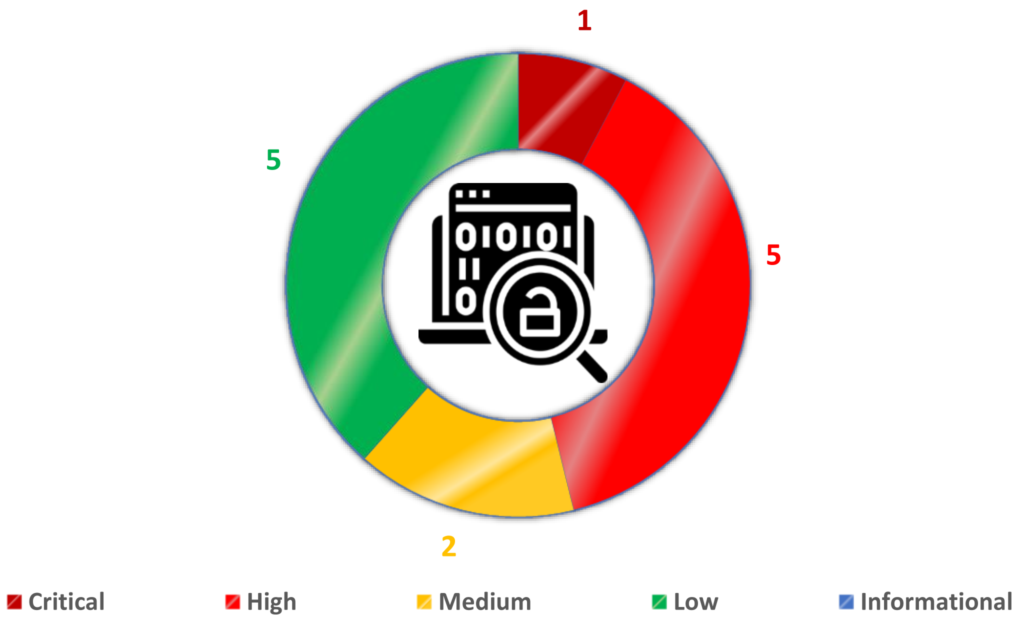
Annexure – IV

URL: https://www.mjvaluemart.com/

OVERALL VULNERABILITIES



Summary of Findings:

Sl. No.	Vulnerability Name	Vulnerability Risk Type
1	Out of date Version (Crypto JS)	Critical
2	Application-level DOS at Registration page	High
3	Insecure Authentication: OTP Bypass	
4	Out-of-date Version (Moment.js)	
5	Cross Site Scripting	
6	Out-of-date Version (Underscore.js)	
7	Out-of-date Version (jQuery)	Medium
8	Out-of-date Version (Knockout)	
9	Version Disclosure (Bootstrapjs)	Low
10	Version Disclosure (jQuery)	
11	Version Disclosure (jQuery Migrate)	
12	Version Disclosure (Underscorejs)	
13	Internal Server Error	
14	HTTP Strict Transport Security (HSTS) Policy Not Enabled	

➢ Detail Findings:

1. Vulnerability Name: Out of date Version (Crypto JS)
Vulnerability Rating: Critical

CVSS: 9.1 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N **CVE-**2023-46233,**CWE-**916

Vulnerability Description:

crypto-js is a JavaScript library of crypto standards. Prior to version 4.2.0, crypto-js PBKDF2 is 1,000 times weaker than originally specified in 1993, and at least 1,300,000 times weaker than current industry standard. This is because it both defaults to SHA1, a cryptographic hash algorithm considered insecure since at least 2005, and defaults to one single iteration, a 'strength' or 'difficulty' value specified at 1,000 when specified in 1993. PBKDF2 relies on iteration count as a countermeasure to preimage and collision attacks.

Affected URL(s):

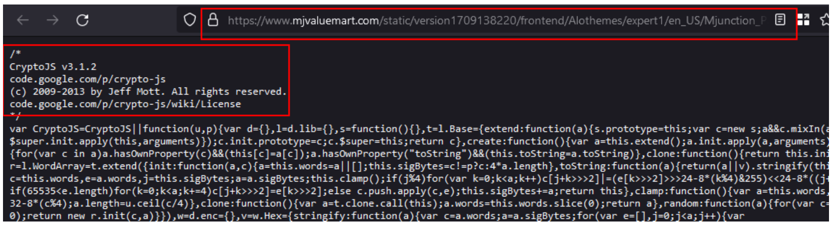
https://www.mjvaluemart.com/static/version1709138220/frontend/Alothemes/expert1/en_US/Mjunction_PassEncrypt/js/cryptojs-aes.min.js

Impact:

If used to protect passwords, the impact is high. If used to generate signatures, the impact is high. Version 4.2.0 contains a patch for this issue. As a workaround, configure crypto-js to use SHA256 with at least 250,000 iterations.

Proof of Concept:

Go to the Affected URL.



https://www.mjvaluemart.com/static/version1709138220/frontend/Alothemes/expert1/en_US/Mjunction_P

```
/*
CryptoJS v3.1.2
code.google.com/p/crypto-js
(c) 2009-2013 by Jeff Mott. All rights reserved.
code.google.com/p/crypto-js/wiki/License
*/
var CryptoJS=CryptoJS||function(u,p){var d={},l=d.lib={},s=function(){},t=l.Base={extend:function(a){s.prototype=this;var c=new s;a&&c.mixIn(a
$super.init.apply(this,arguments)});c.init.prototype=c;c.$super=this;return c},create:function(){var a=this.extend();a.init.apply(a,arguments)
{for(var c in a)a.hasOwnProperty(c)&&(this[c]=a[c]);a.hasOwnProperty("toString")&&(this.toString=a.toString)},clone:function(){return this.ini
r=l.WordArray=t.extend({init:function(a,c){a=this.words=a||[];this.sigBytes=c!=p?c:4*a.length},toString:function(a){return(a||v).stringify(thi
c=this.words,e=a.words,j=this.sigBytes;a=a.sigBytes;this.clamp();if(j%4)for(var k=0;k<a;k++)c[j+k>>>2]|=(e[k>>>2]>>>24-8*(k%4)&255)<<24-8*((j+
if(65535<e.length)for(k=0;k<a;k+=4)c[j+k>>>2]=e[k>>>2];else c.push.apply(c,e);this.sigBytes+=a;return this},clamp:function(){var a=this.words,
32-8*(c%4);a.length=u.ceil(c/4)},clone:function(){var a=t.clone.call(this);a.words=this.words.slice(0);return a},random:function(a){for(var c=
0);return new r.init(c,a)}}),w=d.enc={},v=w.Hex={stringify:function(a){var c=a.words;a=a.sigBytes;for(var e=[],j=0;j<a;j++){var
```

