HomeShopping.pk-Scan-Report

Generated with ZAP on Tue 20 Dec 2022, at 17:00:04

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://tpc.googlesyndication.com
- https://socialplugin.facebook.net
- https://static.xx.fbcdn.net
- https://www.google.com
- https://www.googletagservices.com
- https://fonts.googleapis.com
- https://adservice.google.com
- https://partner.googleadservices.com
- https://adservice.google.com.pk
- https://t.sharethis.com
- https://www.facebook.com
- https://buttons-config.sharethis.com
- https://l.sharethis.com

- https://api-v3.findify.io
- https://stats.g.doubleclick.net
- https://pagead2.googlesyndication.com
- https://cdn.cloudkibo.com
- https://googleads.g.doubleclick.net
- https://platform-api.sharethis.com
- https://connect.facebook.net
- https://checkout.foree.co
- https://www.google-analytics.com
- https://mcbpk.gateway.mastercard.com
- https://bid.g.doubleclick.net
- https://www.googleadservices.com
- https://assets.findify.io
- https://cdn.checkout.com
- https://static.cloudflareinsights.com
- https://findify-assets-2bveeb6u8ag.netdna-ssl.com
- https://www.googletagmanager.com
- https://homeshopping.pk

(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%)	1 (3.2%)	0 (0.0%)	0 (0.0%)	1 (3.2%)
	Medium	0 (0.0%)	4 (12.9%)	3 (9.7%)	1 (3.2%)	8 (25.8%)
	Low	0 (0.0%)	4 (12.9%)	8 (25.8%)	1 (3.2%)	13 (41.9%)
	Informational	0 (0.0%)	1 (3.2%)	3 (9.7%)	5 (16.1%)	9 (29.0%)
	Total	0 (0.0%)	10 (32.3%)	14 (45.2%)	7 (22.6%)	31 (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://static.xx.fbcdn.net	1 (1)	0 (1)	0 (1)	0 (1)
	https://www.facebook.com	0 (0)	1 (1)	0 (1)	2 (3)
	https://l.sharethis.com	0 (0)	0 (0)	0 (0)	1 (1)
	https://cdn.cloudkibo.com	0 (0)	2 (2)	1 (3)	0 (3)
	https://googleads.g.doubleclick.net	0 (0)	0 (0)	0 (0)	1 (1)
	https://checkout.foree.co	0 (0)	0 (0)	1 (1)	0 (1)
	https://mcbpk.gateway.mastercard.com	0 (0)	1 (1)	0 (1)	1 (2)
	https://bid.g.doubleclick.net	0 (0)	0 (0)	1 (1)	1 (2)
	https://static.cloudflareinsights.com	0 (0)	0 (0)	1 (1)	0 (1)
	https://findify-assets-2bveeb6u8ag.netdna-ssl.com	0 (0)	0 (0)	1 (1)	2 (3)

	Risk			
	High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
https://www.googletagmanager.com	0 (0)	1 (1)	1 (2)	1 (3)
https://homeshopping.pk	0 (0)	3 (3)	7 (10)	0 (10)

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
PII Disclosure	High	46 (148.4%)
Absence of Anti-CSRF Tokens	Medium	11538 (37,219.4%)
CSP: Wildcard Directive	Medium	19 (61.3%)
CSP: script-src unsafe-inline	Medium	17 (54.8%)
CSP: style-src unsafe-inline	Medium	19 (61.3%)
Total		31

Alert type	Risk	Count
Content Security Policy (CSP) Header Not Set	Medium	3669 (11,835.5%)
Cross-Domain Misconfiguration	Medium	17 (54.8%)
Missing Anti-clickjacking Header	Medium	3616 (11,664.5%)
Vulnerable JS Library	Medium	4 (12.9%)
Application Error Disclosure	Low	1 (3.2%)
CSP: Notices	Low	3 (9.7%)
Cookie No HttpOnly Flag	Low	3655 (11,790.3%)
Cookie Without Secure Flag	Low	3650 (11,774.2%)
Cookie with SameSite Attribute None	Low	12 (38.7%)
Cookie without SameSite Attribute	Low	3650 (11,774.2%)
Cross-Domain JavaScript Source File Inclusion	Low	26480 (85,419.4%)
Secure Pages Include Mixed Content	Low	54 (174.2%)
Total		31

