

Contents

1. [About this report](#)

1. [Report parameters](#)
2. [Summaries](#)

1. [Alert counts by risk and confidence](#)

2. [Alert counts by site and risk](#)

3. [Alert counts by alert type](#)
3. [Alerts](#)

1. [Risk=Высокий, Confidence=Высокий \(1\)](#)

2. [Risk=Средний, Confidence=Высокий \(4\)](#)

3. [Risk=Средний, Confidence=Средний \(4\)](#)

4. [Risk=Средний, Confidence=Низкий \(1\)](#)

5. [Risk=Низкий, Confidence=Высокий \(4\)](#)

6. [Risk=Низкий, Confidence=Средний \(7\)](#)

7. [Risk=Низкий, Confidence=Низкий \(1\)](#)

8. [Risk=Информационный, Confidence=Высокий \(1\)](#)

9. [Risk=Информационный, Confidence=Средний \(4\)](#)

10. [Risk=Информационный, Confidence=Низкий \(5\)](#)
4. [Appendix](#)

1. [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:

- <http://trudvsem.ru>
- <https://play.google.com>
- <https://www.googleadservices.com>
- <https://yandex.ru>
- <https://core-renderer-tiles.maps.yandex.net>
- <https://google.com>
- <https://beacons.gcp.gvt2.com>
- <https://update.googleapis.com>
- <https://yastatic.net>
- <https://api-maps.yandex.ru>
- <https://mc.yandex.ru>
- <https://trudvsem.ru>
- <https://content-autofill.googleapis.com>
- <https://www.googleapis.com>
- <https://fonts.gstatic.com>
- <https://apis.google.com>
- <https://ogads-pa.googleapis.com>
- <https://www.gstatic.com>
- <https://www.google.com>
- <https://optimizationguide-pa.googleapis.com>
- <https://accounts.google.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: Высокий, Средний, Низкий, Информационный

Excluded: None

Confidence levels

Included: Пользователь подтвержден , Высокий, Средний, Низкий

Excluded: Пользователь подтвержден , Высокий, Средний, Низкий, Ложно-положительное

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				Total
		Пользователь подтвержден	Высокий	Средний	Низкий	
Risk	Высокий	0 (0,0 %)	1 (3,1 %)	0 (0,0 %)	0 (0,0 %)	1 (3,1 %)
	Средний	0 (0,0 %)	4 (12,5 %)	4 (12,5 %)	1 (3,1 %)	9 (28,1 %)
	Низкий	0 (0,0 %)	4 (12,5 %)	7 (21,9 %)	1 (3,1 %)	12 (37,5 %)
	Информационный	0 (0,0 %)	1 (3,1 %)	4 (12,5 %)	5 (15,6 %)	10 (31,2 %)
	Total	0 (0,0 %)	10 (31,2 %)	15 (46,9 %)	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			
Высокий (= Высокий)	Средний (>= Средний)	Низкий (>= Низкий)	Информационный (>= Информационный)

	Risk				
	Высокий (= Высокий)	Средний (>= Средний)	Низкий (>= Низкий)	Информационный (>= Информационный)	
Site	https://trudvsem.ru	1 (1)	3 (4)	5 (9)	1 (10)
	https://www.googleapis.com	0 (0)	0 (0)	1 (1)	0 (1)
	https://apis.google.com	0 (0)	1 (1)	0 (1)	0 (1)
	https://www.gstatic.com	0 (0)	0 (0)	0 (0)	2 (2)
	https://www.google.com	0 (0)	3 (3)	3 (6)	6 (12)
	https://optimizationguide-pa.googleapis.com	0 (0)	2 (2)	3 (5)	1 (6)

