Sri Lanka Institute of Information Technology

Individual Assignment

Bug Bounty Report

Cross-Site Scripting (XSS)

Web Security - IE2062

BSc Honors in Information Technology Specializing in Cyber Security

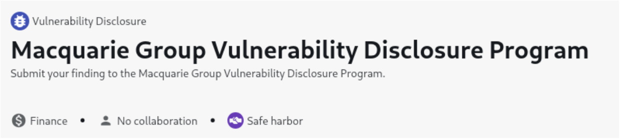
CASE STUDY NAME	BUG BOUNTY Report 03 - Cross-Site Scripting (XSS)
CAMPUS/CENTER	SLIIT KANDY UNI

Student Details

	Student Registration Number	Student Name
1	IT23222854	JAYASINGHE B. I

Table of Contents

Domain – https://www.macquarie.com/hk/en.html

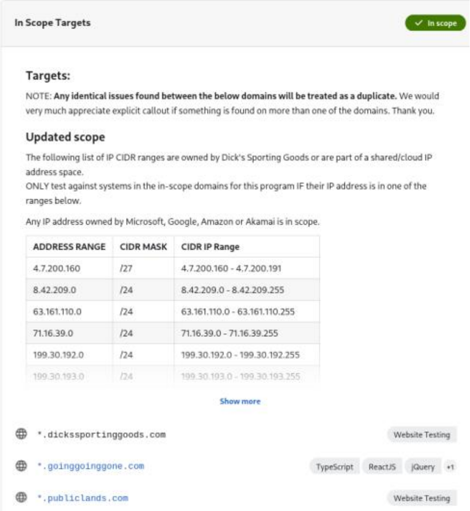


Vulnerability Disclosure

Macquarie Group Vulnerability Disclosure Program

Submit your finding to the Macquarie Group Vulnerability Disclosure Program.

Finance • No collaboration • Safe harbor



In Scope Targets ✓ In scope

Targets:

NOTE: **Any identical issues found between the below domains will be treated as a duplicate.** We would very much appreciate explicit callout if something is found on more than one of the domains. Thank you.

Updated scope

The following list of IP CIDR ranges are owned by Dick's Sporting Goods or are part of a shared/cloud IP address space.
ONLY test against systems in the in-scope domains for this program IF their IP address is in one of the ranges below.

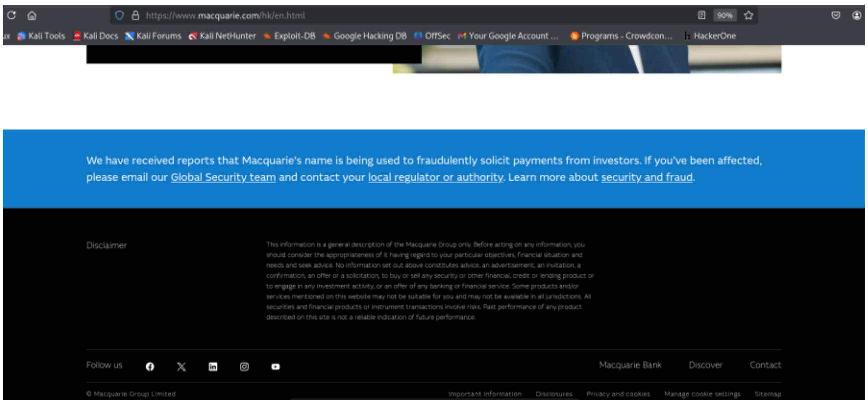
Any IP address owned by Microsoft, Google, Amazon or Akamai is in scope.

ADDRESS RANGE	CIDR MASK	CIDR IP Range
4.7.200.160	/27	4.7.200.160 - 4.7.200.191
8.42.209.0	/24	8.42.209.0 - 8.42.209.255
63.161.110.0	/24	63.161.110.0 - 63.161.110.255
71.16.39.0	/24	71.16.39.0 - 71.16.39.255
199.30.192.0	/24	199.30.192.0 - 199.30.192.255
199.30.193.0	/24	199.30.193.0 - 199.30.193.255

Show more

*.dickssportinggoods.com	Website Testing
*.goinggoinggone.com	TypeScript ReactJS jQuery +1
*.publiclands.com	Website Testing

- Link - **https://www.macquarie.com/hk/en.html**
- Category – Vulnerability Disclosure Program (VDP)
- Type - Corporate and financial services website.



https://www.macquarie.com/hk/en.html
90%
ux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Your Google Account ... Programs - Crowdcon... HackerOne

We have received reports that Macquarie's name is being used to fraudulently solicit payments from investors. If you've been affected, please email our Global Security team and contact your local regulator or authority. Learn more about security and fraud.

