Sri Lanka Institute of Information Technology



Individual Assignment

Bug Bounty Report

Web Security - IE2062

BSc Honors in Information Technology Specializing in Cyber Security



Web Security - IE2062

Year 2 Semester 2 - 2025

CASE STUDY NAME	BUG BOUNTY Report 09
CAMPUS/CENTER	SLIIT KANDY UNI

Student Details

	Student Registration Number	Student Name
1	IT23222854	JAYASINGHE B. I



Web Security - IE2062

Year 2 Semester 2 - 2025

Contents

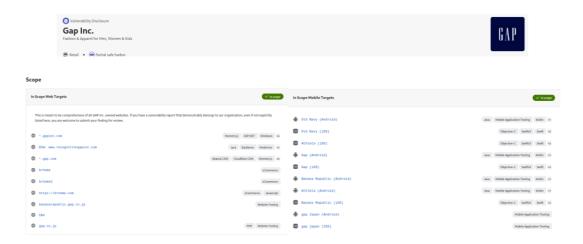
Domain – https://www.gapinc.com/en-us/	4
1.Sensitive data Exposure	5
1.1. nslookup & whois Enumeration	
1.2 Retire.js	6
Summary fo the above vulnerabilities	6
1.3 Wappalyzer	7
1.4 Netcraft	7
1.5 Katana	10
2. Firewall Detection	12
2.1. Wafw00f	12
3. Multi tool web Vulnerability Scanning	12
3.1 Rapidscan	12
4. OWASP ZAP	12



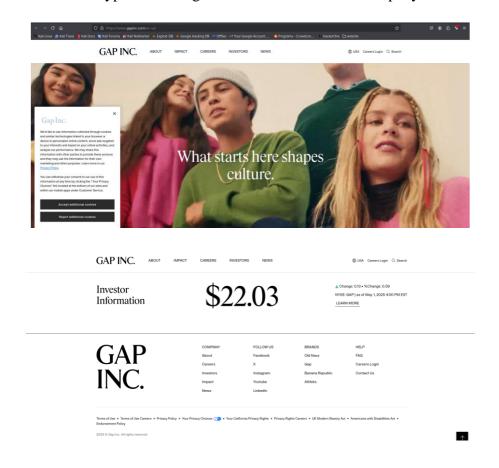
Web Security - IE2062

Year 2 Semester 2 - 2025

Domain - https://www.gapinc.com/en-us/



- Link https://www.gapinc.com/en-us/
- Category Vulnerability Disclosure Program (VDP)
- Type Clothing and accessories retailer Company





Web Security - IE2062

Year 2 Semester 2 - 2025

1. Sensitive data Exposure

1.1. nslookup & whois Enumeration

```
mentanges: 102,180.4 & 102.180.202.205

ICHR: 102,180.4 % 102.180.6 & 102.180.202.205

Merthane: PRIVATE-ADDRESS-CRUK-BFC1921-IDAN-RESERVED

METHOD: REPORT OF THE PROPERTY OF
```

Internet Assigned Numbers Authority OrgId: Address: IANA 12025 Waterfront Drive Address: Suite 300 City: Los Angeles StateProv: CA PostalCode: 90292 Country: Updated: 2024-05-24 https://rdap.arin.net/registry/entity/IANA

OrgTechHandle: IANA-IP-ARIN
OrgTechName: ICANN
OrgTechPhone: +1-310-301-5820
OrgTechEmail: abuse@iana.org
OrgTechRef: https://rdap.arin.net/registry/entity/IANA-IP-ARIN
OrgAbuseHandle: IANA-IP-ARIN
OrgAbuseName: ICANN
OrgAbusePhone: +1-310-301-5820
OrgAbuseEmail: abuse@iana.org
OrgAbuseRef: https://rdap.arin.net/registry/entity/IANA-IP-ARIN

The nslookup and whois information that have gathered provides insight into the website's domain and the associated IP address.

Here's how this information could potentially be used by malicious actors.

- Information disclosure
- DNS-related attacks
- Phishing
- Network reconnaissance
- IP address blocking

These are some remedies.

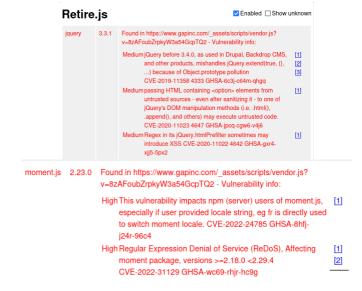
- Ensure that sensitive information such as server IP addresses, software versions, and network configurations are not publicly disclosed.
 - Implement DNS security best practices.
- Educate users about phishing techniques and encourage them to verify the authenticity of emails and websites before providing sensitive information.
 - Regularly audit your network for vulnerabilities.
 - Implement firewall rules and other security measures.