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
Раскрытие PII	Высокий	2274 (7 106,2 %)
CSP: script-src unsafe-eval	Средний	17 (53,1 %)
CSP: style-src небезопасный встроенный	Средний	17 (53,1 %)
CSP: Директива подстановочного знака	Средний	17 (53,1 %)
Заголовок Content Security Policy (CSP) не задан	Средний	1696 (5 300,0 %)
Междоменная неправильная конфигурация	Средний	11 (34,4 %)
Отсутствует заголовок (Header) для защиты от клидджекинга	Средний	10 (31,2 %)
Отсутствуют токены против CSRF атак	Средний	3 (9,4 %)
Параметр X-Frame-Options искажен	Средний	564 (1 762,5 %)
Уязвимость JS Библиотеки (Library)	Средний	10 (31,2 %)
CSP: Уведомления	Низкий	17 (53,1 %)
Cookie No HttpOnly Flag	Низкий	2308 (7 212,5 %)
Cookie без атрибута SameSite	Низкий	2289 (7 153,1 %)
Cookie с атрибутом SameSite нет	Низкий	43 (134,4 %)
Включение исходного файла междоменного JavaScript	Низкий	193 (603,1 %)
Заголовок Strict-Transport-Security не установлен	Низкий	675 (2 109,4 %)
Заголовок X-Content-Type-Options отсутствует	Низкий	756 (2 362,5 %)
Множественные записи заголовков Strict-Transport-Security (несовместимы со спецификацией)	Низкий	638 (1 993,8 %)
Раскрытие информации - сообщения об ошибках отладки	Низкий	1 (3,1 %)
Раскрытие отметки времени - Unix	Низкий	488 (1 525,0 %)
Раскрытие ошибок приложения	Низкий	11 (34,4 %)
Сервер утечка информации о версии через поле заголовка HTTP-ответа «Server»	Низкий	2 (6,2 %)
Cookie с произвольным ограничением	Информационный	95 (296,9 %)
Session Management Response Identified	Информационный	1248 (3 900,0 %)
Атрибут элемента HTML, управляемый пользователем (потенциальный XSS)	Информационный	136 (425,0 %)
Кодировка, управляемая пользователем	Информационный	1 (3,1 %)
Обнаружен заголовок только для отчетов политики безопасности содержимого (CSP)	Информационный	564 (1 762,5 %)
Пересмотрите директивы управления кэшем	Информационный	97 (303,1 %)
Получено из кеша	Информационный	12 (37,5 %)
Раскрытие информации - конфиденциальная информация в URL	Информационный	17 (53,1 %)
Раскрытие информации - подозрительные комментарии	Информационный	1519 (4 746,9 %)
Современное веб-приложение	Информационный	1143 (3 571,9 %)
Total		32

Alerts

1. Risk=Высокий, Confidence=Высокий (1)

1. https://trudvsem.ru (1)

1. [Раскрытие PII](#) (1)

1. ► GET https://trudvsem.ru/

2. Risk=Средний, Confidence=Высокий (4)

1. https://www.google.com (3)

1. [CSP: script-src unsafe-eval](#) (1)

1. ► POST https://www.google.com/gen_204?s=web&t=aft&atyp=csi&ei=oeMGZ43yJMSkwPAPkbDo-

QY&rt=wsrt.606,aft.124,afts.124,frts.68,frvt.68,hst.34,prt.154,sct.64&frtp=719&imn=8&ima=0&imad=0&imac=3&wh=873&aft=1&aftp=1349&opi=89978449&dt=&ts=361857

2. [CSP: style-src небезопасный встроенный](#) (1)

1. ▶ POST https://www.google.com/gen_204?s=web&t=aft&atyp=csi&ei=oeMGZ43yJMSkwPAPkbDo-QY&rt=wsrt.606,aft.124,afts.124,frts.68,frvt.68,hst.34,prt.154,sct.64&frtp=719&imn=8&ima=0&imad=0&imac=3&wh=873&aft=1&aftp=1349&opi=89978449&dt=&ts=361857

3. [CSP: Директива подстановочного знака](#) (1)

1. ▶ POST https://www.google.com/gen_204?s=web&t=aft&atyp=csi&ei=oeMGZ43yJMSkwPAPkbDo-QY&rt=wsrt.606,aft.124,afts.124,frts.68,frvt.68,hst.34,prt.154,sct.64&frtp=719&imn=8&ima=0&imad=0&imac=3&wh=873&aft=1&aftp=1349&opi=89978449&dt=&ts=361857

2. [https://optimizationguide-pa.googleapis.com](#) (1)

1. [Заголовок Content Security Policy \(CSP\) не задан](#) (1)

1. ▶ GET https://optimizationguide-pa.googleapis.com/downloads?name=1726498979&target=OPTIMIZATION_TARGET_NOTIFICATION_PERMISSION_PREDICTIONS

3. **Risk=Средний, Confidence=Средний** (4)

1. [https://trudvsem.ru](#) (2)

1. [Параметр X-Frame-Options искажен](#) (1)