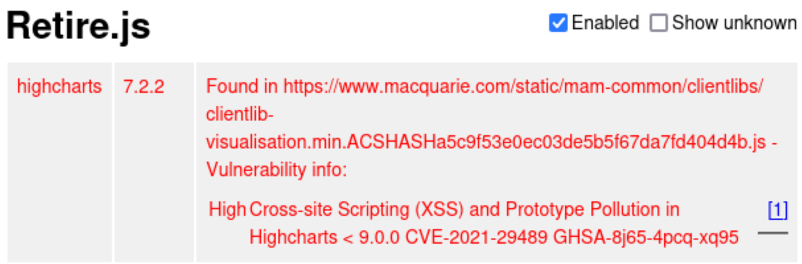
Disclaimer

This information is a general description of the Macquarie Group only. Before acting on any information, you should consider the appropriateness of it having regard to your particular objectives, financial situation and needs and seek advice. No information set out above constitutes advice, an advertisement, an invitation, a confirmation, an offer or a solicitation, to buy or sell any security or other financial, credit or lending product or to engage in any investment activity, or an offer of any banking or financial service. Some products and/or services mentioned on this website may not be suitable for you and may not be available in all jurisdictions. All securities and financial products or instrument transactions involve risks. Past performance of any product described on this site is not a reliable indication of future performance.

1. JavaScript Vulnerability Scanner

1.1 Retire.js

This tool is used to detect the use of JavaScript libraries and Node.js modules with known vulnerabilities.



Retire.js ☑ Enabled □ Show unknown

highcharts	7.2.2	Found in https://www.macquarie.com/static/mam-common/clientlibs/clientlib-visualisation.min.ACSHASHa5c9f53e0ec03de5b5f67da7fd404d4b.js - Vulnerability info: High Cross-site Scripting (XSS) and Prototype Pollution in Highcharts < 9.0.0 CVE-2021-29489 GHSA-8j65-4pcq-xq95 [1]

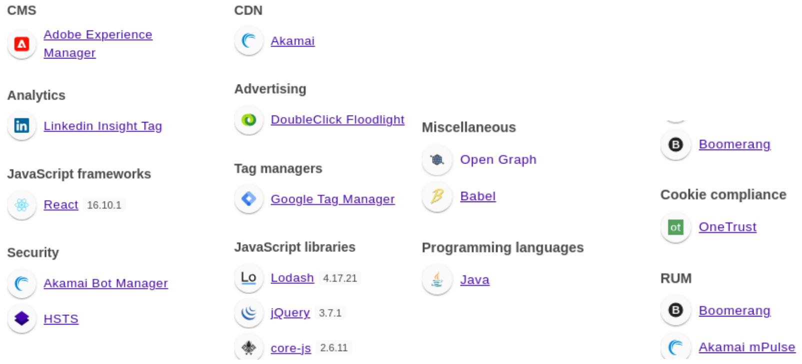
Summary of the above vulnerabilities

Library	**Version**	**Found at URL**	**Vulnerability Description**	**Severity**	**Reference (CVE/GHSA)**
Highcharts	**7.2.2**	Clientlib-visualisation.min.js	**Cross-Site Scripting (XSS)** and **Prototype Pollution** in versions < 9.0.0	High	CVE-2021-29489, GHSA-8j65-4pcq-xq95

1. Sensitive Data Exposure

1.1 Wappalyzer

The services below were detected from the domain but none of the versions could be identified. Hence could find any information about version-specific vulnerabilities. Even though disclosing services of a site is dangerous since a threat agent can exploit a known vulnerability of a service.