Remediation:

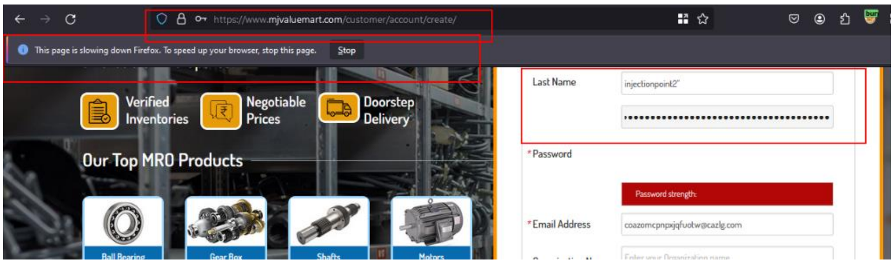
This vulnerability can be avoided by setting PBKDF2 to use SHA-256 instead of SHA-1 and increasing the number of iterations to a sufficiently high value depending on the intended use. See, for example, the OWASP PBKDF2 Cheat Sheet for recommendations.

Reference Link(s):

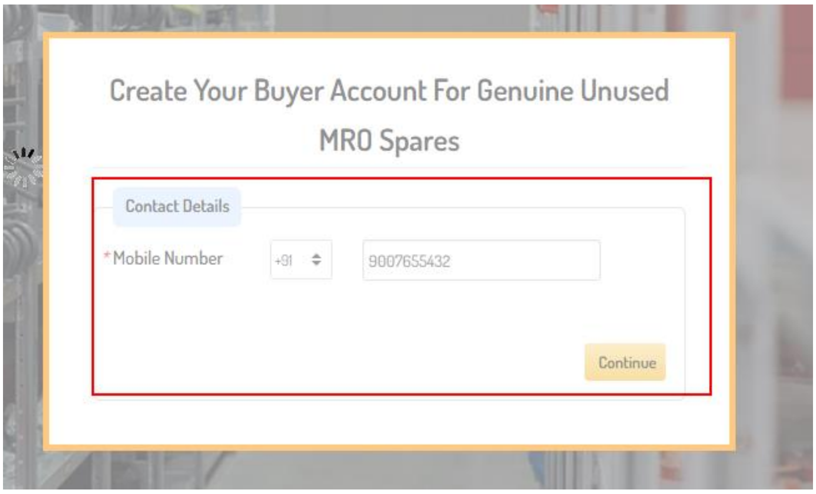
https://nvd.nist.gov/vuln/detail/cve-2020-11022

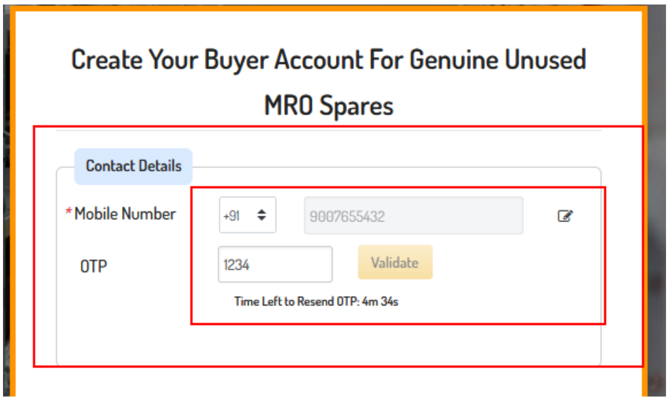
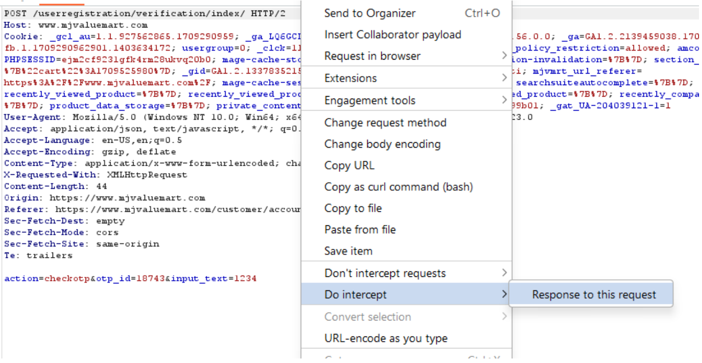
https://security.snyk.io/vuln/SNYK-JS-CRYPTOJS-6028119

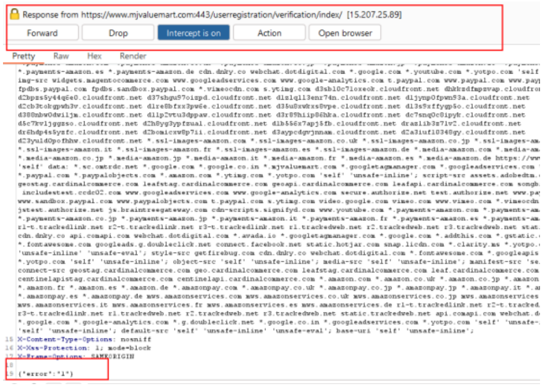
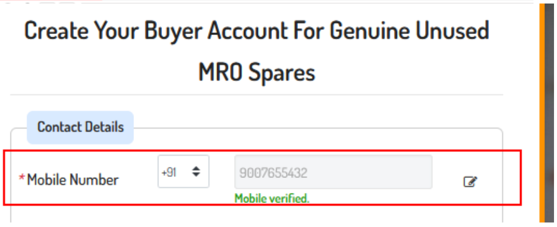
2. Vulnerability Name: Application-level DOS at Registration page
Vulnerability Rating: High

CVSS: 7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Vulnerability Description:	A Denial-of-Service (DoS) vulnerability has been identified in the authentication mechanism of the client's website, a web application/service. This vulnerability arises when an attacker submits an unusually long password during the login process. Upon receiving such input, the website becomes unresponsive, ultimately leading to a state of service degradation or complete unavailability. This vulnerability can be exploited by malicious actors to execute a Distributed Denial-of-Service (DDoS) attack, disrupting legitimate users' access to the website. **Affected URL(s):** https://www.mjvaluemart.com/customer/account/create/
Impact:	It's possible to cause a denial a service attack on the server. This may lead to the website becoming unavailable or unresponsive.
Proof of Concept: **Step #** Go to the affected URL and Create and User. In the Password Field enter **character Greater than 1000**. The website Gets Unresponsive for more than 1 hour.	 https://www.mjvaluemart.com/customer/account/create/ This page is slowing down Firefox. To speed up your browser, stop this page. Last Name injectionpoint2" Email Address coazomcpnpxjqfuotw@cazlg.com Stop Verified Inventories Negotiable Prices Doorstep Delivery Our Top MRO Products Ball Bearing Gear Box Shafts Motors *Password Password strength: Enter your Organization name
Remediation:	The password hashing implementation must be fixed to limit the maximum length of accepted passwords. **Reference Link(s):** https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

