

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 06
CAMPUS/CENTER	SLIIT KANDY UNI

Student Details



	Student Registration Number	Student Name
1	IT23222854	JAYASINGHE B. I

Domain – Bath & Body Works Vulnerability Disclosure Program



Bath & Body Works Vulnerability Disclosure Program

Bath & body works, Inc. makes the world a brighter, happier place through the power of fragrance. Please submit your findings to this Vulnerability Disclosure Program.

 Retail •
  Safe harbor

Testing period

Ongoing

Started at Apr 01, 2023

Status

In progress

01 Apr 2023 18:00:00 UTC

Last updated: 26 May 2023 14:57:52 UTC [View changes](#)

Vulnerabilities accepted

63

Validation within

12 days

75% of submissions are accepted or rejected within 12 days

No technology is perfect and Bath & body works believes that working with skilled security researchers across the globe is crucial in identifying weaknesses in any technology. We are excited for you to participate as a security researcher to help us identify vulnerabilities in our target. Good luck, and happy hunting!

Ratings/Rewards:

For the initial prioritization of findings, this program will use the [Bugcrowd Vulnerability Rating Taxonomy](#). However, it is important to note that in some cases a vulnerability priority will be modified due to its likelihood or impact. In any instance where an issue is downgraded, a full, detailed explanation will be provided to the researcher - along with the opportunity to appeal, and make a case for a higher priority.

Scope

In Scope Targets

[bathandbodyworks.com](#) [Website Testing](#)

[bathandbodyworks.us](#) [Retail](#)

[bathandbodyworks.us](#) [Android](#)

[bathandbodyworks.us](#) [iOS](#)

Testing is only authorized on the targets listed as in scope. Any domain/property of Bath & body works not listed in the targets section is out of scope. This includes any/all subdomains not listed above. If you happen to identify a security vulnerability on a target that is not in scope, but it demonstrably belongs to Bath & body works, you can report it. However, be aware that it is ineligible for rewards or points-based compensation.

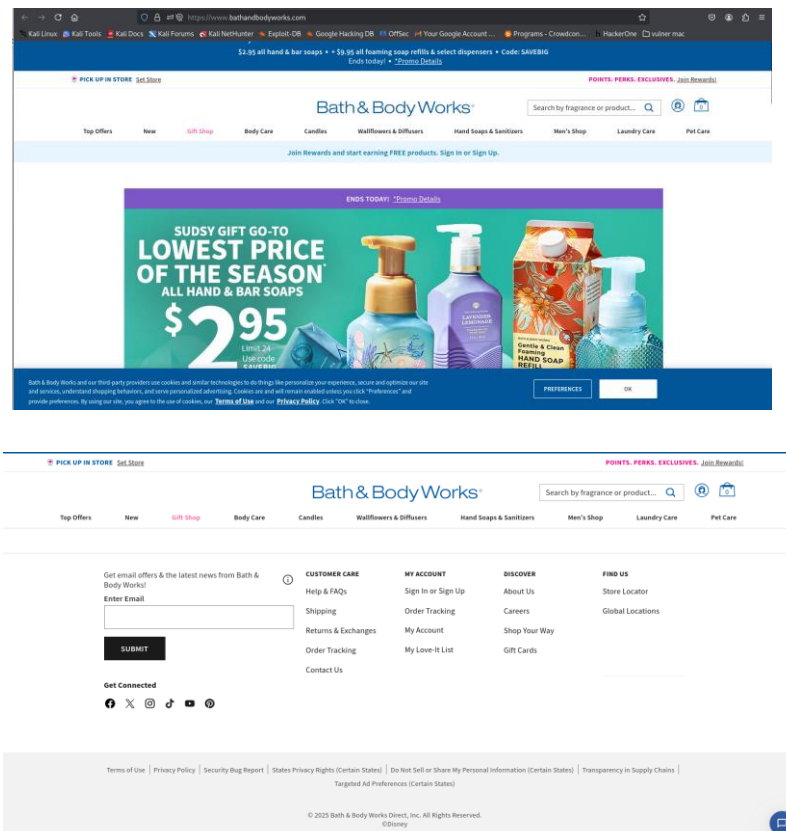
Access:

- Target is accessible via public internet

Credentials:

- None

- Link - <https://www.bathandbodyworks.com/>
- Type – Personal care and home fragrance products