CMS
- Adobe Experience Manager

Analytics
- Linkedin Insight Tag

JavaScript frameworks
- React 16.10.1

Security
- Akamai Bot Manager
- HSTS

CDN
- Akamai

Advertising
- DoubleClick Floodlight

Tag managers
- Google Tag Manager

JavaScript libraries
- Lodash 4.17.21
- jQuery 3.7.1
- core-js 2.6.11

Miscellaneous
- Open Graph
- Babel

Programming languages
- Java

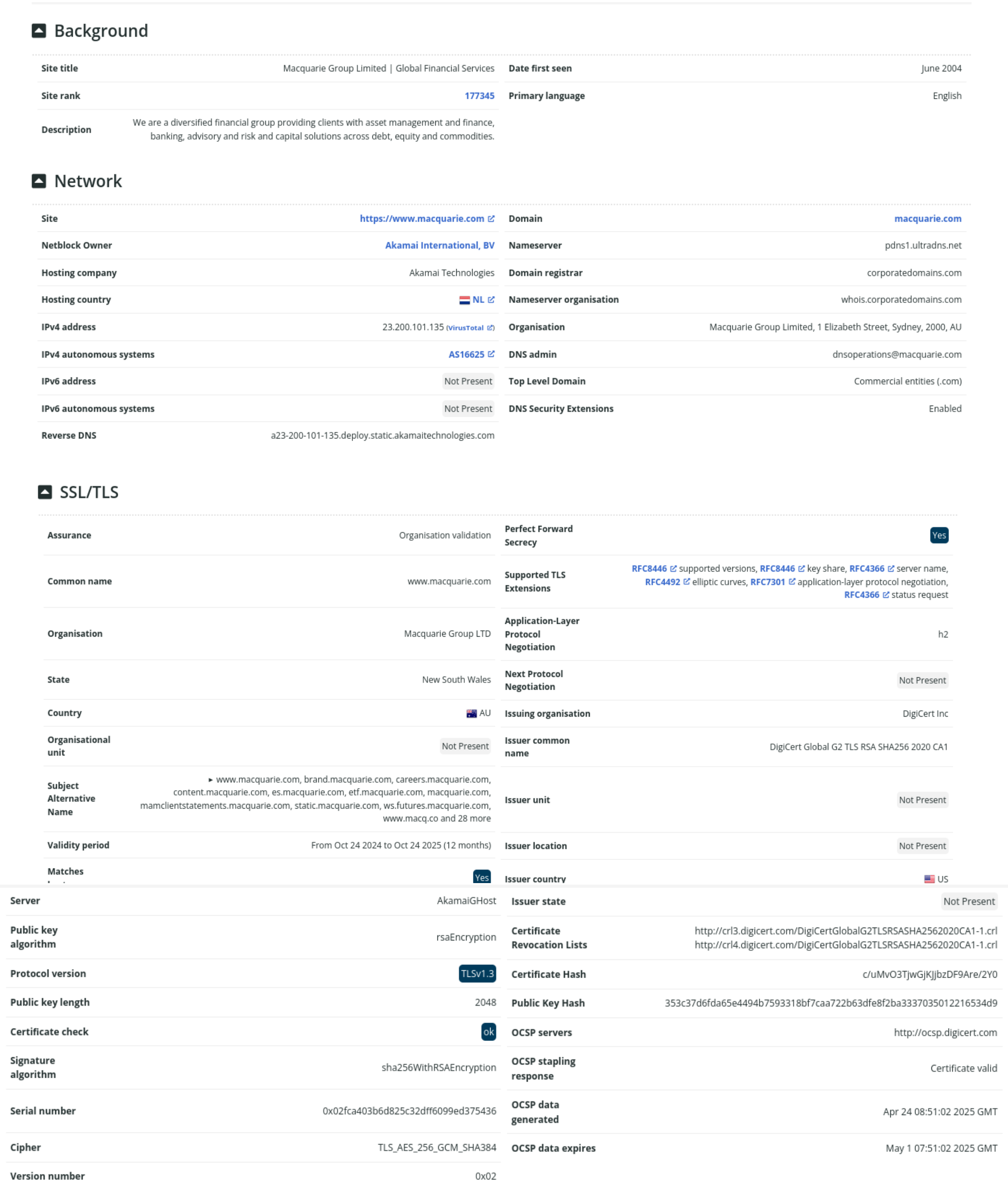
- Boomerang

Cookie compliance
- OneTrust

RUM
- Boomerang
- Akamai mPulse

1.2 Netcraft

The Netcraft Site Report tool can be utilized for site mining purposes.
Following its analysis the information below was gathered regarding the site



Background

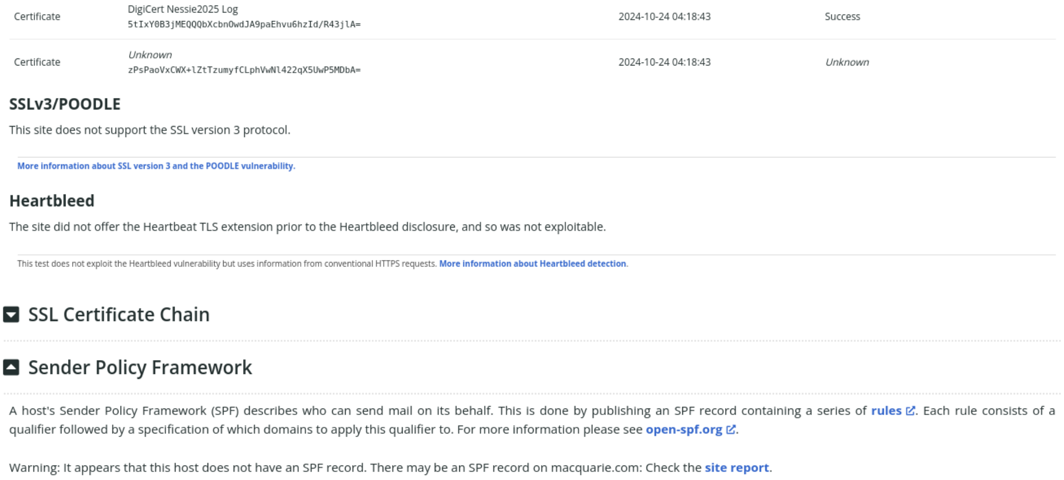
Site title	Macquarie Group Limited | Global Financial Services	**Date first seen**	June 2004
Site rank	177345	**Primary language**	English
Description	We are a diversified financial group providing clients with asset management and finance, banking, advisory and risk and capital solutions across debt, equity and commodities.		