1. ▶ GET https://trudvsem.ru/

2. [Уязвимость JS Библиотеки \(Library\)](#) (1)

1. ▶ GET https://trudvsem.ru/assets/redesign-theme/scripts/purify.min.js?r=1728383766103

2. [https://apis.google.com](#) (1)

1. [Междоменная неправильная конфигурация](#) (1)

1. ▶ GET https://apis.google.com/_/scs/abc-static/_js/k=gapi.gapi.en.7LPvRDgzcqA.O/m=gapi_iframes.googleapis_client/rt=j/sv=1/d=1/ed=1/am=AACA/rs=AHpOoo9wdgI3D0Cd5pn6O1gZXHwWdc_oTg/cb=gapi.loaded_0

3. [https://optimizationguide-pa.googleapis.com](#) (1)

1. [Отсутствует заголовок \(Header\) для защиты от клидджекинга](#) (1)

1. ▶ GET https://optimizationguide-pa.googleapis.com/downloads?name=1726498979&target=OPTIMIZATION_TARGET_NOTIFICATION_PERMISSION_PREDICTIONS

4. **Risk=Средний, Confidence=Низкий** (1)

1. [https://trudvsem.ru](#) (1)

1. [Отсутствуют токены против CSRF атак](#) (1)

1. ▶ POST https://trudvsem.ru/%7B%7B%20loginUrl%20%7D%7D

5. **Risk=Низкий, Confidence=Высокий** (4)

1. [https://trudvsem.ru](#) (1)

1. [Множественные записи заголовков Strict-Transport-Security \(несовместимы со спецификацией\)](#) (1)

1. ▶ GET https://trudvsem.ru/

2. [https://www.googleapis.com](#) (1)

1. [Сервер утечка информации о версии через поле заголовка HTTP-ответа «Server»](#) (1)

1. ▶ POST https://www.googleapis.com/geolocation/v1/geolocate?key=AlzaSyBOTi4mM-6x9WDnZlJleyEU21OpBXqWBgw

3. [https://www.google.com](#) (1)

1. [CSP: Уведомления](#) (1)

1. ▶ POST https://www.google.com/gen_204?s=web&t=aft&atyp=csi&ei=oeMGZ43yJMSkwPAPkbDo-QY&rt=wsrt.606,aft.124,afts.124,frts.68,frvt.68,hst.34,prt.154,sct.64&frtp=719&imn=8&ima=0&imad=0&imac=3&wh=873&aft=1&aftp=1349&opi=89978449&dt=&ts=361857

4. [https://optimizationguide-pa.googleapis.com](#) (1)

1. [Заголовок Strict-Transport-Security не установлен](#) (1)

1. ▶ POST https://optimizationguide-pa.googleapis.com/v1:GetModels?key=AlzaSyBOTi4mM-6x9WDnZlJleyEU21OpBXqWBgw

6. **Risk=Низкий, Confidence=Средний** (7)

1. [https://trudvsem.ru](#) (4)

1. [Cookie No HttpOnly Flag](#) (1)

1. ▶ GET https://trudvsem.ru/

2. [Cookie без атрибута SameSite](#) (1)

1. ▶ GET https://trudvsem.ru/

3. [Раскрытие информации - сообщения об ошибках отладки](#) (1)

1. ▶ GET https://trudvsem.ru/information/questionnaire-service/v1/interview/current

4. [Раскрытие ошибок приложения](#) (1)

1. ▶ GET https://trudvsem.ru/iblocks/job_card

2. [https://www.google.com](#) (2)

1. [Cookie с атрибутом SameSite нет](#) (1)

1. ▶ GET https://www.google.com/search?q=%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%B0+%D0%B2+%D1%80%D0%BE%D1%81%D1%81%D0%B8%D0%B8&aq=%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%B0+%D0%B8

2. [Включение исходного файла междоменного JavaScript](#) (1)

1. ▶ GET https://www.google.com/search?q=%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%B0+%D0%B2+%D1%80%D0%BE%D1%81%D1%81%D0%B8%D0%B8&aq=%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%B0+%D0%B8

3.

https://optimizationguide-pa.googleapis.com (1)

1.

Заголовок X-Content-Type-Options отсутствует (1)

1.