3. Vulnerability Name: Insecure Authentication: OTP Bypass
Vulnerability Rating: High

CVSS: 7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
Vulnerability Description:	The website's registration page includes OTP (One-Time Password) validation as an additional security measure to ensure that the user registering is legitimate. However, the system allows attackers to bypass this OTP validation by manipulating the response during the registration process. This means that even without providing the valid OTP, an attacker can successfully register using any legitimate user account. **Affected URL(s):** https://www.mjvaluemart.com/customer/account/create/
Impact:	The impact of this vulnerability is significant as it undermines the security mechanism put in place to verify the authenticity of user registrations. By bypassing OTP validation, attackers can exploit this vulnerability to create unauthorized accounts using legitimate user credentials. This can lead to various malicious activities such as identity theft, fraud, unauthorized access to sensitive information, or even compromise of the entire system.
Proof of Concept: **Step 1#** Go to the Affected URL and Enter Victims Phone Number and send it for verification.	 Create Your Buyer Account For Genuine Unused MRO Spares Contact Details *Mobile Number +91 9007655432 Continue

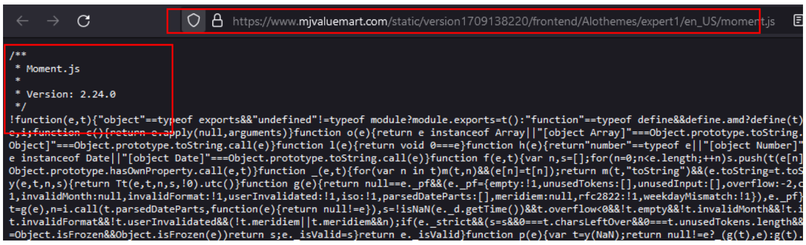
Step 2#
Enter a random otp and click on validate OTP and intercept using any Proxy tool.
	
	Create Your Buyer Account For Genuine Unused MRO Spares
	Contact Details
	*Mobile Number +91 9007655432
	OTP 1234 Validate
	Time Left to Resend OTP: 4m 34s
	
	`POST /userregistration/verification/index/ HTTP/2`
	`Host: www.mjvaluemart.com`
	`Cookie: _gcl_au=1.1.927562865.1709290959; _ga_LQ6GCI 56.0.0; _ga=GA1.2.2139459038.170`
	`fb.1.1709290962901.1403634172; usergroup=0; _clck=1l _policy_restriction=allowed; amco`
	`PHPSESSID=ejm2cf9231gfk4rm28ukvq20b0; mage-cache-sto ion-invalidation=%7B%7D; section_`
	`%7B%22cart%22%3A1709525980%7D; _gid=GA1.2.1337835215 i; mjvmrt_url_referer=`
	`https%3A%2F%2Fwww.mjvaluemart.com%2F; mage-cache-ses searchsuiteautocomplete=%7B%7D;`
	`recently_viewed_product=%7B%7D; recently_viewed_proc ed_product=%7B%7D; recently_compa`
	`%7B%7D; product_data_storage=%7B%7D; private_content 99b01; _gat_UA-204039121-1=1`
	`User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64 23.0`
	`Accept: application/json, text/javascript, */*; q=0.`
	`Accept-Language: en-US,en;q=0.5`
	`Accept-Encoding: gzip, deflate`
	`Content-Type: application/x-www-form-urlencoded; cha`
	`X-Requested-With: XMLHttpRequest`
	`Content-Length: 44`
	`Origin: https://www.mjvaluemart.com`
	`Referer: https://www.mjvaluemart.com/customer/accour`
	`Sec-Fetch-Dest: empty`
	`Sec-Fetch-Mode: cors`
	`Sec-Fetch-Site: same-origin`
	`Te: trailers`
	
	`action=checkotp&otp_id=18743&input_text=1234`
	 Send to Organizer Ctrl+O
	Insert Collaborator payload
	Request in browser
	Extensions
	Engagement tools
	Change request method
	Change body encoding
	Copy URL
	Copy as curl command (bash)
	Copy to file
	Paste from file
	Save item
	Don't intercept requests
	Do intercept
	Response to this request
	Convert selection
	URL-encode as you type

Step 3#
Now change the Error Response form server from
{"error":"1"} -> {"error":"0"}
	
