IMMUNIWEB WEBSITE SECURITY TEST

API Documentation v 3.2.1

FEBRUARY 28, 2022

Table of Contents

1. General Overview

The detailed scoring methodology of the Website Security Test can be found here: https://www.immuniweb.com/websec/#scoring

API Specifications

Field Name	Value
Protocol	HTTP/HTTPS
Request Type	POST
URLs	To initiate the test: https://www.immuniweb.com/websec/api/v1/chsec/[ustamp].html To fetch the results: https://www.immuniweb.com/websec/api/v1/get_result/[ustamp].html Where [ustamp] is an arbitrary UNIX time-stamp (must be an integer). Such construction is done to prevent caching on client side.

POST Data Specifications

Field Name	Value
tested_url	The URL of the domain to be tested.
dnsr	Stands for “do not show results”. "on" will not show the result in the Recent tests on ImmuniWeb.com
recheck	"false" will use results from cache if the server has been tested within the past 24 hours, "true" will perform a new test without looking at the cache.
choosen_ip	IP address of tested server (if tested domain resolves to multiple addresses).
token	Value of the token sent by the server if the tested domain is resolved into several IP addresses.
api_key	Secret token which you can submit alongside with the request (used only for commercial access).

Examples of Transactions using CURL

Step 1: Starting the test

curl -d “tested_url=example.com&dnsr=off&recheck=false&choosen_ip=any” https://www.immuniweb.com/websec/api/v1/chsec/1451425590.html

If you receive the “test_cached” status in response, please proceed to Step 2.b

If you receive the “test_started” status in response, please proceed to Step 2.a

Response Example (if the test has been found in the cache)


```
{
  "test_id": "c84936eeff5ffc43f38ddb91adfd90ac27fb416bd0b21fe2edb1004",
  "status": "test_cached",
  "status_id": 3,
  "message": "Test is cached"
}
```


Response Example (if the test has **not** been found in the cache)


```
{
  "debug": true,
  "job_id": "2a9e1f1bc92dc0c7a4bde8771eea6d36988208d34163c5496227b8dc",
  "status": "test_started",
  "status_id": 1,
  "message": "Test has started"
}
```

Step 2.a: Fetching the results if the test has not been found in the cache (call this until the test is finished)

curl -d “job_id=[job_id FROM THE STEP 1 RESPONSE]”
https://www.immuniweb.com/websec/api/v1/get_result/1451425590.html

Response Example (if the test is **not** finished yet):

```
{
  "job_id": "2a9e1f17a4bde930dff488771eea6d36988208d34163c5496227b8dc",
  "status": "in_progress",
  "status_id": 2,
  "message": "Your test is in progress"
}
```

Step 2.b: Fetching the results if the test has been found in the cache (“test_cached” status)

curl -d “id=[test_id FROM THE STEP 1 RESPONSE]”
https://www.immuniweb.com/websec/api/v1/get_result/1451425590.html

Example with error

curl -d “tested_url=0.0.0.0&&dnsr=off&recheck=false&choosen_ip=any”
https://www.immuniweb.com/websec/api/v1/chsec/1451425590.html

```
{
  "error": "The domain name does not exist",
  "error_id": 9
}
```

How to download the PDF

curl -d “api_key=YOUR-API-KEY”
“https://www.immuniweb.com/websec/gen_pdf/[test_id]” > report.pdf

Successful Response Example


```
{
  "tested_url": "https://twitter.com/",
  "hostname": "twitter.com",
  "server_ip": "104.244.42.129",
  "http_response": "200 OK",
  "company_name": "Twitter, Inc.",
  "page_title": "Twitter. It’s what’s happening / Twitter",
  "server_location": "Winter Haven, United States",
  "country": "United States",
  "city": "Winter Haven",
  "lat": 28.022200000000002,
  "lng": -81.732902999999993,
  "ts": 1582634202,
  "id": "d38d77b1eaee5592dc7d63623dbe2ee5da3df9e869496831bcd36af186b",
  "short_id": "KVOQyiJv",
  "score": 90,
  "grade": "A",
  "redirect_to": "",
  "is_firewalled": "0",
  "compliance_pci_dss": false,
  "compliance_gdpr": false,
  "dnsr": "off",
  "reverse_dns": "-",
  "server_signature": "-",
  "w_id": "WORKER03",
  "http_additional_info": {…},
  "http_headers": {…},
  "http_verbs": {…},
  "http_cookies": […],
  "pci_dss": {…},
  "gdpr": {…},
  "internals": {…},
  "third_party_content": […],
  "third_party_content_stats": {…},
  "global_highlights": […],
  "highlights": […]
}
```

The output will be detailed later in these sections of the document:

- meta-information: contains basic server info, like IP, port, reverse DNS and a general overview of the test results
- http_additional_info: details if the server supports content_encoding, waf, etc.
- http_headers: contains all information about returned http headers
- http_verbs: contains all information about allowed http verbs
- http_cookies: contains all information about returned cookies
- pci_dss: contains information regarding PCI DSS compliance
- gdpr: contains information regarding GDPR compliance
- internals: contains internal information such as city, country, server IP, etc.
- third_party_content: containing all the third-party content

2. Meta-information

Contains basic server info, like IP, port, reverse DNS and a general overview of the test.