The screenshot shows the Bath & Body Works website. At the top, there's a navigation bar with links like 'Kali Linux', 'Kali Tools', 'Kali Docs', 'Kali Forums', 'Kali NetHunter', 'Exploit-DB', 'Google Hacking DB', 'OffSec', 'Your Google Account', 'Programs', 'CrowdSec', 'HackerOne', and 'vulnmap'. Below the navigation bar, there's a large banner for 'SUDSY GIFT GO-TO LOWEST PRICE OF THE SEASON ALL HAND & BAR SOAPS \$2.95'. The banner includes images of various soap bottles and boxes. Below the banner, there's a section for 'CUSTOMER CARE' with links like 'Help & FAQs', 'Shipping', 'Returns & Exchanges', and 'Contact Us'. There's also a section for 'MY ACCOUNT' with links like 'Sign In or Sign Up', 'Order Tracking', 'My Account', and 'My Love It List'. At the bottom, there's a footer with links for 'Terms of Use', 'Privacy Policy', 'Security Bug Report', 'States Privacy Rights (Certain States)', 'Do Not Sell or Share My Personal Information (Certain States)', 'Transparency in Supply Chains', and 'Targeted Ad Preferences (Certain States)'. The footer also includes the copyright notice '© 2023 Bath & Body Works Direct, Inc. All Rights Reserved. ©2023'.

1. Multi Tool Web Vulnerability Scanning

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		
axios	1.7.4	Found in https://objects.githubusercontent.com/github-production-release-asset-2e65be/838377826/675599c9-eb64-467d-9659-58bb91a4d64c Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=releaseassetproduction%2F20250428%2Fus-east-1%2Fsa%3Faws4_request&X-Amz-Date=20250428T005846Z&Expires=300&X-Amz-Signature=1061744095002499bfa8e19d59e6b2e2f1d2e70407858dAmz-SignedHeaders=host&response-content-disposition=attachment%3B%20filename%3Dwebchat.js&response-content-type=application%2Foctet-stream - Vulnerability info: High axios Requests Vulnerable To Possible SSRF and Credential Leakage via Absolute URL CVE-2025-27152 GHSA-j5f-v2jy-69x8
jquery-ui-dialog	1.11.2	Found in https://www.bathandbodyworks.com/on/demandware.static/BathAndBodyWorks-Site/-/en_US/v1745747208540/lib/jquery/ui/jquery-ui-dialog Vulnerability info: Medium XSS Vulnerability on closeText option CVE-2016-7103 2810 hpcl-8vf9-q4gj
jquery-ui	1.11.2	Found in https://www.bathandbodyworks.com/on/demandware.static/BathAndBodyWorks-Site/-/en_US/v1745747208540/lib/jquery/ui/jquery-ui Vulnerability info: Medium XSS in the 'altField' option of the Datepicker widget CVE-2020-11023 4647 GHSA-jpcq-cgw6-v4j6
jquery-ui	1.11.2	Found in https://www.bathandbodyworks.com/on/demandware.static/BathAndBodyWorks-Site/-/en_US/v1745747208540/lib/jquery/ui/jquery-ui Vulnerability info: Medium XSS in the 'altField' option of the Datepicker widget CVE-2020-11023 4647 GHSA-jpcq-cgw6-v4j6
jquery-ui	1.11.2	Found in https://www.bathandbodyworks.com/on/demandware.static/BathAndBodyWorks-Site/-/en_US/v1745747208540/lib/jquery/ui/jquery-ui Vulnerability info: Medium XSS in the 'altField' option of the Datepicker widget CVE-2020-11023 4647 GHSA-jpcq-cgw6-v4j6
jquery-validation	1.13.1	Found in https://www.bathandbodyworks.com/on/demandware.static/BathAndBodyWorks-Site/-/en_US/v1745747208540/lib/jquery/jquery-validation Vulnerability info: High Regular Expression Denial of Service vulnerability CVE-2020-jpwx-85vp-gvwm Low ReDoS vulnerability in URL2 validation CVE-2021-43306 24 h2pv-wvph High ReDoS vulnerability in url and URL2 validation CVE-2022-3-ftmh-x56j-9rc3 Medium Potential XSS via showLabel 2462
jquery	2.1.1.min	Found in https://www.bathandbodyworks.com/on/demandware.static/BathAndBodyWorks-Site/-/en_US/v1745747208540/lib/jquery/jquery Vulnerability info: Low jQuery 1.x and 2.x are End-of-Life and no longer receiving security updates 73 162 Medium 3rd party CORS request may execute 2432 CVE-2015-9251 rmxg-73gg-4p98 Medium jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution CVE-2019-11358 4333 GHSA-6c- Medium passing HTML containing <option> elements from untrusted even after sanitizing it - to one of jQuery's DOM manipulation (i.e. .html(), .append(), and others) may execute untrusted code CVE-2020-11023 4647 GHSA-jpcq-cgw6-v4j6 Medium Regex in its jQuery.htmlPrefilter sometimes may introduce XSS CVE-2020-11022 4642 GHSA-gxr4-xjj5-5px2

Summary for the above vulnerabilities.