	Response from https://www.mjvaluemart.com:443/userregistration/verification/index/ [15.207.25.89]
	 Forward Drop Intercept is on Action Open browser
	Pretty Raw Hex Render
	`*.payments-amazon.es *.payments-amazon.de cdn.dnky.co webchat.dotdigital.com *.google.com *.youtube.com *.yotpo.com 'self`
	`img-src widgets.magentocommerce.com www.googleadservices.com www.google-analytics.com t.paypal.com www.paypal.com www.payp`
	`fpdbs.paypal.com fpdbs.sandbox.paypal.com *.vimeocdn.com s.ytimg.com d3sbl0c7loxeok.cloudfront.net dhkkzdfmpzvap.cloudfro`
	`d2bpss6y44q6e0.cloudfront.net d37shgu97oizpd.cloudfront.net dlslql13enr74n.cloudfront.net dljymp0fpwn93a.cloudfront.net`
	`d2cb3tokgpwh3v.cloudfront.net dlre8bfxx3pw6e.cloudfront.net d35u8xwkxs8vpe.cloudfront.net dl3s9xffygp5o.cloudfront.net`
	`d388nbw0dwiljm.cloudfront.net dllp2vtu3dppaw.cloudfront.net d3r89hiip86hka.cloudfront.net dc7snq0c8ipyk.cloudfront.net`
	`d5c7kvljggzso.cloudfront.net d2h8yg3ypfzual.cloudfront.net dlb556x7apj5fb.cloudfront.net drazlib3z71v2.cloudfront.net`
	`dr6hdp4s5yzfc.cloudfront.net d2bomicxw8p7ii.cloudfront.net d3aypcdgvjnnam.cloudfront.net d2a3iufl0348gy.cloudfront.net`
	`d23yuld0pofhhw.cloudfront.net *.ssl-images-amazon.com *.ssl-images-amazon.co.uk *.ssl-images-amazon.co.jp *.ssl-images-am`
	`*.ssl-images-amazon.it *.ssl-images-amazon.fr *.ssl-images-amazon.es *.ssl-images-amazon.de *.media-amazon.com *.media-am`
	`*.media-amazon.co.jp *.media-amazon.jp *.media-amazon.it *.media-amazon.fr *.media-amazon.es *.media-amazon.de https://ww`
	`'self' data: *.sc.omtrdc.net *.google.com *.google.co.in *.mjvaluemart.com *.googletagmanager.com *.googleadservices.com`
	`*.paypal.com *.paypalobjects.com *.amazon.com *.ytimg.com *.yotpo.com 'self' 'unsafe-inline'; script-src assets.adobedtm.`
	`geostag.cardinalcommerce.com leafstag.cardinalcommerce.com geoapi.cardinalcommerce.com leafapi.cardinalcommerce.com songb`
	`includestest.ccdc02.com www.googleadservices.com www.google-analytics.com secure.authorize.net test.authorize.net www.pa`
	`www.sandbox.paypal.com www.paypalobjects.com t.paypal.com s.ytimg.com video.google.com vimeo.com www.vimeo.com *.vimeocdn`
	`jstest.authorize.net js.braintreegateway.com cdn-scripts.signifyd.com www.youtube.com *.payments-amazon.com *.payments-am`
	`*.payments-amazon.co.jp *.payments-amazon.jp *.payments-amazon.it *.payments-amazon.fr *.payments-amazon.es *.payments-am`
	`rl-t.trackedlink.net r2-t.trackedlink.net r3-t.trackedlink.net rl.trackedweb.net r2.trackedweb.net r3.trackedweb.net stat`
	`cdn.dnky.co api.comapi.com webchat.dotdigital.com *.avada.io *.googletagmanager.com *.google.com *.addthis.com *.gstatic.`
	`*.fontawesome.com googleads.g.doubleclick.net connect.facebook.net static.hotjar.com snap.licdn.com *.clarity.ms *.yotpo.`
	`'unsafe-inline' 'unsafe-eval'; style-src getfirebug.com cdn.dnky.co webchat.dotdigital.com *.fontawesome.com *.googleapis`
	`*.yotpo.com 'self' 'unsafe-inline'; object-src 'self' 'unsafe-inline'; media-src 'self' 'unsafe-inline'; manifest-src 'se`
	`connect-src geostag.cardinalcommerce.com geo.cardinalcommerce.com leafstag.cardinalcommerce.com leaf.cardinalcommerce.com`
	`centinelapistag.cardinalcommerce.com centinelapi.cardinalcommerce.com *.amazon.com *.amazon.co.uk *.amazon.co.jp *.amazon`
	`*.amazon.fr *.amazon.es *.amazon.de *.amazonpay.com *.amazonpay.co.uk *.amazonpay.co.jp *.amazonpay.jp *.amazonpay.it *.a`
	`*.amazonpay.es *.amazonpay.de mws.amazonservices.com mws.amazonservices.co.uk mws.amazonservices.co.jp mws.amazonservices`
	`mws.amazonservices.it mws.amazonservices.fr mws.amazonservices.es mws.amazonservices.de rl-t.trackedlink.net r2-t.tracked`
	`r3-t.trackedlink.net rl.trackedweb.net r2.trackedweb.net r3.trackedweb.net static.trackedweb.net api.comapi.com webchat.d`
	`*.google.com *.google-analytics.com *.g.doubleclick.net *.google.co.in *.googleadservices.com *.yotpo.com 'self' 'unsafe-`
	`'self' 'unsafe-inline'; default-src 'self' 'unsafe-inline' 'unsafe-eval'; base-uri 'self' 'unsafe-inline';`
	`X-Content-Type-Options: nosniff`
	`X-Xss-Protection: 1; mode=block`
	`X-Frame-Options: SAMEORIGIN`
	
	`{"error":"1"}`
	
	Create Your Buyer Account For Genuine Unused MRO Spares
	Contact Details
	*Mobile Number +91 9007655432
	Mobile verified.

Remediation:	**Implement Server-Side Validation**: Ensure that OTP validation is performed securely on the server-side rather than relying solely on client-side validation. This prevents attackers from bypassing validation by manipulating client responses. **Reference Link(s):** https://www.outsystems.com/forums/discussion/67148/otp-validation-server-side/

4. Vulnerability Name: Out-of-date Version (Moment.js)
Vulnerability Rating: High

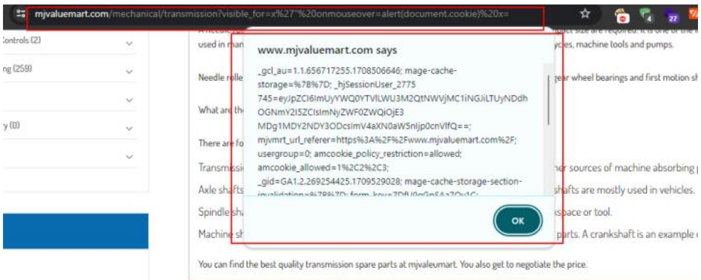
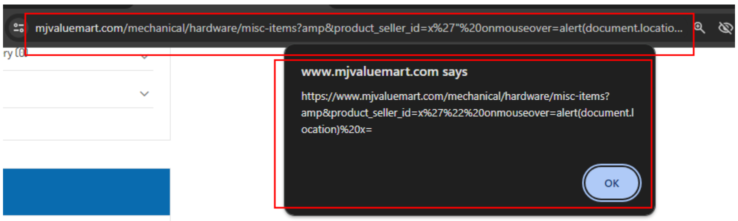
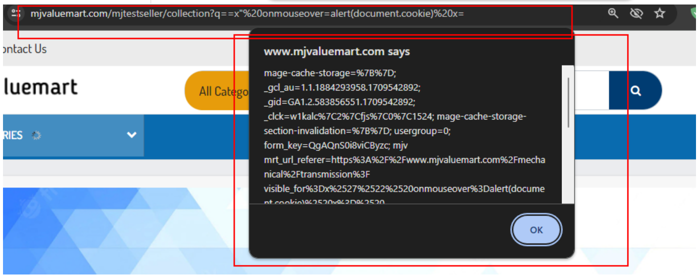
CVSS: 7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	**CVE-**2022-31129

