Daraz.pk-ZAP Scanning Report

Generated with ZAP on Sun 18 Dec 2022, at 16:07:58

Contents

About this report

Report parameters

Contexts

No contexts were selected, so all contexts were included by default.

Sites

The following sites were included:

- https://fonts.gstatic.com
- https://cdnjs.cloudflare.com
- https://maxcdn.bootstrapcdn.com
- https://pages.daraz.pk
- https://www.gstatic.com
- https://accounts.google.com
- https://at.alicdn.com
- https://apis.google.com
- https://dfrnc.com
- https://fonts.googleapis.com
- https://push.services.mozilla.com
- http://detectportal.firefox.com
- https://safebrowsing.googleapis.com
- https://versioncheck-bg.addons.mozilla.org
- https://services.addons.mozilla.org
- https://classify-client.services.mozilla.com
- https://normandy.cdn.mozilla.net

- https://contile.services.mozilla.com
- https://download-installer.cdn.mozilla.net
- https://download.mozilla.org
- https://umlazada.alibaba.com
- https://r3---sn-2uja-pnc6.gvt1.com
- https://www.facebook.com
- https://pixel.tapad.com
- https://redirector.gvt1.com
- https://sg-wum.alibaba.com
- https://stats.g.doubleclick.net
- https://g.alicdn.com
- https://connect.facebook.net
- https://aus5.mozilla.org
- https://analytics.google.com
- https://aswpsdkus.com
- https://daraz-by.accengage.net
- https://www.google-analytics.com
- https://my.daraz.pk
- https://tr.snapchat.com
- https://certify-js.alexametrics.com
- https://c.o-s.io
- https://aswpsdkeu.com
- https://sc-static.net
- https://itscenter.alipay.com
- https://www.googletagmanager.com
- https://dz.mmstat.com
- https://cart.daraz.pk
- https://acs-m.daraz.pk
- https://as.alipayobjects.com
- https://fourier.taobao.com
- https://time-ak.alicdn.com
- https://aeis.alicdn.com
- https://member.daraz.pk
- https://aeu.alicdn.com
- https://assets.alicdn.com
- https://laz-g-cdn.alicdn.com
- https://shavar.services.mozilla.com
- https://www.daraz.pk
- https://daraz.pk

- https://incoming.telemetry.mozilla.org
- http://daraz.pk
- https://content-signature-2.cdn.mozilla.net
- https://www.google.com
- https://firefox.settings.services.mozilla.com
- http://ocsp.pki.goog

(If no sites were selected, all sites were included by default.)

An included site must also be within one of the included contexts for its data to be included in the report.

Risk levels

Included: High, Medium, Low, Informational

Excluded: None

Confidence levels

Included: User Confirmed, High, Medium, Low

Excluded: User Confirmed, High, Medium, Low, False Positive

Summaries

Alert counts by risk and confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	5 (15.6%)	4 (12.5%)	1 (3.1%)	10 (31.2%)
	Low	0 (0.0%)	4 (12.5%)	8 (25.0%)	1 (3.1%)	13 (40.6%)
	Informational	0 (0.0%)	0 (0.0%)	4 (12.5%)	5 (15.6%)	9 (28.1%)
	Total	0 (0.0%)	9 (28.1%)	16 (50.0%)	7 (21.9%)	32 (100%)

Alert counts by site and risk

This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.

Alerts with a confidence level of "False Positive" have been excluded from these counts.

(The numbers in brackets are the number of alerts raised for the site at or above that risk level.)

