Sri Lanka Institute of Information Technology

Report – Insignia Financial

IE2062 - Web security

Submitted by:

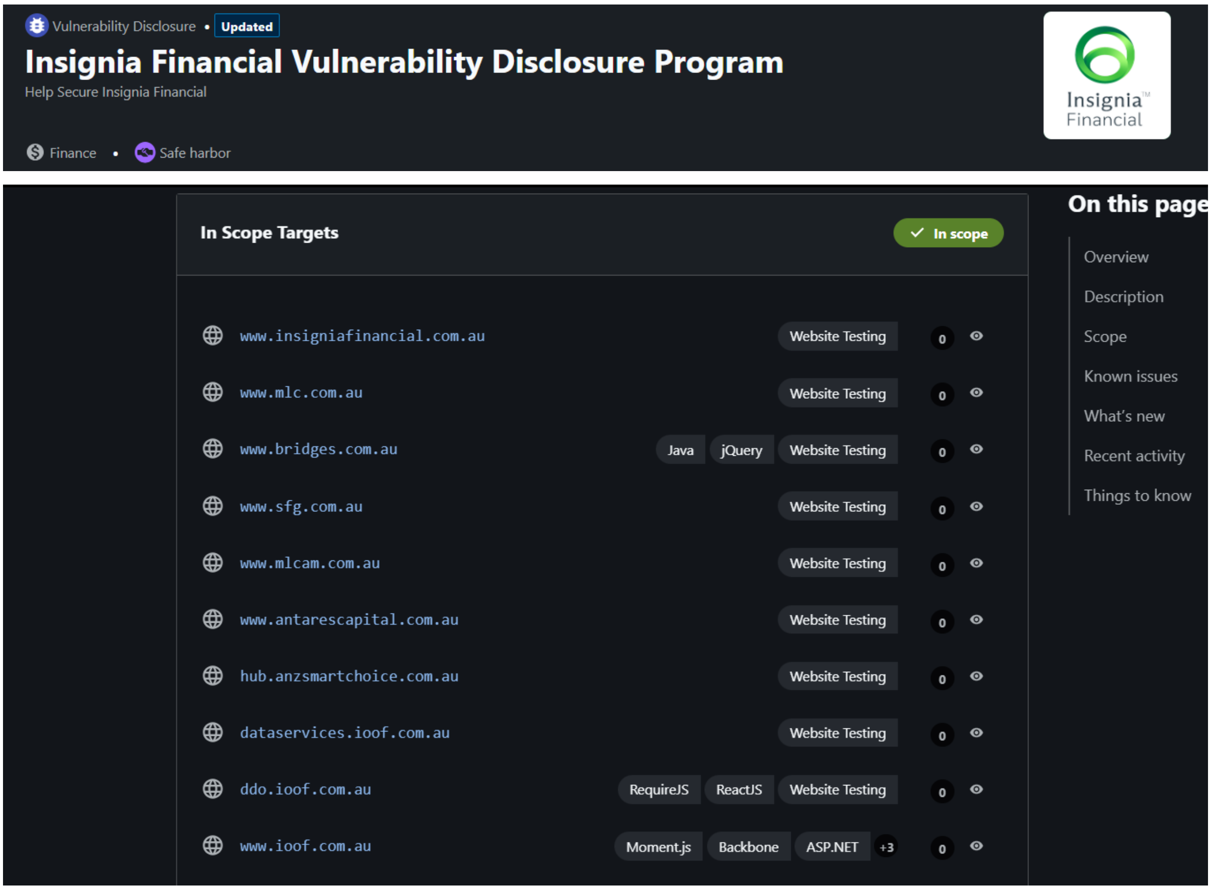
Student Registration Number	Student Name
IT23253476	Bandara S.M.S.N

Date of submission

05/05/2025

Table of Contents

1. Domain: https://www.mlcam.com.au/



Vulnerability Disclosure • Updated

Insignia Financial Vulnerability Disclosure Program

Help Secure Insignia Financial

Finance • Safe harbor

In Scope Targets ✓ In scope

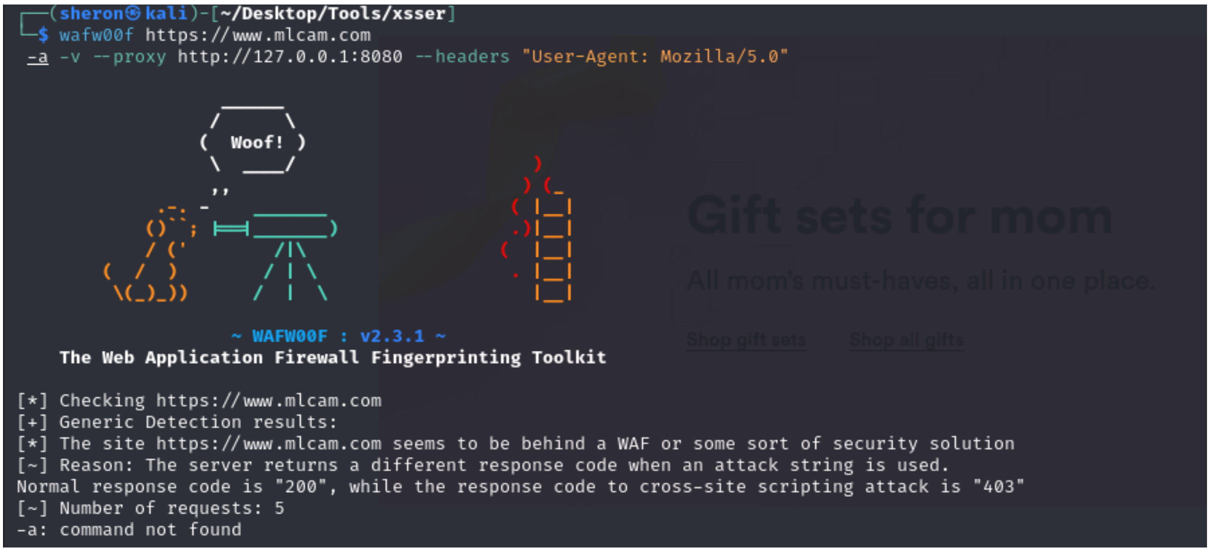
Target	Tags		
www.insigniafinancial.com.au	Website Testing	0	
www.mlc.com.au	Website Testing	0	
www.bridges.com.au	Java, jQuery, Website Testing	0	
www.sfg.com.au	Website Testing	0	
www.mlcam.com.au	Website Testing	0	
www.antarescapital.com.au	Website Testing	0	
hub.anzsmartchoice.com.au	Website Testing	0	
dataservices.ioof.com.au	Website Testing	0	
ddo.ioof.com.au	RequireJS, ReactJS, Website Testing	0	
www.ioof.com.au	Moment.js, Backbone, ASP.NET, +3	0	

