

TourRadar ZAP Scanning Report

Generated with  ZAP on Thu 16 Mar 2023, at 09:29:40

Contents

- [About this report](#)
 - [Report parameters](#)
- [Summaries](#)
 - [Alert counts by risk and confidence](#)
 - [Alert counts by site and risk](#)
 - [Alert counts by alert type](#)
- [Alerts](#)
 - [Risk=High, Confidence=Medium \(1\)](#)
 - [Risk=Medium, Confidence=High \(5\)](#)
 - [Risk=Medium, Confidence=Medium \(2\)](#)
 - [Risk=Low, Confidence=High \(3\)](#)
 - [Risk=Low, Confidence=Medium \(6\)](#)
 - [Risk=Low, Confidence=Low \(1\)](#)
 - [Risk=Informational, Confidence=High \(1\)](#)

- Risk=Informational, Confidence=Medium (3).
- Risk=Informational, Confidence=Low (5).
- Appendix
 - Alert types

About this report

Report parameters

Contexts

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

Sites

The following sites were included:

- https://aus5.mozilla.org
- https://firefox-settings-attachments.cdn.mozilla.net
- https://csm.fr.eu.criteo.net
- https://x.bidswitch.net
- https://exchange.mediavine.com
- https://ad.360yield.com
- https://ad.yieldlab.net
- https://simage2.pubmatic.com
- https://secure.adnxs.com
- https://ups.analytics.yahoo.com
- https://visitor.omnitagjs.com
- https://criteo-sync.teads.tv
- https://cm.g.doubleclick.net
- https://rtb-csync.smartadserver.com
- https://a.twiago.com
- https://matching.ivitrack.com
- https://sslwidget.criteo.com
- https://ag.gbc.criteo.com
- https://gem.gbc.criteo.com

- <https://www.gstatic.com>
- <https://www.facebook.com>
- <https://in.hotjar.com>
- <https://dnacdn.net>
- <https://accounts.google.com>
- <https://script.hotjar.com>
- <https://gum.criteo.com>
- <https://connect.facebook.net>
- <https://static.criteo.net>
- <https://static.hotjar.com>
- <https://apis.google.com>
- <https://storage.googleapis.com>
- <https://www.google.com>
- <https://stats.g.doubleclick.net>
- <https://www.google.at>
- <https://region1.analytics.google.com>
- <https://omnimize.tourradar.com>
- <https://csp.tourradar.com>
- <https://www.google-analytics.com>
- <https://cdn.tourradar.com>
- <https://www.googletagmanager.com>
- <https://tracking-protection.cdn.mozilla.net>
- <https://www.tourradar.com>
- <https://shavar.services.mozilla.com>
- <https://content-signature-2.cdn.mozilla.net>
- <https://firefox.settings.services.mozilla.com>
- <https://location.services.mozilla.com>

(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

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				
Risk		User Confirmed	High	Medium	Low	Total
	High	0 (0.0%)	0 (0.0%)	1 (3.7%)	0 (0.0%)	1 (3.7%)
	Medium	0 (0.0%)	5 (18.5%)	2 (7.4%)	0 (0.0%)	7 (25.9%)
	Low	0 (0.0%)	3 (11.1%)	6 (22.2%)	1 (3.7%)	10 (37.0%)
	Informational	0 (0.0%)	1 (3.7%)	3 (11.1%)	5 (18.5%)	9 (33.3%)
	1					
	Total	0 (0.0%)	9 (33.3%)	12 (44.4%)	6 (22.2%)	27 (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.)