Field Name	Type	Always present	Description
tested_url	string	Yes	The URL that was tested.
hostname	string	Yes	The hostname of the tested website.
server_ip	string	Yes	The IP address of the tested website.
http_response	string	Yes	Status code of the response (e.g. 200 OK).
company_name	string	Yes	The company's name.
page_title	string	Yes	The title of the webpage tested.
server_location	string	Yes	The location of the server.
country	string	Yes	The country in which the IP address resides.
city	string	Yes	The city in which the IP address resides.
lat	float	Yes	The latitude of the IP address tested.

lng	float	Yes	The longitude of the IP address tested.
ts	integer	Yes	The time-stamp of the test.
id	string	Yes	The id of the test.
short_id	string	Yes	The short id of the test.
score	integer	Yes	The score of the test.
grade	string	Yes	The grade of the test.
redirect_to	string	Yes	Where it redirects to.
is_firewalled	string	Yes	Is the website firewall protected?
compliance_pci_dss	bool	Yes	Is the website PCI DSS compliant?
compliance_gdpr	bool	Yes	Is the website GDPR compliant?
server_signature	string	Yes	The signature of the server (e.g. “cloudflare”).
dnsr	string	Yes	Do not show result on the ImmuniWeb site.
reverse_dns	string	Yes	Details the reverse DNS record of the website.
w_id	string	Yes	Indicates the worker ID.
http_additional_info	object	Yes	Contains information regarding content encoding, WAF, sri, etc. Will be detailed later in the document.
http_headers	object	Yes	Contains all information about returned HTTP headers. Will be detailed later in the document.
http_verbs	object	Yes	Contains all information about allowed HTTP verbs. Will be detailed later in the document.
http_cookies	array	Yes	Contains all information about returned cookies. Will be detailed later in the document.
pci_dss	object	Yes	Contains information regarding the PCI DSS compliance. Will be detailed later in the document.
gdpr	object	Yes	Contains information regarding the GDPR compliance. Will be detailed later in the document.

internals	object	Yes	Contains internal information such as city, country, server IP. Will be detailed later in the document.
third_party_ content	array	Yes	Contains detail about all third-party content. Will be detailed later in the document.
third_party_ content_stats	object	No	Contains information about found external content – images, JS/CSS files, etc., and number of requests that failed. Syntax `{ "found": “int”, "failed": “int” }`
highlights	array	Yes	“Highlights” is an array of object that holds a general overview of the test results. The returned integer will correspond to one of the following highlights: **1)** All the HTTP methods supported by the web server are properly configured. **2)** Some HTTP headers related to security and privacy are missing. **3)** All cookies sent by the web application have secure flags and attributes. Syntax: `{ "location": "string", "highlight": "string [integer]" }`
global_highlights	array	Yes	Details the global highlights of the test.

3. HTTP Additional Info

Contains additional details on what the web server supports, such as content encoding and protocol negotiation. The structure is as follows:

Field Name	Type	Always present	Description
content_encoding	array	Yes	Array of the content encoding formats.
redirect_chain	array	Yes	Details the redirect chain.
cryptojacking	array	No	Array of details concerning the cryptojacking malware detection. Syntax: `[ { "url": "string", "ip": "string", "pattern": "string", "country": "string", "city": "string", "country_code": "string" } ]`
dirlist	array	Yes	Details of a directory listing enabled implementation.
third_party_ content_not_ resolved	bool	Yes	“true” if there is third-party content that point to unresolvable domains
hosting_provider	string or array	Yes	Array of details regarding the domain presence in hosting provider detection.
viewstate	string or array	Yes	Contains details regarding the viewstate.
is_it_phishing	array	Yes	Array of details concerning the domain presence in phishing blacklists detection.
protocol_ negotitation	object	No	Contains details of the supported protocol negotiation. Syntax: `{ "npn": [“string”, ...], "alpn": “bool”/”string” }` "npn" (array) contains protocols advertised by the