- Link: https://www.mlcam.com.au/
- Category: Vulnerability Disclosure Program (VDP)
- Type: Finance

2. Scanning

2.1. Wafw00f

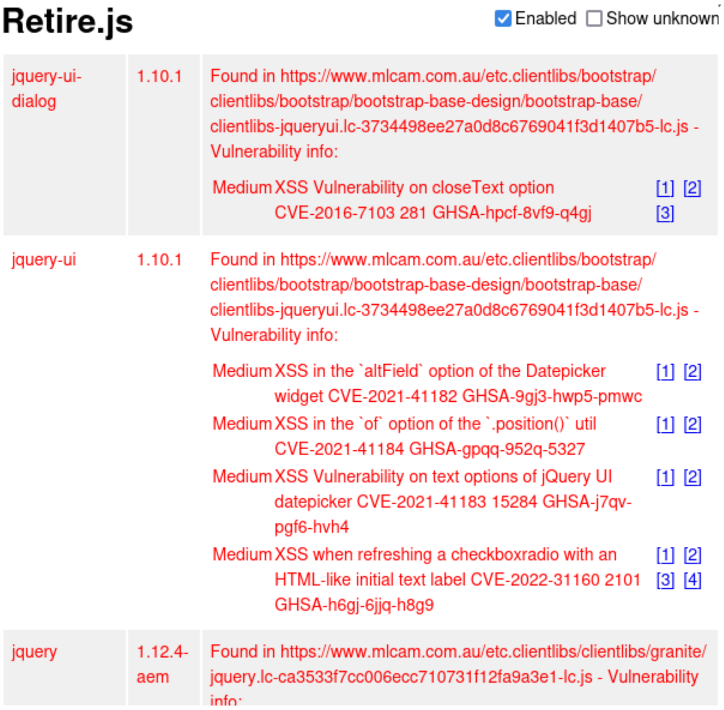
This tool is used to look for the web application firewall used by the web site. By knowing the version, the attacker can try to bypass by exploiting known vulnerabilities of that website. The scan revealed that the web application is using a web application firewall, but it is hidden.



```
┌──(sheron㉿kali)-[~/Desktop/Tools/xsser]
└─$ wafw00f https://www.mlcam.com
 -a -v --proxy http://127.0.0.1:8080 --headers "User-Agent: Mozilla/5.0"

                   ______
                  /      \
                 (  Woof! )
                  \  ____/                      )
                  ,,                           ) (_
             .-. -    _______                 ( |__|
            ()``; |==|_______)                .)|__|
            / ('      /|\                    (  |__|
        (  /  )      / | \                    . |__|
         \(_)_))    /  |  \                     |__|

                   ~ WAFW00F : v2.3.1 ~
    The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://www.mlcam.com
[+] Generic Detection results:
[*] The site https://www.mlcam.com seems to be behind a WAF or some sort of security solution
[~] Reason: The server returns a different response code when an attack string is used.
Normal response code is "200", while the response code to cross-site scripting attack is "403"
[~] Number of requests: 5
-a: command not found
```

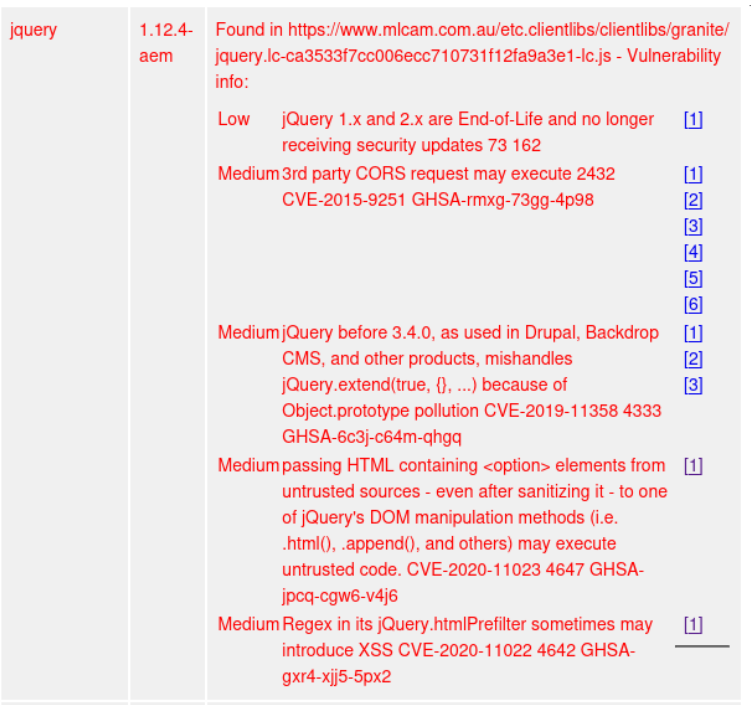
2.2. Retire.js

Retire.js is popular browser extension which finds for vulnerabilities in web sites. It can detect vulnerabilities of java script libraries used and will give details about the vulnerability along with the CVE and links to popular websites like nist or git to see full details and mitigation methods. Running the scan found the following vulnerabilities.



Retire.js

☑ Enabled ☐ Show unknown



jquery-ui-dialog	1.10.1	Found in https://www.mlcam.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-8vf9-q4gj	[1] [2] [3]
jquery-ui	1.10.1	Found in https://www.mlcam.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.mlcam.com.au/etc.clientlibs/clientlibs/granite/jquery.lc-ca3533f7cc006ecc710731f12fa9a3e1-lc.js - Vulnerability info:		
		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]

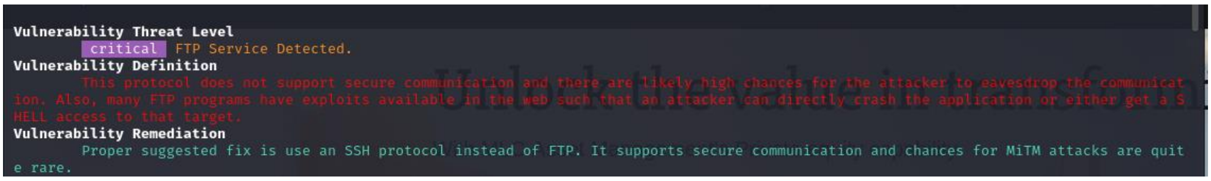
The tool has found the following vulnerabilities. Below is a summary of the CVE's and the vulnerabilities they poses.