		Risk			
		High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site	https://accounts.google.com	0 (0)	3 (3)	1 (4)	0 (4)

	Risk			
	High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
https://aus5.mozilla.org	0 (0)	0 (0)	0 (0)	1 (1)
https://analytics.google.com	0 (0)	1 (1)	0 (1)	0 (1)
https://tr.snapchat.com	0 (0)	0 (0)	0 (0)	1 (1)
https://sc-static.net	0 (0)	0 (0)	1 (1)	0 (1)
https://acs-m.daraz.pk	0 (0)	0 (0)	1 (1)	0 (1)
https://member.daraz.pk	0 (0)	0 (0)	1 (1)	0 (1)
https://laz-g-cdn.alicdn.com	0 (0)	2 (2)	0 (2)	1 (3)
https://www.daraz.pk	0 (0)	3 (3)	7 (10)	6 (16)
http://daraz.pk	0 (0)	0 (0)	1 (1)	0 (1)
https://content-signature-2.cdn.mozilla.net	0 (0)	0 (0)	1 (1)	0 (1)
https://firefox.settings.services.mozilla.com	0 (0)	1 (1)	0 (1)	0 (1)

Alert counts by alert type

This table shows the number of alerts of each alert type, together with the alert type's risk level.

(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

Alert type	Risk	Count
Absence of Anti-CSRF Tokens	Medium	24 (75.0%)
Application Error Disclosure	Medium	1 (3.1%)
CSP: Wildcard Directive	Medium	3 (9.4%)
CSP: script-src unsafe-inline	Medium	2 (6.2%)
CSP: style-src unsafe-inline	Medium	3 (9.4%)
Content Security Policy (CSP) Header Not Set	Medium	33 (103.1%)
Cross-Domain Misconfiguration	Medium	109 (340.6%)
Missing Anti-clickjacking Header	Medium	28 (87.5%)
Session ID in URL Rewrite	Medium	12 (37.5%)
Total		32

Alert type	Risk	Count
Vulnerable JS Library	Medium	4 (12.5%)
Big Redirect Detected (Potential Sensitive Information Leak)	Low	1 (3.1%)
CSP: Notices	Low	3 (9.4%)
Cookie No HttpOnly Flag	Low	37 (115.6%)
Cookie Without Secure Flag	Low	42 (131.2%)
Cookie with SameSite Attribute None	Low	11 (34.4%)
Cookie without SameSite Attribute	Low	45 (140.6%)
Cross-Domain JavaScript Source File Inclusion	Low	139 (434.4%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	10 (31.2%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	34 (106.2%)
Strict-Transport-Security Header Not Set	Low	168 (525.0%)
Strict-Transport-Security Multiple Header Entries (Non-compliant with Spec)	Low	18 (56.2%)
Total		32

Alert type	Risk	Count
Timestamp Disclosure - Unix	Low	233 (728.1%)
X-Content-Type-Options Header Missing	Low	180 (562.5%)
Charset Mismatch	Informational	3 (9.4%)
Content-Type Header Missing	Informational	2 (6.2%)
Cookie Poisoning	Informational	1 (3.1%)
Information Disclosure - Sensitive Information in URL	Informational	24 (75.0%)
Information Disclosure - Suspicious Comments	Informational	177 (553.1%)
Loosely Scoped Cookie	Informational	58 (181.2%)
Modern Web Application	Informational	43 (134.4%)
Re-examine Cache-control Directives	Informational	105 (328.1%)
Retrieved from Cache	Informational	65 (203.1%)
Total		32

Alerts

Risk=Medium, Confidence=High (5)

https://accounts.google.com (3)

CSP: Wildcard Directive (1)

▶ GET https://accounts.google.com/o/oauth2/iframe

CSP: script-src unsafe-inline (1)

▶ GET https://accounts.google.com/o/oauth2/iframe

CSP: style-src unsafe-inline (1)

▶ GET https://accounts.google.com/o/oauth2/iframe

https://analytics.google.com (1)

Session ID in URL Rewrite (1)

▶ POST https://analytics.google.com/g/collect?v=2&tid=G-5L4FRV3KPW&gtm=2oebu0&_p=1987612587&_gaz=1&cid=1373456046.1670931013&ul=en-us&sr=1366x768&_s=1&sid=1670931014&sct=1&seg=0&dl=https%3A%2F%2Fwww.daraz.pk%2F&dt=Online%20Shopping%20in%20Pakistan%3A%20Fashion%2C%20Electronics%20%26%20Books%20-%20Daraz.pk&en=page_view&_fv=1&_ss=1

https://www.daraz.pk (1)