Library	Version	Vulnerability Description	Severity	Found At URL	Reference (CVE/Git Hub)
axios	1.7.4	Potential issue raised in GitHub repository	Unknown	https://objects.githubusercontent.com/github-production-release-asset-2e65be/...	https://github.com/axios/axios/issues/5346
jquery-ui-dialog	1.11.2	XSS Vulnerability on closeText option (CVE-2016-7103)	Medium	https://www.bathandbodyworks.com/on/demandware.static/Sites-	CVE-2016-7103

Web Security - IE2062
Year 2 Semester 2 - 2025

jQuery-ui	1.11.2	XSS Vulnerability in altField option of the Datepicker widget (CVE-2016-7103)	Medium	https://www.bathandbodyworks.com/on/demandware.static/Sites-BathAndBodyWorks-Site/-/en_US/js/jquery-ui.js	CVE-2016-7103
------------------	--------	---	--------	---	---------------

Library	Version	Vulnerability Description	Severity	Reference (CVE/GHSA)	Found at URL
jQuery-ui	1.11.2	Medium XSS in "altField" option of Datepicker widget	Medium	CVE-2021-41183, GHSA-9gj3-hsp5-7mcf	https://www.bathandbodyworks.com/jquery-ui/jquery-ui.js
		Medium XSS in "of" option of "position" utility	Medium	CVE-2021-41183, GHSA-9gj3-hsp5-7mcf	
		Medium XSS in text options of Datepicker	Medium	CVE-2021-41183, GHSA-9gj3-hsp5-7mcf	
		XSS in checkbox selection with an HTML file in the "label"	Medium	CVE-2022-31160, GHSA-6jgj-hsp5-7mcf	
jQuery-validation	1.13.1	High Regular Expression Denial of Service (ReDoS) vulnerability	High	CVE-2022-43306, GHSA-6jgj-hsp5-7mcf	https://www.bathandbodyworks.com/jquery-validation/jquery-validation.js
		Low ReDoS vulnerability in URL2 validation	Low	CVE-2021-43306, GHSA-6jgj-hsp5-7mcf	
		High ReDoS vulnerability in URL and URL2 validation	High	CVE-2022-43306, GHSA-6jgj-hsp5-7mcf	
		Medium Potential XSS via "showLabel"	Medium		
jQuery	2.1.1.min	Medium XSS in "showLabel"	Medium		https://www.bathandbodyworks.com/jquery/jquery.js

Web Security - IE2062
Year 2 Semester 2 - 2025

Library	Version	Source URL	Vulnerability Description	Severity	Reference (CVE/GHSA)
jQuery	2.1.1.min	jQuery Source	jQuery 1.x and 2.x are End-of-Life and no longer receiving security updates	Low	-
			3rd party CORS requests may execute untrusted code	Medium	CVE-2015-9251, GHSA-mxrg-739g-4p98
			Mishandles jQuery.extend(true, ...) due to Object.prototype pollution	Medium	CVE-2019-11358, GHSA-c2h3-6vqh-wj42
			Passing HTML containing elements to jQuery DOM manipulation methods may execute untrusted code	Medium	CVE-2020-11022, GHSA-gxr4-xjj5-5px2
			Regex in its jQuery.htmlPrefilter may introduce XSS	Medium	CVE-2020-11022, GHSA-gxr4-xjj5-5px2

2 Rapidscan

```
(binosh@BINZ)-[~/Desktop/WS Assingment/Tools/rapidscan]
$ python3 rapidscan.py -u https://www.bathandbodyworks.com/
```

Out of 80 vulnerabilities checked for <https://www.bathandbodyworks.com/> **4 vulnerabilities** were detected

```
Vulnerability Threat Level
medium Secure Client Initiated Renegotiation is supported.
Vulnerability Definition
Otherwise termed as Plain-text Injection attack, which allows MITM attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context.
Vulnerability Remediation
Detailed steps of remediation can be found from these resources. https://securingtomorrow.mcafee.com/technical-how-to/tips-securing-ssl-renegotiation/ https://www.digicert.com/news/2011-06-03-ssl-renego/
```