Web Security - IE2062

Year 2 Semester 2 - 2025

1.2 Retire.js



Summary fo the above vulnerabilities.

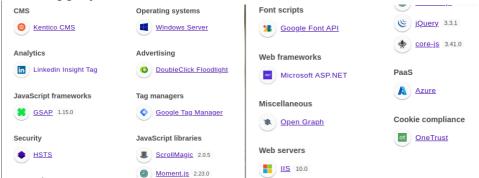
Library	Version	Vulnerability	Severity	Reference	Mitigation Strategy
		Description		(CVE/GHSA)	
Moment.js	2.14.1	Regular	High	CVE-2022-31160,	Upgrade to Moment.js
		Expression		GHSA-2fr6-h9rk-35g3	2.29.4 or later ; limit input
		Denial of			complexity.
		Service			
		(ReDoS)			
		User-	Medium	CVE-2022-43306,	Upgrade to Moment.js
		provided		GHSA-xpf4-46gq-	2.29.2 or later; sanitize
		locale may		29qx	locale inputs.
		lead to			
		unintended			
		execution			
Moment.js	2.23.0	User-	High	CVE-2022-24785,	Upgrade to Moment.js
		provided		GHSA-8hfj-j24r-96c4	2.29.2 or later ; sanitize
		locale may			locale inputs.
		lead to			
		unintended			
		execution			
		Regular	High	CVE-2022-31129,	Upgrade to Moment.js
		Expression		GHSA-wc69-rhjr-hc9g	2.29.4 or later ; limit input
		Denial of			complexity.
		Service			
		(ReDoS)			
		affecting			
		regex parsing			



Web Security - IE2062

Year 2 Semester 2 - 2025

1.3 Wappalyzer



Wappalyzer detects the **CMS**, **JavaScript libraries**, **server technologies**, and **marketing tools** running on a website. This helps in:

- Understanding the backend and frontend frameworks used (e.g., WordPress, ASP.NET, PHP).
- Identifying third-party integrations (e.g., Google Analytics, HubSpot, PubMatic).

Security Features & Risks

- Security Headers: The presence of HSTS indicates that the website enforces HTTPS connections, reducing the risk of man-in-the-middle attacks.
- JavaScript Libraries: Outdated versions (like jQuery 3.3.1) could pose risks, such as XSS vulnerabilities.
- CMS & Plugins: If Yoast SEO or WordPress plugins are outdated, they may introduce security flaws.

Potential Attack Vectors

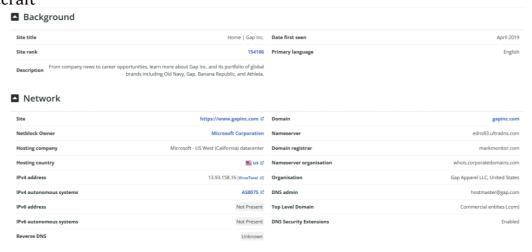
Wappalyzer can highlight technologies that might have known vulnerabilities, assess risks. For instance:

- If outdated jQuery or Moment.js is detected, attackers might attempt XSS or ReDoS attacks.
- Unpatched CMS versions can be a vector for SQL injection, plugin exploits, or privilege escalation.

Competitive & SEO Insights

- Websites running Yoast SEO might be optimizing content for search rankings.
- Identifying advertising platforms (Microsoft Advertising, PubMatic) provides insights into monetization strategies.

1.4 Netcraft



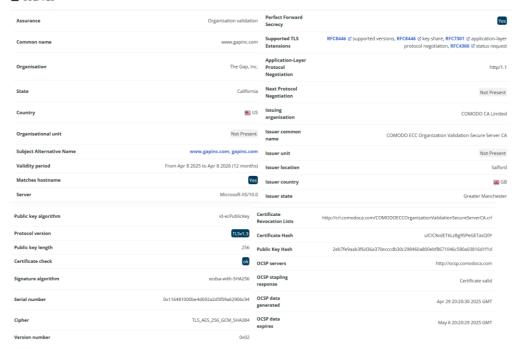


Web Security - IE2062

P delegation

Year 2 Semester 2 - 2025

SSL/TLS



Certificate Transparency

Signed Certificate Timestamps (SCTs)

Source	Log	Timestamp	Signature Verification
Certificate	Unknown 1pdkv1VY1633Q4doNuhCd+nuOtX2pPH2bkakSn/KqcY+	2025-04-08 15:30:24	Unknown
Certificate	Unknown GYblxy1gb/664294Kk88kar0LXIXD670XXBBLSVMsqv=	2025-04-08 15:30:24	Unknown
Certificate	Unknown DlebvPOugT4zGyy287P3kN+buj1xM1xd1ak1-GHFT1E=	2025-04-08 15:30:24	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

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.

2 known trackers were identified.