			server: [“h2”, “http/1.1”, …] `"alpn"` (boolean or string) can take one of the following values: • true – Yes (deprecated) • false - N/A • protocol name – “h2”, “http/1.1”, etc.
supported_ protocols	array	Yes	Contains information on supported protocols. Possible fields in the objects: “`name`”: contains the protocol’s name (e.g. HTTP/1.0, HTTP/2) “`status_code`”: the status code sent by the server in response to a request with the aforementioned protocol “`supported`”: a boolean indicating whether the protocol is supported “`reason`”: indicates the reason why the protocol isn’t supported. Possible reasons are: • “`protocol_changed`”: the server responded with a protocol different from the one used to make the request • “`empty_response`”: indicates a lack of response from the server • “`invalid_status”code`”: server responded with an error status code (e.g. 404, 403, 503) • “`unexpected_protocol`”: an unrecognized protocol has been used in response “`response_protocol`”: indicates the protocol used in response, if the response protocol is different from the one used to make the request.
waf	array	Yes	Contains details of a Web Application Firewall implementation.
spamlist	array	Yes	Array of servers that listed server’s IP as spam.
sri	array	Yes	Array of objects detailing the SubResource Integrity configuration. Will be detailed later in the document.
app_scan	object	Yes	Contains information regarding the CMS and components. Will be detailed later in the document.

3.1. Subresource Integrity

Contains details regarding the SubResource Integrity configuration.

Field Name	Type	Always present	Description
tag	string	Yes	Contains the tag.
location	string	Yes	Indicates the location of the file.
hash_type	string	Yes	Details the hash type.
original_hash	string	Yes	Contains the original hash.
calculated_hash	string	Yes	Contains the calculated hash.
original_html	string	Yes	Contains the original HTML.
suggested_html	string	Yes	Contains the suggested HTML.
error	bool	Yes	Details if there was an error.

3.2. Application Scan

Contains information regarding the CMS and components. The structure is as follows:

Field Name	Type	Always present	Description
status	bool	Yes	Indicates the status of the scan.
is_firewalled	bool	Yes	Indicates if the scan was interrupted by the WAF or any other defense system.
is_timeouted	bool	Yes	Indicates if the scan was timeouted.
result	object	Yes	Contains the results of the application scan. Will be detailed shortly in the document.

The structure of the “result” object is as follows:

Field Name	Type	Always present	Description
STATUS	string	No	Indicates the status of the scan.
FIREWALL	string	No	Indicates if the scan was interrupted by the WAF or any other defense system.
TIMEOUT	string	No	Indicates if the scan was timeouted.
DOMAIN	string	No	Indicates the tested domain.
IP_ADDRESS	string	No	Indicates the IP address.

DESCRIPTION	object	No	Syntax:
			`{ "ID": "string",`
			`"NAME": "string",`
			`"STATUS": "string" }`

stats	object	Yes	Contains basic statistics on the found software, their versions and vulnerabilities. Example:
			`"stats": {`
			`// shows the number of software with…`
			`"unknown": "int",`
			`// unknown version`
			`"outdated": "int",`
			`// outdated version`
			`"vulnerable": "int",`
			`// version with known vulnerabilities`
			`"vulnerabilities": "int",`
			`// shows the total of all vulnerabilities`
			`"cms": "int",`
			`// the number of detected CMS`
			`"components": "int",`
			`// the number of detected JS-libraries`
			`"found": "int"`
			`// the total number of detected software`
			`}`

RESULT	object	Yes	Contains information regarding the CMS, JS-libraries and their vulnerabilities. Will be detailed later in the document.

3.2.1. Application Scan Results

Contains details about the CMS and components if any were found.

Field Name	Type	Always present	Description
VERSION	string/ array	Yes	Provides an array with the suspected versions of the CMS.
SOFT	object	Yes	Contains information about the found CMS. Will be detailed later in the document.
COMPONENTS	string/ object	Yes	Contains information about the found components. Will be detailed later in the document.
VULNS	string/ object	Yes	Contains information about the found vulnerabilities. Will be detailed later in the document.
CPE	object	No	Contains short information about the fingerprinted CMS and components. Syntax: `"CPE": { "SOFT": [ "string" ], "COMPONENTS": [ "string" ] }`

3.2.1.1. Software

The “SOFT” object contains information about the found CMS. The structure is as follows:

Field Name	Type	Always present	Description
ID	string	No	Indicates the ID of the CMS.
NAME	string	No	The name of the CMS.
LINK	string	No	The link to the official page.
CPE	string/ array	Yes	Contains the CPE names.
SOFT_TYPE	string	No	Indicates the type of the software.
LAST_VERSION	string/ array	Yes	The last known version of the CMS.
STATUS	string	No	Indicates whether the CMS is updatable or not.
IS_ UPGREADABLE	string/ bool	Yes	Details whether the CMS can be updated.