Vulnerability Description:	Moment is a JavaScript date library for parsing, validating, manipulating, and formatting dates. Affected versions of moment were found to use an inefficient parsing algorithm. Specifically using string-to-date parsing in moment (more specifically rfc2822 parsing, which is tried by default) has quadratic (N^2) complexity on specific inputs. Users may notice a noticeable slowdown is observed with inputs above 10k characters. Users who pass user-provided strings without sanity length checks to moment constructor are vulnerable to (Re)DoS attacks. The problem is patched in 2.29.4, the patch can be applied to all affected versions with minimal tweaking. Users are advised to upgrade. Users unable to upgrade should consider limiting date lengths accepted from user input. **Affected URL(s):** https://www.mjvaluemart.com/static/version1709138220/frontend/Alothemes/expert1/en_US/moment.js
Impact:	Since this is an old version of the software, it may be vulnerable to attacks.
Proof of Concept:	
Remediation:	Please upgrade your installation of Moment.js to the latest stable version. **Reference Link(s):** https://momentjs.com/downloads/moment.js

https://www.mjvaluemart.com/static/version1709138220/frontend/Alothemes/expert1/en_US/moment.js

```
/**
 * Moment.js
 *
 * Version: 2.24.0
 */
!function(e,t){"object"==typeof exports&&"undefined"!=typeof module?module.exports=t():"function"==typeof define&&define.amd?define(t)
e,i;function c(){return e.apply(null,arguments)}function o(e){return e instanceof Array||"[object Array]"===Object.prototype.toString.
Object]"===Object.prototype.toString.call(e)}function l(e){return void 0===e}function h(e){return"number"==typeof e||"[object Number]"
e instanceof Date||"[object Date]"===Object.prototype.toString.call(e)}function f(e,t){var n,s=[];for(n=0;n<e.length;++n)s.push(t(e[n]
Object.prototype.hasOwnProperty.call(e,t)}function _(e,t){for(var n in t)m(t,n)&&(e[n]=t[n]);return m(t,"toString")&&(e.toString=t.toS
y(e,t,n,s){return Tt(e,t,n,s,!0).utc()}function g(e){return null==e._pf&&(e._pf={empty:!1,unusedTokens:[],unusedInput:[],overflow:-2,c
1,invalidMonth:null,invalidFormat:!1,userInvalidated:!1,iso:!1,parsedDateParts:[],meridiem:null,rfc2822:!1,weekdayMismatch:!1}),e._pf}
t=g(e),n=i.call(t.parsedDateParts,function(e){return null!=e}),s=!isNaN(e._d.getTime())&&t.overflow<0&&!t.empty&&!t.invalidMonth&&!t.i
t.invalidFormat&&!t.userInvalidated&&(!t.meridiem||t.meridiem&&n);if(e._strict&&(s=s&&0===t.charsLeftOver&&0===t.unusedTokens.length&&
=Object.isFrozen&&Object.isFrozen(e))return s;e._isValid=s}return e._isValid}function p(e){var t=y(NaN);return null!=e?_(g(t),e):g(t).
```

5. Vulnerability Name: Cross Site Scripting
Vulnerability Rating: High

CVSS: 7.4 CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N	**CWE-**79
Vulnerability Description:	Cross-site Scripting, which allows an attacker to execute a dynamic script (JavaScript, VBScript) in the context of the application.
Impact:	There are many different attacks that can be leveraged through the use of cross-site scripting, including: Hijacking user's active session. Mounting phishing attacks. Intercepting data and performing man-in-the-middle attacks. **Affected URL(s):** https://www.mjvaluemart.com/mechanical/transmission?visible_for=x%27%22%20onmouseover=alert(document.cookie)%20x= https://www.mjvaluemart.com/mechanical/hardware/misc-items?amp&product_seller_id=x%27%22%20onmouseover=alert(document.location)%20x= https://www.mjvaluemart.com/mjtestseller/collection?q==x%22%20onmouseover=alert(document.cookie)%20x=
Proof of Concept: **Step#** Go to the affected URL's	 mjvaluemart.com/mechanical/transmission?visible_for=x%27"%20onmouseover=alert(document.cookie)%20x= www.mjvaluemart.com says _gcl_au=1.1.656717255.1708506646; mage-cache-storage=%7B%7D; _hjSessionUser_2775745=eyJpZCI6ImUyYWQ0YTVlLWU3M2QtNWVjMC1iNGJiLTUyNDdhOGNmY2I5ZCIsImNyZWF0ZWQiOjE3MDg1MDY2NDY3ODcsImV4aXN0aW5nIjp0cnVlfQ==; mjvmrt_url_referer=https%3A%2F%2Fwww.mjvaluemart.com%2F; usergroup=0; amcookie_policy_restriction=allowed; amcookie_allowed=1%2C2%2C3; _gid=GA1.2.269254425.1709529028; mage-cache-storage-section- OK  mjvaluemart.com/mechanical/hardware/misc-items?amp&product_seller_id=x%27"%20onmouseover=alert(document.locatio... www.mjvaluemart.com says https://www.mjvaluemart.com/mechanical/hardware/misc-items?amp&product_seller_id=x%27%22%20onmouseover=alert(document.location)%20x= OK  mjvaluemart.com/mjtestseller/collection?q==x"%20onmouseover=alert(document.cookie)%20x= www.mjvaluemart.com says mage-cache-storage=%7B%7D; _gcl_au=1.1.1884293958.1709542892; _gid=GA1.2.583856551.1709542892; _clck=w1kalc%7C2%7Cfjs%7C0%7C1524; mage-cache-storage-section-invalidation=%7B%7D; usergroup=0; form_key=QgAQnS0i8viCByzc; mjvmrt_url_referer=https%3A%2F%2Fwww.mjvaluemart.com%2Fmechanical%2Ftransmission%3Fvisible_for%3Dx%2527%2522%2520onmouseover%3Dalert(document.cookie)%2520x%3D%2520 OK
Remediation:	The issue occurs because the browser interprets the input as active HTML, JavaScript or VBScript. To avoid this, output should be encoded according to the output location and context. For example, if the output goes in to a JavaScript block within the HTML document, then output needs to be encoded accordingly. Encoding can get very complex; therefore, it's strongly recommended to use an encoding library such as OWASP ESAPI and Microsoft Anti-cross-site scripting. Additionally, you should implement a strong Content Security Policy (CSP) as a defense-in-depth measure if an XSS vulnerability is mistakenly introduced. Due to the complexity of XSS-Prevention and the lack of secure standard behavior in programming languages and frameworks, XSS vulnerabilities are still common in web applications. CSP will act as a safeguard that can prevent an attacker from

	successfully exploiting Cross-site Scripting vulnerabilities in your website and is advised in any kind of application. Please make sure to scan your application again with Content Security Policy checks enabled after implementing CSP, in order to avoid common mistakes that can impact the effectiveness of your policy. There are a few pitfalls that can render your CSP policy useless and we highly recommend reading the resources linked in the reference section before you start to implement one. **Reference Link(s):** https://www.owasp.org/index.php/AntiSamy

6. Vulnerability Name: Out-of-date Version (Underscore.js)
Vulnerability Rating: High

CVSS: 7.5 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H **CVE-**2022-31129

Vulnerability Description:

The package underscore from 1.13.0-0 and before 1.13.0-2, from 1.3.2 and before 1.12.1 are vulnerable to Arbitrary Code Injection via the template function, particularly when a variable property is passed as an argument as it is not sanitized.

