

Sri Lanka Institute of Information Technology



Individual Assignment

Bug Bounty Report

Web Security - IE2062

BSc Honors in Information Technology Specializing in Cyber Security

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


Student Details

	Student Registration Number	Student Name
1	IT23222854	JAYASINGHE B. I

Contents


Domain – https://www.gapinc.com/en-us/	4
1.Sensitive data Exposure	5
1.1. nslookup & whois Enumeration	5
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 Rapsidsan	12
4. OWASP ZAP	12

Domain – <https://www.gapinc.com/en-us/>



Gap Inc.
Fashion & Apparel for Men, Women & Kids

🛒 Retail • 🛡️ Partial safe harbor



Scope

In Scope Web Targets ✔ 10 targets

This is meant to be a comprehensive list of all Gap Inc. owned websites. If you have a vulnerability report that demonstrably belongs to our organization, even if not explicitly listed here, you are welcome to submit your finding for review.

- 🌐 *.gapinc.com Moment.js ASP.NET Windows v4
- 🌐 826* www.recognitiongapinc.com Java Backbone Modernizr v3
- 🌐 *.gap.com Amazon CDN CloudFlare CDN Moment.js v4
- 🌐 brhose eCommerce
- 🌐 brhose2 eCommerce
- 🌐 https://brhose.com eCommerce Javascript
- 🌐 bananarepublic1.gap.co.jp Website Testing
- 🌐 CB4
- 🌐 gap.co.jp PHP Website Testing

In Scope Mobile Targets ✔ 10 targets

- 📱 016 Navy (Android) Java Mobile Application Testing Kotlin v1
- 📱 016 Navy (iOS) Objective-C Swift v2
- 📱 Achlata (iOS) Objective-C Swift v2
- 📱 Gap (Android) Java Mobile Application Testing Kotlin v1
- 📱 Gap (iOS) Objective-C Swift v2
- 📱 Banana Republic (Android)
- 📱 Achlata (Android)
- 📱 Banana Republic (iOS)
- 📱 gap Japan (Android) Mobile Application Testing
- 📱 gap Japan (iOS) Mobile Application Testing

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

[Gap Inc.](#)
[ABOUT](#)
[IMPACT](#)
[CAREERS](#)
[INVESTORS](#)
[NEWS](#)

[USA](#)
[Careers Login](#)
[Search](#)

Gap Inc.

We're able to use information collected through cookies and similar technologies linked to your browser or device to personalize online content, serve ads targeted to your interests and improve your online activities, and analyze our performance. We may share this information with other parties to provide these services and they may use the information for their own marketing and other purposes. Learn more in our [Privacy Policy](#)

You can withdraw your consent to our use of this information at any time by clicking the "Your Privacy Choices" link located at the bottom of our site and within our mobile apps under Customer Service.

[Accept additional cookies](#)

[Reject additional cookies](#)

What starts here shapes culture.

[Gap Inc.](#)
[ABOUT](#)
[IMPACT](#)
[CAREERS](#)
[INVESTORS](#)
[NEWS](#)

[USA](#)
[Careers Login](#)
[Search](#)

Investor Information

\$22.03

▲ Change: 0.13 • %Change: 0.59

NYSE: GAP | as of May 1, 2025 4:00 PM EST

[LEARN MORE](#)

GAP INC.

COMPANY

[About](#)
[Careers](#)
[Investors](#)
[Impact](#)
[News](#)

FOLLOW US

[Facebook](#)
[X](#)
[Instagram](#)
[Youtube](#)
[LinkedIn](#)

BRANDS

[Old Navy](#)
[Gap](#)
[Banana Republic](#)
[Athleta](#)

HELP

[FAQ](#)
[Careers Login](#)
[Contact Us](#)

[Terms of Use](#) •
[Terms of Use Careers](#) •
[Privacy Policy](#) •
[Your Privacy Choices](#)
[Your California Privacy Rights](#) •
[Privacy Rights Careers](#) •
[UK Modern Slavery Act](#) •
[Americans with Disabilities Act](#) •
[Endorsement Policy](#)