3.2.1.2. Components

Field Name	Type	Always present	Description
VERSION	array	No	An array with the suspected versions of the CMS.
NAME	string	No	Details the name of the component.
SOFT	object	No	Contains detailed information regarding the software's name, vendor's name and the version.
CPE	array	No	Contains the CPE names.
IS_ UPGREADABLE	bool	No	Details whether the component can be updated.

An example of the "COMPONENTS" object:

```
        "COMPONENTS": {
            "cpe:/a:aFarkas:html5shiv:": {
              "VERSION": ["3.7.3"],
              "NAME": "aFarkas",
              "SOFT": {
                "ID": "",
                "NAME": "html5shiv",
                "CPE": "html5shiv",
                "LINK": "",
                "LAST_VERSION": "3.7.3",
                "STATUS": "",
                "VENDOR_NAME": "aFarkas",
                "VENDOR_CPE": "aFarkas"
              },
              "CPE": ["cpe:/a:afarkas:html5shiv:3.7.3"],
              "IS_UPGREADABLE": false
               "stats": {
                  "bulletines": 0
                  "vulnerabilities": 0
              }
            },
            "cpe:/a:jquery:jquery:": {...},
            "cpe:/a:FezVrasta:popper.js:": {...}
      }
```

3.2.1.3. Vulnerabilities

An object containing information about found vulnerabilities. Commonly found fields are:

Field Name	Type	Always present	Description
CODE	string	No	Details the code of the bulletin.
TITLE	string	No	Details the title of the bulletin.
DATE_CREATE	string	No	Details the date of creation of the bulletin.
SEVERITY	string	No	Details the overall severity of the vulnerabilities.
PATCH	string	No	Details if the vulnerability is patched.
URL	string	No	The URL with details on the vulnerability.
DATA	array	No	Contains detailed information on vulnerabilities.

3.2.1.3.1. Vulnerabilities Data

Field Name	Type	Always present	Description
TITLE	string	No	Contains the title of the vulnerability.
DETAIL_TEXT	string	No	Contains the details about the vulnerability.
CVSSv3	string	No	Contains the CVSSv3 calculation.
CVSSv3_SCORE	string	No	Contains the CVSSv3 score of the vulnerability.
SEVERITY	string	No	Indicates the severity of the vulnerability.
REMEDIATION	string	No	Contains information on possible remediation.
LINKS	string	No	Contains links to vulnerability report.
CVE	array	No	Contains the CVE reference codes.
CWE	array	No	Contains the CWE reference codes.

4. HTTP headers

This section lists the returned security related HTTP headers and relevant information regarding them. It is composed of the following main subsections. Every subsection will be detailed later in the document.

Header Name	Description
Content-Security-Policy	(CSP) defines allowed sources for each type of content (e.g. text, images), helping to defend against XSS attacks. It also controls browser's settings, from sandbox enforcement to value of HTTP Referrer header.
Content-Security-Policy-Report-Only	ReportOnly allows for testing without enforcement, meaning that your website will remain reachable if the header is incorrectly configured.
Public-Key-Pins	HTTP-Public-Key-Pinning (HPKP) header prevents Man-In-The-Middle attacks against the website by whitelisting allowed certificates in the trust chain.
Public-Key-Pins-Report-Only	ReportOnly allows testing without enforcement (i.e. the website will remain reachable even if HPKP is not correctly configured).
Referrer-Policy	ReferrerPolicy HTTP header governs which referrer information [sent in the Referer header] should be included into the HTTP requests.
Server	Server header is usually sent by websites to advertise their version.
Strict-Transport-Security	HTTP_Strict_Transport_Security (HSTS) header forces browsers to access the website via HTTPS.
X-Content-Type-Options	XContentTypeOptions can direct browsers to disable the ability to sniff the pages content-type and only to use the content-type defined in the directive itself. This provides protection against XSS or Drive-by-Download attacks.
X-Frame-Options	X_Frame_Options header specifies whether the website should allow itself to be framed, and from which origin. Blocking framing helps defend against attacks such as Clickjacking.
X-XSS-Protection	X_XSS_Protection defines how browsers should enforce XSS protection.
X-Powered-By	X_Powered_By header is commonly used to display web server's software or it components (e.g. programming language or CMS).
X-AspNet-Version	Specifies the version of ASP.NET being used.
Access-Control-Allow-Origin	Access_Control_Allow_Origin is one of the CORS HTTP headers that defines which external domains can access specific resources (e.g. fonts or images) of the website.

Expect-CT	Expect_CT header allows a website to determine if it is ready for the upcoming Chrome requirements and/or enforce their CTpolicy.
Expect-Staple	The Expect-Staple header allows you to determine if your site is delivering proper OCSP Staples with certificates.
Feature-Policy	"Feature_Policy HTTP header allows to enable, disable, or modify behavior of web browser's APIs and features (e.g. access to camera, Geolocation, etc.).