CVE Number	Vulnerability Name
CVE-2016-7103	Medium XSS Vulnerability on closeText option
CVE-2021-41182	Medium XSS in the altField option of the Datepicker widget
CVE-2021-41184	Medium XSS in the of option of the .position() util
CVE-2021-41183	Medium XSS Vulnerability on text options of jQuery UI datepicker
CVE-2022-31160	Medium XSS when refreshing a checkboxradio with an HTML-like initial text label
CVE-2015-9251	Medium 3rd party CORS request may execute
CVE-2019-11358	Medium jQuery mishandles jQuery.extend(true, {}, ...) due to Object.prototype pollution
CVE-2020-11023	Medium passing HTML containing <option> elements from untrusted sources may execute untrusted code
CVE-2020-11022	Medium Regex in its jQuery.htmlPrefilter may introduce XSS

2.3. Rapid Scanner

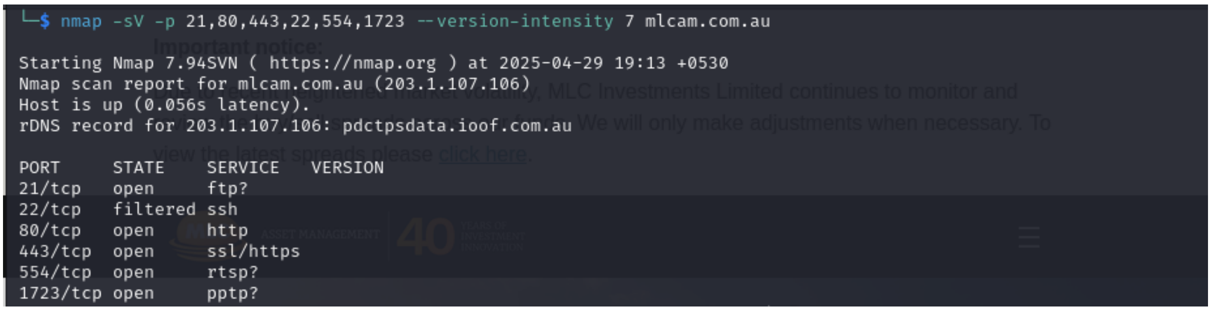
Rapid scanner is a power full tool which utilizes 82 tools to look for vulnerabilities which could be exploited by threat agents. After performing rapid scan the following were discovered.

First vulnerability – Nmap has found that ftp service is open which could potentially be exploited to perform eves dropping to possibly run shell scripts.



```
Vulnerability Threat Level
        critical  FTP Service Detected.
Vulnerability Definition
        This protocol does not support secure communication and there are likely high chances for the attacker to eavesdrop the communicat
ion. Also, many FTP programs have exploits available in the web such that an attacker can directly crash the application or either get a S
HELL access to that target.
Vulnerability Remediation
        Proper suggested fix is use an SSH protocol instead of FTP. It supports secure communication and chances for MiTM attacks are quit
e rare.
```

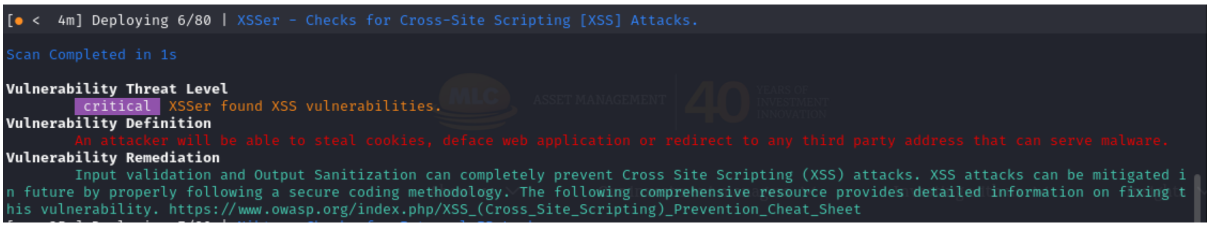
You can use nmap to see if the ftp port is open.



```
└─$ nmap -sV -p 21,80,443,22,554,1723 --version-intensity 7 mlcam.com.au

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-29 19:13 +0530
Nmap scan report for mlcam.com.au (203.1.107.106)
Host is up (0.056s latency).
rDNS record for 203.1.107.106: pdctpsdata.ioof.com.au

PORT     STATE    SERVICE  VERSION
21/tcp   open     ftp?
22/tcp   filtered ssh
80/tcp   open     http
443/tcp  open     ssl/https
554/tcp  open     rtsp?
1723/tcp open     pptp?
```

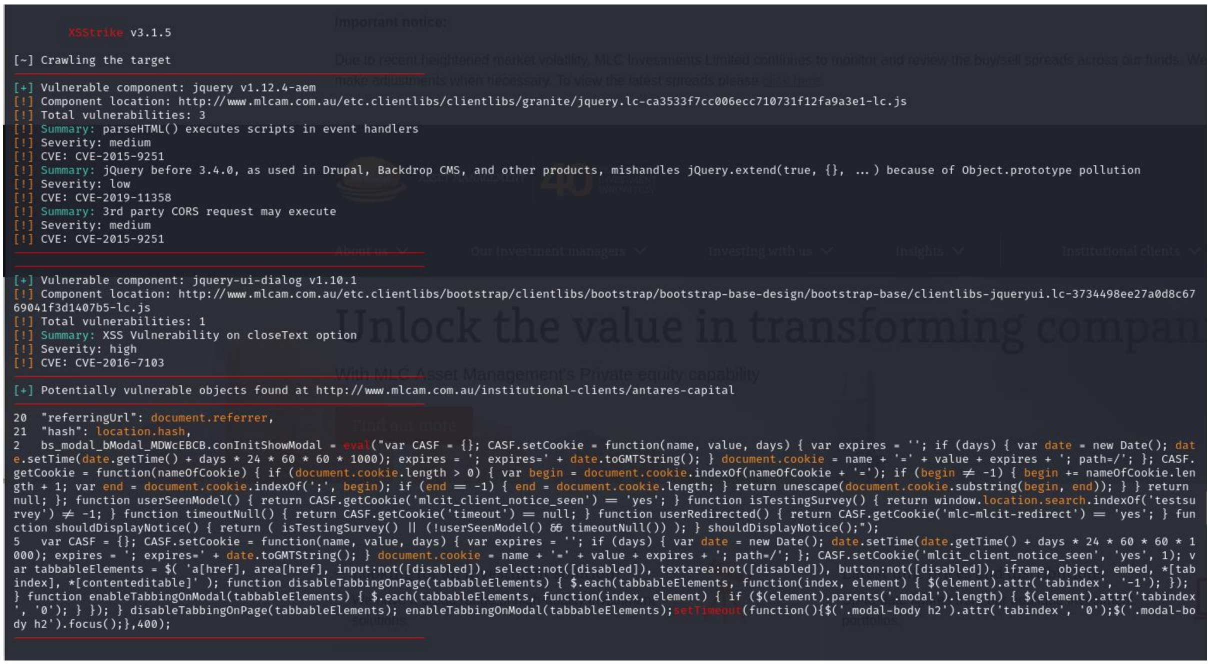
If port 21is open, it doesn’t necessarily mean it is vulnerable. Further testing should be done. But you can remove any un necessary risks by using a more secure protocol like ssh.

