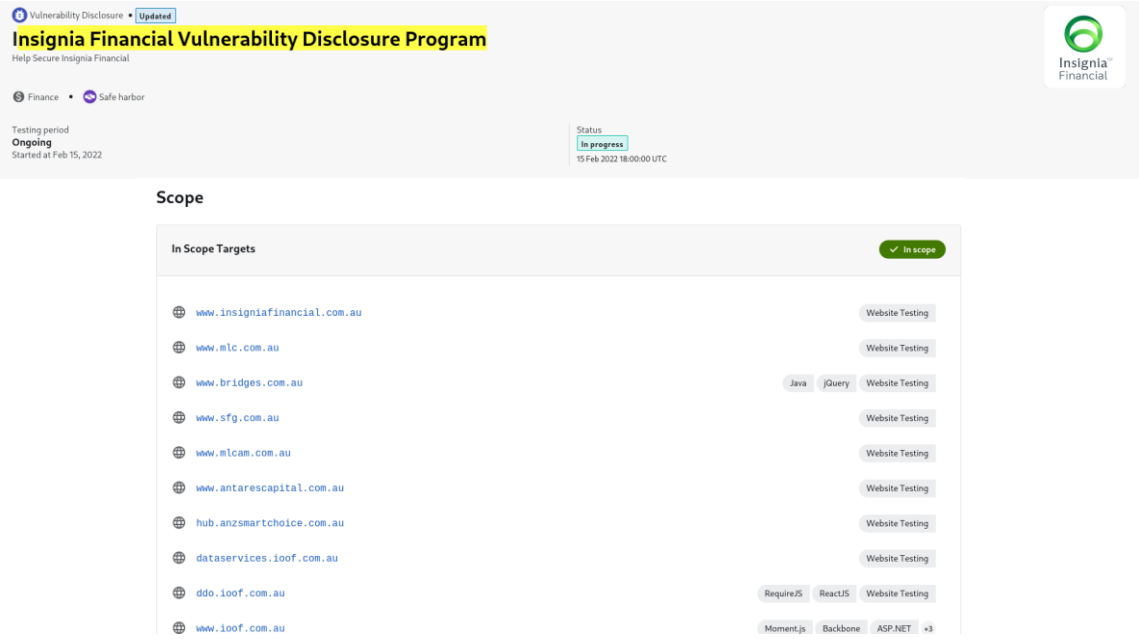
BSc Honors in Information Technology Specializing in Cyber Security

CASE STUDY NAME	BUG BOUNTY Report 07
CAMPUS/CENTER	SLIIT KANDY UNI

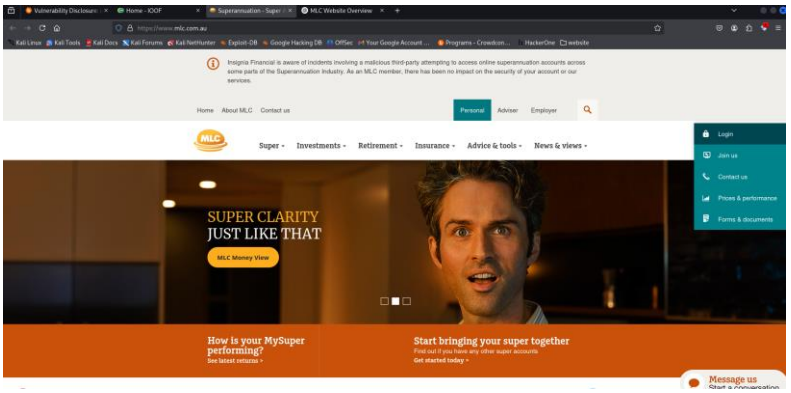
Student Details

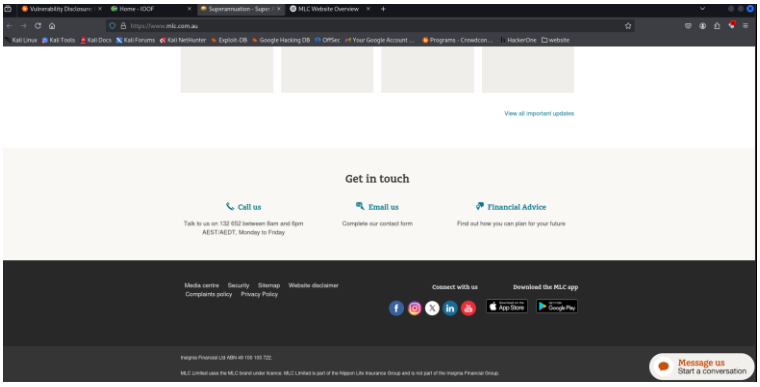
	Student Registration Number	Student Name
1	IT23222854	JAYASINGHE B. I

Domain – Insignia Financial Vulnerability Disclosure Program



- Link - https://www.mlc.com.au/
- Type – Financial services





1. Sensitive Data Exposure

1.Retire.js

Retire.js ☑ Enabled ☐ Show unknown

angularjs	1.3.15	Found in https://www.mlc.com.au/etc.clientlibs/common/clientlibs/common/common/angular/clientlibs-angular.lc-00e7acf4889dcbadf070c5f13224a538-lc.js - Vulnerability info:		
		Medium	XSS through xlink:href attributes CVE-2019-14863 GHSA-r5fx-8r73-v86c	[1] [2]
		Medium	The attribute usemap can be used as a security exploit 49	[1]
		Medium	Cross-Site Scripting via JSONP GHSA-28hp-fgcr-2r4h	[1]
		Medium	DOS in $sanitize 52	[1] [2]
		Medium	Universal CSP bypass via add-on in Firefox 51	[1] [2]
		Low	XSS in $sanitize in Safari/Firefox 53	[1]
		High	Prototype pollution 47 GHSA-89mq-4x47-5v83 CVE-2019-10768	[1] [2]
		Medium	XSS via JQLite DOM manipulation functions in AngularJS GHSA-5cp4-xmrw-59wf	[1]
		Medium	XSS may be triggered in AngularJS applications that sanitize user-controlled HTML snippets before passing them to JQLite methods like JQLite.prepend, JQLite.after, JQLite.append, JQLite.replaceWith, JQLite.append, new JQLite	[1] [2]