► GET https://optimizationguide-pa.googleapis.com/downloads?name=1726498979&target=OPTIMIZATION_TARGET_NOTIFICATION_PERMISSION_PREDICTIONS
7. Risk=Низкий, Confidence=Низкий (1)
1.

https://optimizationguide-pa.googleapis.com (1)

1.

Раскрытие отметки времени - Unix (1)

1.

► POST https://optimizationguide-pa.googleapis.com/v1/GetModels?key=AlzaSyBOTi4mM-6x9WDnZijleyEU21OpBXqWBgw
8. Risk=Информационный, Confidence=Высокий (1)
1.

https://trudvsem.ru (1)

1.

Обнаружен заголовок только для отчетов политики безопасности содержимого (CSP) (1)

1.

► GET https://trudvsem.ru/
9. Risk=Информационный, Confidence=Средний (4)
1.

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

1.

Получено из кеша (1)

1.

► GET https://www.gstatic.com/og/_/ss/k=og.qtm.LAa13Y-4SXU.L.W.O/m=qmd,qcwid/excm=qaaw,qabr,qadd,qaid,qalo,qebr,qein,qhaw,qhawgm3,qhba,qhbr,qhbrgm3,qhch,qhchgm3,qhga,qhid,qhidgm3,qhin,qhlo,qhlogm3,qhmn,qhpc,qhsf,qhsfgm3,qhtt/d=1/ed

2.

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

1.

Session Management Response Identified (1)

1.

► GET https://www.google.com/search?q=%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%B0+%D0%B2+%D1%80%D0%BE%D1%81%D1%81%D0%B8%D0%B8&ok=%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%B0+%D0%8

2.

Раскрытие информации - конфиденциальная информация в URL (1)

1.

► GET https://www.google.com/complete/search?q=%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%B0%20%D0%B2%20%D1%80%D0%BE%D1%81%D1%81%D0%B8%D0%B8&cp=0&client=desktop-gws-wiz-on-focus-serp&xssi=t&gs_port=3&hl=ru&authuser=0&pq=%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%B0%20%D0%B2%20%D1%80%D0%BE%D1%81%D1%81%D0%B8%D0%B8&psi=oeMGZ43yJlQY.1728504739399&dpr=1&ofp=EAEYo4zo75u686HTARi2h5Tb1evvQhjvwZrtiJPW59cBGKXH_u7W8JmmuQEY1aeY5feH6LjyATLFAwo8CjrRgNCw0LHQvtGC0LAg0LIg0YDQvtGB0YHQuNC4INGH00YLYQsCDRgNC-0YHRgdC40Lgg0LLRhdC-0LQKYQpf0YDQsNCx0L7RgtCwINCyiNGA0L7RgdGB0LjQuCDQQu9C40YfQvdGL0Lkg0LrQsNCx0LjQvdC10YIgl0LLRhdC-0LQg0YfQtdGA0LXQtyDQs9C-0YHRg9GB0LvRg9Cz0LgKLwot0YDQsNCx0L7RgtCwINCyiNGA0L7RgdGB0LjQuCDRgtGA0YPQINcy0YHQtdC8CisKKdGA0LDQsdC-0YLYQsCDQsiDRgNC-0YHRgdC40Lgg0YDQtdC30Y7QvNC1Ci8KLdGA0LDQsdC-0YLYQsCDQsiDRgNC-0YHRgdC40Lgg0L7QsdGD0YfQtdC90LjQtQo-CjzRgNCw0LHQvtGC0LAg0LIg0YDQvtGB0YHQuNC4INGG0LXQu9C10LLQvtC1INC-0LHRg9GH0LXQvdC40LUQRw
3.
- Современное веб-приложение (1)
1.

► POST https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://trudvsem.ru/&ved=2ahUKEwjNxoL3jYKJAXVEEHAIHREYOm8QFnoECAkQAQ

10. Risk=Информационный, Confidence=Низкий (5)

1.

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

1.

Раскрытие информации - подозрительные комментарии (1)

1.

► GET https://www.gstatic.com/og/_/js/k=og.qtm.en_US.6T6r_9V_Ciw.2019.O/rt=/m=q_dnp,qmd,qcwid,qapid,qald,qads,q_dg/exm=qaaw,qabr,qadd,qaid,qalo,qebr,qein,qhaw,qhawgm3,qhba,qhbr,qhbrgm3,qhIADuEe1tzdVix-MATZjg

2.

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

1.

Cookie с произвольным ограничением (1)

1.