4. OWASP

```
CSP: Failure to Define Directive with No Fallback
URL: https://www.bathandbodyworks.com/
Risk: Medium
Confidence: High
Parameter: content-security-policy
Attack:
img-src 'self' *.commercloud.salesforce.com *.bathandbodyworks.com data: *.yottaa.net bat.bing.com *.google.com *.tealumiq.com *.smaato.net *.pubmatic.com *.rubiconproject.com *.doubleclick.net *.casalemedia.com *.3lift.com *.adnxs.com *.ads.audiothisisidax.com *.analytics.yahoo.com *.dotomi.com *.openx.net *.contextweb.com *.crb.kargo.com *.ap.illit.com *.id.sinc.livestreamworld.com *.sync.bfmio.com *.partners.tremorhub.com *.contextual.media.net *.ps.eyota.net *.idsync.ricdn.com *.match.adsvr.org *.exchange-match.mediaplex.com *.sync.1rx.io *.us.ck-ie.com *.sync.targeting.unrulymedia.com *.assets.gelplatform.s3.amazonaws.com *.agentcore.s3.amazonaws.com *.alvo-assets.s3.amazonaws.com *.cdn.jideli.net *.bazaarvoice.com *.brsrvr.com *.cm.everesttech.net *.ads.stickyadstv.com *.tags.bluekai.com *.match.sharethrough.com *.sync.ipredictive.com *.sync.mathtag.com *.cs.openwebng.com *.dpm.demdex.net *.curialate.com *.cdn.cookiecove.com *.brightcove.com *.brightcovecdn.com *.paypalobjects.com *.googleapis.com *.gstatic.com *.onetrust.com *.cookiecove.com *.zineone.com https://www.googletagmanager.com *.v2assets.zopim.io *.bathandbodyworkscs.zendesk.com *.pinterest.com *.pinterest.com *.omtrdc.net *.omtrdc.net *.mountain.com *.mountain.com *.script-src 'self' 'unsafe-inline' *.blo.b.storage.googleapis.com *.localhost:3000 *.code.jquery.com *.tags.tiqcdn.com *.yottaa.net *.attn.tv *.bbwi-us.attn.tv *.events.attentivemobile.com *.www.googletagmanager.com *.doubleclick.net *.cdn.quantummetric.com *.bathandbodyworks.com *.bat.bing.com *.sc-static.net *.agentbot.net *.pepperjam.com *.monetate.net *.engine-global.monetate.net *.privacymanager.io *.tealumiq.com *.attentivemobile.com *.assets.adobedtm.com *.dotomi.com *.smaato.net *.kamplify.com *.zineone.com *.bazaarvoice.com *.mpsnare.lesnare.com *.cookiecove.com *.brcdn.com *.cnstrc.com *.bathandbodyworks-pixel.netlify.app https://www.google.com/recaptcha/ *.googleapis.com *.gstatic.com *.onetrust.com *.cdn-apple.com *.curialate.com *.ordergrove.com *.cdn.cookiecove.com *.brightcove.net *.brightcovecdn.com *.github.com *.objects.githubusercontent.com *.dev.zopim.com *.static.zdassets.com *.paypal.com *.privacyportal-cdn.onetrust.com *.rdf.radial.com *.tst-rdf.radial.com https://s.pinimg.com *.7316103.collect.lgodigital.com https://*.yottaa.com https://*.yottaa.net https://*.px-cloud.net https://*.px-cdn.net *.pinterest.com *.byspotify.com *.unsafe-eval https://runtime.commercloud.com *.connect-src 'self' *.api.quotient.com *.localhost:3000 *.dpm.demdex.net *.bbwi-us.attn.tv *.events.attentivemobile.com *.aa.bathandbodyworks.com *.tealumiq.com *.bathandbodyworks.com *.ingest.quantummetric.com *.restapi.ordergrove.com *.bazaarvoice.com *.googleapis.com *.gstatic.c
```

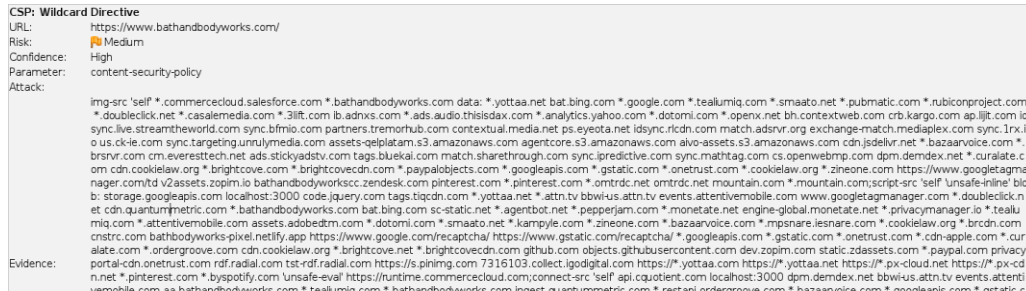
CSRF (Cross-Site Request Forgery) vulnerability related to failure in the Content Security Policy directive.

Web Security - IE2062
Year 2 Semester 2 - 2025

Vulnerability Overview: The system lacks a defined fallback for the Content Security Policy (content-security-policy parameter), specifically for the img-src directive.

Risk Level: Medium, with High confidence in the report findings.

Issue: The provided img-src directive allows images from numerous external sources. This expansive list increases the risk of CSRF attacks as malicious actors could exploit insecure



Content Security Policy (CSP). The report flags the use of a **wildcard directive**, marking it as a medium-risk issue with high confidence.

Risk Level: Medium - While not critical, this could lead to vulnerabilities such as resource misuse or unauthorized external interactions.