		Medium	angular vulnerable to regular expression denial of service via the $resource service CVE-2023-26117 GHSA-2qqx-w9hr-q5gx	[1]
		Medium	angular vulnerable to regular expression denial of service via the angular.copy() utility CVE-2023-26116 GHSA-2vrf-hf26-jrp5	[1]
		Medium	Angular (deprecated package) Cross-site Scripting CVE-2022-25869 GHSA-prc3-vjfx-vhm9	[1]
		Medium	angular vulnerable to regular expression denial of service via the <input type="url"> element GHSA-qwqh-hm9m-p5hr CVE-2023-26118	[1]
		Low	AngularJS allows attackers to bypass common image source restrictions CVE-2024-8373 GHSA-mqm9-c95h-x2p6	[1] [2] [3] [4] [5]
		High	angular vulnerable to super-linear runtime due to backtracking CVE-2024-21490 GHSA-4w4v-5hc9-xrr2	[1] [2] [3] [4] [5] [6] [7]
		Low	AngularJS allows attackers to bypass common image source restrictions CVE-2024-8372 GHSA-m9gf-397r-hwpg	[1] [2] [3] [4] [5]

		Low	End-of-Life: Long term support for AngularJS has been discontinued as of December 31, 2021 54	[1]
angularjs	1.5.5	Found in https://www.mlc.com.au/etc.clientlibs/mlc/clientlibs/bootstrap/bootstrap-base-mlc-design/angular/mlcLtd/mlcLtdApp.lc-483784efed1593646ba5a765752892bb-lc.js - Vulnerability info:		
		Medium	Cross-Site Scripting via JSONP GHSA-28hp-fgcr-2r4h	[1]
		Medium	DOS in $sanitize 52	[1] [2]
		Medium	Universal CSP bypass via add-on in Firefox 51	[1] [2]
		Low	XSS in $sanitize in Safari/Firefox 53	[1]
		Low	XSS through SVG if enableSvg is set 48	[1] [2]
		High	Prototype pollution 47 GHSA-89mq-4x47-5v83 CVE-2019-10768	[1] [2]
		Medium	XSS via JQLite DOM manipulation functions in AngularJS GHSA-5cp4-xmrw-59wf	[1]
		Medium	XSS may be triggered in AngularJS applications that sanitize user-controlled HTML snippets before passing them to JQLite methods like JQLite.prepend, JQLite.after, JQLite.append, JQLite.replaceWith, JQLite.append, new JQLite and angular.element. CVE-2020-7676 GHSA-mhp6-pxh8-r675	[1] [2]

		Medium	angular vulnerable to regular expression denial of service via the $resource service CVE-2023-26117 GHSA-2qqx-w9hr-q5gx	[1]
		Medium	angular vulnerable to regular expression denial of service via the angular.copy() utility CVE-2023-26116 GHSA-2vrf-hf26-jrp5	[1]
		Medium	Angular (deprecated package) Cross-site Scripting CVE-2022-25869 GHSA-prc3-vjfx-vhm9	[1]
		Medium	angular vulnerable to regular expression denial of service via the <input type="url"> element GHSA-qwqh-hm9m-p5hr CVE-2023-26118	[1]
		Low	AngularJS allows attackers to bypass common image source restrictions CVE-2024-8373 GHSA-mqm9-c95h-x2p6	[1] [2] [3] [4] [5]
		High	angular vulnerable to super-linear runtime due to backtracking CVE-2024-21490 GHSA-4w4v-5hc9-xrr2	[1] [2] [3] [4] [5] [6] [7]
		Low	AngularJS allows attackers to bypass common image source restrictions CVE-2024-8372 GHSA-m9gf-397r-hwpg	[1] [2] [3] [4] [5]

		Low	End-of-Life: Long term support for AngularJS has been discontinued as of December 31, 2021 54	[1]
angularjs	1.5.5	Found in https://www.mlc.com.au/etc.clientlibs/common-designs/clientlibs/common-designs/angular/1.5.5/angular.lc-5e2d2057d96976d43c756dcc1efaa1dc-lc.js - Vulnerability info:		
		Medium	Cross-Site Scripting via JSONP GHSA-28hp-fgcr-2r4h	[1]
		Medium	DOS in $sanitize 52	[1] [2]
		Medium	Universal CSP bypass via add-on in Firefox 51	[1] [2]
		Low	XSS in $sanitize in Safari/Firefox 53	[1]
		Low	XSS through SVG if enableSvg is set 48	[1] [2]
		High	Prototype pollution 47 GHSA-89mq-4x47-5v83 CVE-2019-10768	[1] [2]
		Medium	XSS via JQLite DOM manipulation functions in AngularJS GHSA-5cp4-xmrw-59wf	[1]
		Medium	XSS may be triggered in AngularJS applications that sanitize user-controlled HTML snippets before passing them to JQLite methods like JQLite.prepend, JQLite.after, JQLite.append, JQLite.replaceWith, JQLite.append, new JQLite and angular.element. CVE-2020-7676 GHSA-mhp6-pxh8-r675	[1] [2]