Content Security Policy (CSP) Header Not Set (1)

▶ GET https://www.daraz.pk/

Risk=Medium, Confidence=Medium (4)

https://laz-g-cdn.alicdn.com (2)

Application Error Disclosure (1)

▶ GET https://laz-g-cdn.alicdn.com/lzdmod/im/5.0.86/index.js

Vulnerable JS Library (1)

▶ GET https://laz-g-cdn.alicdn.com/??lzdpage/homepage-daraz/5.3.84/components/countdown/pc/index.js,mui/countdown/5.0.2/index.js,lzdmod/desktop-footer-daraz/5.2.49/pc/index.js,lzdmod/jquery/5.0.9/index.js,lzdmod/desktop-footer-daraz/5.2.49/pc/reqwest/index.js,lzdmod/site-nav-pc-daraz/5.4.28/pc/index.js,lzdmod/site-nav-pc-daraz/5.4.28/assets/links-bar/index.js,lzdmod/site-nav-pc-daraz/5.4.28/assets/reqwest/index.js,lzdmod/site-nav-pc-daraz/5.4.28/assets/common/popper/index.js,lzdmod/site-nav-pc-daraz/5.4.28/assets/cart/index.js,lzdmod/site-nav-pc-daraz/5.4.28/assets/download-app/index.js,lzdmod/site-nav-pc-daraz/5.4.28/i18n.js,lzdmod/site-nav-pc-daraz/5.4.28/assets/track-order/index.js,lzdmod/site-nav-pc-daraz/5.4.28/assets/switch-lang/index.js,lzdmod/site-nav-pc-daraz/5.4.28/assets/user-info/index.js,lzdmod/site-nav-pc-daraz/5.4.28/assets/affiliate/index.js,lzdmod/site-nav-pc-daraz/5.4.28/assets/logo-bar/index.js,lzdmod/site-nav-pc-daraz/5.4.28/assets/search-box/index.js,lzdmod/site-nav-pc-daraz/5.4.28/assets/liveup/index.js

https://www.daraz.pk (1)

Missing Anti-clickjacking Header (1)

▶ GET https://www.daraz.pk/

https://firefox.settings.services.mozilla.com (1)

Cross-Domain Misconfiguration (1)

▶ GET https://firefox.settings.services.mozilla.com/v1/buckets/monitor/collections/changes/changeset?_expected=%221670921834943%22

Risk=Medium, Confidence=Low (1)

https://www.daraz.pk (1)

Absence of Anti-CSRF Tokens (1)

▶ GET https://www.daraz.pk/

Risk=Low, Confidence=High (4)

https://accounts.google.com (1)

CSP: Notices (1)

▶ GET https://accounts.google.com/o/oauth2/iframe

https://member.daraz.pk (1)

Strict-Transport-Security Multiple Header Entries (Non-compliant with Spec) (1)

▶ GET https://member.daraz.pk/user/api/getContextInfo

https://www.daraz.pk (1)

Strict-Transport-Security Header Not Set (1)

▶ GET https://www.daraz.pk/customer/

https://content-signature-2.cdn.mozilla.net (1)

Server Leaks Version Information via "Server" HTTP Response Header Field (1)

▶ GET https://content-signature-2.cdn.mozilla.net/chains/remote-settings.content-signature.mozilla.org-2023-01-19-10-06-33.chain

Risk=Low, Confidence=Medium (8)

https://sc-static.net (1)

Cookie with SameSite Attribute None (1)

▶ GET https://sc-static.net/scevent.min.js

https://acs-m.daraz.pk (1)

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (1)

▶ POST https://acs-m.daraz.pk/h5/mtop.alibaba.global.holmes.customevent.upload/1.0/?