■ Site Technology (fetched today)



Web Security - IE2062

Year 2 Semester 2 - 2025

■ Site Technology (fetched today)

Cloud & Paat

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). Platform as a service (PaaS) is a category of cloud computing services that provide a computing platform and a solution stack as a service.

Technology	Description	Popular sites using this technology
Windows Azure Pf	Microsoft's cloud platform	

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
Atlas 🗹	A set of ASP.NET extensions for implementing Ajax functionality	www.comptia.org, www.eccexam.com, www.catalog.update.microsoft.com
Using ASP.NET ☑	ASP.NET is running on the server	www.inoreader.com, www.index.hr, www.wordreference.com

Client-Side

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

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 16	Widely-supported programming language commonly used to power client-	www.amazon.com, www.netflix.com, www.linkedin.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.virustotal.com, www.coingecko.com, www.nexusmods.com

Web Stats

Web analytics is the measurement, collection, analysis and reporting of internet data for purposes of understanding and optimizing web usage.

Technology	Description	Popular sites using this technology
Google Webmaster Tools	Set of tools allowing webmasters to check indexing status and optimize visibility of their websites on Google	www.chess.com, www.ebay.com, www.amazon.ca

Character Encoding

A character encoding system consists of a code that pairs each character from a given repertoire with something else such as a bit pattern, sequence of natural numbers, octets, or electrical pulses in order to facilitate the transmission of data (generally numbers or text) through telecommunication networks or for data storage.

Technology	Description	Popular sites using this technology
UTF8 📽	UCS Transformation Format 8 bit	

HTTP Compression

HTTP compression is a capability that can be built into web servers and web clients to make better use of available bandwidth, and provide greater transmission speeds between both.

Technology	Description	Popular sites using this technology
Gzip Content Encoding ♂	Gzip HTTP Compression protocol	www.amazon.com.mx, www.amazon.co.jp, www.amazon.de

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.

fechnology	Description	Popular sites using this technology
Document Compatibility Mode 📽	A meta-tag used in Internet Explorer 8 to enable compatibility mode	erp.fxpro.com, app.powerbl.com, mail.google.com
Content-Type-Options 📽	Browser MIME type sniffing is disabled	docs.google.com, chatgpt.com
	Web security policy mechanism whereby a web server declares that	
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-Frame-Options Same Origin	Do not allow this site to be rendered within an iframe	www.tiktok.com, stackoverflow.com

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	webmail.vinccihoteles.com, mail.yahoo.com, accounts.google.com

HTML 5

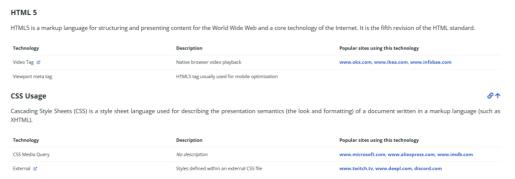
HTML5 is a markup language for structuring and presenting content for the World Wide Web and a core technology of the Internet. It is the fifth revision of the HTML standard.

Technology	Description	Popular sites using this technology
Video Tag	Native browser video playback	www.okx.com, www.ikea.com, www.infobae.com
Viewport meta tas	HTMLE tag usually used for mobile optimization	



Web Security - IE2062

Year 2 Semester 2 - 2025



Attackers can pull the gathered information to,

- Identify a website's technology stack.
- Pinpoint vulnerabilities and target outdated software.
- Craft convincing phishing attacks.
- Map out a target's internet infrastructure for planning sophisticated attacks.

Mitigation strategies

- Regular software updates.
- Implementation of strong authentication measures.
- Adherence to security best practices.

1.5 Katana

./main -u https://www.gapinc.com/en-us/ -jc -d 2 | grep "js\$" | uniq | sort > ~/gapnic/katana.txt

 $-jc \rightarrow$ To include JavaScript files in the output.

-d $2 \rightarrow$ To specify the depth of the search, which is set to 2 levels deep.

grep "js\$" → To include only lines that end with js (which indicates JavaScript files).

| unique | sort \rightarrow To sort the output and remove duplicate lines.

> ~/Gapnic/katana.txt → This saves the sorted and filtered list of JavaScript files to the file katana.txt.

The JavaScript Files below were gathered by the tool. This scanning result list can be used in the SecretFinder tool to find any sensitive data from these JavaScript files.