			mhp6-pxh8-r675	
		Medium	angular vulnerable to regular expression denial of service via the $resource service CVE-2023-26117 GHSA-2qqx-w9hr-q5gx	[1]
		Medium	angular vulnerable to regular expression denial of service via the angular.copy() utility CVE-2023-26116 GHSA-2vrf-hf26-jrp5	[1]
		Medium	Angular (deprecated package) Cross-site Scripting CVE-2022-25869 GHSA-prc3-vjfx-vhm9	[1]
		Medium	angular vulnerable to regular expression denial of service via the <input type="url"> element GHSA-qwqh-hm9m-p5hr CVE-2023-26118	[1]
		Low	AngularJS allows attackers to bypass common image source restrictions CVE-2024-8373 GHSA-mqm9-c95h-x2p6	[1] [2] [3] [4] [5]
		High	angular vulnerable to super-linear runtime due to backtracking CVE-2024-21490 GHSA-4w4v-5hc9-xrr2	[1] [2] [3] [4] [5] [6] [7]
		Low	AngularJS allows attackers to bypass common image source restrictions CVE-2024-8372 GHSA-m9gf-397r-hwpg	[1] [2] [3] [4]

		Low	End-of-Life: Long term support for AngularJS has been discontinued as of December 31, 2021 54	[1]
bootstrap	3.3.1	Found in https://www.mlc.com.au/etc.clientlibs/mlc-designs/clientlibs/bootstrap/bootstrap-managed-designs/bootstrap-mlc/clientlibs.lc-ecc365673f590325a92b3411377c8334-lc.js - Vulnerability info:		
		Medium	In Bootstrap before 3.4.0, XSS is possible in the tooltip data-viewport attribute. 27044 CVE-2018-20676 GHSA-3mgp-fx93-9xv5	[1]
		Medium	XSS in data-container property of tooltip 20184 CVE-2018-14042 GHSA-7mvr-5x2g-wfc8	[1]
		Medium	In Bootstrap before 3.4.0, XSS is possible in the affix configuration target property. CVE-2018-20677 GHSA-ph58-4vrj-w6hr	[1]
		Medium	XSS in data-target property of scrollspy 20184 CVE-2018-14041 GHSA-pj7m-g53m-7638	[1] [2]
		Medium	XSS is possible in the data-target attribute. CVE-2016-10735 GHSA-4p24-vmcr-4gqj	[1]
		Medium	Bootstrap Cross-Site Scripting (XSS) vulnerability for data-* attributes CVE-2024-6485 GHSA-vxmc-5x29-h64v	[1] [2] [3] [4]
		Medium	XSS in data-template, data-content and data-title properties of tooltip/popover 28236 CVE-2019-8331 GHSA-9v3m-8fp8-mj99	[1] [2]
		Medium	Bootstrap Cross-Site Scripting (XSS) vulnerability CVE-2024-6484 GHSA-9mvj-f7w8-	[1] [2] [3] [4]

		Low	Bootstrap before 4.0.0 is end-of-life and no longer maintained. 72	[1]
jquery-ui-dialog	1.10.1	Found in https://www.mlc.com.au/etc.clientlibs/bootstrap/clientlibs/bootstrap/bootstrap-base-design/bootstrap-base/clientlibs-jqueryui.lc-3734498ee27a0d8c6769041f3d1407b5-lc.js - Vulnerability info:		
		Medium	XSS Vulnerability on closeText option CVE-2016-7103 281 GHSA-hpcf-6vf9-q4gj	[1] [2] [3]
jquery-ui	1.10.1	Found in https://www.mlc.com.au/etc.clientlibs/bootstrap/clientlibs/bootstrap/bootstrap-base-design/bootstrap-base/clientlibs-jqueryui.lc-3734498ee27a0d8c6769041f3d1407b5-lc.js - Vulnerability info:		
		Medium	XSS in the `altField` option of the Datepicker widget CVE-2021-41182 GHSA-9gj3-hwp5-pmwc	[1] [2]
		Medium	XSS in the `of` option of the `.position()` util CVE-2021-41184 GHSA-gpqq-952q-5327	[1] [2]
		Medium	XSS Vulnerability on text options of jQuery UI datepicker CVE-2021-41183 15284 GHSA-j7qv-pgf6-hvh4	[1] [2]
		Medium	XSS when refreshing a checkboxradio with an HTML-like initial text label CVE-2022-31160 2101 GHSA-h6gj-6jjq-h8g9	[1] [2] [3] [4]
jquery	1.12.4-aem	Found in https://www.mlc.com.au/etc.clientlibs/clientlibs/granite/jquery.lc-ca3533f7cc006ecc710731f12fa9a3e1-lc.js - Vulnerability		

		Low	jQuery 1.x and 2.x are End-of-Life and no longer receiving security updates 73 162	[1]
		Medium	3rd party CORS request may execute 2432 CVE-2015-9251 GHSA-rmxg-73gg-4p98	[1] [2] [3] [4] [5] [6]
		Medium	jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution CVE-2019-11358 4333 GHSA-6c3j-c64m-qhgq	[1] [2] [3]
		Medium	passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. CVE-2020-11023 4647 GHSA-jpcq-cgw6-v4j6	[1]
		Medium	Regex in its jQuery.htmlPrefilter sometimes may introduce XSS CVE-2020-11022 4642 GHSA-gxr4-xjj5-5px2	[1]
moment.js	2.14.1	Found in https://www.mlc.com.au/etc.clientlibs/mlc/clientlibs/bootstrap/bootstrap-base-mlc-design/angular/mlcLtd/mlcLtdApp.lc-483784efed1593646ba5a765752892bb-lc.js - Vulnerability info:		

moment.js	2.14.1	Found in https://www.mlc.com.au/etc.clientlibs/mlc/clientlibs/bootstrap/bootstrap-base-mlc-design/angular/mlcLtd/mlcLtdApp.lc-483784efed1593646ba5a765752892bb-lc.js - Vulnerability info:		
		Medium	Regular Expression Denial of Service (ReDoS) 22	[1]
		High	Regular Expression Denial of Service (ReDoS) CVE-2017-18214 GHSA-446m-mv8f-q348	[1] [2] [3]
		High	This vulnerability impacts npm (server) users of moment.js, especially if user provided locale string, eg fr is directly used to switch moment locale. CVE-2022-24785 GHSA-8hfj-j24r-96c4	[1]

Summary fo the above vulnerabilities.