Second vulnerability – Xsser tool has found a vulnerability regarding a xss attack. It will allow the user’s cookies to be stolen, and users could be redirected to other web sites which could be malicious. This was also confirmed by the retie.js scan as well. It had multiple vulnerabilities regarding xss.



```
[● <  4m] Deploying 6/80 | XSSer - Checks for Cross-Site Scripting [XSS] Attacks.

Scan Completed in 1s

Vulnerability Threat Level
        critical  XSSer found XSS vulnerabilities.
Vulnerability Definition
        An attacker will be able to steal cookies, deface web application or redirect to any third party address that can serve malware.
Vulnerability Remediation
        Input validation and Output Sanitization can completely prevent Cross Site Scripting (XSS) attacks. XSS attacks can be mitigated i
n future by properly following a secure coding methodology. The following comprehensive resource provides detailed information on fixing t
his vulnerability. https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet
```

Let’s confirm the XSS vulnerability using **XSStrike tool**. A parameter ‘test’ will be used to test for XSS.



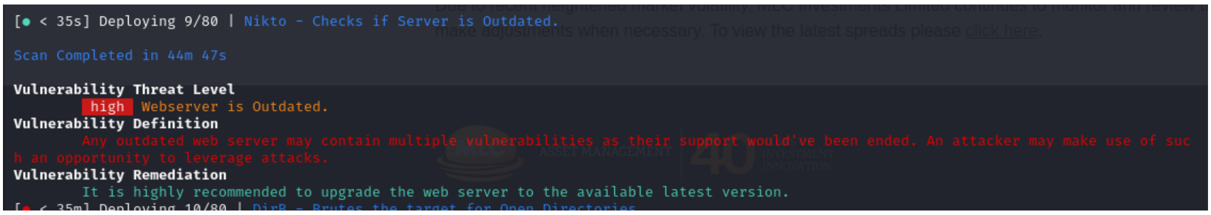
```
      XSStrike v3.1.5

[~] Crawling the target

[+] Vulnerable component: jquery v1.12.4-aem
[!] Component location: http://www.mlcam.com.au/etc.clientlibs/clientlibs/granite/jquery.lc-ca3533f7cc006ecc710731f12fa9a3e1-lc.js
[!] Total vulnerabilities: 3
[!] Summary: parseHTML() executes scripts in event handlers
[!] Severity: medium
[!] CVE: CVE-2015-9251
[!] Summary: jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution
[!] Severity: low
[!] CVE: CVE-2019-11358
[!] Summary: 3rd party CORS request may execute
[!] Severity: medium
[!] CVE: CVE-2015-9251

[+] Vulnerable component: jquery-ui-dialog v1.10.1
[!] Component location: http://www.mlcam.com.au/etc.clientlibs/bootstrap/clientlibs/bootstrap/bootstrap-base-design/bootstrap-base/clientlibs-jqueryui.lc-3734498ee27a0d8c67
69041f3d1407b5-lc.js
[!] Total vulnerabilities: 1
[!] Summary: XSS Vulnerability on closeText option
[!] Severity: high
[!] CVE: CVE-2016-7103

[+] Potentially vulnerable objects found at http://www.mlcam.com.au/institutional-clients/antares-capital

20  "referringUrl": document.referrer,
21  "hash": location.hash,
2   bs_modal_bModal_MDWcEBCB.conInitShowModal = eval("var CASF = {}; CASF.setCookie = function(name, value, days) { var expires = ''; if (days) { var date = new Date(); dat
e.setTime(date.getTime() + days * 24 * 60 * 60 * 1000); expires = '; expires=' + date.toGMTString(); } document.cookie = name + '=' + value + expires + '; path=/'; }; CASF.
getCookie = function(nameOfCookie) { if (document.cookie.length > 0) { var begin = document.cookie.indexOf(nameOfCookie + '='); if (begin ≠ -1) { begin += nameOfCookie.len
gth + 1; var end = document.cookie.indexOf(';', begin); if (end == -1) { end = document.cookie.length; } return unescape(document.cookie.substring(begin, end)); } } return
null; }; function userSeenModel() { return CASF.getCookie('mlcit_client_notice_seen') == 'yes'; } function isTestingSurvey() { return window.location.search.indexOf('testsu
rvey') ≠ -1; } function timeoutNull() { return CASF.getCookie('timeout') == null; } function userRedirected() { return CASF.getCookie('mlc-mlcit-redirect') == 'yes'; } fun
ction shouldDisplayNotice() { return ( isTestingSurvey() || (!userSeenModel() && timeoutNull()) ); } shouldDisplayNotice();");
5   var CASF = {}; CASF.setCookie = function(name, value, days) { var expires = ''; if (days) { var date = new Date(); date.setTime(date.getTime() + days * 24 * 60 * 60 * 1
000); expires = '; expires=' + date.toGMTString(); } document.cookie = name + '=' + value + expires + '; path=/'; }; CASF.setCookie('mlcit_client_notice_seen', 'yes', 1); v
ar tabbableElements = $( 'a[href], area[href], input:not([disabled]), select:not([disabled]), textarea:not([disabled]), button:not([disabled]), iframe, object, embed, *[tab
index], *[contenteditable]' ); function disableTabbingOnPage(tabbableElements) { $.each(tabbableElements, function(index, element) { $(element).attr('tabindex', '-1'); });
} function enableTabbingOnModal(tabbableElements) { $.each(tabbableElements, function(index, element) { if ($(element).parents('.modal').length) { $(element).attr('tabindex
', '0'); } }); } disableTabbingOnPage(tabbableElements); enableTabbingOnModal(tabbableElements);setTimeout(function(){$('.modal-body h2').attr('tabindex', '0');$('.modal-bo
dy h2').focus();},400);
```

XSStrike has successfully located the vulnerabilities and their affected components along with the CVE codes of the vulnerabilities.