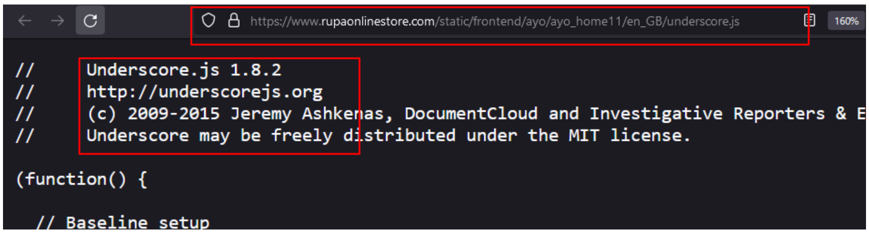
Affected URL(s):

https://www.mjvaluemart.com/static/version1709138220/frontend/Alothemes/expert1/en_US/underscore.js

Impact:

Since this is an old version of the software, it may be vulnerable to attacks.

Proof of Concept:



https://www.rupaonlinestore.com/static/frontend/ayo/ayo_home11/en_GB/underscore.js
160%

```
//     Underscore.js 1.8.2
//     http://underscorejs.org
//     (c) 2009-2015 Jeremy Ashkenas, DocumentCloud and Investigative Reporters & E
//     Underscore may be freely distributed under the MIT license.

(function() {

  // Baseline setup
```

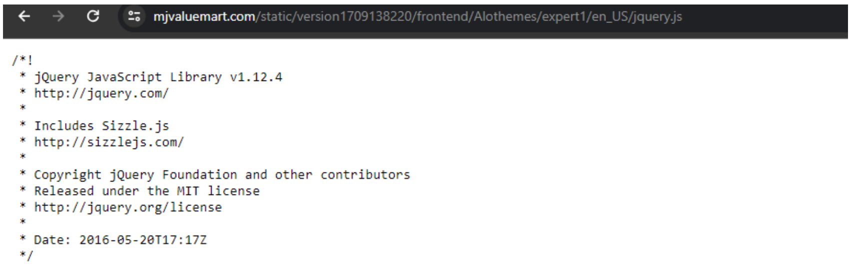
Remediation:

Please upgrade your installation of Underscore.js to the latest stable version.

Reference Link(s):

https://underscorejs.org/

7. Vulnerability Name: Out-of-date Version (jQuery)
Vulnerability Rating: Medium

CVSS: 6.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N **CVE-**2020-11023 **CWE-**1035,937
Vulnerability Description:	In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML 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. This problem is patched in jQuery 3.5.0. **Affected URL(s):** https://www.mjvaluemart.com/static/version1709138220/frontend/Alothemes/expert1/en_US/jquery.js
Impact:	Since this is an old version of the software, it may be vulnerable to attacks.
Proof of Concept:	 mjvaluemart.com/static/version1709138220/frontend/Alothemes/expert1/en_US/jquery.js /*! * jQuery JavaScript Library v1.12.4 * http://jquery.com/ * * Includes Sizzle.js * http://sizzlejs.com/ * * Copyright jQuery Foundation and other contributors * Released under the MIT license * http://jquery.org/license * * Date: 2016-05-20T17:17Z */
Remediation:	Please upgrade your installation of jQuery to the latest stable version. **Reference Link(s):** https://jquery.com/download/

8. Vulnerability Name: Out-of-date Version (Knockout)

Vulnerability Rating: Medium

CVSS: 6.1 CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N **CWE-**79

Vulnerability Description:

There is a vulnerability in knockout before version 3.5.0-beta, where after escaping the context of the web application, the web application delivers data to its users along with other trusted dynamic content, without validating it.

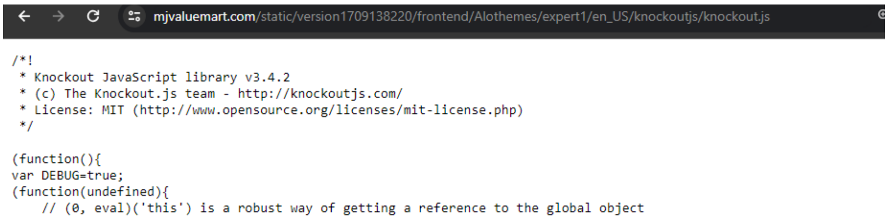
Affected URL(s):

https://www.mjvaluemart.com/static/version1709138220/frontend/Alothemes/expert1/en_US/knockoutjs/knockout.js

Impact:

Since this is an old version of the software, it is vulnerable to attacks.

Proof of Concept:



```
/*!
 * Knockout JavaScript library v3.4.2
 * (c) The Knockout.js team - http://knockoutjs.com/
 * License: MIT (http://www.opensource.org/licenses/mit-license.php)
 */

(function(){
var DEBUG=true;
(function(undefined){
    // (0, eval)('this') is a robust way of getting a reference to the global object
```

Remediation:

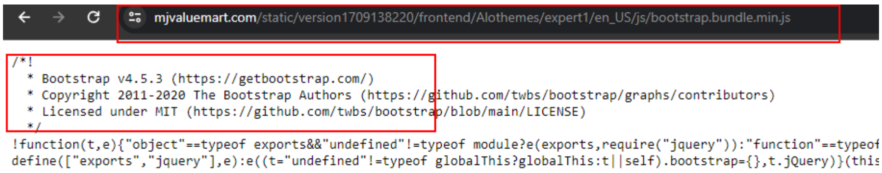
Please upgrade your installation of Knockout to the latest stable version.