Library	Version	Vulnerability Description	Severity	Reference (CVE/GHSA)
Angular		Regular expression denial of service via $resource service	Medium	CVE-2023-21117, GHSA-q3w7-v9fw-q6gx
		Regular expression denial of service via angular.copy() utility	Medium	CVE-2023-26116, GHSA-2m7j-h62r-j996
		Deprecated package vulnerable to Cross-Site Scripting (XSS)	Medium	CVE-2022-25896, GHSA-1q3j-v9fx-vh6h
		Vulnerable to XSS via elements	Medium	CVE-2023-26117, GHSA-4w6m-h6vm-p6fv
AngularJS		Allows attackers to bypass common image source restrictions	Low	CVE-2024-8373, GHSA-mjmg-cd9h-x2pk
		Allows attackers to bypass common image source restrictions	Low	CVE-2024-8373, GHSA-mjmg-3h7h-hagg
Angular		Vulnerable to super-linear runtime due to backtracking	High	CVE-2024-21490, GHSA-4w6m-5hch-xrj2

Library	Version	Vulnerability Description	Severity	Reference (CVE/GHSA)
Angular	-	Regular Expression Denial of Service via $resource service	Medium	CVE-2023-26117, GHSA-2q9v-v9fw-q6gx
	-	Regular Expression Denial of Service via angular.copy() utility	Medium	CVE-2023-26116, GHSA-2v7f-hj26-jp6j

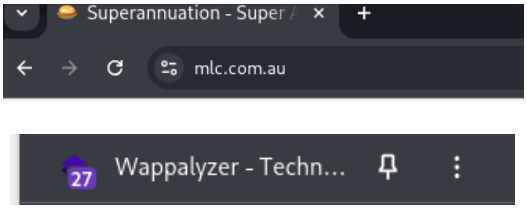
	-	Cross-Site Scripting (XSS) via $sce service	Medium	CVE-2023-25859, GHSA-9r3j-9w6m-6j9g
	-	Regular Expression Denial of Service via input type="password" directive	Medium	CVE-2023-26118, GHSA-4w6m-p6hr-9w9v
	-	Super-linear runtime due to backtracking vulnerability	High	CVE-2023-21990, GHSA-6w5v-5h3r-xn92
AngularJS	-	Allows attackers to bypass common image source restrictions	Low	CVE-2020-8373, GHSA-m9g8-3h7h-hwpg
	-	Allows attackers to bypass common image source restrictions	Low	CVE-2020-8372, GHSA-m9g8-3h7h-hwpg

Library	Version	Vulnerability Description	Severity	Reference (CVE/GHSA)	Found at URL
jQuery-ui-dialog	1.10.1	Bootstrap before 4.0.0 is End-of-Life and no longer maintained	Low	[GHSA-hj6q-6c4v-9fgh]	https://www.mic.com.au/etc.clientlibs/bootstrap/clientlibs/bootstrap-base-design/bootstrap-base-clientlibs/jquery-ui.js
		XSS vulnerability on closeText option	Medium	CVE-2016-7103	
jQuery-ui	1.10.1	XSS in the altField option of the Datepicker widget	Medium	CVE-2021-41184	https://www.mic.com.au/etc.clientlibs/bootstrap/clientlibs/bootstrap-base-design/bootstrap-base-clientlibs/jquery-ui.js
		XSS when refreshing a checkboxradio with HTML in the label	Medium	CVE-2022-31160	
jQuery-ui-aem	1.12.4	XSS when refreshing a checkboxradio with HTML in the label	Medium	CVE-2022-31160	https://www.mic.com.au/etc.clientlibs/clientlibs/granite/jquery-le0c4353f0000ecee7c7037f3f1a4aebc/jquery-ui.js

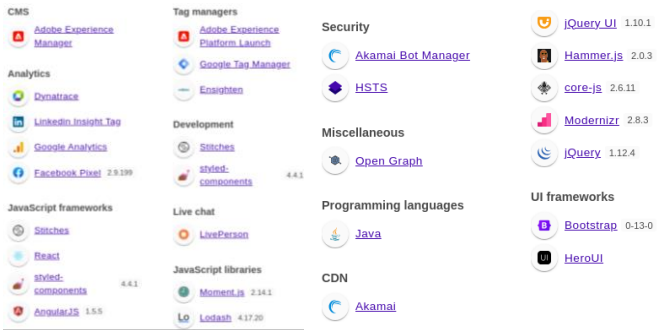
Library	Version	Vulnerability Description	Severity	Reference (CVE/GHSA)
jQuery	1.x, 2.x	End-of-Life—no longer receiving security updates	Low	-
jQuery	< 3.4.0	Mishandles jQuery.extend(true, ...)—potential Object.prototype pollution	Medium	CVE-2019-11358, GHSA-c6qr-hxjj-8vh3
jQuery	< 3.5.0	HTML containing elements may execute arbitrary code	Medium	CVE-2020-11022, GHSA-gxr4-xjj5-5px2
jQuery	< 3.5.0	jQuery.htmlPrefilter may introduce XSS	Medium	CVE-2020-11023, GHSA-q6qp-xvpc-9m8c
Moment.js	2.14.1	Various vulnerabilities, references provided in GitHub issues	Unknown	GitHub Issues