Concern: The wildcard directive in the CSP could allow unintended external domains to interact with the website. This might introduce risks like data leakage or malicious scripts.

Evidence: A detailed list of external domains (e.g., Salesforce, Google, Facebook) indicates widespread reliance on third-party resources, which could be exploited if not tightly controlled.

Implications

Security Risks: Improperly configured CSPs may expose the site to potential attacks, including Cross-Site Scripting (XSS).

Mitigation: It's advisable to avoid using wildcards in CSPs and restrict allowable domains to trusted ones.



Cross-Domain Misconfiguration vulnerability.

URL Affected: The bathandbodyworks.com domain.

Web Security - IE2062
Year 2 Semester 2 - 2025
Risk Level: Medium (Confidence: Medium).

Issue: A misconfiguration of Cross-Origin Resource Sharing (CORS) settings on the web server.

Key Parameter: Access-Control-Allow-Origin:

Impact


This misconfiguration allows third-party domains to make cross-domain read requests. While browser implementations prevent reading authenticated API responses from third-party domains, unauthenticated APIs could still be exploited.

Implications

Attackers could potentially exploit this misconfiguration to access sensitive data that relies on additional security measures (e.g., IP address whitelisting). Although this issue affects unauthenticated APIs, it can still pose risks if sensitive information is inadvertently exposed.

Mitigation Steps

Review and restrict CORS policy to allow only specific trusted domains.
 Avoid using wildcards (*) in CORS configurations, especially for sensitive resources.

CSP: style-src unsafe-inline
 URL: https://www.bathandbodyworks.com/
 Risk:  Medium
 Confidence: High
 Parameter: content-security-policy
 Attack:
 img-src 'self' *.commercecloud.salesforce.com *.bathandbodyworks.com data: *.yottaa.net bat.bing.com *.google.com *.tealumiq.com *.smaato.net *.pubmatic.com *.rubiconproject.com *.doubleclick.net *.casalemedia.com *.3lift.com lb.adnxs.com *.ads.audio.thisisdax.com *.analytics.yahoo.com *.dotomi.com *.openx.net bh.contextweb.com crb.kargo.com ap.lijit.com id.sync.live.streamtheworld.com sync.bfmio.com partners.tremorhub.com contextual.media.net ps.eyetoa.net idsync.ricdn.com match.adsrvr.org exchange-match.mediaplex.com sync.1rx.io us.ck-le.com sync.targeting.unrulymedia.com assets-qelplatam.s3.amazonaws.com agentcore.s3.amazonaws.com alvo-assets.s3.amazonaws.com cdn.jsdelivr.net *.bazaavoice.com *.brsivr.com cm.everesttech.net ads.stickyadstv.com tags.bluekai.com match.sharethrough.com sync.ipredictive.com sync.mathtag.com cs.openwebmp.com dpm.demdex.net *.curalete.com cdn.cookiecave.org *.brightcovecdn.com *.paypalobjects.com *.googleapis.com *.gstatic.com *.onetrust.com *.cookiecave.org *.zineone.com https://www.googletagmanager.com/mtd/v2/assets.zopim.io bathandbodyworksc.zendesk.com pinterest.com *.pinterest.com *.omtrdc.net omtrdc.net mountain.com *.mountain.com/script-src 'self' 'unsafe-inline' blob: storage.googleapis.com localhost:3000 code.jquery.com tags.tiqcdn.com *.yottaa.net *.attn.tv bbw-us.attn.tv events.attentivemobile.com www.googletagmanager.com *.doubleclick.net cdn.quantummetric.com *.bathandbodyworks.com bat.bing.com sc-static.net *.agentbot.net *.pepperjam.com *.monetate.net engine-global.monetate.net *.privacymanager.io *.tealumiq.com *.attentivemobile.com assets.adobedtm.com *.dotomi.com *.smaato.net *.kampyle.com *.zineone.com *.bazaavoice.com *.mpsnare.iesnare.com *.cookiecave.org *.brcdn.com cnstrc.com bathandbodyworks-pixel.netlify.app https://www.google.com/recaptcha/ https://www.gstatic.com/recaptcha/ *.googleapis.com *.gstatic.com *.onetrust.com *.cdn-apple.com *.curalete.com *.ordergroove.com cdn.cookiecave.org *.brightcove.net *.brightcovecdn.com github.com objects.githubusercontent.com dev.zopim.com static.zdassets.com *.paypal.com privacyportal-cdn.onetrust.com rdf.radial.com tst-rdf.radial.com https://s.pinimg.com/7361/03/collect.igodigital.com https://*.yottaa.com https://*.yottaa.net https://*.px-cloud.net https://*.px-cdn.net *.pinterest.com *.byspotify.com 'unsafe-eval' https://runtime.commercecloud.com/connect-src 'self' api.cquotient.com localhost:3000 dpm.demdex.net bbw-us.attn.tv events.attentivemobile.com aa.bathandbodyworks.com *.tealumiq.com *.bathandbodyworks.com ingest.quantummetric.com *.restapi.ordergroove.com *.bazaavoice.com *.googleapis.com *.gstatic.com

Content Security Policy (CSP). The report flags the use of a **wildcard directive**, marking it as a medium-risk issue with high confidence.