Components affected:

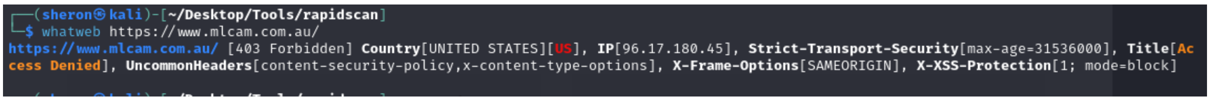
Component	CVE	Details
jquery v1.12.4-aem	CVE-2015-9251	*parseHTML() executes scripts in event handlers* (Severity: Medium)
	CVE-2019-11358	*Object.prototype pollution via jQuery.extend(true, {}, ...)* (Severity: Low)
	CVE-2015-9251	*3rd party CORS request may execute* (Severity: Medium)
jquery-ui-dialog v1.10.1	CVE-2016-7103	*XSS Vulnerability on closeText option* (Severity: High)

Third vulnerability – A high severity vulnerability regarding an outdated server version. More information regarding the vulnerability will be discussed later in this report.



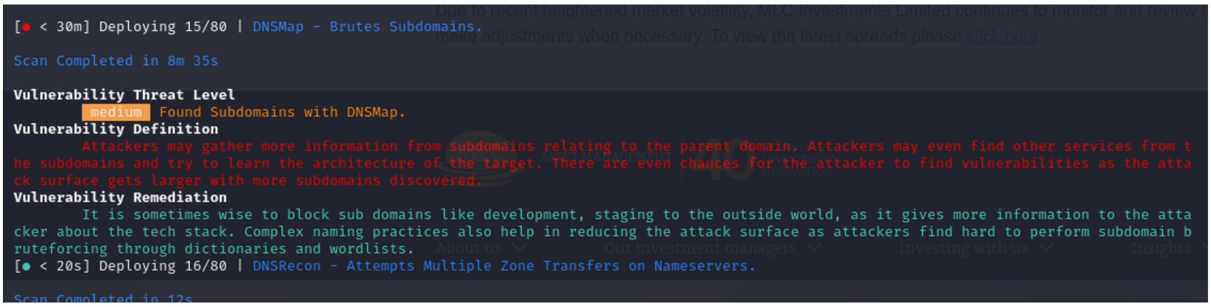
```
[● < 35s] Deploying 9/80 | Nikto - Checks if Server is Outdated.

Scan Completed in 44m 47s

Vulnerability Threat Level
         high  Webserver is Outdated.
Vulnerability Definition
         Any outdated web server may contain multiple vulnerabilities as their support would've been ended. An attacker may make use of suc
h an opportunity to leverage attacks.
Vulnerability Remediation
         It is highly recommended to upgrade the web server to the available latest version.
[● < 35m] Deploying 10/80 | DirB - Brutes the target for Open Directories
```

Attempting to get the version information of the web server did not work since its hidden. After trying to get the version information of the web server from popular tools like nmap and whatweb, it did not provide with results hence further testing is needed.



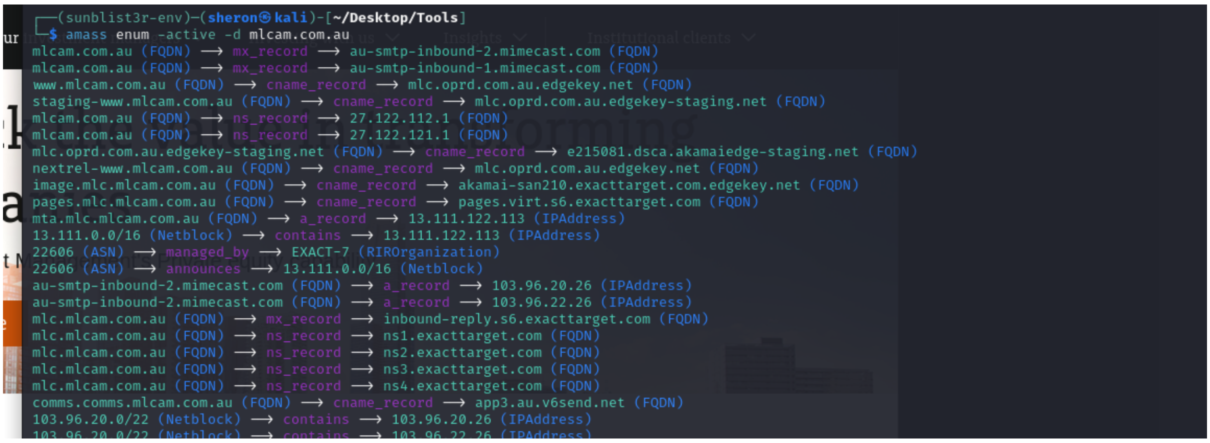
```
┌──(sheron㉿kali)-[~/Desktop/Tools/rapidscan]
└─$ whatweb https://www.mlcam.com.au/
https://www.mlcam.com.au/ [403 Forbidden] Country[UNITED STATES][US], IP[96.17.180.45], Strict-Transport-Security[max-age=31536000], Title[Ac
cess Denied], UncommonHeaders[content-security-policy,x-content-type-options], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[1; mode=block]
```

Forth vulnerability – This vulnerability has discovered details regarding sub domain. The attacker may find information on the parent domain using the subdomains. Also, it possible to find other details regarding the architecture or service running in the domain.