Library	Version	Vulnerability Description	Severity	Reference (CVE/GHSA)	Found at URL
Moment.js	2.14.1	Regular Expression Denial of Service (ReDoS) vulnerability	High	CVE-2022-31160, GHSA-2fr6-h9rk-35g3	https://www.example.com/moment.js
		User-provided locale may lead to unintended script execution	Medium	CVE-2022-43306, GHSA-xpf4-46gq-29qx	

1.2 Wappalyzer



Here are the results of the Wappalyzer detect



2. Multi Tool Webs Vulnerability Scanning

2.1 Rapidscan

```
┌──(binosh㉿BINZ)-[~/Desktop/WS Assingment/Tools/rapidscan]
└─$ python3 rapidscan.py -u https://www.bathandbodyworks.com/
```

Out of 80 vulnerabilities checked for https://www.mlc.com.au/ **4 vulnerabilities were detected**

```
Vulnerability Threat Level
        medium  X-XSS Protection is not Present
Vulnerability Definition
        As the target is lacking this header, older browsers will be prone to Reflected XSS attacks.
Vulnerability Remediation
        Modern browsers does not face any issues with this vulnerability (missing headers). However, older browsers are strong
ly recommended to be upgraded.
```

3. OWASP ZAP

```
PII Disclosure
URL:        https://www.mlc.com.au/personal/insights/2024-calendar-year-in-review
Risk:       High
Confidence: High
Parameter:
Attack:
Evidence:   5794539934276
CWE ID:     359
WASC ID:    13
Source:     Passive (10062 - PII Disclosure)
Input Vector:
Description:
The response contains Personally Identifiable Information, such as CC number, SSN and
similar sensitive data.
```

Detected Vulnerability: PII (Personally Identifiable Information) Disclosure

The identified PII disclosure vulnerability poses a high security risk and must be addressed promptly to mitigate data exposure and regulatory concerns. A comprehensive security plan should be implemented to protect sensitive information and prevent future occurrences.

- **Risk Level:** High
- **Confidence Level:** High
- **Vulnerability Type:** Exposure of sensitive data
- **CWE ID:** 359 – Exposure of Sensitive Information to an Unauthorized Actor
- **WASC ID:** 13 – Information Leakage
- **Evidence of Exposure:** 5794539934276 (Potentially a credit card or identification number
- **Scan Type:** Passive scan (10062 - PII Disclosure)

Impact Assessment

Potential Risks

- Unauthorized access to sensitive financial or personal information
- Identity theft, fraud, or regulatory violations
- Loss of user trust and potential legal implications

Recommended Remediation

Short-Term Fixes

- Mask or redact exposed PII in responses
- Implement proper input validation and sanitization
- Conduct a thorough security review to identify other exposures

Long-Term Fixes

- Implement stricter access controls for sensitive data
- Apply encryption for storage and transmission of PII
- Regularly audit application security using OWASP best practices

Vulnerable JS Library

URL:	https://www.mlc.com.au/etc.clientlibs/common-designs/clientlibs/common-designs/angular/1.5.5/angular.lc-5e2d2057d96976d43c756dcc1efaa1dc-lc.js
Risk:	High
Confidence:	Medium
Parameter:	
Attack:	
Evidence:	/* AngularJS v1.5.5
CWE ID:	1395
WASC ID:	
Source:	Passive (10003 - Vulnerable JS Library (Powered by Retire.js))
Input Vector:	

Description:

The identified library appears to be vulnerable.

Detected Vulnerability: Use of Vulnerable JavaScript Library

The presence of an outdated AngularJS library (v1.5.5) introduces potential security vulnerabilities. Immediate action is recommended to patch or upgrade the affected JavaScript library, ensuring robust client-side security measures to mitigate risks.

- **Library:** AngularJS v1.5.5
- **Risk Level:** High
- **Confidence Level:** Medium
- **Vulnerability Type:** Potential security flaws in outdated JavaScript framework
- **CWE ID:** 1395 – Use of Web Platform Features That Might Cause Security Risks
- **WASC ID:** 10 – Improper Input Handling

Details of Vulnerability

- **Source:** Passive scan (10003 - Vulnerable JS Library)
- **Evidence of Vulnerability:** AngularJS v1.5.5

Impact Assessment

Potential Risks:

- Exploitable security flaws due to outdated AngularJS version
- Increased risk of client-side attacks such as **Cross-Site Scripting (XSS)**
- Possible exposure to known vulnerabilities impacting application security

Recommended Remediation

Short-Term Fixes:

- Review known vulnerabilities for AngularJS v1.5.5 and apply available patches
- Implement client-side security controls such as **Content Security Policy (CSP)**

Long-Term Fixes

- Upgrade AngularJS to the latest stable version or migrate to a supported framework
- Regularly audit and update dependencies to minimize security risks

Absence of Anti-CSRF Tokens

URL:	https://bourkestreetgreen.com.au/
Risk:	Medium
Confidence:	Low
Parameter:	
Attack:	
Evidence:	<form method="POST" action="/" id="_content_racv_microsites_bourke-street-green_jcr_content_par_canvas_2096355623_canvas_par_gridcolumn_1_start" name="_content_racv_microsites_bourke-street-green_jcr_content_par_canvas_2096355623_canvas_par_gridcolumn_1_start" enctype="multipart/form-data">
CWE ID:	352
WASC ID:	9
Source:	Passive (10202 - Absence of Anti-CSRF Tokens)
Input Vector:	

Description:

Detected Vulnerability: Absence of Anti-CSRF Tokens

The absence of Anti-CSRF Tokens in form submissions introduces a medium security risk. To mitigate potential CSRF attacks, token-based validation and server-side protections should be implemented to secure user transactions.