Risk Level: Medium — While not critical, this could lead to vulnerabilities such as resource misuse or unauthorized external interactions.

Concern: The wildcard directive in the CSP could allow unintended external domains to interact with the website. This might introduce risks like data leakage or malicious scripts.

Evidence: A detailed list of external domains (e.g., Salesforce, Google, Facebook) indicates widespread reliance on third-party resources, which could be exploited if not tightly controlled.
Implications:

Security Risks: Improperly configured CSPs may expose the site to potential attacks, including Cross-Site Scripting (XSS).

Web Security - IE2062
Year 2 Semester 2 - 2025

Mitigation: It's advisable to avoid using wildcards in CSPs and restrict allowable domains to trusted ones.

CSP: script-src unsafe-inline	
URL:	https://www.bathandbodyworks.com/
Risk:	Medium
Confidence:	High
Parameter:	content-security-policy
Attack:	img-src 'self' *.commercecloud.salesforce.com *.bathandbodyworks.com data: *.yottaa.net bat.bing.com *.google.com *.tealiumiq.com *.smaato.net *.pubmatic.com *.rubiconproject.com *.doubleclick.net *.casalemedia.com *.3lift.com *.ib.adnxs.com *.ads.audio.thisisdax.com *.analytics.yahoo.com *.dotomi.com *.openx.net *.contextweb.com *.crb.kargo.com *.ap.lijt.com *.sync.live.streamtheworld.com *.sync.bfmio.com *.partners.tremorhub.com *.contextual.media.net *.ps.eyota.net *.idsync.ricdn.com *.match.adsrvr.org *.exchange-match.mediaplex.com *.sync.1rx.io *.us.ck-ie.com *.sync.targeting.unrulymedia.com *.assets-qelplatam.s3.amazonaws.com *.agentcore.s3.amazonaws.com *.alvo-assets.s3.amazonaws.com *.cdn.jsdelivr.net *.bazaarvoice.com *.brsrvr.com *.cm.everesttech.net *.ads.stickyadstv.com *.tags.bluekal.com *.match.sharethrough.com *.sync.ipredictive.com *.sync.mathtag.com *.cs.openwebmp.com *.dpm.demdex.net *.curalate.com *.cdn.cookiecove.com *.brightcove.com *.brightcovecdn.com *.paypalobjects.com *.googleapis.com *.gstatic.com *.onetrust.com *.cookielaw.org *.zineone.com https://www.googletagmanager.com *.v2assets.zopim.io *.bathandbodyworkssc.zendesk.com *.pinterest.com *.pinterest.com *.omtrdc.net *.omtrdc.net *.mountain.com *.mountain.com *.script-src 'self' 'unsafe-inline' blob:storage.googleapis.com *.localhost:3000 *.code.jquery.com *.tags.tiqcdn.com *.yottaa.net *.attn.tv *.bbwi-us.attn.tv *.events.attentivemobile.com *.www.googletagmanager.com *.doubleclick.net *.cdn.quantummetric.com *.bathandbodyworks.com *.bat.bing.com *.sc-static.net *.agentbot.net *.pepperjam.com *.monetate.net *.engine-global.monetate.net *.privacymanager.io *.tealiumiq.com *.attentivemobile.com *.assets.adobedtm.com *.dotomi.com *.smaato.net *.kamptyle.com *.zineone.com *.bazaarvoice.com *.mpnsare.iesnare.com *.cookielaw.org *.brcdn.com *.cnstrc.com *.bathbodyworks-pixel.netlify.app https://www.google.com/recaptcha/ https://www.gstatic.com/recaptcha/ *.googleapis.com *.gstatic.com *.onetrust.com *.cdn-apple.com *.curalate.com *.ordergroove.com *.cdn.cookiecove.com *.brightcove.net *.brightcovecdn.com *.github.com *.objects.githubusercontent.com *.dev.zopim.com *.static.zdassets.com *.paypal.com *.privacyportal-cdn.onetrust.com *.rdf.radial.com *.tst-rdf.radial.com https://s.pinimg.com *.7316103.collect.igodigital.com https://*.yottaa.com https://*.yottaa.net https://*.px-cloud.net https://*.px-cdn.net *.pinterest.com *.byspotify.com 'unsafe-eval' https://runtime.commercecloud.com *.connect-src 'self' *.api.cquotient.com *.localhost:3000 *.dpm.demdex.net *.bbwi-us.attn.tv *.events.attentivemobile.com *.aa.bathandbodyworks.com *.tealiumiq.com *.bathandbodyworks.com *.ingest.quantummetric.com *.restapi.ordergroove.com *.bazaarvoice.com *.googleapis.com *.gstatic.com
Evidence:	

Content-Security-Policy (CSP) vulnerability on the website

"https://www.bathandbodyworks.com/" with a **medium risk level**. The parameter in question, script-src unsafe-inline, indicates that the site's security policies allow potentially unsafe inline JavaScript execution. This can expose the website to various attacks, such as cross-site scripting (XSS).