Network

Site	https://www.macquarie.com	**Domain**	macquarie.com
Netblock Owner	Akamai International, BV	**Nameserver**	pdns1.ultradns.net
Hosting company	Akamai Technologies	**Domain registrar**	corporatedomains.com
Hosting country	NL	**Nameserver organisation**	whois.corporatedomains.com
IPv4 address	23.200.101.135 (VirusTotal)	**Organisation**	Macquarie Group Limited, 1 Elizabeth Street, Sydney, 2000, AU
IPv4 autonomous systems	AS16625	**DNS admin**	dnsoperations@macquarie.com
IPv6 address	Not Present	**Top Level Domain**	Commercial entities (.com)
IPv6 autonomous systems	Not Present	**DNS Security Extensions**	Enabled
Reverse DNS	a23-200-101-135.deploy.static.akamaitechnologies.com		

SSL/TLS

Assurance	Organisation validation	**Perfect Forward Secrecy**	Yes
Common name	www.macquarie.com	**Supported TLS Extensions**	RFC8446 supported versions, RFC8446 key share, RFC4366 server name, RFC4492 elliptic curves, RFC7301 application-layer protocol negotiation, RFC4366 status request
Organisation	Macquarie Group LTD	**Application-Layer Protocol Negotiation**	h2
State	New South Wales	**Next Protocol Negotiation**	Not Present
Country	AU	**Issuing organisation**	DigiCert Inc
Organisational unit	Not Present	**Issuer common name**	DigiCert Global G2 TLS RSA SHA256 2020 CA1
Subject Alternative Name	▸ www.macquarie.com, brand.macquarie.com, careers.macquarie.com, content.macquarie.com, es.macquarie.com, etf.macquarie.com, macquarie.com, mamclientstatements.macquarie.com, static.macquarie.com, ws.futures.macquarie.com, www.macq.co and 28 more	**Issuer unit**	Not Present
Validity period	From Oct 24 2024 to Oct 24 2025 (12 months)	**Issuer location**	Not Present
Matches	Yes	**Issuer country**	US
Server	AkamaiGHost	**Issuer state**	Not Present
Public key algorithm	rsaEncryption	**Certificate Revocation Lists**	http://crl3.digicert.com/DigiCertGlobalG2TLSRSASHA2562020CA1-1.crl http://crl4.digicert.com/DigiCertGlobalG2TLSRSASHA2562020CA1-1.crl
Protocol version	TLSv1.3	**Certificate Hash**	c/uMvO3TjwGjKJjbzDF9Are/2Y0
Public key length	2048	**Public Key Hash**	353c37d6fda65e4494b7593318bf7caa722b63dfe8f2ba33370350122165 34d9
Certificate check	ok	**OCSP servers**	http://ocsp.digicert.com
Signature algorithm	sha256WithRSAEncryption	**OCSP stapling response**	Certificate valid
Serial number	0x02fca403b6d825c32dff6099ed375436	**OCSP data generated**	Apr 24 08:51:02 2025 GMT
Cipher	TLS_AES_256_GCM_SHA384	**OCSP data expires**	May 1 07:51:02 2025 GMT
Version number	0x02		



Certificate	DigiCert Nessie2025 Log `5tIxY0B3jMEQQQbXcbnOwdJA9paEhvu6hzId/R43jlA=`	2024-10-24 04:18:43	Success
Certificate	*Unknown* `zPsPaoVxCWX+lZtTzumyfCLphVwNl422qX5UwP5MDbA=`	2024-10-24 04:18:43	*Unknown*

SSLv3/POODLE

This site does not support the SSL version 3 protocol.

More information about SSL version 3 and the POODLE vulnerability.

Heartbleed

The site did not offer the Heartbeat TLS extension prior to the Heartbleed disclosure, and so was not exploitable.