► GET https://www.google.com/search?q=%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%B0+%D0%B2+%D1%80%D0%BE%D1%81%D1%81%D0%B8%D0%B8&ok=%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%B0+%D0%8

2.

Атрибут элемента HTML, управляемый пользователем (потенциальный XSS) (1)

1.

► POST https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://trudvsem.ru/&ved=2ahUKEwjNxoL3jYKJAXVEEHAIHREYOm8QFnoECAkQAQ

3.

Кодировка, управляемая пользователем (1)

1.

► GET https://www.google.com/search?q=%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%B0+%D0%B2+%D1%80%D0%BE%D1%81%D1%81%D0%B8%D0%B8&ok=%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%B0+%D0%8

3.

https://optimizationguide-pa.googleapis.com (1)

1.

Пересмотрите директивы управления кэшем (1)

1.

► GET https://optimizationguide-pa.googleapis.com/downloads?name=1726498979&target=OPTIMIZATION_TARGET_NOTIFICATION_PERMISSION_PREDICTIONS

Appendix

Alert types

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

1. Раскрытие PII

Source raised by a passive scanner ([Раскрытие PII](#))
CWE ID [359](#)
WASC ID 13

2. CSP: script-src unsafe-eval

Source raised by a passive scanner ([CSP](#))
CWE ID [693](#)
WASC ID 15

1. <https://www.w3.org/TR/CSP/>
2. <https://caniuse.com/#search=content+security+policy>
3. <https://content-security-policy.com/>
4. <https://github.com/HtmlUnit/htmlunit-csp>
5. https://developers.google.com/web/fundamentals/security/csp/policy_applies_to_a_wide_variety_of_resources

Source raised by a passive scanner ([CSP](#))
CWE ID [693](#)
WASC ID 15

Source raised by a passive scanner ([CSP](#))
CWE ID [693](#)
WASC ID 15

Source raised by a passive scanner ([Заголовок Content Security Policy \(CSP\) не задан](#))
CWE ID [693](#)
WASC ID 15

Source raised by a passive scanner ([Междоменная неправильная конфигурация](#))
CWE ID [264](#)
WASC ID 14

Source raised by a passive scanner ([Заголовок против клидджекинга](#))
CWE ID [1021](#)
WASC ID 15

Source raised by a passive scanner ([Отсутствуют токены против CSRF атак](#))

CWE ID [352](#)

WASC ID 9

Reference

1. https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html
2. <https://cwe.mitre.org/data/definitions/352.html>

Source raised by a passive scanner ([Заголовок против клиджекинга](#))
CWE ID [1021](#)
WASC ID 15
Reference 1. <https://tools.ietf.org/html/rfc7034#section-2.1>

Source	raised by a passive scanner (Уязвимая JS-библиотека (на платформе Retire.js))
CWE ID	829
Reference	<ol style="list-style-type: none"> 1. https://nvd.nist.gov/vuln/detail/CVE-2024-45801 2. https://github.com/cure53/DOMPurify/security/advisories/GHSA-mmxh-hmjr-r674 3. https://github.com/cure53/DOMPurify 4. https://github.com/advisories/GHSA-mmxh-hmjr-r674 5. https://github.com/cure53/DOMPurify/commit/26e1d69ca7f769f5c558619d644d90dd8bf26ebc 6. https://github.com/cure53/DOMPurify/commit/1e5026262bf4c66b5efda49e2316d6d1246ca7b21

Source raised by a passive scanner ([CSP](#))
CWE ID [693](#)
WASC ID 15

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

CWE ID [1004](#)

WASC ID 13

Reference 1. <https://owasp.org/www-community/HttpOnly>

Source raised by a passive scanner ([Cookie без атрибута SameSite](#))

CWE ID [1275](#)
WASC ID 13
Reference 1. <https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site>

14. Cookie с атрибутом SameSite нет

Source raised by a passive scanner ([Cookie без атрибута SameSite](#))
CWE ID [1275](#)
WASC ID 13
Reference 1. <https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site>

15. Включение исходного файла междоменного JavaScript

Source raised by a passive scanner ([Включение исходного файла междоменного JavaScript](#))
CWE ID [829](#)
WASC ID 15