Risk Level: Medium suggests this issue is significant enough to warrant attention, but it's not immediately critical.

Parameter: The CSP header defines trusted sources for loading scripts. Unsafe inline scripts in this case are risky, as they bypass the CSP's protective measures.

Attack Type: Exploiting this vulnerability could allow attackers to inject malicious scripts.

Mitigation of this vulnerability: involves configuring the CSP header to disallow unsafe inline scripts and ensuring all scripts are served from trusted, verified sources.

CSP: script-src unsafe-eval	
URL:	https://www.bathandbodyworks.com/
Risk:	Medium
Confidence:	High
Parameter:	content-security-policy
Attack:	img-src 'self' *.commercecloud.salesforce.com *.bathandbodyworks.com data: *.yottaa.net bat.bing.com *.google.com *.tealiumiq.com *.smaato.net *.pubmatic.com *.rubiconproject.com *.doubleclick.net *.casalemedia.com *.3lift.com *.ib.adnxs.com *.ads.audio.thisisdax.com *.analytics.yahoo.com *.dotomi.com *.openx.net *.contextweb.com *.crb.kargo.com *.ap.lijt.com *.sync.live.streamtheworld.com *.sync.bfmio.com *.partners.tremorhub.com *.contextual.media.net *.ps.eyota.net *.idsync.ricdn.com *.match.adsrvr.org *.exchange-match.mediaplex.com *.sync.1rx.io *.us.ck-ie.com *.sync.targeting.unrulymedia.com *.assets-qelplatam.s3.amazonaws.com *.agentcore.s3.amazonaws.com *.alvo-assets.s3.amazonaws.com *.cdn.jsdelivr.net *.bazaarvoice.com *.brsrvr.com *.cm.everesttech.net *.ads.stickyadstv.com *.tags.bluekal.com *.match.sharethrough.com *.sync.ipredictive.com *.sync.mathtag.com *.cs.openwebmp.com *.dpm.demdex.net *.curalate.com *.cdn.cookiecove.com *.brightcove.com *.brightcovecdn.com *.paypalobjects.com *.googleapis.com *.gstatic.com *.onetrust.com *.cookielaw.org *.zineone.com https://www.googletagmanager.com *.v2assets.zopim.io *.bathandbodyworkssc.zendesk.com *.pinterest.com *.pinterest.com *.omtrdc.net *.omtrdc.net *.mountain.com *.mountain.com *.script-src 'self' 'unsafe-inline' blob:storage.googleapis.com *.localhost:3000 *.code.jquery.com *.tags.tiqcdn.com *.yottaa.net *.attn.tv *.bbwi-us.attn.tv *.events.attentivemobile.com *.www.googletagmanager.com *.doubleclick.net *.cdn.quantummetric.com *.bathandbodyworks.com *.bat.bing.com *.sc-static.net *.agentbot.net *.pepperjam.com *.monetate.net *.engine-global.monetate.net *.privacymanager.io *.tealiumiq.com *.attentivemobile.com *.assets.adobedtm.com *.dotomi.com *.smaato.net *.kamptyle.com *.zineone.com *.bazaarvoice.com *.mpnsare.iesnare.com *.cookielaw.org *.brcdn.com *.cnstrc.com *.bathbodyworks-pixel.netlify.app https://www.google.com/recaptcha/ https://www.gstatic.com/recaptcha/ *.googleapis.com *.gstatic.com *.onetrust.com *.cdn-apple.com *.curalate.com *.ordergroove.com *.cdn.cookiecove.com *.brightcove.net *.brightcovecdn.com *.github.com *.objects.githubusercontent.com *.dev.zopim.com *.static.zdassets.com *.paypal.com *.privacyportal-cdn.onetrust.com *.rdf.radial.com *.tst-rdf.radial.com https://s.pinimg.com *.7316103.collect.igodigital.com https://*.yottaa.com https://*.yottaa.net https://*.px-cloud.net https://*.px-cdn.net *.pinterest.com *.byspotify.com 'unsafe-eval' https://runtime.commercecloud.com *.connect-src 'self' *.api.cquotient.com *.localhost:3000 *.dpm.demdex.net *.bbwi-us.attn.tv *.events.attentivemobile.com *.aa.bathandbodyworks.com *.tealiumiq.com *.bathandbodyworks.com *.ingest.quantummetric.com *.restapi.ordergroove.com *.bazaarvoice.com *.googleapis.com *.gstatic.com
Evidence:	

Content Security Policy (CSP). The report flags the use of a **wildcard directive**, marking it as a medium-risk issue with high confidence.