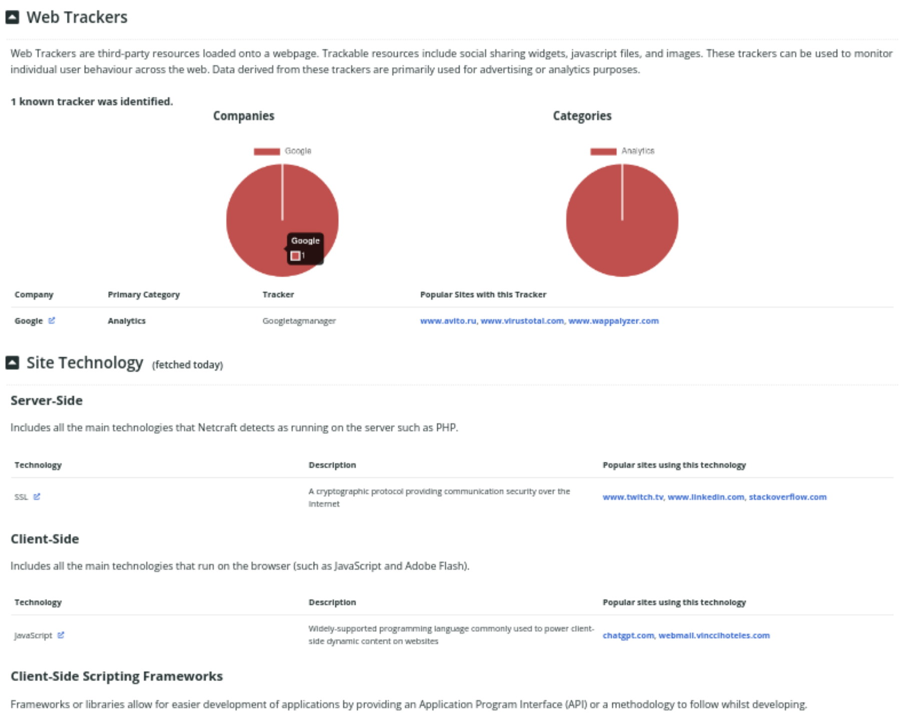
This test does not exploit the Heartbleed vulnerability but uses information from conventional HTTPS requests. More information about Heartbleed detection.

SSL Certificate Chain

Sender Policy Framework

A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of rules. Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see open-spf.org.

Warning: It appears that this host does not have an SPF record. There may be an SPF record on macquarie.com: Check the site report.



Web Trackers

Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. These trackers can be used to monitor individual user behaviour across the web. Data derived from these trackers are primarily used for advertising or analytics purposes.

1 known tracker was identified.

Companies **Categories**

Company	Primary Category	Tracker	Popular Sites with this Tracker
Google	Analytics	Googletagmanager	www.avito.ru, www.virustotal.com, www.wappalyzer.com

Site Technology (fetched today)

Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description	Popular sites using this technology
SSL	A cryptographic protocol providing communication security over the Internet	www.twitch.tv, www.linkedin.com, stackoverflow.com

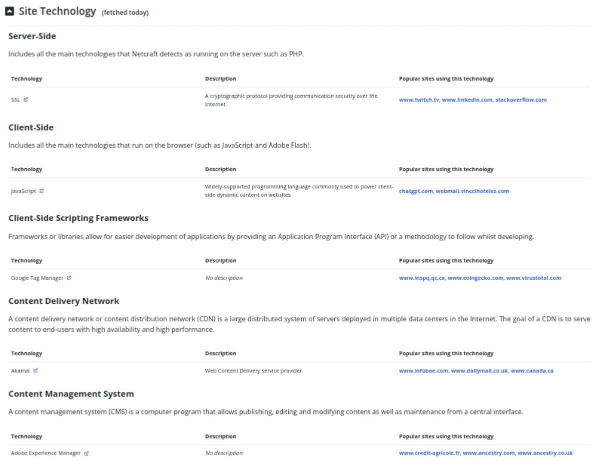
Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

Technology	Description	Popular sites using this technology
JavaScript	Widely-supported programming language commonly used to power client-side dynamic content on websites	chatgpt.com, webmail.vincciholeles.com

Client-Side Scripting Frameworks

Frameworks or libraries allow for easier development of applications by providing an Application Program Interface (API) or a methodology to follow whilst developing.



Site Technology (fetched today)

Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description	Popular sites using this technology
SSL	A cryptographic protocol providing communication security over the Internet	www.twitch.tv, www.linkedin.com, stackoverflow.com

Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

Technology	Description	Popular sites using this technology
JavaScript	Widely-supported programming language commonly used to power client-side dynamic content on websites	chatgpt.com, webmail.vincciholeles.com

Client-Side Scripting Frameworks

Frameworks or libraries allow for easier development of applications by providing an Application Program Interface (API) or a methodology to follow whilst developing.