Each HTTP header contains its own list that details its implementation details, such as directives and highlights.

The following headers all have the same structure:

- X-Powered-By
- X-AspNet-Version
- X-Frame-Options (additionally can have a "DENY" field as a string)
- X-Content-Type-Options (additionally can have a "no-sniff" field as a string)
- Content-Security-Policy-Report-Only
- Access-Control-Allow Origin
- Public-Key-Pins
- Public-Key-Pins-Report-Only
- Expect-CT
- Expect-Staple
- Feature-Policy
- Referrer-Policy (additionally can have a "no-referrer-when-downgraded" field as a string)
- Server

The structure is as follows:

Field Name	Type	Always present	Description
description	string	No	A high-level general description of the header.
highlight	array	No	Highlight details on the header implementation.
raw	string	No	The returned raw header.
colored-raw	array	No	An array representing the returned results.

4.1. X-XSS-Protection

This section is a list of details for the X-XSS-Protection header.

Field Name	Type	Always present	Description
description	string	No	A high-level general description of the 'x-xss-protection' header.
highlight	array	No	Highlight details on the header implementation.
raw	string	No	The returned raw header.
colored-raw	array	No	An array representing the returned results.
1	string	No	The value of '1' indicates that the directive is correctly informing the browser to implement heuristic protection.
mode=block	string	No	Forces browser to block server's response when heuristic protection detects an XSS.

4.2. Strict-Transport-Security

This section is a list of details for the strict-transport-security header. The list will contain values populated by the observed strict-transport security implementation.

Field Name	Type	Always present	Description
description	string	No	A high-level general description of the 'Strict-Transport-Security' header.
highlight	array	No	Highlight details on the header implementation.
raw	string	No	The returned raw header.
colored-raw	array	No	An array representing the returned results.
enforced	bool	Yes	Set to 'true' if the header is present.
includeSubdomains	object	No	A high-level general description of the 'includeSubdomains' directive.
max-age	object	No	A high-level general description of the 'max-age' directive.
preload	object	No	A high-level general description of the 'preload' directive. Syntax: {"description": string, "tag": int}

4.3. Content-Security-Policy

This section is a list of content-security policy directive information. Some directives have their own list with entries regarding implementation details and descriptions. CSP section contains the following:

Field Name	Type	Always present	Description
description	string	Yes	An overview of the content-security-policies purpose.
raw	string	Yes	The raw returned content-security-policy.
colored-raw	array	Yes	An array of objects representing the returned results. Syntax: { description: string, tag: int}
highlight	array	Yes	A high-level overview of the implementation, each integer will correspond to a highlight of the implementation. Syntax: [value: string, tag: int]
block_all_mixed_content	object	No	Contains detailed information regarding the returned block-all-mixed content directive. Syntax: {description: string, tag: int}
report_uri	object	No	Contains detailed information regarding the returned report-uri directive.
form-action	object	No	Contains details of form-action.
default-src	object	No	Contains detailed information regarding the returned default-src directive. Each found 'default-src' domain value will be populated with the appropriate message string. The description field will describe the directive. Syntax: {value: string, description: string, tag: int}
font-src	object	No	Contains detailed information regarding the returned font-src directive. Syntax: {value: string, description: string, tag: int}

frame-src	object	No	Contains detailed information regarding the returned frame-src directive. Syntax: {value: string, description: string, tag: int}
img-src	object	No	Contains detailed information regarding the returned img-src directive. Syntax: {value: string, description: string, tag: int}
manifest-src	object	No	Contains detailed information regarding the returned manifest-src directive. Syntax: {value: string, description: string, tag: int}
media-src	object	No	Contains detailed information regarding the returned media-src directive. Syntax: {value: string, description: string, tag: int}
object-src	object	No	Contains detailed information regarding the returned object-src directive. Syntax: {value: string, description: string, tag: int}
script-src	object	No	Contains detailed information regarding the returned script-src directive. Syntax: {value: string, description: string, tag: int}
style-src	object	No	Contains detailed information regarding the returned style-src directive. Syntax: {value: string, description: string, tag: int}
worker-src	object	No	Contains detailed information regarding the returned worker-src directive. Syntax: {value: string, description: string, tag: int}

5. HTTP verbs

This section details the server's allowed HTTP verbs.