- **Risk Level:** Medium
- **Confidence Level:** Low
- **Vulnerability Type:** Cross-Site Request Forgery (CSRF) Risk
- **CWE ID:** 352 – Cross-Site Request Forgery (CSRF)
- **WASC ID:** 9 – CSRF

Details of Vulnerability

- **Parameter Affected:** Form method "POST"
- **Evidence:** Form method POST includes the IDs: content and canvas, but lacks anti-CSRF protection
- **Source:** Passive scan (10202 - Absence of Anti-CSRF Tokens)

Impact Assessment

Potential Risks:

Attackers could trick users into making unauthorized requests

Malicious CSRF attacks could lead to account compromise or unauthorized transactions

Increased risk of exploitation on forms requiring authentication

Recommended Remediation

Short-Term Fixes:

Implement CSRF tokens in all forms handling sensitive user actions

Validate CSRF tokens server-side before processing requests

Long-Term Fixes

Adopt security measures like **SameSite cookies** to limit unauthorized requests

Regularly audit forms and authentication mechanisms for CSRF vulnerabilities

CSP: Failure to Define Directive with No Fallback

URL:	https://www.mlc.com.au/
Risk:	Medium
Confidence:	High
Parameter:	Content-Security-Policy
Attack:	
Evidence:	frame-ancestors 'self'
CWE ID:	693
WASC ID:	15
Source:	Passive (10055 - CSP)
Alert Reference:	10055-13
Input Vector:	

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.

Detected Vulnerability: CSP Failure to Define Directive with No Fallback

The misconfiguration in **Content-Security-Policy** creates potential security **weaknesses** that could be exploited for Clickjacking attacks or unauthorized content embedding. **Immediate CSP policy adjustments** are recommended to enforce stricter security measures and mitigate risks.

- **Risk Level:** Medium
- **Confidence Level:** High
- **Vulnerability Type:** Weak Content Security Policy Implementation
- **CWE ID:** 693 – Protection Mechanism Failure
- **WASC ID:** 15 – Application Misconfiguration

Details of Vulnerability

- **Key Parameter Affected:** Content-Security-Policy
- **Attack Vector:** frame-ancestors 'self'
- **Evidence:** CSP directive missing fallback protections
- **Source:** Passive scan (10055 - CSP)

Impact Assessment

Potential Risks

- Weak CSP configurations may allow unauthorized framing of content
- Potential exploitation for **Clickjacking** attacks
- Insufficient directive definitions can lead to **data exfiltration vulnerabilities**

Recommended Remediation

Short-Term Fixes

- Define explicit fallback directives within the CSP header
- Ensure frame-ancestors policy restricts only **trusted origins**

Long-Term Fixes

- Conduct regular CSP audits to detect misconfigurations
- Strengthen security policies to prevent Clickjacking attempts
- Implement **strict CSP policies** with default-src 'none' and precise resource definitions

CSP: Wildcard Directive
URL: https://www.mlc.com.au/
Risk: Medium
Confidence: High
Parameter: Content-Security-Policy
Attack:
Evidence: frame-ancestors 'self'
CWE ID: 693
WASC ID: 15
Source: Passive (10055 - CSP)
Alert Reference: 10055-4
Input Vector:
Description:
Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data

Detected Vulnerability: CSP Wildcard Directive Misconfiguration

The CSP Wildcard Directive Misconfiguration introduces security risks, particularly Clickjacking and Content Injection vulnerabilities. Immediate policy adjustments are needed to enhance website security and prevent unauthorized embedding.

- **Risk Level:** Medium
- **Confidence Level:** High
- **Vulnerability Type:** Weak Content Security Policy Implementation
- **Key Parameter:** Content-Security-Policy
- **Attack Vector:** frame-ancestors 'self'
- **Alert Reference:** 10055-4

Details of Vulnerability

- **Source:** Passive scan (10055 - CSP)
- **Issue Description:** CSP is misconfigured, allowing potential cross-site attacks
- **Impact:** Inadequate protections against **Cross-Site Scripting (XSS)** and **Clickjacking**

Impact Assessment

Potential Risks

- Web pages could be embedded within **malicious iframes**, leading to clickjacking
- Weak CSP definitions may allow **unauthorized content injection**
- Potential risk of **data exfiltration** through unrestricted content origins

Recommended Remediation

Short-Term Fixes

- Restrict frame-ancestors to **trusted domains only**
- Strengthen CSP definitions by removing wildcard (*) entries

Long-Term Fixes

- Implement strict CSP policies with directives such as default-src 'none'
- Conduct regular CSP audits to **detect misconfigurations**
- Enforce **XSS protection mechanisms** to mitigate unauthorized script execution

CSP: script-src unsafe-inline

URL:	https://www.mlc.com.au/
Risk:	Medium
Confidence:	High
Parameter:	Content-Security-Policy
Attack:	
Evidence:	frame-ancestors 'self'
CWE ID:	693
WASC ID:	15
Source:	Passive (10055 - CSP)
Alert Reference:	10055-5
Input Vector:	

Description:

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including (but not limited to) Cross Site Scripting (XSS), and data

Detected Vulnerability: CSP Directive Misconfiguration

The CSP Directive Misconfiguration introduces security risks, particularly Clickjacking and Content Injection vulnerabilities. Immediate policy adjustments are needed to enhance website security and prevent unauthorized embedding.