jsv=2.4.11&appKey=30133426&t=1670931000675&sign=552637ef661714b43
3454464259beec9&api=mtop.alibaba.global.holmes.customEvent.upload
&v=1.0&type=originaljson&isSec=1&AntiCreep=true&timeout=20000&nee
dLogin=true&dataType=json&sessionOption=AutoLoginOnly&x-i18n-
language=en-PK&x-i18n-regionID=PK

https://www.daraz.pk (5)

Cookie No HttpOnly Flag (1)

▶ GET https://www.daraz.pk/shop/*.htm

Cookie Without Secure Flag (1)

▶ GET https://www.daraz.pk/shop/*.htm

Cookie without SameSite Attribute (1)

▶ GET https://www.daraz.pk/shop/*.htm

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://www.daraz.pk/

X-Content-Type-Options Header Missing (1)

▶ GET https://www.daraz.pk/robots.txt

http://daraz.pk (1)

Big Redirect Detected (Potential Sensitive Information Leak) (1)

▶ GET http://daraz.pk/

Risk=Low, Confidence=Low (1)

https://www.daraz.pk (1)

Timestamp Disclosure - Unix (1)

▶ GET https://www.daraz.pk/

Risk=Informational, Confidence=Medium (4)

https://laz-g-cdn.alicdn.com (1)

Information Disclosure - Sensitive Information in URL (1)

▶ GET https://laz-g-cdn.alicdn.com/??lzdpage/homepage-daraz/5.3.84/components/countdown/pc/index.js,mui/countdown/5.0.2/index.js,lzdmod/desktop-footer-daraz/5.2.49/pc/index.js,lzdmod/jquery/5.0.9/index.js,lzdmod/desktop-footer-daraz/5.2.49/pc/reqwest/index.js,lzdmod/site-nav-pc-daraz/5.4.28/pc/index.js,lzdmod/site-nav-pc-daraz/5.4.28/assets/links-bar/index.js,lzdmod/site-nav-pc-daraz/5.4.28/assets/reqwest/index.js,lzdmod/site-nav-pc-daraz/5.4.28/assets/common/popper/index.js,lzdmod/site-nav-pc-daraz/5.4.28/assets/cart/index.js,lzdmod/site-nav-pc-daraz/5.4.28/assets/download-app/index.js,lzdmod/site-nav-pc-daraz/5.4.28/i18n.js,lzdmod/site-nav-pc-daraz/5.4.28/assets/track-order/index.js,lzdmod/site-nav-pc-daraz/5.4.28/assets/switch-lang/index.js,lzdmod/site-nav-pc-daraz/5.4.28/assets/user-info/index.js,lzdmod/site-nav-pc-daraz/5.4.28/assets/affiliate/index.js,lzdmod/site-nav-pc-daraz/5.4.28/assets/logo-bar/index.js,lzdmod/site-nav-pc-daraz/5.4.28/assets/search-box/index.js,lzdmod/site-nav-pc-daraz/5.4.28/assets/liveup/index.js

https://www.daraz.pk (3)

Content-Type Header Missing (1)

▶ GET https://www.daraz.pk/robots.txt

Modern Web Application (1)

▶ GET https://www.daraz.pk/

Retrieved from Cache (1)

▶ GET https://www.daraz.pk/

Risk=Informational, Confidence=Low (5)

https://aus5.mozilla.org (1)

Charset Mismatch (1)

▶ GET https://aus5.mozilla.org/update/3/GMP/106.0.5/20221104133228/WINNT_x86_64-msvc-x64/en-US/release/Windows_NT%2010.0.0.0.19044.2251%20(x64)/default/default/update.xml

https://tr.snapchat.com (1)

Cookie Poisoning (1)

▶ POST https://tr.snapchat.com/p

https://www.daraz.pk (3)

Information Disclosure - Suspicious Comments (1)

▶ GET https://www.daraz.pk/

Loosely Scoped Cookie (1)

▶ GET https://www.daraz.pk/shop/*.htm

Re-examine Cache-control Directives (1)

▶ GET https://www.daraz.pk/sitemap.xml

Appendix

Alert types

This section contains additional information on the types of alerts in the report.