Technology	Description	Popular sites using this technology
Google Tag Manager	*No description*	www.inspq.qc.ca, www.coingecko.com, www.virustotal.com

Content Delivery Network

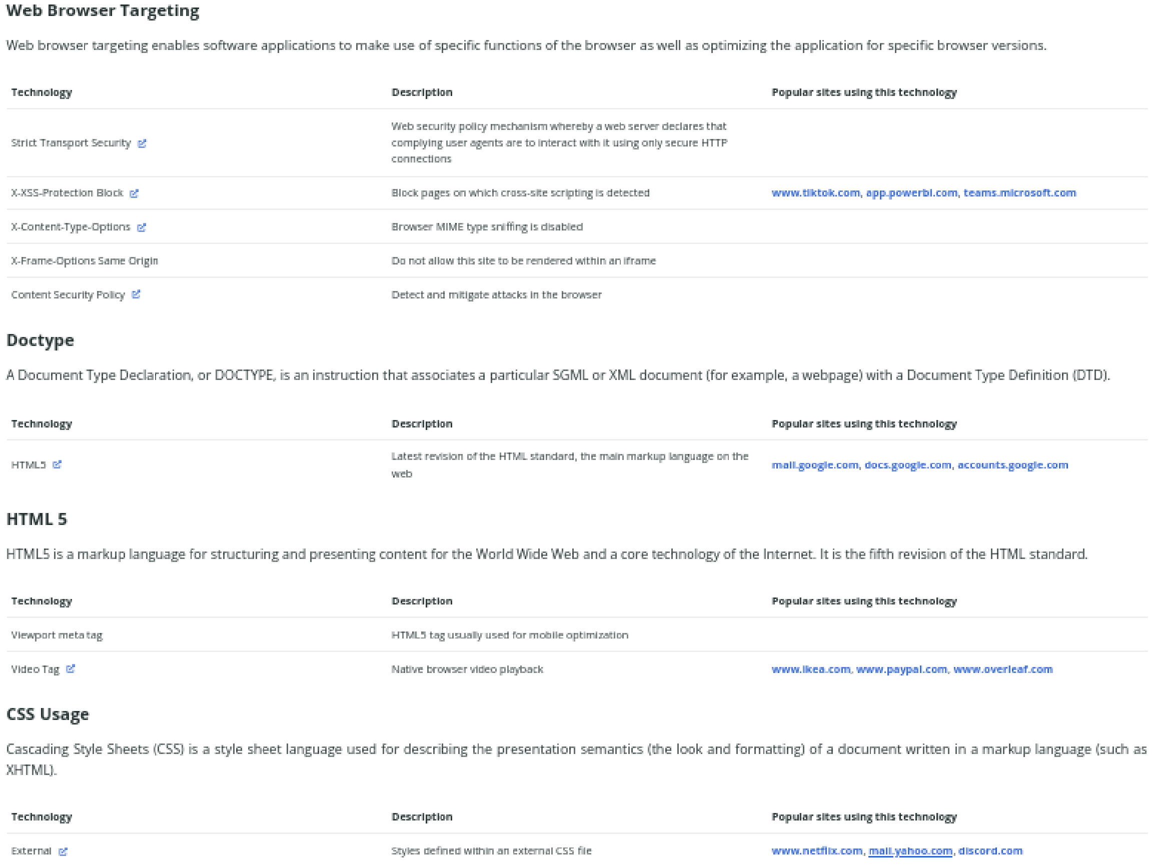
A content delivery network or content distribution network (CDN) is a large distributed system of servers deployed in multiple data centers in the Internet. The goal of a CDN is to serve content to end-users with high availability and high performance.

Technology	Description	Popular sites using this technology
Akamai	Web Content Delivery service provider	www.infobae.com, www.dailymail.co.uk, www.canada.ca

Content Management System

A content management system (CMS) is a computer program that allows publishing, editing and modifying content as well as maintenance from a central interface.

Technology	Description	Popular sites using this technology
Adobe Experience Manager	*No description*	www.credit-agricole.fr, www.ancestry.com, www.ancestry.co.uk



Web Browser Targeting

Web browser targeting enables software applications to make use of specific functions of the browser as well as optimizing the application for specific browser versions.

Technology	Description	Popular sites using this technology
Strict Transport Security	Web security policy mechanism whereby a web server declares that complying user agents are to interact with it using only secure HTTP connections	
X-XSS-Protection Block	Block pages on which cross-site scripting is detected	www.tiktok.com, app.powerbi.com, teams.microsoft.com
X-Content-Type-Options	Browser MIME type sniffing is disabled	
X-Frame-Options Same Origin	Do not allow this site to be rendered within an iframe	
Content Security Policy	Detect and mitigate attacks in the browser	

Doctype

A Document Type Declaration, or DOCTYPE, is an instruction that associates a particular SGML or XML document (for example, a webpage) with a Document Type Definition (DTD).

Technology	Description	Popular sites using this technology
HTML5	Latest revision of the HTML standard, the main markup language on the web	mail.google.com, docs.google.com, accounts.google.com

HTML 5

HTML5 is a markup language for structuring and presenting content for the World Wide Web and a core technology of the Internet. It is the fifth revision of the HTML standard.