Field Name	Type	Always present	Description
GET	string	Yes	GET method allows getting any information (header and body) relative to the URL specified.
POST	string	Yes	POST method is used to send data to a website.
HEAD	string	No	HEAD method is identical to GET except that only the he ade should be returned by the web server. Using it may a llow to bypass some poorly implemented security mecha nisms.
OPTIONS	string	No	OPTIONS method retrieves information about the commu nication options available (such as the allowed HTTP met hods for the specified page).
TRACE	string	No	TRACE is a HTTP request method used for debugging which echo's back input back to the user.
TRACK	string	No	TRACK is an HTTP verb that tells IIS to return the full request back to the client. It is Microsoft's implementation and it is similar to TRACE verb which is RFC complaint.
PUT	string	No	PUT method allows the writing of a file to the web server at the location specified by the URL. It may cause serious security issues when poorlyconfigured.
PATCH	string	No	The PATCH method is a request method supported by the HTTP protocol for making partial changes to an existing resource.
DELETE	string	No	The DELETE method allows deletion of a file on the web server at the location specified by the URL. It may cause serious security issues when poorly configured.
CONNECT	string	No	The CONNECT method converts the request connection to a transparent TCP/IP tunnel. This is usually to facilitate SSL-encrypted communication (HTTPS) through an unencrypted HTTP proxy.

6. HTTP cookies

This HTTP cookies section provides details on the returned web server cookies with all relevant attributes. The structure is as follows:

Field Name	Type	Always present	Description
name	string	No	Contains the name of the cookie.
value	string	No	Contains the value of the cookie.
domain	object	No	`{"description": "Sets the domains where browsers should send this cookie too. [0]", "value": "string" }`
path	object	No	`{"description": "Sets the path of the application where the cookie should be sent. [0]", "value": "string" }`
max-age	object	No	`{"description": "Sets the maximum lifetime of the cookie using a time in seconds. [0]", "value": "string" }`
expires	object	No	`{"description": "Sets the maximum lifetime of the cookie using a date. [0]", "value": "string"}`
secure	object	No	`{"description": "Prevents browsers to send this cookie over an insecure connection. [0]", "value": "string"}`
samesite	object	No	`{"description": "Prevents CSRF attacks by not sending the cookies when the request comes from another website. [0]", "value": "string"}`
httponly	object	No	`{"description": "Prevents client-side scripts to access the cookie by telling browsers to only transmit the cookie over HTTP(S). [0]", "value": "string"}`
is_proxy	bool	No	“true” if the cookie is set by a proxy (e.g. WAF, AWS, CDN).
highlight	object	No	Highlight details on the cookie.
raw	string	No	The returned raw cookie.
colored-raw	array	No	An array representation of the returned results.

7. PCI DSS

Contains information regarding PCI DSS compliance. Syntax:

```
"pci_dss": {
    "compliance": false,
    "requirements": { "6.2": true, "6.5": true, "6.6": false }
  }
```

Field Name	Type	Always present	Description
compliance	bool	Yes	True if the website is compliant with PCI DSS requirements.
6.2	bool	Yes	True if the CMS and all components are up-to-date.
6.5	bool	Yes	True if the CMS and all components don't have known vulnerabilities.
6.6	bool	Yes	True if a WAF is present.

8. GDPR

Contains information regarding GDPR compliance.

Field Name	Type	Always present	Description
compliant	bool or integer	No	Absent in old tests. True if the website is compliant with GDPR requirements.
check_1	bool or integer	Yes	True if Privacy Policy is found
check_2	bool or integer	Yes	True if no vulnerable CMS or components are found.
check_3	bool or integer	Yes	True if the server has SSL/TLS encryption in place.
check_4	bool or integer	Yes	True if no outdated components are found. (this check does not affect the compliance in general way of true/false, but changes the final message from COMPLIANT to NO ISSUES FOUND).
check_5	bool or integer	Yes	True if cookies have httponly and secure flag.
check_6	bool or integer	Yes	True if the website has cookie consent banner.

9. Internals

Contains internal information such as city, country, server IP and more.

Field Name	Type	Always present	Description
id	string	Yes	The short id of the test.
grade_ norm	string	Yes	The grade of the test.
title	string	Yes	The title of the test.
heading	string	Yes	The heading of the test.
server_ip	string	Yes	The IP address of the tested server.
city	string	Yes	The city of the tested server.
country	string	Yes	The country of the tested server
title_twitter	string	Yes	The official title of the test to be displayed on twitter.
description	string	Yes	A description of the free service.
description _twitter	string	Yes	The description of the free service to be displayed on twitter.
can_index	bool	Yes	Set to 'true' if the result can be indexed.
errors	integer	Yes	Contains the number of found errors.
scores	object	Yes	Contains information about the number of found issues concerning HTTP Headers, CSP, GDPR, PCI DSS and AppScan.