16. Заголовок Strict-Transport-Security не установлен

Source raised by a passive scanner ([Заголовок строгой транспортной безопасности](#))
CWE ID [319](#)
WASC ID 15
Reference 1. https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
2. <https://owasp.org/www-community/Security-Headers>
3. https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
4. <https://caniuse.com/stricttransportsecurity>
5. <https://datatracker.ietf.org/doc/html/rfc6797>

17. Заголовок X-Content-Type-Options отсутствует

Source raised by a passive scanner ([Заголовок X-Content-Type-Options отсутствует](#))
CWE ID [693](#)
WASC ID 15
Reference 1. [https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941\(v=vs.85\)](https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85))
2. <https://owasp.org/www-community/Security-Headers>

18. Множественные записи заголовков Strict-Transport-Security (несовместимы со спецификацией)

Source raised by a passive scanner ([Заголовок строгой транспортной безопасности](#))
CWE ID [319](#)
WASC ID 15
Reference 1. <https://datatracker.ietf.org/doc/html/rfc6797#section-8.1>

19. Раскрытие информации - сообщения об ошибках отладки

Source raised by a passive scanner ([Раскрытие информации - сообщения об ошибках отладки](#))
CWE ID [200](#)
WASC ID 13

20. Раскрытие отметки времени - Unix

Source raised by a passive scanner ([Раскрытие отметки времени](#))
CWE ID [200](#)
WASC ID 13
Reference 1. <https://cwe.mitre.org/data/definitions/200.html>

21. Раскрытие ошибок приложения

Source raised by a passive scanner ([Раскрытие ошибок приложения](#))
CWE ID [200](#)
WASC ID 13

22. Сервер утечка информации о версии через поле заголовка HTTP-ответа «Server»

Source raised by a passive scanner ([Заголовок ответа HTTP-сервера](#))
CWE ID [200](#)
WASC ID 13
Reference 1. <https://httpd.apache.org/docs/current/mod/core.html#servertokens>
2. [https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552\(v=pandp.10\)](https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10))
3. <https://www.troyhunt.com/shhh-dont-let-your-response-headers/>

23. Cookie с произвольным ограничением

Source raised by a passive scanner ([Cookie с произвольным ограничением](#))
CWE ID [565](#)
WASC ID 15
Reference 1. <https://tools.ietf.org/html/rfc6265#section-4.1>
2. 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
3. https://code.google.com/p/browsersec/wiki/Part2#Same-origin_policy_for_cookies

24. Session Management Response Identified

Source raised by a passive scanner ([Session Management Response Identified](#))
Reference 1. <https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id>

25. Атрибут элемента HTML, управляемый пользователем (потенциальный XSS)

Source raised by a passive scanner ([Атрибут элемента HTML, управляемый пользователем \(потенциальный XSS\)](#))
CWE ID [20](#)
WASC ID 20
Reference 1. https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html

26. Кодировка, управляемая пользователем

Source raised by a passive scanner ([Кодировка, управляемая пользователем](#))
CWE ID [20](#)

WASC ID 20

27. Обнаружен заголовок только для отчетов политики безопасности содержимого (CSP)

Source raised by a passive scanner ([Заголовок Content Security Policy \(CSP\) не задан](#))

CWE ID [693](#)

WASC ID 15

- Reference
1. <https://www.w3.org/TR/CSP2/>
 2. <https://w3c.github.io/webappsec-csp/>
 3. <https://caniuse.com/#feat=contentsecuritypolicy>
 4. <https://content-security-policy.com/>

28. Пересмотрите директивы управления кэшем

Source raised by a passive scanner ([Пересмотрите директивы управления кэшем](#))

CWE ID [525](#)

WASC ID 13

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

29. Получено из кеша

Source raised by a passive scanner ([Получено из кеша](#))

- Reference
1. <https://tools.ietf.org/html/rfc7234>
 2. <https://tools.ietf.org/html/rfc7231>
 3. <https://www.rfc-editor.org/rfc/rfc9110.html>

30. Раскрытие информации - конфиденциальная информация в URL

Source raised by a passive scanner ([Раскрытие информации - конфиденциальная информация в URL](#))

CWE ID [200](#)

WASC ID 13

31. Раскрытие информации - подозрительные комментарии

Source raised by a passive scanner ([Раскрытие информации - подозрительные комментарии](#))

CWE ID [200](#)

WASC ID 13

32. Современное веб-приложение

Source raised by a passive scanner ([Современное веб-приложение](#))