Site	Risk				Informational
	High (= High)	Medium (>= Medium)	Low (>= Low)	Low (>= Low)	
https://aus5.mozilla.org	0 (0)	0 (0)	0 (0)	1 (1)	
https://exchange.mediavine.com	0 (0)	0 (0)	0 (0)	1 (1)	
https://cm.g.doubleclick.net	0 (0)	0 (0)	0 (0)	1 (1)	
https://accounts.google.com	0 (0)	3 (3)	1 (4)	0 (4)	
https://gum.criteo.com	1 (1)	0 (1)	2 (3)	1 (4)	
https://region1.analytics.google.com	0 (0)	1 (1)	0 (1)	0 (1)	
https://www.google-analytics.com	0 (0)	0 (0)	0 (0)	1 (1)	
https://cdn.tourradar.com	0 (0)	0 (0)	1 (1)	0 (1)	
https://www.tourradar.com	0 (0)	2 (2)	2 (4)	2 (6)	
https://shavar.services.mozilla.com	0 (0)	0 (0)	1 (1)	0 (1)	
https://content-signature-2.cdn.mozilla.net	0 (0)	0 (0)	3 (3)	1 (4)	

Risk

	Informational			
	High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
https://firefox.settings.services.mozilla.com	0 (0)	0 (0)	0 (0)	1 (1)
https://location.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
Open Redirect	High	1 (3.7%)
CSP: Wildcard Directive	Medium	3 (11.1%)
CSP: script-src unsafe-inline	Medium	2 (7.4%)
CSP: style-src unsafe-inline	Medium	3 (11.1%)
Content Security Policy (CSP) Header Not Set	Medium	7 (25.9%)
Cross-Domain Misconfiguration	Medium	64
Total		27

Alert type	Risk	Count (237.0%)
<u>Missing Anti-clickjacking Header</u>	Medium	6 (22.2%)
<u>Session ID in URL Rewrite</u>	Medium	1 (3.7%)
<u>CSP: Notices</u>	Low	3 (11.1%)
<u>Cookie No HttpOnly Flag</u>	Low	13 (48.1%)
<u>Cookie with SameSite Attribute None</u>	Low	16 (59.3%)
<u>Cookie without SameSite Attribute</u>	Low	4 (14.8%)
<u>Cross-Domain JavaScript Source File Inclusion</u>	Low	2 (7.4%)
<u>Private IP Disclosure</u>	Low	2 (7.4%)
<u>Server Leaks Version Information via "Server" HTTP Response Header Field</u>	Low	1546 (5,725.9%)
<u>Strict-Transport-Security Header Not Set</u>	Low	1554 (5,755.6%)
<u>Timestamp Disclosure - Unix</u>	Low	78 (288.9%)
<u>X-Content-Type-Options Header Missing</u>	Low	1568 (5,807.4%)
Total		27

Alert type	Risk	Count
<u>Charset Mismatch</u>	Informational	1 (3.7%)
<u>Content Security Policy (CSP) Report- Only Header Found</u>	Informational	2 (7.4%)
<u>Cookie Poisoning</u>	Informational	1 (3.7%)
<u>Information Disclosure - Sensitive Information in URL</u>	Informational	4 (14.8%)
<u>Information Disclosure - Suspicious Comments</u>	Informational	40 (148.1%)
<u>Loosely Scoped Cookie</u>	Informational	7 (25.9%)
<u>Modern Web Application</u>	Informational	4 (14.8%)
<u>Re-examine Cache-control Directives</u>	Informational	47 (174.1%)
<u>Retrieved from Cache</u>	Informational	1588 (5,881.5%)
Total		27

Alerts

Risk=High, Confidence=Medium (1)

<https://gum.criteo.com> (1)

Open Redirect (1)

► GET [https://gum.criteo.com/sync?
c=8&r=1&a=1&u=https%3A%2F%2Fdpm.demdex.net%2Fibs%3Adpid%3D2864
5%26dpuuid%3D%40USERID%40](https://gum.criteo.com/sync?c=8&r=1&a=1&u=https%3A%2F%2Fdpm.demdex.net%2Fibs%3Adpid%3D28645%26dpuuid%3D%40USERID%40)

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://region1.analytics.google.com> (1)

Session ID in URL Rewrite (1)