2025 © Gap Inc. All rights reserved

1. Sensitive data Exposure

1.1. nslookup & whois Enumeration

```

NetRange: 192.168.0.0 - 192.168.255.255
CIDR: 192.168.0.0/16
NetName: PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
NetHandle: NET-192-168-0-0-1
Parent: NET192 (NET-192-0-0-0)
NetType: IANA Special Use
OriginAS:
Organization: Internet Assigned Numbers Authority (IANA)
RegDate: 1998-03-15
Updated: 2024-05-24
Comment: These addresses are in use by many millions of independently operated networks, which might be as small as a single computer connected to a home gateway, and are automatically configured in hundreds of millions of devices. They are only intended for use within a private context and traffic that needs to cross the Internet will need to use a different, unique address.
Comment: These addresses can be used by anyone without any need to coordinate with IANA or an Internet registry. The traffic from these addresses does not come from ICANN or IANA. We are not the source of activity you may see on logs or in e-mail records. Please refer to http://www.iana.org/abuse/answers
Comment: These addresses were assigned by the IETF, the organization that develops Internet protocols, in the Best Current Practice document, RFC 1918 which can be found at: http://datatracker.ietf.org/doc/rfc1918
Ref: https://rdap.arin.net/registry/ip/192.168.0.0
  
```

```

OrgName: Internet Assigned Numbers Authority
OrgId: IANA
Address: 12025 Waterfront Drive
Address: Suite 300
City: Los Angeles
StateProv: CA
PostalCode: 90292
Country: US
RegDate:
Updated: 2024-05-24
Ref: 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.

1.2 Retire.js

Retire.js ☑ Enabled ☐ Show unknown

jquery	3.3.1	<p>Found in https://www.gapinc.com/_assets/scripts/vendor.js?v=8zAFoubZrpkYW3a54GcpTQ2 - Vulnerability info:</p> <p>Medium jQuery before 3.4.0, as used in Drupal,Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution [1] [2] [3] CVE-2019-11358 4333 GHSA-6c3j-c64m-qhgg</p> <p>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. [1] CVE-2020-11023 4647 GHSA-jpcq-cgw6-v4j6</p> <p>Medium Regexp in its jQuery.htmlPrefilter sometimes may introduce XSS CVE-2020-11022 4642 GHSA-gxr4-xj5-5px2 [1]</p>
---------------	-------	--

moment.js	2.23.0	<p>Found in https://www.gapinc.com/_assets/scripts/vendor.js?v=8zAFoubZrpkYW3a54GcpTQ2 - Vulnerability info:</p> <p>High This vulnerability impacts npm (server) users of moment.js, especially if user provided locale string, eg fr is directly used to switch moment locale. CVE-2022-24785 GHSA-8hjf-j24r-96c4 [1]</p> <p>High Regular Expression Denial of Service (ReDoS), Affecting moment package, versions >=2.18.0 <2.29.4 [2] CVE-2022-31129 GHSA-wc69-rhjr-hc9g</p>
------------------	--------	---

Summary for the above vulnerabilities.

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

Web Security - IE2062

Year 2 Semester 2 - 2025

1.3 Wappalyzer

CMS Kentico CMS	Operating systems Windows Server	Font scripts Google Font API	jQuery 3.3.1 core-js 3.41.0
Analytics LinkedIn Insight Tag	Advertising DoubleClick Floodlight	Web frameworks Microsoft ASP.NET	PaaS Azure
JavaScript frameworks GSAP 1.15.0	Tag managers Google Tag Manager	Miscellaneous Open Graph	Cookie compliance OneTrust
Security HSTS	JavaScript libraries ScrollMagic 2.0.5 Moment.js 2.23.0	Web servers IIS 10.0	

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

Background

Site title	Home Gap Inc.	Date first seen	April 2019
Site rank	154186	Primary language	English
Description	From company news to career opportunities, learn more about Gap Inc. and its portfolio of global brands including Old Navy, Gap, Banana Republic, and Athleta.		

Network

Site	https://www.gapinc.com	Domain	gapinc.com
Netblock Owner	Microsoft Corporation	Nameserver	edns83.ultradns.com
Hosting company	Microsoft - US West (California) datacenter	Domain registrar	markmonitor.com
Hosting country	 US	Nameserver organisation	whois.corporatedomains.com
IPv4 address	13.93.158.16 (VirusTotal)	Organisation	Gap Apparel LLC, United States
IPv4 autonomous systems	AS8075	DNS admin	hostmaster@gap.com
IPv6 address	Not Present	Top Level Domain	Commercial entities (.com)
IPv6 autonomous systems	Not Present	DNS Security Extensions	Enabled