- **Risk Level:** Medium
- **Confidence Level:** High
- **Vulnerability Type:** Weak Content Security Policy Implementation
- **CWE ID:** 693 – Protection Mechanism Failure
- **WASC ID:** 15 – Application Misconfiguration

Details of Vulnerability

- **Key Parameter Affected:** Content-Security-Policy
- **Attack Vector:** frame-ancestors 'self'
- **Source:** Passive scan (10055 - CSP)
- **Issue Description:** CSP is misconfigured, allowing potential cross-site attacks
- **Impact:** CSP fails to enforce strong protection against **Cross-Site Scripting (XSS)** and **Clickjacking**

Impact Assessment

Potential Risks

- Web pages could be embedded within **malicious iframes**, leading to Clickjacking attacks
- Weak CSP definitions may allow **unauthorized content injection**
- Potential risk of **data exfiltration** through unrestricted content origins

Recommended Remediation

Short-Term Fixes

- Restrict frame-ancestors to **trusted domains only**
- Strengthen CSP definitions to prevent unauthorized framing

Long-Term Fixes

- Implement strict CSP policies with directives such as default-src 'none'
- Conduct regular CSP audits to **detect misconfigurations**
- Enforce **XSS protection mechanisms** to mitigate unauthorized script execution

Detected Vulnerability: CSP Misconfiguration (Unsafe Style Directive)

The CSP Unsafe Style Directive Misconfiguration introduces security risks, particularly XSS vulnerabilities and content injection risks. Immediate policy adjustments are needed to enhance website security and prevent unauthorized inline styling.

- **Risk Level:** Medium
- **Confidence Level:** High
- **Vulnerability Type:** Weak Content Security Policy Implementation
- **CWE ID:** 693 – Protection Mechanism Failure
- **WASC ID:** 15 – Application Misconfiguration
- **Alert Reference:** 10055-6

Details of Vulnerability

- **Key Parameter Affected:** Content-Security-Policy
- **Attack Vector:** style-src 'unsafe-inline'
- **Evidence:** frame-ancestors 'self'
- **Source:** Passive scan (10055 - CSP)
- **Issue Description:** CSP allows unsafe inline styles, increasing XSS risks
- **Impact:** CSP fails to enforce strong protection against **Cross-Site Scripting (XSS)**

Impact Assessment

Potential Risks

- Inline styles could be exploited for **XSS attacks**
- Weak CSP policies may allow **unauthorized content injection**
- Possible impact on website **security integrity**

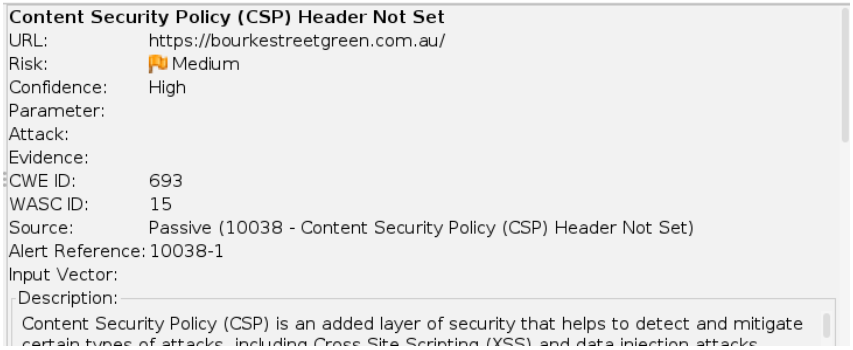
Recommended Remediation

Short-Term Fixes

- Remove 'unsafe-inline' directive from style-src
- Use **nonce-based CSP policies** for inline styling

Long-Term Fixes:

- Implement **strict CSP policies** with default-src 'none'
- Conduct regular CSP audits to **detect misconfigurations**
- Enforce **XSS protection mechanisms** such as CSP header refinements



Content Security Policy (CSP) Header Not Set

URL:	https://bourkestreetgreen.com.au/
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
Input Vector:	

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

Detected Vulnerability: CSP Header Not Set

The missing **Content-Security-Policy Header** presents a **medium security risk**, making the application susceptible to **Cross-Site Scripting (XSS) and content injection vulnerabilities**. **Immediate CSP implementation** is advised to strengthen security defenses.

- **Risk Level:** Medium
- **Confidence Level:** High
- **Vulnerability Type:** Lack of Content Security Policy Header
- **CWE ID:** 693 – Protection Mechanism Failure
- **WASC ID:** 15 – Application Misconfiguration
- **Alert Reference:** 10038-1

Details of Vulnerability

- **Key Parameter Affected:** Content-Security-Policy
- **Attack Vector:** None
- **Evidence:** CSP missing from headers
- **Source:** Passive scan (10038 - Content Security Policy (CSP) Header Not Set)
- **Issue Description:** The web server lacks a CSP header, potentially allowing unsafe content execution

Impact Assessment

Potential Risks

- Increased vulnerability to **Cross-Site Scripting (XSS)** attacks
- Higher risk of **Clickjacking** exploitation
- Possible exposure to unauthorized content injection

Recommended Remediation

Short-Term Fixes:

- Define and set the **Content-Security-Policy** header to restrict allowed content sources
- Implement strict resource loading policies to prevent malicious injections

Long-Term Fixes

- Regularly audit CSP configurations for **completeness and accuracy**
- Apply restrictive CSP directives to mitigate **XSS and Clickjacking risks**
- Ensure CSP headers explicitly specify **trusted content origins**

Cross-Domain Misconfiguration

URL: https://www.mlc.com.au/robots.txt
Risk: Medium
Confidence: Medium
Parameter:
Attack:
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
WASC ID: 14
Source: Passive (10098 - Cross-Domain Misconfiguration)
Input Vector:

Description:

Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

Detected Vulnerability: Cross-Domain Misconfiguration

The Cross-Domain Misconfiguration creates a medium security risk, potentially allowing unauthorized third-party access to web resources. Immediate policy adjustments are recommended to restrict cross-origin requests and enhance security measures.