► POST [https://region1.analytics.google.com/g/collect?
v=2&tid=G-
7ZPYHR1RNC>m=45je33f0h2&_p=1245747370&_gaz=1&cid=318014739.1
678954620&ul=de&sr=1504x1003&_s=1&dl=%2Fd%2Feurope&dt=%2Fd%2Fe
urope&sid=1678954621&sct=1&seg=0&en=page_view&_fv=1&_ss=1&ep.p
age_type=Tours%20List%20Landing%20Page&ep.tour_id=93235%2C1426
3%2C5586%2C46922%2C102280%2C102334%2C52199%2C51199%2C125894%2C
194984%2C198519%2C5624%2C93131%2C194976%2C84477&ep.page_full_u
rl=https%3A%2F%2Fwww.tourradar.com%2Fd%2Feurope&ep.page_domain
=&ep.page_locale=en_US&ep.page_location_en=https%3A%2F%2Fwww.t
ourradar.com%2Fd%2Feurope&ep.internal_traffic=External&upn.tra
veller_id=0](https://region1.analytics.google.com/g/collect?v=2&tid=G-7ZPYHR1RNC>m=45je33f0h2&_p=1245747370&_gaz=1&cid=318014739.1678954620&ul=de&sr=1504x1003&_s=1&dl=%2Fd%2Feurope&dt=%2Fd%2Feurope&sid=1678954621&sct=1&seg=0&en=page_view&_fv=1&_ss=1&ep.page_type=Tours%20List%20Landing%20Page&ep.tour_id=93235%2C14263%2C5586%2C46922%2C102280%2C102334%2C52199%2C51199%2C125894%2C194984%2C198519%2C5624%2C93131%2C194976%2C84477&ep.page_full_url=https%3A%2F%2Fwww.tourradar.com%2Fd%2Feurope&ep.page_domain=&ep.page_locale=en_US&ep.page_location_en=https%3A%2F%2Fwww.tourradar.com%2Fd%2Feurope&ep.internal_traffic=External&upn.traveller_id=0)

<https://www.tourradar.com> (1)

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

► GET <https://www.tourradar.com/d/europe>

Risk=Medium, Confidence=Medium (2)

<https://www.tourradar.com> (1)

Missing Anti-clickjacking Header (1)

► GET <https://www.tourradar.com/d/europe>

<https://location.services.mozilla.com> (1)

Cross-Domain Misconfiguration (1)

► GET <https://location.services.mozilla.com/v1/country?key=7e40f68c-7938-4c5d-9f95-e61647c213eb>

Risk=Low, Confidence=High (3)

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

CSP: Notices (1)

► GET <https://accounts.google.com/o/oauth2/iframe>

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

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-2023-04-30-16-53-14.chain

Strict-Transport-Security Header Not Set (1)

► GET https://content-signature-2.cdn.mozilla.net/chains/remote-settings.content-signature.mozilla.org-2023-04-30-16-53-14.chain

Risk=Low, Confidence=Medium (6)

https://gum.criteo.com (2)

Cookie No HttpOnly Flag (1)

► GET https://gum.criteo.com/syncframe?topUrl=www.tourradar.com&origin=onetag

Cookie with SameSite Attribute None (1)

► GET https://gum.criteo.com/syncframe?topUrl=www.tourradar.com&origin=onetag

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

Private IP Disclosure (1)

► GET
https://cdn.tourradar.com/include/pw/serp/async.v1678885244.cs
s

https://www.tourradar.com (2)

Cookie without SameSite Attribute (1)

► GET <https://www.tourradar.com/d/europe>

Cross-Domain JavaScript Source File Inclusion (1)

► GET <https://www.tourradar.com/d/europe>

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

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

► GET <https://content-signature-2.cdn.mozilla.net/chains/remote-settings.content-signature.mozilla.org-2023-04-30-16-53-14.chain>

Risk=Low, Confidence=Low (1)