Reverse DNS	Unknown		

Web Security - IE2062

IP delegation

Year 2 Semester 2 - 2025

SSL/TLS

Assurance	Organisation validation	Perfect Forward Secrecy	Yes
Common name	www.gapinc.com	Supported TLS Extensions	RFC8446 ↗ supported versions, RFC8446 ↗ key share, RFC7301 ↗ application-layer protocol negotiation, RFC4366 ↗ status request
Organisation	The Gap, Inc.	Application-Layer Protocol Negotiation	http/1.1
State	California	Next Protocol Negotiation	Not Present
Country	US	Issuing organisation	COMODO CA Limited
Organisational unit	Not Present	Issuer common name	COMODO ECC Organization Validation Secure Server CA
Subject Alternative Name	www.gapinc.com, gapinc.com	Issuer unit	Not Present
Validity period	From Apr 8 2025 to Apr 8 2026 (12 months)	Issuer location	Salford
Matches hostname	Yes	Issuer country	GB
Server	Microsoft-IIS/10.0	Issuer state	Greater Manchester
Public key algorithm	id-ecPublicKey	Certificate Revocation Lists	http://crl.comodoca.com/COMODOECCOrganizationValidationSecureServerCA.crl
Protocol version	TLSv1.3	Certificate Hash	u/CIC8vdET6LzBg95PeGETasQOY
Public key length	256	Public Key Hash	2eb7fe9aab3f6d36a370ecccdb30c298460a800ebf8671046c580a03816d1f1d
Certificate check	OK	OCSP servers	http://ocsp.comodoca.com
Signature algorithm	ecdsa-with-SHA256	OCSP stapling response	Certificate valid
Serial number	0x116481000be4d592a2d5f09a62906e94	OCSP data generated	Apr 29 20:20:30 2025 GMT
Cipher	TLS_AES_256_GCM_SHA384	OCSP data expires	May 6 20:20:29 2025 GMT
Version number	0x02		

Certificate Transparency

Signed Certificate Timestamps (SCTs)

Source	Log	Timestamp	Signature Verification
Certificate	Unknown 1pdkv1VY3J3Q4dohuCd+nu0X2pPQ2BkaRhu/Kqcy+	2025-04-08 15:30:24	Unknown
Certificate	Unknown 0Ybixy1qb/66a294K08KaOLX1dE7008BLSVhw9Q+	2025-04-08 15:30:24	Unknown
Certificate	Unknown D1elvPOuqT4zgyz2B7P3kHbwj1u0EMdIak1rGHFT1E+	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.

Companies



Categories



Company	Primary Category	Tracker	Popular Sites with this Tracker
Google ↗	Analytics	Googletagmanager	www.cnn.com , www.coingecko.com , www.virusotal.com
	CDN	Googledcn	www.nexusmods.com , www.inspq.qc.ca , stackoverflow.com

Site Technology (fetched today)

Web Security - IE2062

Year 2 Semester 2 - 2025

■ Site Technology (fetched today)

Cloud & PaaS

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 id	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 id	A set of ASP.NET extensions for implementing Ajax functionality	www.comptia.org , www.eccexam.com , www.catalog.update.microsoft.com
Using ASP.NET id	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 id	Widely-supported programming language commonly used to power client-side dynamic content on websites	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 id	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 id	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 id	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 id	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.

Technology	Description	Popular sites using this technology
Document Compatibility Mode id	A meta-tag used in Internet Explorer 8 to enable compatibility mode	erp.fxpro.com , app.powerbi.com , mail.google.com
X-Content-Type-Options id	Browser MIME type sniffing is disabled	docs.google.com , chatgpt.com
Strict Transport Security id	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 id	Latest revision of the HTML standard, the main markup language on the web	webmail.vincihoteles.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 id	Native browser video playback	www.oxo.com , www.ikea.com , www.infobae.com
Viewport meta tag	HTML5 tag usually used for mobile optimization	

Web Security - IE2062

Year 2 Semester 2 - 2025


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.oxo.com , www.ikea.com , www.infobae.com
Viewport meta tag	HTML5 tag usually used for mobile optimization	

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
CSS Media Query	No description	www.microsoft.com , www.aliexpress.com , www.imdb.com
External 	Styles defined within an external CSS file	www.twitch.tv , www.deepl.com , discord.com

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