Example of the “scores” object:


```
{       "http_headers": {
         "description": "No Major issues Found", "class": "fs-bar-green" },
        "csp": {
         "description": "No Major issues Found", "class": "fs-bar-green" },
        "gdpr": {
         "fs_link": "#gdpr-section",
         "description": "No issues found",
         "class": "fs-bar-green"
       },
       "app_scan": { "description": "No Issues Found", "class": "fs-bar-
green" },
       "pci_dss": { "description": "1 issue found", "class": "fs-bar-orange" }
}
```

10. Third-Party Content

This section contains information concerning third-party content.

The structure is as follows:

Field Name	Type	Always present	Description
url	string	No	The URL of the third-party content.
method	string	No	Specifies the HTTP method used.
redirect_chain	array	No	Details the redirect chain.
resource_type	string	No	Indicates the resource type.
content_type	string	No	Indicates the content type.
status	integer	No	Indicates the response status code.
status_text	string	No	Details the response status.
size	integer	No	Indicates the size of the third-party content.
md5	string	No	Indicates the md5 hash.
sha256	string	No	Indicates the sha256 hash.
selector	string	No	Indicates the selector.
server	object	No	Contains information about the IP and port. Syntax: `{ "ip": "string", "port": "integer" }`
security	object	No	Contains information about the protocol. Syntax: `{ "protocol": "string" }`
headers	object	No	Contains information about received headers. Syntax: `{ "request": { "referer": "string", "user-agent": "string" }, "response": {} }` The "`response`" will be detailed later in the document.

10.1. Third-Party Content Headers Response

This section contains information on the “response” object from the Third-Party Content Headers.

Field Name	Type	Always present	Description
date	string	Yes	Indicates the date of receiving the response.
content-encoding	string	Yes	Details the content-encoding.
last-modified	string	Yes	Details when it was modified the last time.
alt-svc	string	No	Details the cf-ray header alt-svc header.
access-control-allow-origin	string	No	Details the access-control-allow-origin header.
age	string	No	Details the age of the content.
cf-cache-status	string	No	Details the cf-cache-status header.
cf-ray	string	No	Details the cf-ray header.
surrogate-key	string	No	Details the surrogate-key.
etag	string	No	Details the ETag header.
server	string	No	Contains details on the server.
vary	string	No	Details the vary header.
strict-transport-security	string	No	Details the strict-transport-security header.
x-cache	string	No	Details the x-cache header.
x-content-type-options	string	No	Details the x-content-type-options header.
x-xss-protection	string	No	Details the x-xss-protection header.
x-ton-expected-size	string	No	Details the x-ton-expected-size header.
expect-ct	string	No	Details on the expect-ct header.
content-type	string	No	Details the content type.
status	string	No	Details the response status code.
cache-control	string	No	Details the cache-control header.

x-hello-human	string	No	Details the x-hello-human header.
accept-ranges	string	No	Details the accept-ranges header.
timing-allow-origin	string	No	Details the timing-allow-origin header.
content-length	string	No	Details the content-length header.
link	string	No	Contains the link.
expires	string	No	Indicates the expiration date.
served-in-seconds	string	No	Details the served-in-seconds header.

Appendix 1: List of Message values

ID	Value
1	The Referrer header will be omitted entirely. No referrer information is sent along with requests.
2	This is the user agent's default behaviour if no policy is specified. The origin is sent as referrer to a-priori as-much-secure destination (HTTPS->HTTPS) but isn't sent to a less secure destination (HTTPS->HTTP). Only send the origin of the document as the referrer in all cases.
3	Send a full URL when performing a same-origin request, but only send the origin of the document for other cases.
4	A referrer will be sent for same-site origins, but cross-origin requests will contain no referrer information.
5	Only send the origin of the document as the referrer to a-priori as-much-secure destination (HTTPS->HTTPS), but don't send it to a less secure destination (HTTPS->HTTP).
6	Send a full URL when performing a same-origin request, only send the origin of the document to a-priori as-much-secure destination (HTTPS->HTTPS), and send no eader to a less secure destination (HTTPS->HTTP).
7	Send a full URL (stripped from parameters) when performing a same-origin or cross-origin request.
8	Unsafe-url policy will leak origins and paths from TLS-protected resources to insecure origins.

Appendix 2: List of Highlights values

ID	Value
1	No HTTP headers were sent by the server.
2	Some HTTP headers related to security and privacy are missing or misconfigured.
3	All the HTTP methods supported by the web server are properly configured.
4	All HTTP headers related to security and privacy are properly set and configured.
5	Some HTTP headers related to security or privacy may be missing or misconfigured.
6	Some HTTP headers related to security and privacy are missing or misconfigured.
7	No HTTP methods were sent by the server.
8	All the HTTP methods supported by the web server are properly configured.
9	Some potentially insecure HTTP methods supported by the web server require your attention.
10	Some insecure HTTP methods supported by the web server require your attention.
11	No cookies were sent by the web application.
12	All cookies sent by the web application have secure flags and attributes.
13	Some cookies may have missing secure flags or attributes.
14	Some cookies have missing secure flags or attributes.