Alert type	Risk	Count
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	10 (32.3%)
Strict-Transport-Security Header Not Set	Low	4015 (12,951.6%)
Strict-Transport-Security Multiple Header Entries (Non-compliant with Spec)	Low	4 (12.9%)
Timestamp Disclosure - Unix	Low	4222 (13,619.4%)
X-Content-Type-Options Header Missing	Low	3928 (12,671.0%)
Content Security Policy (CSP) Report-Only Header Found	Informational	15 (48.4%)
Cookie Poisoning	Informational	3 (9.7%)
Information Disclosure - Sensitive Information in URL	Informational	7 (22.6%)
Information Disclosure - Suspicious Comments	Informational	10911 (35,196.8%)
Loosely Scoped Cookie	Informational	10 (32.3%)
Modern Web Application	Informational	3681 (11,874.2%)
Re-examine Cache-control Directives	Informational	10 (32.3%)
Total		31

Alert type	Risk	Count
Retrieved from Cache	Informational	19 (61.3%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	3512 (11,329.0%)
Total		31

Alerts

Risk=High, Confidence=High (1)

https://static.xx.fbcdn.net (1)

PII Disclosure (1)

▶ GET https://static.xx.fbcdn.net/rsrc.php/v3iv4Y4/y7/l/en_US/o8i0l9QxLN6.js?_nc_x=Ij3Wp8lg5Kz

Risk=Medium, Confidence=High (4)

https://www.facebook.com (1)

CSP: script-src unsafe-inline (1)

▶ GET https://www.facebook.com/v8.0/plugins/like.php?app_id=&channel=https%3A%2F%2Fstaticxx.facebook.com%2Fx%2Fconnect%2Fxd_arbiter%2F%3Fversion%3D46%23cb%3Df27bcccba8d0ed%26domain%3Dhomeshopping.pk%26is_canvas%3Dfalse%26origin%3Dhttps%253A%252F%252Fhomeshopping.pk%252Ff138879769b9912%26relation%3Dparent.parent&

container_width=0&href=https%3A%2F%2Fhomeshopping.pk%2F&locale=en_US&sdk=joey&share=true&show_faces=true&width=450

https://cdn.cloudkibo.com (2)

CSP: Wildcard Directive (1)

▶ GET https://cdn.cloudkibo.com/public/scripts/widgetAppSrc.js

CSP: style-src unsafe-inline (1)

▶ GET https://cdn.cloudkibo.com/public/scripts/widgetAppSrc.js

https://homeshopping.pk (1)

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

▶ GET https://homeshopping.pk/

Risk=Medium, Confidence=Medium (3)

https://mcbpk.gateway.mastercard.com (1)

Vulnerable JS Library (1)

▶ GET https://mcbpk.gateway.mastercard.com/checkout/public/wro/libs.js?cache=-66d9b23c4995117ea897c44d8dd7c40a

https://www.googletagmanager.com (1)

Cross-Domain Misconfiguration (1)

▶ GET https://www.googletagmanager.com/gtag/js?id=UA-45588538-1

https://homeshopping.pk (1)

Missing Anti-clickjacking Header (1)

▶ GET https://homeshopping.pk/

Risk=Medium, Confidence=Low (1)

https://homeshopping.pk (1)

Absence of Anti-CSRF Tokens (1)

▶ GET https://homeshopping.pk/

Risk=Low, Confidence=High (4)

https://cdn.cloudkibo.com (1)

CSP: Notices (1)

▶ GET https://cdn.cloudkibo.com/public/scripts/widgetAppSrc.js

https://checkout.foree.co (1)

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

▶ GET https://checkout.foree.co/assets/js/crypto/cryptoLibrary.js?version=1671526488550

https://static.cloudflareinsights.com (1)

Strict-Transport-Security Header Not Set (1)

▶ GET https://static.cloudflareinsights.com/beacon.min.js/vaafb692b2aea4879b33c060e79fe94621666317369993

https://findify-assets-2bveeb6u8ag.netdna-ssl.com (1)

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

▶ GET https://findify-assets-2bveeb6u8ag.netdna-ssl.com/search/prod/homeshopping.pk.min.js

Risk=Low, Confidence=Medium (8)

https://bid.g.doubleclick.net (1)

Cookie with SameSite Attribute None (1)

▶ GET https://bid.g.doubleclick.net/xbbe/pixel?d=KAE

https://www.googletagmanager.com (1)

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

▶ GET https://www.googletagmanager.com/gtag/js?id=UA-45588538-1

https://homeshopping.pk (6)

Application Error Disclosure (1)

▶ GET https://homeshopping.pk/blog/

Cookie No HttpOnly Flag (1)

▶ GET https://homeshopping.pk/

Cookie Without Secure Flag (1)

▶ GET https://homeshopping.pk/

Cookie without SameSite Attribute (1)