```
(binosh@BINZ)-[~/Desktop/WS Assingment/Tools]
$ katana -u https://www.gapinc.com/en-us/ grep "js$" uniq sort > katana.txt

projectdiscovery.io

[INF] Current katana version v1.1.3 (latest)
[INF] Started standard crawling for => https://www.gapinc.com/en-us/
```

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

-jc → To include JavaScript files in the output.

-d 2 → 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 → 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.gapinc.com/en-us/contact-us
https://www.gapinc.com/_assets/scripts/+u?typeof(l=null!=(l=p(n,
https://www.gapinc.com/downloadcssasset.ashx?file="+u?c(mull!=(a=mull!+t?ff(t,
https://www.gapinc.com/_assets/scripts/vendor.js?v=82AfouBzrpkW2a34GcpTQ2
https://www.gapinc.com/_assets/scripts/+u?c(mull!=(a=mull!+t?ff(t,
https://www.gapinc.com/CMSPages/GetAzureFile.aspx?path=\\gapcorporatesite\\media\\images\\about\\leadership\\leadership-hero.jpg&hash=adcd4d9c2a33581901f01c9833764fdd585e5a4742917ea1563852908dc6243d
https://www.gapinc.com/en-us/careers/careers-privacy-policy
https://www.gapinc.com/en-us/careers/privacy-policy
https://www.gapinc.com/en-us/impact/esg-resources/human-rights-and-labor-issues/policies-and-approaches-for-human-rights/foreign-contract-workers-and-recruitment
https://www.gapinc.com/en-us/values/sustainability/social/supply-chain-working-conditions/policies-and-approaches-for-human-rights/human-trafficking-and-forced-labor
https://www.gapinc.com/en-us/impact/esg-resources/human-rights-and-labor-issues/policies-and-approaches-for-human-rights/human-trafficking-and-forced-labor
https://www.gapinc.com/CMSPages/GetAzureFile.aspx?path=\\gapcorporatesite\\media\\images\\values\\sustainability\\documents\\gap-inc-code-of-vendor-conduct.pdf&hash=ccf11a639f5d9b945e663b5062973f1721cb4e418a98c4b9dcccfa5b81c8577
https://www.gapinc.com/content/gapinc/html/investors/realstate.html
https://www.gapinc.com/en-us/investors/corporate-compliance/code-of-vendor-conduct
https://www.gapinc.com/fr-ca/careers/careers-privacy-policy
https://www.gapinc.com/Careers
https://www.gapinc.com/CMSPages/GetAzureFile.aspx?path=\\gapcorporatesite\\media\\images\\values\\sustainability\\documents\\gap_inc_foreign_contract_worker_addendum.pdf&hash=129e73f8132d26415d7a985674bad8f25a53818076aeaf2d8471af7149e91b2f
https://www.gapinc.com/en-us/values/sustainability/foreign-contract-workers
https://www.gapinc.com/en-us/impact/esg-resources/human-rights-and-labor-issues/policies-and-approaches-for-human-rights/freedom-of-association
https://www.gapinc.com/en-us/impact/esg-resources/human-rights-and-labor-issues/policies-and-approaches-for-human-rights/unauthorized-subcontracting
https://www.gapinc.com/en-us/impact/esg-resources/human-rights-and-labor-issues/policies-and-approaches-for-human-rights/human-treatment
https://www.gapinc.com/en-us/impact/esg-resources/human-rights-and-labor-issues/policies-and-approaches-for-human-rights/working-hours
https://www.gapinc.com/en-us/impact/esg-resources/human-rights-and-labor-issues/policies-and-approaches-for-human-rights/short-term-contracts
https://www.gapinc.com/Investors
https://www.gapinc.com/content/gapinc/html/investors/stock_information/stock_split.html
https://www.gapinc.com/en-us/impact/esg-resources/human-rights-and-labor-issues/policies-and-approaches-for-human-rights/grievance-mechanisms
https://www.gapinc.com/en-us/impact/esg-resources/human-rights-and-labor-issues/policies-and-approaches-for-human-rights/fire-building-and-electrical-safety
https://www.gapinc.com/en-us/impact/esg-resources/human-rights-and-labor-issues/policies-and-approaches-for-human-rights/wages-and-benefits
https://www.gapinc.com/CMSPages/GetAzureFile.aspx?path=\\gapcorporatesite\\media\\images\\about\\leadership\\hero_option-3.jpg&hash=281006f729ee93a9fab56f1302ccc1dc4fb67db58552db9446f018cca28528d
https://www.gapinc.com/en-us/impact/esg-resources/human-rights-and-labor-issues/policies-and-approaches-for-human-rights/child-labor-and-young-workers
https://www.gapinc.com/en-us/impact/esg-resources/human-rights-and-labor-issues/policies-and-approaches-for-human-rights/discrimination-and-harassment
https://corporate.gapinc.com/en-us/articles/2017/03/ten-tips-for-nailing-your-job-interview-gap-inc-re
https://corporate.gapinc.com/en-us/articles/2017/05/what-to-wear-six-tips-for-dressing-for-your-interv
https://www.gapinc.com/en-us/articles/2017/03/ten-tips-for-nailing-your-job-interview-gap-inc-re
https://www.gapinc.com/en-us/articles/2017/05/what-to-wear-six-tips-for-dressing-for-your-interv
https://www.gapinc.com/Impact/ESG-Resources/Human-Rights-and-Labor-Issues/Policies-and-Approaches-for-Human-Rights
https://www.gapinc.com/content/gapinc/html/investors/fin_information/annualreports.html
https://www.gapinc.com/en-us/articles/2023/07/richard-dickson-appointed-president-and-chief-exec
https://www.gapinc.com/Impact/ESG-Resources/Human-Rights-and-Labor-Issues
https://www.gapinc.com/content/gapinc/html/investors/stock_information/transfersagent.html
https://www.gapinc.com/content/gapinc/html/investors/stock_information/directreg.html
https://www.gapinc.com/Impact
https://www.gapinc.com/Impact/ESG-Resources
https://www.gapinc.com/en-us/articles/2023/10/gap-inc-provides-twelve-free-mental-health-session
https://www.gapinc.com/content/gapinc/html/investors/fin_information/sec_filings.html
https://www.gapinc.com/en-us/articles/tag/378/interview-tips
https://www.gapinc.com/en-us/articles/tag/379/career-advice
  