<https://shavar.services.mozilla.com> (1)

Timestamp Disclosure - Unix (1)

► POST <https://shavar.services.mozilla.com/downloads?client=navclient-auto-ffox&appver=111.0&pver=2.2>

Risk=Informational, Confidence=High (1)

<https://www.tourradar.com> (1)

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

► GET <https://www.tourradar.com/d/europe>

Risk=Informational, Confidence=Medium (3)

<https://cm.g.doubleclick.net> (1)

Information Disclosure - Sensitive Information in URL (1)

► GET https://cm.g.doubleclick.net/pixel?google_nid=cjp&google_sc&google_ula=913071&CriteoUserId=k-aN2TxzdC4Uv8n1vtscWUy_oPmFiAXUCu6ziNcw&google_cm&google_hm=ay1hTjJUeHpkQzRVdjhuMXZ0c2NXVX1fb1BtRm1BWFVDdTZ6aU5jdw

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

Modern Web Application (1)

► GET https://www.tourradar.com/d/europe

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

Retrieved from Cache (1)

► GET https://content-signature-2.cdn.mozilla.net/chains/remote-settings.content-signature.mozilla.org-2023-04-30-16-53-14.chain

Risk=Informational, Confidence=Low (5)

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

Charset Mismatch (1)

► GET
https://aus5.mozilla.org/update/3/SystemAddons/111.0/20230309232128/WINNT_x86_64-msvc-x64/de/release/Windows_NT%2010.0.0.0.19044.2364%20(x64)/default/default/update.xml

https://exchange.mediavine.com (1)

Cookie Poisoning (1)

► GET https://exchange.mediavine.com/usersync/push?partner=criteo&partnerId=k-NoBhRjdC4Uv8n1vtscWUy_oPmFgvlnMoTOHHA5IUXDgSTG4b

https://gum.criteo.com (1)

Loosely Scoped Cookie (1)

► GET https://gum.criteo.com/syncframe?topUrl=www.tourradar.com&origin=onetag

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

Information Disclosure - Suspicious Comments (1)

► GET https://www.google-analytics.com/analytics.js

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

Re-examine Cache-control Directives (1)

► GET
https://firefox.settings.services.mozilla.com/v1/buckets/monitor/collections/changes/changeset?collection=query-stripping&bucket=main&_expected=0

Appendix

Alert types

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

Open Redirect

Source	raised by a passive scanner (Open Redirect)
CWE ID	601
WASC ID	38
Reference	<ul style="list-style-type: none">▪ https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html▪ https://cwe.mitre.org/data/definitions/601.html

CSP: Wildcard Directive

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	<ul style="list-style-type: none">▪ http://www.w3.org/TR/CSP/▪ 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	<ul style="list-style-type: none">■ 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	<ul style="list-style-type: none">■ 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	<ul style="list-style-type: none"> ■ 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=contentsecuritypolice

.y

- <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](#)

CSP: Notices

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	<ul style="list-style-type: none">▪ 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 with SameSite Attribute None

Source	raised by a passive scanner (Cookie without SameSite Attribute)
CWE ID	1275
WASC ID	13
Reference	<ul style="list-style-type: none">▪ 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	<ul style="list-style-type: none">▪ 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

Private IP Disclosure

Source	raised by a passive scanner (Private IP Disclosure)
CWE ID	200
WASC ID	13

Reference

- <https://tools.ietf.org/html/rfc1918>

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>

Timestamp Disclosure - Unix

Source	raised by a passive scanner (Timestamp Disclosure)
CWE ID	200
WASC ID	13
Reference	<ul style="list-style-type: none">▪ 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	<ul style="list-style-type: none">▪ 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	<ul style="list-style-type: none">▪ http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection

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	<ul style="list-style-type: none">▪ 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	<ul style="list-style-type: none">▪ 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	<ul style="list-style-type: none">▪ 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/Par

t2#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).