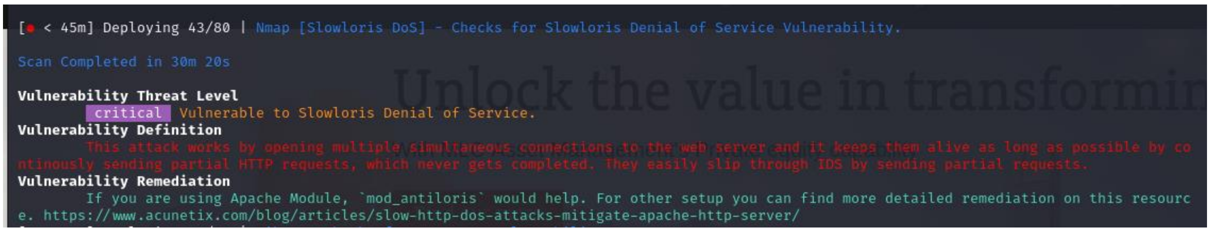
```
[● < 30m] Deploying 15/80 | DNSMap - Brutes Subdomains.

Scan Completed in 8m 35s

Vulnerability Threat Level
        medium  Found Subdomains with DNSMap.
Vulnerability Definition
        Attackers may gather more information from subdomains relating to the parent domain. Attackers may even find other services from t
he subdomains and try to learn the architecture of the target. There are even chances for the attacker to find vulnerabilities as the atta
ck surface gets larger with more subdomains discovered.
Vulnerability Remediation
        It is sometimes wise to block sub domains like development, staging to the outside world, as it gives more information to the atta
cker about the tech stack. Complex naming practices also help in reducing the attack surface as attackers find hard to perform subdomain b
ruteforcing through dictionaries and wordlists.
[● < 20s] Deploying 16/80 | DNSRecon - Attempts Multiple Zone Transfers on Nameservers.

Scan Completed in 12s
```

Using **amass** subdomain enumeration tool, details of sub domains can be extracted. The below is a sample



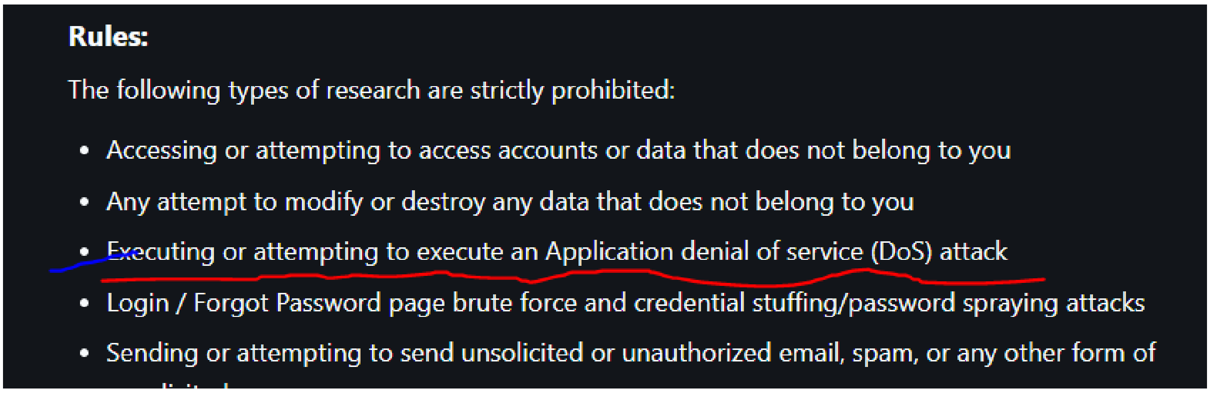
```
┌──(sunblist3r-env)─(sheron㉿kali)-[~/Desktop/Tools]
└─$ amass enum -active -d mlcam.com.au
mlcam.com.au (FQDN) ⟶ mx_record ⟶ au-smtp-inbound-2.mimecast.com (FQDN)
mlcam.com.au (FQDN) ⟶ mx_record ⟶ au-smtp-inbound-1.mimecast.com (FQDN)
www.mlcam.com.au (FQDN) ⟶ cname_record ⟶ mlc.oprd.com.au.edgekey.net (FQDN)
staging-www.mlcam.com.au (FQDN) ⟶ cname_record ⟶ mlc.oprd.com.au.edgekey-staging.net (FQDN)
mlcam.com.au (FQDN) ⟶ ns_record ⟶ 27.122.112.1 (FQDN)
mlcam.com.au (FQDN) ⟶ ns_record ⟶ 27.122.121.1 (FQDN)
mlc.oprd.com.au.edgekey-staging.net (FQDN) ⟶ cname_record ⟶ e215081.dsca.akamaiedge-staging.net (FQDN)
nextrel-www.mlcam.com.au (FQDN) ⟶ cname_record ⟶ mlc.oprd.com.au.edgekey.net (FQDN)
image.mlc.mlcam.com.au (FQDN) ⟶ cname_record ⟶ akamai-san210.exacttarget.com.edgekey.net (FQDN)
pages.mlc.mlcam.com.au (FQDN) ⟶ cname_record ⟶ pages.virt.s6.exacttarget.com (FQDN)
mta.mlc.mlcam.com.au (FQDN) ⟶ a_record ⟶ 13.111.122.113 (IPAddress)
13.111.0.0/16 (Netblock) ⟶ contains ⟶ 13.111.122.113 (IPAddress)
22606 (ASN) ⟶ managed_by ⟶ EXACT-7 (RIROrganization)
22606 (ASN) ⟶ announces ⟶ 13.111.0.0/16 (Netblock)
au-smtp-inbound-2.mimecast.com (FQDN) ⟶ a_record ⟶ 103.96.20.26 (IPAddress)
au-smtp-inbound-2.mimecast.com (FQDN) ⟶ a_record ⟶ 103.96.22.26 (IPAddress)
mlc.mlcam.com.au (FQDN) ⟶ mx_record ⟶ inbound-reply.s6.exacttarget.com (FQDN)
mlc.mlcam.com.au (FQDN) ⟶ ns_record ⟶ ns1.exacttarget.com (FQDN)
mlc.mlcam.com.au (FQDN) ⟶ ns_record ⟶ ns2.exacttarget.com (FQDN)
mlc.mlcam.com.au (FQDN) ⟶ ns_record ⟶ ns3.exacttarget.com (FQDN)
mlc.mlcam.com.au (FQDN) ⟶ ns_record ⟶ ns4.exacttarget.com (FQDN)
comms.comms.mlcam.com.au (FQDN) ⟶ cname_record ⟶ app3.au.v6send.net (FQDN)
103.96.20.0/22 (Netblock) ⟶ contains ⟶ 103.96.20.26 (IPAddress)
103.96.20.0/22 (Netblock) ⟶ contains ⟶ 103.96.22.26 (IPAddress)
```

Fifth vulnerability – This is a critical level vulnerability. It was detected by a tool called Slowloris and the vulnerability is a denial of service. Which can be destructive in some occasions.



```
[● < 45m] Deploying 43/80 | Nmap [Slowloris DoS] - Checks for Slowloris Denial of Service Vulnerability.

Scan Completed in 30m 20s

Vulnerability Threat Level
        critical  Vulnerable to Slowloris Denial of Service.
Vulnerability Definition
        This attack works by opening multiple simultaneous connections to the web server and it keeps them alive as long as possible by co
ntinously sending partial HTTP requests, which never gets completed. They easily slip through IDS by sending partial requests.
Vulnerability Remediation
        If you are using Apache Module, `mod_antiloris` would help. For other setup you can find more detailed remediation on this resourc
e. https://www.acunetix.com/blog/articles/slow-http-dos-attacks-mitigate-apache-http-server/
```

According to the scope performing DOS attack testing is out of the scope.