Absence of Anti-CSRF Tokens

Source	raised by a passive scanner (Absence of Anti-CSRF Tokens)
CWE ID	352
WASC ID	9
Reference	▪ http://projects.webappsec.org/Cross-Site-Request-Forgery ▪ http://cwe.mitre.org/data/definitions/352.html

Application Error Disclosure

Source	raised by a passive scanner (Application Error Disclosure)
CWE ID	200
WASC ID	13

CSP: Wildcard Directive

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	▪ http://www.w3.org/TR/CSP2/ ▪ http://www.w3.org/TR/CSP/ ▪ http://caniuse.com/#search=content+security+policy ▪ http://content-security-policy.com/ ▪ https://github.com/shapesecurity/salvation ▪ https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

CSP: script-src unsafe-inline

Source	raised by a passive scanner (CSP)

CWE ID	693
WASC ID	15
Reference	▪ http://www.w3.org/TR/CSP2/ ▪ http://www.w3.org/TR/CSP/ ▪ http://caniuse.com/#search=content+security+policy ▪ http://content-security-policy.com/ ▪ https://github.com/shapesecurity/salvation ▪ https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

CSP: style-src unsafe-inline

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	▪ http://www.w3.org/TR/CSP2/ ▪ http://www.w3.org/TR/CSP/ ▪ http://caniuse.com/#search=content+security+policy ▪ http://content-security-policy.com/

- https://github.com/shapesecurity/salvation
- https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

Content Security Policy (CSP) Header Not Set

Source	raised by a passive scanner (Content Security Policy (CSP) Header Not Set)
CWE ID	693
WASC ID	15
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html http://www.w3.org/TR/CSP/ http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html http://www.html5rocks.com/en/tutorials/security/content-security-policy/ http://caniuse.com/#feat=contentsecuritypolicy http://content-security-policy.com/

Cross-Domain Misconfiguration

Source	raised by a passive scanner (Cross-Domain Misconfiguration)
CWE ID	264
WASC ID	14
Reference	• https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Missing Anti-clickjacking Header

Source	raised by a passive scanner (Anti-clickjacking Header)
CWE ID	1021
WASC ID	15
Reference	• https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

Session ID in URL Rewrite

Source	raised by a passive scanner (Session ID in URL Rewrite)
CWE ID	200
WASC ID	13
Reference	• http://seclists.org/lists/webappsec/2002/Oct-Dec/0111.html

Vulnerable JS Library

Source raised by a passive scanner (Vulnerable JS Library (Powered by Retire.js))

CWE ID 829

Reference

- https://github.com/jquery/jquery/issues/2432
- http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/
- http://research.insecurelabs.org/jquery/test/
- https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/
- https://nvd.nist.gov/vuln/detail/CVE-2019-11358
- https://nvd.nist.gov/vuln/detail/CVE-2015-9251
- https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b
- https://bugs.jquery.com/ticket/11974
- https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/

Big Redirect Detected (Potential Sensitive Information Leak)

Source raised by a passive scanner (Big Redirect Detected (Potential Sensitive Information Leak))

CWE ID 201

WASC ID 13

CSP: Notices

Source raised by a passive scanner (CSP)

CWE ID 693

WASC ID 15

Reference

- http://www.w3.org/TR/CSP2/
- http://www.w3.org/TR/CSP/
- http://caniuse.com/#search=content+security+policy
- http://content-security-policy.com/
- https://github.com/shapesecurity/salvation
- https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

Cookie No HttpOnly Flag

Source raised by a passive scanner (Cookie No HttpOnly Flag)