Risk Level: Medium — While not critical, this could lead to vulnerabilities such as resource misuse or unauthorized external interactions.

Concern: The wildcard directive in the CSP could allow unintended external domains to interact

Web Security - IE2062**Year 2 Semester 2 - 2025**

with the website. This might introduce risks like data leakage or malicious scripts.

Evidence: A detailed list of external domains (e.g., Salesforce, Google, Facebook) indicates widespread reliance on third-party resources, which could be exploited if not tightly controlled.

Implications

Security Risks: Improperly configured CSPs may expose the site to potential attacks, including Cross-Site Scripting (XSS).

Mitigation: It's advisable to avoid using wildcards in CSPs and restrict allowable domains to trusted ones.

Content Security Policy (CSP) Header Not Set	
URL:	https://www.bathandbodyworks.com/sitemap.xml
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.
Other Info:	

Content Security Policy (CSP) vulnerability affecting
"https://www.bathandbodyworks.com/sitemap.xml."

Risk Level: Medium, meaning it's important but not immediately critical.

Issue: CSP header is missing, which weakens defenses against attacks like Cross Site Scripting (XSS) and data injection.

Impact: Without a CSP, malicious scripts could be injected, leading to data theft, site defacement, or malware distribution.

Recommendations

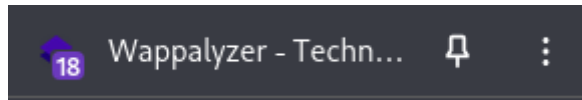
Implement a CSP Header: Ensure only trusted content sources are allowed.

Prevent Unsafe Inline Scripts: Avoid policies that permit inline JavaScript, as it bypasses security measures.























Regular Vulnerability Scanning: Continue testing for security weaknesses to catch issues proactively.

Wappalyzer

bathandbodyworks.com



Here are the results of the Wappalyzer detector

Ecommerce  Salesforce Commerce Cloud	CRM  Salesforce
Security  PerimeterX  HSTS	JavaScript libraries  lit-html 3.2.1  lit-element 4.1.1  OWL Carousel  jQuery UI 1.11.2  jQuery 2.1.1
Caching  Varnish <hr/>  Cloudflare	A/B testing  Monetate  Yottaa
Maps  Google Maps	Personalisation  Monetate
Payment processors  Apple Pay  Ordergroove	Reviews  Bazaarvoice Reviews
Tag managers  Yottaa  Tealium	Performance  Yottaa
	Customer data platform  Tealium

Web Security - IE2062**Year 2 Semester 2 - 2025**

How to mitigate the above Vulnerability

1. Update Libraries

axios: Upgrade to the latest version where vulnerabilities like SSRF, CSRF, and Proxy Authentication Bypass are patched.

bootstrap: Move to version 4.3.1 or later to address XSS vulnerabilities.

jquery: Upgrade to version 3.5.0 or later to mitigate issues like Prototype Pollution and CORS exploitation.

2. Implement Security Best Practices

Cross-Site Scripting (XSS): Sanitize and validate all user inputs.

Use Content Security Policy (CSP) headers to prevent malicious scripts from executing.

Avoid using innerHTML or similar methods for DOM manipulation.

Server-Side Request Forgery (SSRF): Restrict outgoing requests to trusted domains.

Use network-level controls like firewalls to block unauthorized requests.

Cross-Site Request Forgery (CSRF): Implement anti-CSRF tokens in forms and APIs.

Use SameSite cookies to prevent cross-origin requests.

3. Monitor and Audit

Regularly scan your application using tools like Retire.js, Nmap, or Rapidscan to identify outdated libraries and vulnerabilities.

Subscribe to security advisories for libraries you use to stay informed about new vulnerabilities.

4. Apply Patches

For libraries that are no longer maintained (e.g., older versions of jQuery), consider replacing them with actively maintained alternatives or applying custom patches if feasible.

5. Secure Configuration

Disable unnecessary features in libraries that could expose vulnerabilities.

Use secure defaults for configurations, such as enabling HTTPS and disabling insecure protocols.

Proof of report Submission



Bath & Body Works Vulnerability Disclosure Program has received **WS Assingment**

Thank you Binosh ,

We have received your Bugcrowd submission for engagement bbw-vdp-pro.

Submission Details

Submitted

04 May 2025 19:21:47 UTC

Submission ID

d0926684-e180-4b46-9b6e-242b3227b37d

VRT

Cross-Site Request Forgery (CSRF) > Action-Specific > Authenticated Action

[View Submission Details](#)