```

2. Firewall Detection

2.1. Wafw00f

```
(binosh@BINZ)-[~/Desktop/WS Assingment/Tools]
$ wafw00f https://www.gapinc.com/en-us/

      { Woof! }
    (  )  (  )
   (  )  (  )
  (  )  (  )
 (  )  (  )
(  )  (  )

~ WAFW00F : v2.3.1 ~

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.


- >  Content Security Policy (CSP) Header Not Set (1948)
- >  Missing Anti-clickjacking Header (4)
- >  Vulnerable JS Library (3)
- >  Application Error Disclosure (4)
- >  Cookie Without Secure Flag (1069)
- >  Cookie with SameSite Attribute None (2)
- >  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)
- >  Strict-Transport-Security Header Not Set (3)
- >  Timestamp Disclosure - Unix (701)
- >  X-AspNet-Version Response Header (3534)
- >  Cookie Poisoning (464)
- >  Information Disclosure - Suspicious Comments (9)
- >  Modern Web Application (1947)
- >  Re-examine Cache-control Directives (119)
- >  Session Management Response Identified (5)
- >  User Controllable HTML Element Attribute (Potential XSS) (615)

Content Security Policy (CSP) Header Not Set

URL: <https://www.gapinc.com/en-us/>
 Risk:  Medium
 Confidence: High
 Parameter:
 Attack:
 Evidence:
 CWE ID: 693
 WASC ID: 15
 Source: Passive (10038 - Content Security Policy (CSP) Header Not Set)
 Alert Reference: 10038-1
 Input Vector:


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**

URL: <https://www.gapinc.com/en-us/consumer-privacy-policy>
Risk:  Medium
Confidence: Medium
Parameter: x-frame-options
Attack:
Evidence:
CWE ID: 1021
WASC ID: 15
Source: 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.

Other Info:
The identified library jquery, version 3.3.1 is vulnerable.
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 ($\geq 2.29.4$).
- **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**Gap Inc. has received WS Assinngment**

Thank you Binosh ,

We have received your Bugcrowd submission for engagement gapinc.

Submission DetailsSubmitted
04 May 2025 19:35:32 UTCSubmission ID
73354480-2182-489d-84cb-280b68375ddfVRT
Sensitive Data Exposure > Weak Password Reset Implementation >
Token Leakage via Host Header Poisoning[View Submission Details](#)