CWE ID 1004

WASC ID 13

Reference

- https://owasp.org/www-community/HttpOnly

Cookie Without Secure Flag

Source	raised by a passive scanner (Cookie Without Secure Flag)
CWE ID	614
WASC ID	13
Reference	▪ https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html

Cookie with SameSite Attribute None

Source	raised by a passive scanner (Cookie without SameSite Attribute)
CWE ID	1275
WASC ID	13
Reference	▪ https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site

Cookie without SameSite Attribute

Source	raised by a passive scanner (Cookie without SameSite Attribute)
CWE ID	1275
WASC ID	13
Reference	▪ https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site

Cross-Domain JavaScript Source File Inclusion

Source	raised by a passive scanner (Cross-Domain JavaScript Source File Inclusion)
CWE ID	829
WASC ID	15

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Source	raised by a passive scanner (Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s))
CWE ID	200
WASC ID	13
Reference	▪ http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx ▪ http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

Server Leaks Version Information via "Server" HTTP Response Header Field

Source	raised by a passive scanner (HTTP Server Response Header)
CWE ID	200
WASC ID	13

Reference

- http://httpd.apache.org/docs/current/mod/core.html#servertokens
- http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007
- http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
- http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

Strict-Transport-Security Header Not Set

Source raised by a passive scanner (Strict-Transport-Security Header)

CWE ID 319

WASC ID 15

Reference

- https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
- https://owasp.org/www-community/Security_Headers
- http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
- http://caniuse.com/stricttransportsecurity
- http://tools.ietf.org/html/rfc6797

Strict-Transport-Security Multiple Header Entries (Non-compliant with Spec)

Source	raised by a passive scanner (Strict-Transport-Security Header)
CWE ID	319
WASC ID	15
Reference	▪ http://tools.ietf.org/html/rfc6797#section-8.1

Timestamp Disclosure - Unix

Source	raised by a passive scanner (Timestamp Disclosure)
CWE ID	200
WASC ID	13
Reference	▪ http://projects.webappsec.org/w/page/13246936/Information%20Leakage

X-Content-Type-Options Header Missing

Source	raised by a passive scanner (X-Content-Type-Options Header Missing)
CWE ID	693
WASC ID	15
Reference	▪ http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx

- https://owasp.org/www-community/Security_Headers

Charset Mismatch

Source	raised by a passive scanner (Charset Mismatch)
CWE ID	436
WASC ID	15
Reference	- http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection

Content-Type Header Missing

Source	raised by a passive scanner (Content-Type Header Missing)
CWE ID	345
WASC ID	12
Reference	- http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx

Cookie Poisoning

Source	raised by a passive scanner (Cookie Poisoning)
CWE ID	20
WASC ID	20
Reference	- http://websecuritytool.codeplex.com/wikipage?

title=Checks#user-controlled-cookie

Information Disclosure - Sensitive Information in URL

Source	raised by a passive scanner (Information Disclosure - Sensitive Information in URL)
CWE ID	200
WASC ID	13

Information Disclosure - Suspicious Comments

Source	raised by a passive scanner (Information Disclosure - Suspicious Comments)
CWE ID	200
WASC ID	13

Loosely Scoped Cookie

Source	raised by a passive scanner (Loosely Scoped Cookie)
CWE ID	565
WASC ID	15
Reference	▪ https://tools.ietf.org/html/rfc6265#section-4.1 ▪ https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html

- http://code.google.com/p/browsersec/wiki/Part2#Same-origin_policy_for_cookies

Modern Web Application

Source raised by a passive scanner (Modern Web Application)

Re-examine Cache-control Directives

Source raised by a passive scanner (Re-examine Cache-control Directives)

CWE ID 525

WASC ID 13

Reference

- https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control
- https://grayduck.mn/2021/09/13/cache-control-recommendations/

Retrieved from Cache

Source raised by a passive scanner (Retrieved from Cache)

Reference

- https://tools.ietf.org/html/rfc7234
- https://tools.ietf.org/html/rfc7231

- http://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html (obsoleted by rfc7234)