▶ GET https://homeshopping.pk/

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://homeshopping.pk/

Secure Pages Include Mixed Content (1)

▶ GET https://homeshopping.pk/categories/Generator-Price-in-Pakistan/

Risk=Low, Confidence=Low (1)

https://homeshopping.pk (1)

Timestamp Disclosure - Unix (1)

▶ GET https://homeshopping.pk/

Risk=Informational, Confidence=High (1)

https://www.facebook.com (1)

Content Security Policy (CSP) Report-Only Header Found (1)

▶ GET https://www.facebook.com/v8.0/plugins/like.php?app_id=&channel=https%3A%2F%2Fstaticxx.facebook.com%2Fx%2Fconnect%2Fxd_arbiter%2F%3Fversion%3D46%23cb%3Df27bcccba8d0ed%26domain%3Dhomeshopping.pk%26is_canvas%3Dfalse%26origin%3Dhttps%253A%252F%252Fhomeshopping.pk%252Ff138879769b9912%26relation%3Dparent.parent&container_width=0&href=https%3A%2F%2Fhomeshopping.pk%2F&locale=en_US&sdk=joey&share=true&show_faces=true&width=450

Risk=Informational, Confidence=Medium (3)

https://www.facebook.com (1)

Information Disclosure - Sensitive Information in URL (1)

▶ GET https://www.facebook.com/tr/?id=4162797060459573&ev=PageView&dl=https%3A%2F%2Fhomeshopping.pk%2F&rl=&if=false&ts=1671526501671&sw=1280&sh=720&v=2.9.90&r=stable&ec=0&o=30&fbp=fb.1.1671379221081.141113476&it=1671526494577&coo=false&rqm=GET

https://findify-assets-2bveeb6u8ag.netdna-ssl.com (2)

Modern Web Application (1)

▶ GET https://findify-assets-2bveeb6u8ag.netdna-ssl.com/search/prod/homeshopping.pk.min.js

Retrieved from Cache (1)

▶ GET https://findify-assets-2bveeb6u8ag.netdna-ssl.com/search/prod/homeshopping.pk.min.js

Risk=Informational, Confidence=Low (5)

https://l.sharethis.com (1)

Cookie Poisoning (1)

▶ GET https://l.sharethis.com/sc?event=pview&hostname=homeshopping.pk&location=%2F&product=inline-share-buttons&url=https%3A%2F%2Fhomeshopping.pk%2F&source=sharethis.js&fcmp=false&fcmpv2=false&has_segmentio=false&title=Online%20Shopping%20In%20Pakistan%20-%20Home%20Shopping&cms=sop&publisher=5e70738636e4ca00125482b3&embeds_csv=https%3A%2F%2Fzap%2F%2FzapCallBackUrl%2F4283279442250179713%2Ffile%2Fmanagement.html%3Furl%3Dhttps%3A%2F%2Fhomeshopping.pk%2F%26frameId%3Dmanagement%26tabId%3D6483018-304%2Chttps%3A%2F%2Fzap%2F%2FzapCallBackUrl%2F4283279442250179713%2Ffile%2Fpanel.html%3Furl%3Dhttps%3A%2F%2Fhomeshopping.pk%2F%26orientation%3Dleft%26frameId%3DleftPanel%26tabId%3D6483018-304%2Chttps%3A%2F%2Fzap%2F%2FzapCallBackUrl%2F4283279442250179713%2Ffile%2Fpanel.html%3Furl%3Dhttps%3A%2F%2Fhomeshopping.pk%2F%26orientation%3Dright%26frameId%3DrightPanel%26tabId%3D6483018-304%2Chttps%3A%2F%2Fzap%2F%2FzapCallBackUrl%2F4283279442250179713%2Ffile%2Fdrawer.html%3Furl%3Dhttps%3A%2F%2Fhomeshopping.pk%2F%26frameId%3Ddrawer%26tabId%3D6483018-304%2Chttps%3A%2F%2Fzap%2F%2FzapCallBackUrl%2F4283279442250179713%2Ffile%2Fdisplay.html%3Furl%3Dhttps%3A%2F%2Fhomeshopping.pk%2F%26frameId%3Ddisplay%26tabId%3D6483018-304%2Chttps%3A%2F%2Fzap%2F%2FzapCallBackUrl%2F4283279442250179713%2Ffile%2FgrowlerAlerts.html%3Furl%3Dhttps%3A%2F%2Fhomeshopping.pk%2F%26frameId%3DgrowlerAlerts%26tabId%3D6483018-304%2Chttps%3A%2F%2Fbid.g.doubleclick.net%2Fxbbe%2Fpixel%3Fd%3DKA