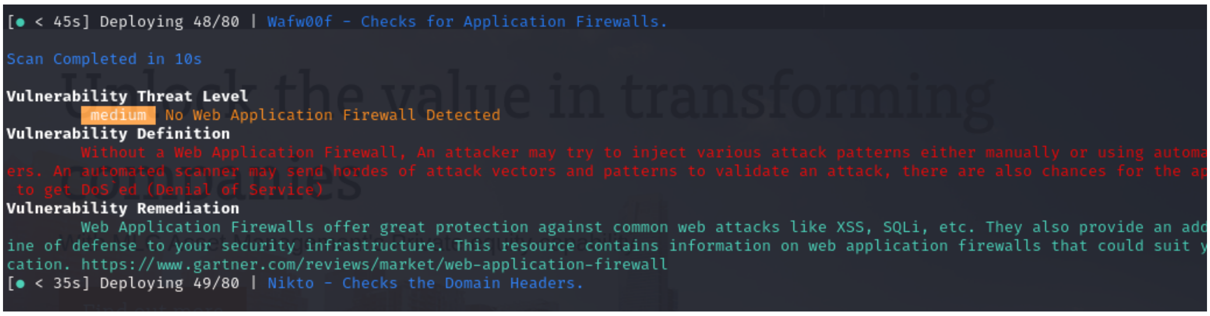
Rules:

The following types of research are strictly prohibited:

- Accessing or attempting to access accounts or data that does not belong to you
- Any attempt to modify or destroy any data that does not belong to you
- Executing or attempting to execute an Application denial of service (DoS) attack
- Login / Forgot Password page brute force and credential stuffing/password spraying attacks
- Sending or attempting to send unsolicited or unauthorized email, spam, or any other form of

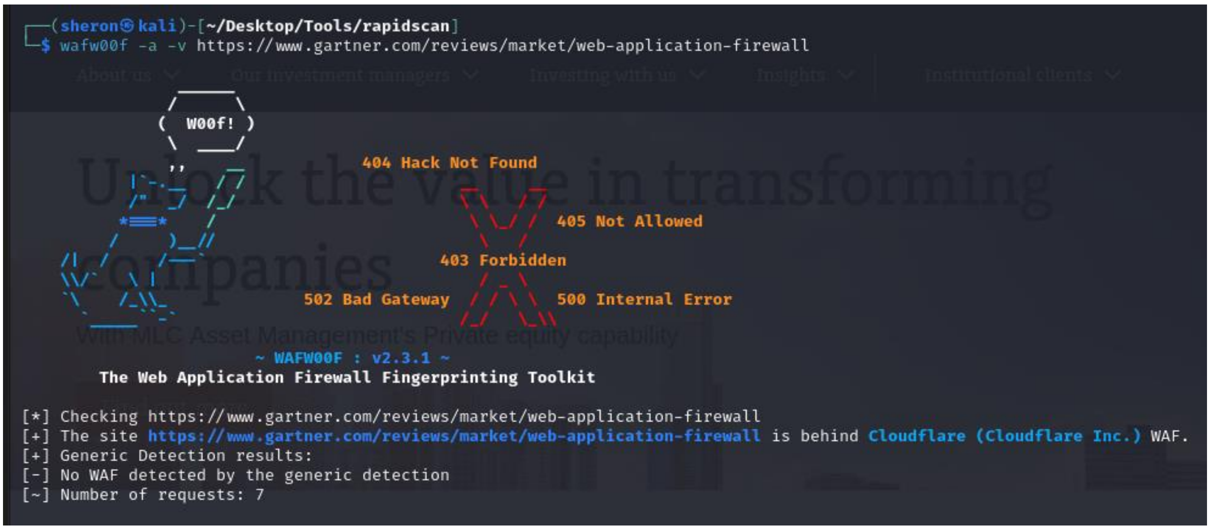
#

Sixth vulnerability – It has found that there is no firewall in the web application. Which is essential to have. Fire walls can block various types of attacks like XSS attacks, SQL injection attacks and many more.



```
[● < 45s] Deploying 48/80 | Wafw00f - Checks for Application Firewalls.

Scan Completed in 10s

Vulnerability Threat Level
        medium  No Web Application Firewall Detected
Vulnerability Definition
        Without a Web Application Firewall, An attacker may try to inject various attack patterns either manually or using automa
ers. An automated scanner may send hordes of attack vectors and patterns to validate an attack, there are also chances for the ap
 to get DoS`ed (Denial of Service)
Vulnerability Remediation
        Web Application Firewalls offer great protection against common web attacks like XSS, SQLi, etc. They also provide an add
ine of defense to your security infrastructure. This resource contains information on web application firewalls that could suit y
cation. https://www.gartner.com/reviews/market/web-application-firewall
[● < 35s] Deploying 49/80 | Nikto - Checks the Domain Headers.
```

Let us run **wafw00f** and see if it finds anything

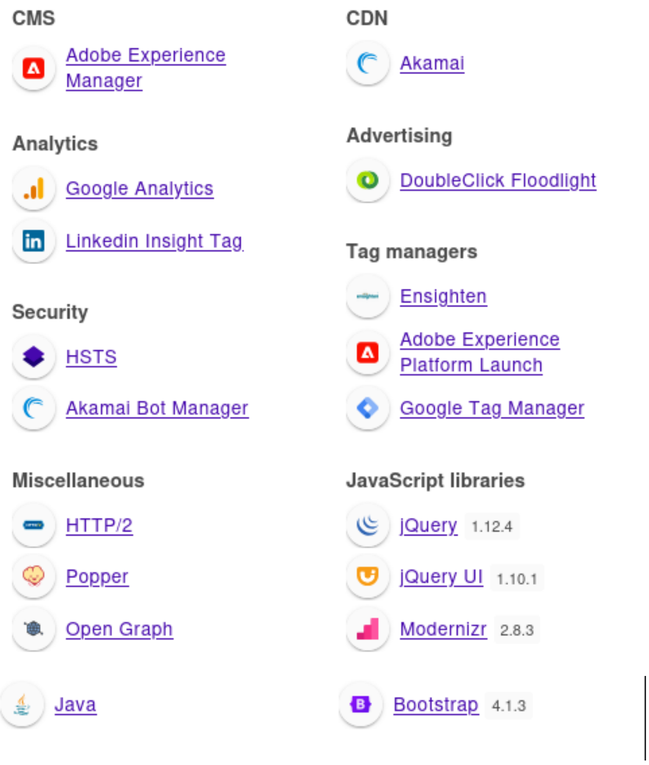


```
┌──(sheron㉿kali)-[~/Desktop/Tools/rapidscan]
└─$ wafw00f -a -v https://www.gartner.com/reviews/market/web-application-firewall

                ( W00f! )

                          404 Hack Not Found
                                              405 Not Allowed
                                403 Forbidden
                      502 Bad Gateway          500 Internal Error

                    ~ WAFW00F : v2.3.1 ~
        The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://www.gartner.com/reviews/market/web-application-firewall
[+] The site https://www.gartner.com/reviews/market/web-application-firewall is behind Cloudflare (Cloudflare Inc.) WAF.
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7
```