Reference Link(s):

http://knockoutjs.com/downloads/index.html

9. Vulnerability Name: Version Disclosure (Bootstrapjs)
Vulnerability Rating: Low

CVSS: 3.7	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N **CWE-**205
Vulnerability Description:	A version disclosure (Bootstrapjs) in the target web server's HTTP response. This information can help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of jQuery. **Affected URL(s):** https://www.mjvaluemart.com/static/version1709138220/frontend/Alothemes/expert1/en_US/js/bootstrap.bundle.min.js
Impact:	An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

Proof of Concept:	
	mjvaluemart.com/static/version1709138220/frontend/Alothemes/expert1/en_US/js/bootstrap.bundle.min.js
	`/*!`
	` * Bootstrap v4.5.3 (https://getbootstrap.com/)`
	` * Copyright 2011-2020 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors)`
	` * Licensed under MIT (https://github.com/twbs/bootstrap/blob/main/LICENSE)`
	` */`
	`!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports,require("jquery")):"function"==typeof`
	`define(["exports","jquery"],e):e((t="undefined"!=typeof globalThis?globalThis:t||self).bootstrap={},t.jQuery)}(this`

Remediation:	Configure your web server to prevent information leakage.

10. Vulnerability Name: Version Disclosure (jQuery)
Vulnerability Rating: Low

CVSS: 3.7 CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N **CWE-**205

Vulnerability Description:

A version disclosure (jQuery) in the target web server's HTTP response. This information can help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of jQuery.

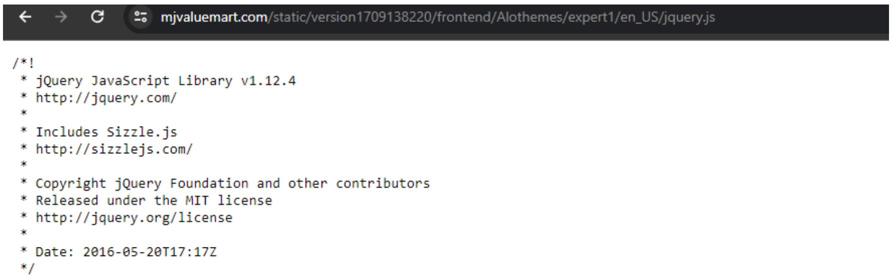
Affected URL(s):

https://www.mjvaluemart.com/static/version1709138220/frontend/Alothemes/expert1/en_US/jquery.js

Impact:

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

Proof of Concept:



mjvaluemart.com/static/version1709138220/frontend/Alothemes/expert1/en_US/jquery.js

```
/*!
 * jQuery JavaScript Library v1.12.4
 * http://jquery.com/
 *
 * Includes Sizzle.js
 * http://sizzlejs.com/
 *
 * Copyright jQuery Foundation and other contributors
 * Released under the MIT license
 * http://jquery.org/license
 *
 * Date: 2016-05-20T17:17Z
 */
```

Remediation:

Configure your web server to prevent information leakage.

11. Vulnerability Name: Version Disclosure (jQuery Migrate)
Vulnerability Rating: Low

CVSS: 3.7 CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N **CWE-**205

Vulnerability Description:

A version disclosure (jQuery Migrate) in the target web server's HTTP response. This information can help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of jQuery.

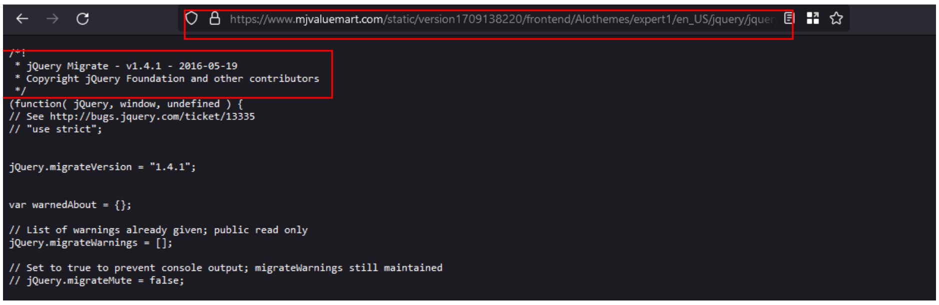
Affected URL(s):

https://www.mjvaluemart.com/static/version1709138220/frontend/Alothemes/expert1/en_US/jquery/jquery-migrate.js

Impact:

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

Proof of Concept:



https://www.mjvaluemart.com/static/version1709138220/frontend/Alothemes/expert1/en_US/jquery/jquer

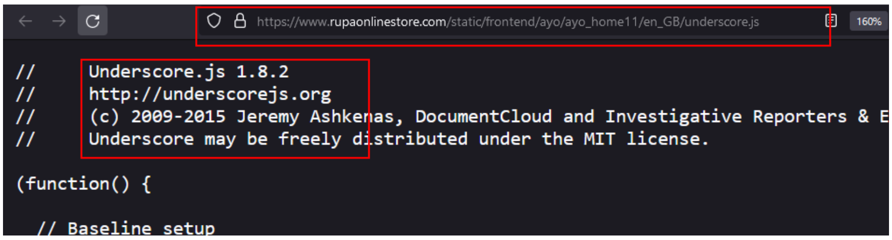
```
/*!
 * jQuery Migrate - v1.4.1 - 2016-05-19
 * Copyright jQuery Foundation and other contributors
 */
(function( jQuery, window, undefined ) {
// See http://bugs.jquery.com/ticket/13335
// "use strict";


jQuery.migrateVersion = "1.4.1";


var warnedAbout = {};

// List of warnings already given; public read only
jQuery.migrateWarnings = [];

// Set to true to prevent console output; migrateWarnings still maintained
// jQuery.migrateMute = false;
```

Remediation:

Configure your web server to prevent information leakage.

12. Vulnerability Name: Version Disclosure (Underscorejs) Vulnerability Rating: Low

CVSS: 3.7 CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N	**CWE-**205
Vulnerability Description:	A version disclosure (Underscorejs) in the target web server's HTTP response. This information can help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of jQuery. **Affected URL(s):** https://www.mjvaluemart.com/static/version1709138220/frontend/Alothemes/expert1/en_US/underscore.js
Impact:	An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

Proof of Concept:	
	https://www.rupaonlinestore.com/static/frontend/ayo/ayo_home11/en_GB/underscore.js
	`//     Underscore.js 1.8.2`
	`//     http://underscorejs.org`
	`//     (c) 2009-2015 Jeremy Ashkenas, DocumentCloud and Investigative Reporters & E`
	`//     Underscore may be freely distributed under the MIT license.`
	`(function() {`
	`  // Baseline setup`

Remediation:	Configure your web server to prevent information leakage.

13. Vulnerability Name: Internal Server Error
Vulnerability Rating: Low

CVSS: 3.1 CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N **CWE-**550

Vulnerability Description:

The website is vulnerable to a verbose internal server error disclosure, exposing internal path files. When certain erroneous requests are made, the server responds with detailed error messages that contain the full file paths of the Magento installation directory or other sensitive internal files. This disclosure enables potential attackers to gather valuable information about the server's directory structure and potentially exploit further vulnerabilities.