Technology	Description	Popular sites using this technology
Viewport meta tag	HTML5 tag usually used for mobile optimization	
Video Tag	Native browser video playback	www.ikea.com, www.paypal.com, www.overleaf.com

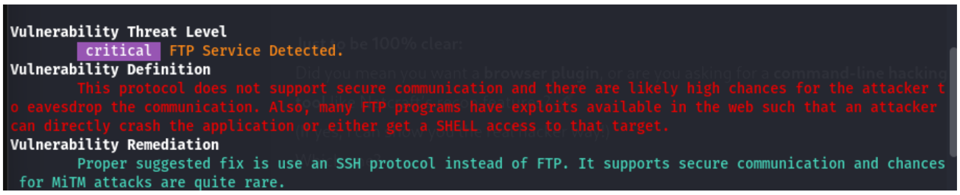
CSS Usage

Cascading Style Sheets (CSS) is a style sheet language used for describing the presentation semantics (the look and formatting) of a document written in a markup language (such as XHTML).

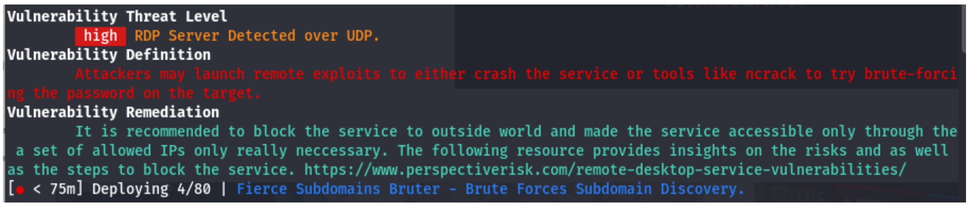
Technology	Description	Popular sites using this technology
External	Styles defined within an external CSS file	www.netflix.com, mail.yahoo.com, discord.com

2. Multi Tool Web Vulnerability Scanning

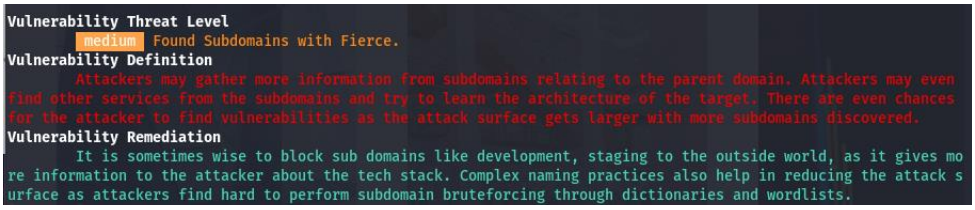
2.1 Rapid scanner



```
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 t
o eavesdrop the communication. Also, many FTP programs have exploits available in the web such that an attacker
can directly crash the application or either get a SHELL 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 quite rare.
```



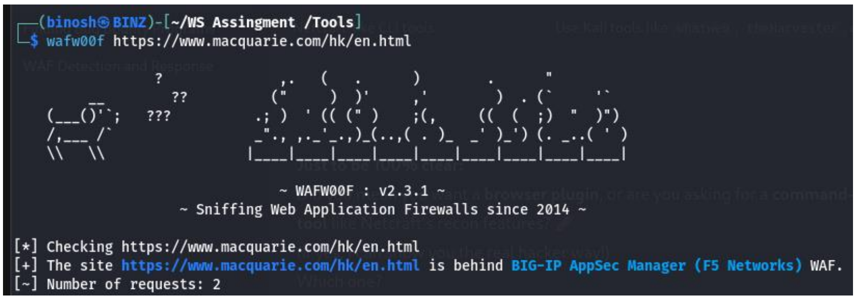
```
Vulnerability Threat Level
        high  RDP Server Detected over UDP.
Vulnerability Definition
        Attackers may launch remote exploits to either crash the service or tools like ncrack to try brute-forci
ng the password on the target.
Vulnerability Remediation
        It is recommended to block the service to outside world and made the service accessible only through the
 a set of allowed IPs only really neccessary. The following resource provides insights on the risks and as well
as the steps to block the service. https://www.perspectiverisk.com/remote-desktop-service-vulnerabilities/
[● < 75m] Deploying 4/80 | Fierce Subdomains Bruter - Brute Forces Subdomain Discovery.
```



```
Vulnerability Threat Level
        medium  Found Subdomains with Fierce.
Vulnerability Definition
        Attackers may gather more information from subdomains relating to the parent domain. Attackers may even
find other services from the subdomains and try to learn the architecture of the target. There are even chances
for the attacker to find vulnerabilities as the attack 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 mo
re information to the attacker about the tech stack. Complex naming practices also help in reducing the attack s
urface as attackers find hard to perform subdomain bruteforcing through dictionaries and wordlists.
```