This sub domain is not protected by a fire wall. This confirms the result by rapid.

2.4. Wappalyzer

This is a tool that can help us to see all the technologies used in one place. It shows us the versions used. This would help us to find vulnerabilities in the outdated versions used.



CMS

Adobe Experience Manager

CDN

Akamai

Analytics

Google Analytics

Linkedin Insight Tag

Advertising

DoubleClick Floodlight

Tag managers

Ensighten

Adobe Experience Platform Launch

Google Tag Manager

Security

HSTS

Akamai Bot Manager

Miscellaneous

HTTP/2

Popper

Open Graph

JavaScript libraries

jQuery 1.12.4

jQuery UI 1.10.1

Modernizr 2.8.3

Java

Bootstrap 4.1.3

After inspecting the versions that were used the following vulnerabilities regarding the version used were discovered.

Library	Version	Known Vulnerabilities
jQuery	1.12.4	- CVE-2019-11358: Mishandles jQuery.extend(true, {}, ...) due to Object.prototype pollution.
jQuery UI	1.10.1	- CVE-2021-41182: XSS in the altField option of the Datepicker widget.
Modernizr	2.8.3	- CVE-2014-4671: Prototype pollution vulnerability.
Bootstrap	4.1.3	- CVE-2018-14041: XSS vulnerability in tooltip and popover components.

The above vulnerabilities were discovered in the versions used. Most of them co relate with the other vulnerabilities that were found during the retire.js scan. This confirms the vulnerabilities found within the website.

3. Components Affected

The following table represents the summary of the affected components. It contains details such as the component name, version, CVE and the impact.

Component	Type	Vulnerability	CVE Code	Severity	Impact
jQuery v1.12.4-aem	JavaScript Library	Object.prototype pollution via jQuery.extend(true, {}, ...)	CVE-2019-11358	Medium	Can allow unintended prototype modifications, leading to unpredictable behavior
jQuery UI Dialog v1.10.1	JavaScript Library	XSS vulnerability on closeText option	CVE-2016-7103	High	Allows attackers to inject malicious scripts via user input
Modernizr v2.8.3	JavaScript Library	Prototype pollution vulnerability	CVE-2014-4671	Medium	Can enable attackers to modify global JavaScript objects
Bootstrap v4.1.3	JavaScript Library	XSS vulnerability in tooltip and popover components	CVE-2018-14041	Medium	Allows malicious script execution within tooltips
FTP Service	Network Service	Potential unauthorized access risk	-	High	May allow attackers to intercept file transfers or escalate privileges
Web Server (Outdated Version)	Server Infrastructure	Remote Code Execution (RCE) & Authentication Bypass	-	High	Older versions may allow attackers to execute arbitrary commands
Subdomain Enumeration	Security Misconfiguration	Exposure of underlying architecture	-	Medium	Attackers can gain insight into services running on subdomains
Lack of Web Application Firewall	Security Misconfiguration	No protection against XSS, SQL injection	-	High	Increases susceptibility to web-based attacks
Denial-of-Service (DoS) Risk	Network Vulnerability	Slowloris DoS attack	-	Critical	Can lead to server exhaustion, making the service unavailable

4. Vulnerabilities

4.1. XSS – cross site scripting

XSS attacks are done by running malicious code or scripts in the victim's browser. This payload may have different levels of destructive power depending on the situation. Many fire walls and security headers in browsers protect against these types of attacks. Mainly there are three types of XSS vulnerabilities,

- Stored XSS
- Reflective XSS
- DOM XSS

During the scanning of this web application, many errors were discovered regarding the XSS attacks by different tools. This is possibly because of usage of vulnerable version or not using firewalls.

4.2. FTP service

FTP service also file transfer protocol is used to transfer files between networks. FTP could be vulnerable if,

- It uses plaintext transmission
- Anonymous Access
- Default or weak credentials
- Outdated FTP software
- No encryption

But after some testing, it didn’t use plain text nor let anonymous access. And default or weak credentials. Nmap was used to test the above. Hence it will need more testing to determine if its vulnerable or not.

4.3. Outdated server

When an outdated component is present in a web application it needs to be upgraded to the latest versions. Outdated components such as web servers can cause,

- Remote code execution
- Privilege Escalation
- Authentication Bypass
- Buffer overflows

4.4. Subdomain Enumeration

Subdomain enumeration can be done by an attacker to gain information about the website. If the architecture of the website is compromised it is easy for attacker to launch sophisticated attacks.

5. Mitigation Methods

5.1. XSS – mitigation

The main cause for the XSS vulnerability is due to outdated components. To fix this, simply update the affected libraries to the latest versions. And also in some sub directories the web application firewall has been turned off. Make sure to turn on the firewall to prevent XSS and other vulnerabilities.

5.2. FTP services

FTP services vulnerabilities can be fixed through adapting to SSH protocol. It is a more secure method to transfer files between networks.

5.3. Outdated webserver

Even though didn't find the exact version of the web server. It is recommended to upgrade to the latest server or if not, find another web server without such vulnerabilities.

5.4. Subdomain enumeration

Attacker can gain information about the architecture of the website. This may help them to find technologies used, protocols used or any other important pieces of information.

6. Conclusion

The web application seems to need some polishing as it contains many vulnerabilities regarding the versions used. Most of the versions are outdated and must be updated to prevent vulnerabilities. To gain customer trust and protect their information mitigation of the vulnerabilities is a must.