Affected URL(s):

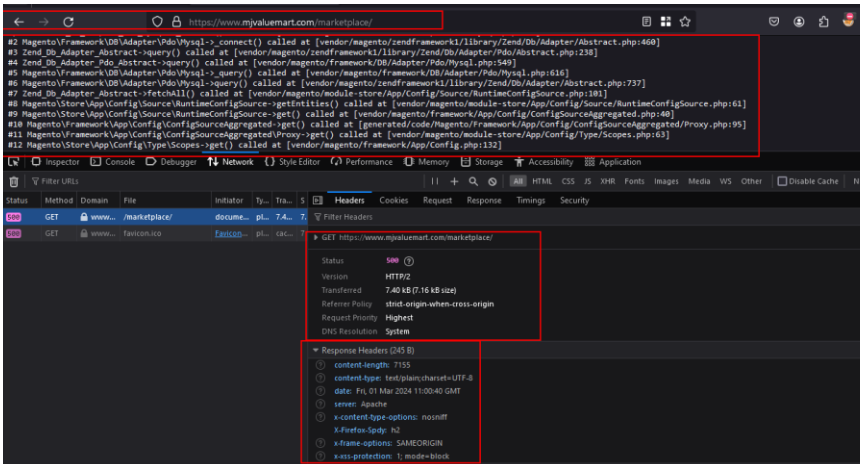
https://www.mjvaluemart.com/marketplace/

*Due to Lot of Request’s

Impact:

The errors provide attackers with valuable insights into the website's underlying architecture, including file locations and potentially confidential information. With this knowledge, attackers could devise targeted attacks to exploit other vulnerabilities within the Magento platform or launch more sophisticated attacks, such as directory traversal or code injection attacks. Furthermore, the exposure of internal path files could compromise the confidentiality, integrity, and availability of the website and its data, leading to potential financial losses, reputational damage, and legal repercussions for the organization.

Proof of Concept:



https://www.mjvaluemart.com/marketplace/

```
#2 Magento\Framework\DB\Adapter\Pdo\Mysql->_connect() called at [vendor/magento/zendframework1/library/Zend/Db/Adapter/Abstract.php:460]
#3 Zend_Db_Adapter_Abstract->query() called at [vendor/magento/zendframework1/library/Zend/Db/Adapter/Pdo/Abstract.php:238]
#4 Zend_Db_Adapter_Pdo_Abstract->query() called at [vendor/magento/framework/DB/Adapter/Pdo/Mysql.php:549]
#5 Magento\Framework\DB\Adapter\Pdo\Mysql->_query() called at [vendor/magento/framework/DB/Adapter/Pdo/Mysql.php:616]
#6 Magento\Framework\DB\Adapter\Pdo\Mysql->query() called at [vendor/magento/zendframework1/library/Zend/Db/Adapter/Abstract.php:737]
#7 Zend_Db_Adapter_Abstract->fetchAll() called at [vendor/magento/module-store/App/Config/Source/RuntimeConfigSource.php:101]
#8 Magento\Store\App\Config\Source\RuntimeConfigSource->getEntities() called at [vendor/magento/module-store/App/Config/Source/RuntimeConfigSource.php:61]
#9 Magento\Store\App\Config\Source\RuntimeConfigSource->get() called at [vendor/magento/framework/App/Config/ConfigSourceAggregated.php:40]
#10 Magento\Framework\App\Config\ConfigSourceAggregated->get() called at [generated/code/Magento/Framework/App/Config/ConfigSourceAggregated/Proxy.php:95]
#11 Magento\Framework\App\Config\ConfigSourceAggregated\Proxy->get() called at [vendor/magento/module-store/App/Config/Type/Scopes.php:63]
#12 Magento\Store\App\Config\Type\Scopes->get() called at [vendor/magento/framework/App/Config.php:132]
```

Status	Method	Domain	File	Initiator	Ty...	Tra...
500	GET	www...	/marketplace/	docume...	pl...	7.4...
500	GET	www...	favicon.ico	Favicon...	pl...	cac...

GET https://www.mjvaluemart.com/marketplace/

Status	500
Version	HTTP/2
Transferred	7.40 kB (7.16 kB size)
Referrer Policy	strict-origin-when-cross-origin
Request Priority	Highest
DNS Resolution	System

Response Headers (245 B)

```
content-length: 7155
content-type: text/plain;charset=UTF-8
date: Fri, 01 Mar 2024 11:00:40 GMT
server: Apache
x-content-type-options: nosniff
X-Firefox-Spdy: h2
x-frame-options: SAMEORIGIN
x-xss-protection: 1; mode=block
```

Remediation:

Analyze this issue and review the application code in order to handle unexpected errors; this should be a generic practice, which does not disclose further information upon an error. All errors should be handled server-side only.

14. Vulnerability Name: HTTP Strict Transport Security (HSTS) Policy Not Enabled

Vulnerability Rating: Low

CVSS: 3.1 CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N **CWE-**523

Vulnerability Description:

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.

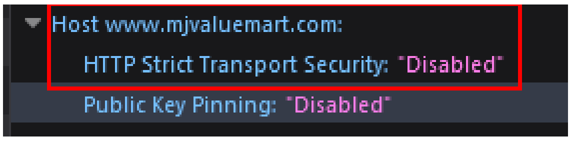
Affected URL(s):

https://www.mjvaluemart.com/

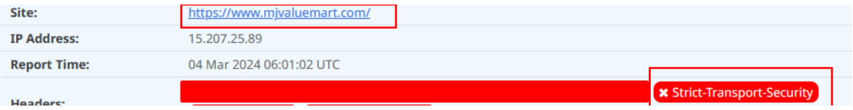
Impact:

To exploit this vulnerability, an attacker must be suitably positioned to intercept and modify 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 defenses 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.

Proof of Concept:



```
Host www.mjvaluemart.com:
    HTTP Strict Transport Security: "Disabled"
    Public Key Pinning: "Disabled"
```



Site: https://www.mjvaluemart.com/
IP Address: 15.207.25.89
Report Time: 04 Mar 2024 06:01:02 UTC
Headers: [redacted] ✖ Strict-Transport-Security

Remediation:

It is recommended to, Serve an HSTS header on the base domain for HTTPS requests:

- The max-age must be at least 31536000 seconds (1 year)
- The includeSubDomainsdirective must be specified
- The preloaddirective must be specified If you are serving an additional redirect from your HTTPS site, that redirect must have the HSTS header (rather than the page it redirects to).

Reference Link(s):

https://support.cloudways.com/en/articles/5129574-how-to-enable-http-strict-transport-security-hsts-policy