E%2Chttps%3A%2F%2Fmcbpk.gateway.mastercard.com%2Fcheckout%2FhostedCheckout&sop=true&version=st_sop.js&lang=en&fpestid=gGXtL6cwscJugnvoVzm00p7pb6HCJ0p_uUDD6mY4Vr538GxuOy_wEowU1ldlPTRPKMqecA&description=The%20Largest%20Store%20For%20Online%20Shopping%20In%20Pakistan%20To%20Provide%20Thousands%20Of%20Products%20At%20One%20Stop%20Like%20Mobiles%2C%20Cameras%2C%20Fashion%2C%20Computers%20And%20More.&samesite=None

https://googleads.g.doubleclick.net (1)

User Controllable HTML Element Attribute (Potential XSS) (1)

▶ GET https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-1493908824641892&output=html&adk=1812271804&adf=3025194257&lmt=1671526505&plat=1%3A1024%2C2%3A16778240%2C3%3A2097152%2C4%3A2097152%2C9%3A32776%2C16%3A8388608%2C17%3A32%2C24%3A32%2C25%3A32%2C30%3A1081344%2C32%3A32%2C41%3A32&format=0x0&url=https%3A%2F%2Fhomeshopping.pk%2F&ea=0&pra=5&wgl=1&dt=1671526497090&bpp=16&bdt=16121&idt=6596&shv=r20221207&mjsv=m202212010101&ptt=9&saldr=aa&abxe=1&cookie=ID%3D11d975a0055779c8-2267e95ae0d7006a%3AT%3D1671379229%3ART%3D1671379229%3AS%3DALNI_MYk9J54VTGud0QBYxtov7E6pEOL3w&gpic=UID%3D00000baec65a5bbc%3AT%3D1671379229%3ART%3D1671526503%3AS%3DALNI_MZad-2d_WZ6a7uKzgEEguLRnQWKLA&nras=1&correlator=5678276958597&frm=20&pv=2&ga_vid=1318397310.1671379218&ga_sid=1671526505&ga_hid=1937267572&ga_fc=1&u_tz=300&u_his=2&u_h=720&u_w=1280&u_ah=680&u_aw=1280&u_cd=24&u_sd=2&adx=-12245933&ady=-12245933&biw=1263&bih=578&scr_x=0&scr_y=0&eid=44759875%2C44759926%2C44759837%2C44774648%2C44774652%2C44780792%2C44769661&oid=2&pvsid=2700466277832714&tmod=1479280860&nvt=1&eae=2&fc=1920&brdim=-7%2C-7%2C-7%2C-7%2C1280%2C0%2C1293%2C693%2C1280%2C595&vis=2&rsz=%7C%7Cs%7C&abl=NS&fu=33792&bc=31&ifi=1&uci=a!1&fsb=1&dtd=8285

https://mcbpk.gateway.mastercard.com (1)

Re-examine Cache-control Directives (1)

▶ GET
https://mcbpk.gateway.mastercard.com/checkout/hostedCheckout

https://bid.g.doubleclick.net (1)

Loosely Scoped Cookie (1)

▶ GET https://bid.g.doubleclick.net/xbbe/pixel?d=KAE

https://www.googletagmanager.com (1)

Information Disclosure - Suspicious Comments (1)

▶ GET https://www.googletagmanager.com/gtag/js?id=UA-45588538-1

Appendix

Alert types

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

PII Disclosure

Source	raised by a passive scanner (PII Disclosure)
CWE ID	359
WASC ID	13

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

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+p

olicy

- 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

Vulnerable JS Library

Source	raised by a passive scanner (Vulnerable JS Library (Powered by Retire.js))
CWE ID	829

Reference	▪ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ ▪ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 ▪ https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b ▪ https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/

Application Error Disclosure

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

Secure Pages Include Mixed Content

Source	raised by a passive scanner (Secure Pages Include Mixed Content)

CWE ID	311
WASC ID	4
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.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

Content Security Policy (CSP) Report-Only Header Found

Source raised by a passive scanner (Content Security Policy (CSP) Header Not Set)

CWE ID 693

WASC ID 15

Reference
- https://www.w3.org/TR/CSP2/
- https://w3c.github.io/webappsec-csp/
- http://caniuse.com/#feat=contentsecuritypolicy
- http://content-security-policy.com/

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)

User Controllable HTML Element Attribute (Potential XSS)

Source raised by a passive scanner (User Controllable HTML Element Attribute (Potential XSS))

CWE ID 20

WASC ID 20

Reference
- http://websecuritytool.codeplex.com/wikipage?title=Checks#user-controlled-html-attribute