4. Firewall Detection

4.1 Wafw00f

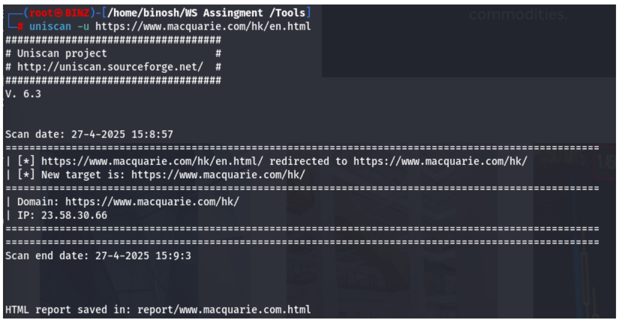


```
┌──(binosh㉿BINZ)-[~/WS Assingment /Tools]
└─$ wafw00f https://www.macquarie.com/hk/en.html

                    ?              ,.   (   .      )        .      "
        __          ??          ("     )  )'     ,'        )  . (`     '`
   (___()'`;   ???          .; )  ' (( (" )    ;(,    ((  (  ;)  "  )")
   /,___ /`                 _"., ,._'_.,)_(..,( . )_  _' )_') (. _..( ' )
   \\   \\                 |____|____|____|____|____|____|____|____|____|

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

[*] Checking https://www.macquarie.com/hk/en.html
[+] The site https://www.macquarie.com/hk/en.html is behind BIG-IP AppSec Manager (F5 Networks) WAF.
[~] Number of requests: 2
```

5. Injection

5.1 Uniscan

Command: **uniscan -u https://www.macquarie.com/hk/en.html -qd**



```
┌──(root㉿BINZ)-[/home/binosh/WS Assingment /Tools]
└─# uniscan -u https://www.macquarie.com/hk/en.html
####################################
# Uniscan project                  #
# http://uniscan.sourceforge.net/  #
####################################
V. 6.3


Scan date: 27-4-2025 15:8:57
===================================================================================================
| [*] https://www.macquarie.com/hk/en.html/ redirected to https://www.macquarie.com/hk/
| [*] New target is: https://www.macquarie.com/hk/
===================================================================================================
| Domain: https://www.macquarie.com/hk/
| IP: 23.58.30.66
===================================================================================================
===================================================================================================
Scan end date: 27-4-2025 15:9:3



HTML report saved in: report/www.macquarie.com.html
```

qd → To enable directory and dynamic checks.

The scan results indicate that the analysis was successfully completed, with the crawler identifying one accessible URL during the process. However, no vulnerabilities or issues were discovered concerning FCKeditor File Upload, Web Backdoors, Source Code Disclosure, PHPinfo() Disclosure, exposed E-mails, File Upload Forms, External Hosts, or known vulnerabilities such as Timthumb <= 1.32.

How to mitigate the above Vulnerability

Regular Software Updates to fix known vulnerabilities, make sure libraries like DOMPurify, jQuery, and Highcharts are up to date with the most recent stable versions.

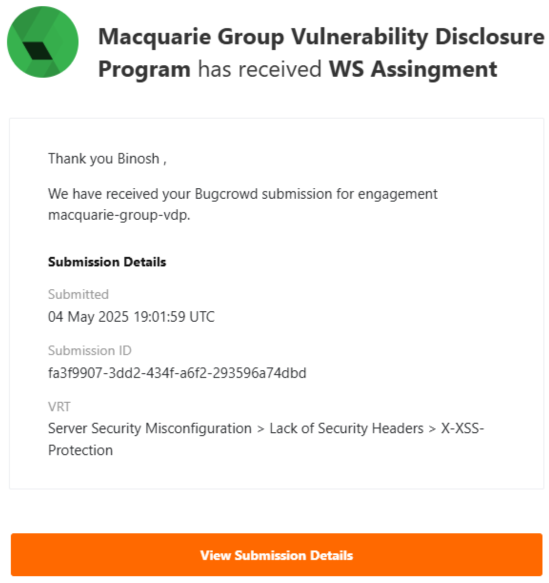
Dependency Auditing to find and fix out-of-date or weak dependencies, use tools such as npm audit. Commands like npm audit repair --force should be used with caution as they may cause breaking changes.

Robust Authentication Measures to improve access security, use multi-factor authentication (MFA) and enforce stringent password regulations.

Best Practices for Security to use monitoring tools, firewalls, and intrusion prevention systems to identify and stop hostile activity. To find and fix vulnerabilities, do routine security audits and penetration tests.

Updating to latest versions or later fixes serious XSS and prototype pollution issues for apps that use Highcharts. XSS threats are further reduced by implementing Content Security Policy (CSP) headers and cleaning user input.

Proof of report Submission



Macquarie Group Vulnerability Disclosure Program has received **WS Assingment**

Thank you Binosh ,

We have received your Bugcrowd submission for engagement macquarie-group-vdp.

Submission Details

Submitted
04 May 2025 19:01:59 UTC

Submission ID
fa3f9907-3dd2-434f-a6f2-293596a74dbd

VRT
Server Security Misconfiguration > Lack of Security Headers > X-XSS-Protection