- **Risk Level:** Medium
- **Confidence Level:** Medium
- **Vulnerability Type:** Improper Cross-Origin Resource Sharing (CORS) configuration
- **Key Parameter:** Access-Control-Allow-Origin: *
- **CWE ID:** 264 – Permissions, Privileges, and Access Controls
- **WASC ID:** 14 – Server Misconfiguration
- **Alert Reference:** 10098 - Cross-Domain Misconfiguration

Details of Vulnerability

- **Source:** Passive scan (10098 - Cross-Domain Misconfiguration)
- **Issue Description:** Misconfigured CORS settings may allow unauthorized resource loading
- **Impact:** Potential for unauthorized data exposure through relaxed origin rules

Impact Assessment

Potential Risks

- Third-party domains can retrieve resources without explicit authorization
- Increased risk of **data theft** or **resource abuse**
- Possible exposure of API responses meant for internal or trusted environments

Recommended Remediation

Short-Term Fixes:

- Restrict Access-Control-Allow-Origin to specific trusted domains
- Avoid using wildcard (*) settings for CORS configuration

Long-Term Fixes:

- Conduct security audits to **verify and test access control settings**
- Implement **strict authentication mechanisms** before allowing cross-origin requests
- Regularly update server security policies to **prevent unintended data exposure**

Vulnerable JS Library

URL: https://www.mlc.com.au/etc.clientlibs/bootstrap/clientlibs/bootstrap/bootstrap-base-design/bootstrap-base/clientlibs-jqueryui.lc-3734498ee27a0d8c6769041f3d1407b5-lc.js
Risk: Medium
Confidence: Medium
Parameter:
Attack:
Evidence: /*! jQuery UI - v1.10.1
CWE ID: 1395
WASC ID:
Source: Passive (10003 - Vulnerable JS Library (Powered by Retire.js))
Input Vector:
Description:
The identified library appears to be vulnerable.

Detected Vulnerability: Outdated JavaScript Library

The presence of an outdated **jQuery UI library (v1.10.1)** introduces potential security vulnerabilities. Immediate **patching or upgrading** the affected JavaScript library is recommended to improve web application security.

- **Library:** jQuery UI v1.10.1
- **Risk Level:** Medium
- **Confidence Level:** Medium
- **Vulnerability Type:** Security flaws due to outdated JavaScript framework
- **CWE ID:** 1395 – Use of Web Platform Features That Might Cause Security Risks
- **WASC ID:** 10 – Improper Input Handling

Details of Vulnerability

- **Source:** Passive scan (10003 - Vulnerable JS Library)
- **Issue Description:** Outdated **jQuery UI** library may contain security vulnerabilities
- **Impact:** Potential exposure to **Cross-Site Scripting (XSS), security bypass issues, or other client-side attacks**

Impact Assessment

Potential Risks

- Possible exploitation of known vulnerabilities due to outdated jQuery UI version
- Increased risk of **XSS attacks** from unpatched flaws
- Potential compromise of web application security

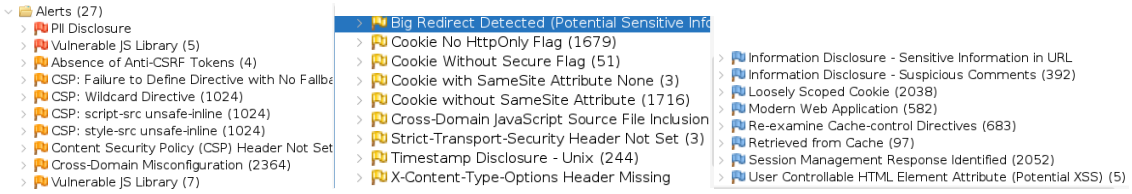
Recommended Remediation

Short-Term Fixes

- Review known vulnerabilities for jQuery UI v1.10.1 and apply available patches
- Implement **Content Security Policy (CSP)** to mitigate script-based attacks

Long-Term Fixes

- Upgrade jQuery UI to the **latest stable version**
- Conduct regular dependency audits to minimize security risks



How to mitigate the Vulnerability

- To install security patches, update to the most recent version of Angular.
- Verify and clean user inputs to avoid going back too far
- Strict Content Security Policy (CSP) headers should be used to stop illegal script execution.
- Switch to an updated, security-patched version of Angular.
- Regular expressions should be optimized to reduce undue computing complexity.
- To install security patches, update to the most recent version of Angular.
- Verify and clean user inputs to avoid going back too far.
- Adopt stringent Content Security Policy (CSP) headers to stop scripts from running without authorization.
- Switch to an updated, security-patched version of Angular.
- Regular expressions should be optimized to reduce undue computing complexity.
- Make sure you use an Angular patched version.
- The best course of action is to switch to Angular as AngularJS is nearing the end of its existence.
- Use CSP headers to limit the origins of dangerous images.
- To get security updates and ongoing support, update to Bootstrap 4.0.0 or later.
- Update to jQuery UI 1.13.2 or later, as this problem has been fixed.
- Clean user inputs before transferring them to user interface elements.
- Use CSP headers to prevent malicious scripts from running.
- Clean up locale inputs before sending them to functions in Moment.js.
- Limit dynamic locale changes to those values that you can trust.

Proof of Report Submission

Insignia Financial Vulnerability Disclosure Program has received **WS Assingment**

Thank you Binosh ,

We have received your Bugcrowd submission for engagement insigniafinancial.

Submission Details

Submitted
04 May 2025 19:27:46 UTC

Submission ID
193870de-f8e9-4841-9c80-acec1424f2a5

VRT
Cryptographic Weakness > Broken Cryptography > Use of Vulnerable Cryptographic Library

View Submission Details