Appendix 3: List of Header and Cookie Highlights values

ID	Value
1	The header is properly set
	Unsafe-url policy will leak origins and paths from TLS-protected resources to insecure origins
2	This header is deprecated and will not work in modern browsers. Use Content-SecurityPolicy HTTP header instead
3	Content-Security Policy is enforced
4	This directive should have a value
5	The header contains empty directive(s) that should have a value
6	The header contains unknown directive(s)
7	The header contains unknown value(s)
8	The directive is not expected to have a value
9	The header contains directive(s) that have a value while they should not
10	The header is properly set
11	The directive is expected to have a single value
12	The header contains directive(s) that have several values while only one was expected
13	Some directives have an unknown value
14	Some directives have an invalid value
15	Some directives have value considered as unsafe
16	Some directives have values that are too permissive, like wildcards
17	Some values were not recognized
18	Header max-age value is short
19	The header is properly set. Any dangerous XSS content will be escaped.
20	Report URL does not seem to be valid
21	The header contains unknown value(s)
22	The XSS Protection is disabled, even if it's enabled in the client's browser
23	This directive will be ignored as protection is disabled
24	Allow-From directive contains an invalid URL
25	Allow-From directive must be followed by one URL
26	X-AspNet-Version header advertises the ASP.Net version running on the server

27	Webserver does not send detailed information about its ASP.NET version
28	Webserver does not send detailed information about its version
29	The header contains duplicate directive(s)
30	The header is disabled due to max-age value
31	The header contains directive(s) that have a value while they should not
32	Unknown directive
33	This directive is mandatory and is missing. Header must be ignored by browsers
34	Mandatory directive is missing
35	Because of a syntax error, header must be ignored by browsers
36	A cookie must start with the following: 'name=value'. The cookie must be ignored.
37	A cookie must start with the following: 'name=value’
38	The cookie name is empty, the cookie must be ignored
39	Some values do not have attribute name associated.
40	The value does not have attribute name associated
41	Some values are invalid.
42	The attribute is expected to have a value.
43	Some attributes are set twice
44	The value should be a domain name
45	The cookie has an invalid path
46	The path is invalid, browsers will use default path instead
47	The value enables CSRF protection when using every HTTP Methods
48	The value is unknown, enforcing Strict policy for SameSite attribute
49	The cookie contains unknown attributes
50	The attribute is unknown
51	The cookie has the Secure flag set and will only be sent over a secure connection
52	The cookie name contains the __Secure- prefix, making sure it can't be altered using non secure protocols
53	The cookie name contains the __Secure- prefix but has been set using HTTP, it will be ignored
54	The cookie name contains the __Secure- prefix but does not have the secure flag set, it will be ignored
55	The cookie name contains the __Host- prefix, making impossible to alter it from subdomains
56	The cookie name contains the __Host- prefix but does not have the secureflag set, it will be ignored

57	The cookie has the Secure flag set and will only be sent over a secure connection
58	The cookie name contains the __Host- prefix but does have the domain flag set, it will be ignored
59	The cookie name contains the __Host- prefix but does not have the path flag set to /, it will be ignored
60	The cookie has neither Secure nor HttpOnly flags set, make sure it does not store sensitive information
61	The cookie has the following attributes set: Secure attribute; HttpOnly attribute

Appendix 4: List of Error messages

error_id	error
0	Unknown error. Please contact us.
1	You have performed [N] [ACTIONS] in the last 3 minutes. Please try again a bit later.
2	You have performed [N] [ACTIONS] in the last 24 hours. But premium API to run more tests.
3	Sorry, our systems are very busy now. Please try again in a few minutes.
4	You have running [N] concurrent [ACTIONS]. Please try again a bit later.
5	Sorry, there is a problem with your API key. Please double-check it or contact us.
6	Test is forbidden. Please contact us.
7	The domain name cannot be resolved. Please double-check it or contact us.
9	The domain name does not exist. Please double-check it or contact us.
10	An error has occured while checking DNS records of domain. Please double-check it or contact us.
11	Invalid IP address. Please double-check
12	Error with token. Our API has changed, please double-check it or contact us.
13	We could not conduct the requested test because a timeout occurred.
14	Arbitrary error from the engine.
16	Domain name was resolved in an invalid IP address.
17	An error occurred while encoding results.
18	Test does not exist.
19	PDF rendering problem has occurred.
20	Please register to [ACTION]
21	Your API key has exceeded the action-per-time limits. Please wait or contact us

	to increase the limits.
22	Your API key has expired. Please contact us to get a new one.
23	Your API key has been issued for another service.
24	Your API key does not exist.
25	Access denied for [IP].