Web Security - IE2062

Year 2 Semester 2 - 2025

https://www.ppin.com/sents/cript-vileyperf(tent).t(t.ps/)
properties (com/sents/cript/vileyperf(tent).t(t.ps/)
properties (com/sents/vileyperf(tent).t(t.ps/)
propert



Web Security - IE2062

Year 2 Semester 2 - 2025

2. Firewall Detection

2.1. Wafw00f

```
BINZ)-[~/Desktop/WS Assingment/Tools]
$ wafw00f https://www.gapinc.com/en-us/
  The Web Application Firewall Fingerprinting Toolkit
 Checking https://www.gapinc.com/en-us/
  Generic Detection results:
  No WAF detected by the generic detection
  Number of requests: 7
```

3. Multi tool web Vulnerability Scanning

3.1 Rapidscan

```
(binosh®BINZ)-[~/Desktop/WS Assingment/Tools/rapidscan]
-$ python3 rapidscan.py -u "https://www.gapinc.com/en-us/"
```

4. OWASP ZAP

There are 3 medium risk alerts shown below.

```
Pacontent Security Policy (CSP) Header Not Set (1948)
  🎮 Missing Anti-clickjacking Header (4)
  Nulnerable JS Library (3)
  🔁 Application Error Disclosure (4)
 Cookie Without Secure Flag (1069)
Cookie with SameSite Attribute None (2)
                                                                                                 > Na Cookie Poisoning (464)
  Cookie without SameSite Attribute (1069)
 Cross-Domain JavaScript Source File Inclusion (72)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (4375)
Server Leaks Version Information via "Server" HTTP Response Header Field (4375)
                                                                                                   Information Disclosure - Suspicious Comments (9)
                                                                                                   Modern Web Application (1947)
                                                                                                 > Re-examine Cache-control Directives (119)
  Strict-Transport-Security Header Not Set (3)
                                                                                                   Session Management Response Identified (5)
 Timestamp Disclosure - Unix (701)
                                                                                                 > Number Controllable HTML Element Attribute (Potential XSS) (615)
> N X-AspNet-Version Response Header (3534)
```

```
Content Security Policy (CSP) Header Not Set
URL:
Risk:
Confidence:
                                 https://www.gar
Medium
                                 High
Parameter
Attack:
Evidence
CWE ID:
WASC ID:
                                 15
Source: Passive (
Alert Reference: 10038-1
Input Vector:
                                 Passive (10038 - Content Security Policy (CSP) Header Not Set)
 Description:
  Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
```



Web Security - IE2062

Year 2 Semester 2 - 2025

Missing Anti-clickjacking Header

https://www.gapinc.com/en-us/consumer-privacy-policy URL:

Risk: Confidence: Medium

Parameter: x-frame-options

Attack: Evidence:

1021 CWE ID: WASC ID: 15

Passive (10020 - Anti-clickjacking Header)

Alert Reference: 10020-1

Input Vector:

Description:

The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.

Vulnerable JS Library

URL: https://www.gapinc.com/_assets/scripts/vendor.js?v=8zAFoubZrpkyW3a54GcpTQ2

Risk: Medium

Confidence: Medium

Parameter:
Attack:
Evidence: /*! jQuery v3.3.1

CWE ID: 1395

WASC ID:
Source: Passive (10003 - Vulnerable JS Library (Powered by Retire.js))

Input Vector:
Description:
The identified library appears to be vulnerable.

The identified library appears to be vulnerable.

Other Info:
The identified library jquery, version 3.3.1 is wilnerable.
CVE-2020-11023
CVE-2020-11022



Web Security - IE2062

Year 2 Semester 2 - 2025

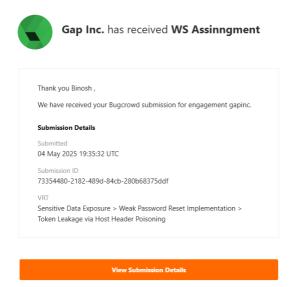
Mitigation method

- **Upgrade Dependencies:** Ensure that you're using the latest stable version of Moment.js (>= 2.29.4).
- **Input Validation:** Apply regex constraints to prevent excessive backtracking and limit user input complexity.
- Locale Sanitization: Validate locale values to prevent unexpected execution paths.
- **Dependency Monitoring:** Regularly audit libraries with tools like npm audit or Snyk to detect vulnerabilities early.
- Use X-Frame-Options Header: Set X-Frame-Options: DENY or SAMEORIGIN to prevent unauthorized framing.
- **Implement Content-Security-Policy (CSP):** Use the frame-ancestors 'none' directive for stricter enforcement.
- **Regular Audits:** Scan for missing security headers using tools like OWASP ZAP or SecurityHeaders.io.
- Application Whitelisting: Allow framing only from trusted sources if embedding is necessary.
- Enable CSP Headers: Define a strict CSP policy to control allowed sources for scripts, styles, and media

Content-Security-Policy: default-src 'self'; script-src 'self' 'trusted-cdn.com'; object-src 'none'

- **Restrict Inline Scripts:** Avoid unsafe-inline directives to prevent XSS vulnerabilities.
- Monitor CSP Violations: Implement CSP report-only mode first to detect potential policy conflicts before enforcement.
- Regular Security Audits: Use tools like SecurityHeaders.io, OWASP ZAP, or Burp Suite for continuous monitoring.

Proof of Report Submission



14