High -Tech Bridge's Web Server Security Service

API Developer Documentation

Version v1.6

August 7th 2018

General Overview

API Documentation and How-To

API Specifications

Field Name	Value
Protocol	HTTP/HTTPS
Request Type	GET
URL	https://www.htbridge.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	"true" will not show the result in the Recent tests
recheck	"false" will use results from cache if the server has been tested within the past 30 days, "true" will perform a new test without looking at the cache.
follow_redirects	"true" will allow the following of redirections.
token	value of the token sent by the server if the tested domain is resolved into several IP addresses.

Example of Transactions using CURL

 # New test (not cached)

$ curl -XPOST -d 'tested_url=twitter.com&choosen_ip=any&dnsr=off&recheck=false&follow_redirects=true&verbosity=1' 'https://www.htbridge.com/websec/api/v1/chsec/1451425590.html'

{"debug":true,"job_id":"2a9e1f1bc92dc0c7a4bde930dff488771eea6d36988208d34163c5496227b8dc","status":"test_started","status_id":1,"message":"Test has started"}

 # You need to keep calling this until test is finished

$ curl -XPOST -d 'job_id=2a9e1f1bc92dc0c7a4bde930dff488771eea6d36988208d34163c5496227b8dc' 'https://www.htbridge.com/websec/api/v1/get_result/1451425590.html'

{"job_id":"2a9e1f1bc92dc0c7a4bde930dff488771eea6d36988208d34163c5496227b8dc","status":"in_progress","status_id":2,"eta":2,"message":"Your test is in progress"}

 # New test (cached)

$ curl -XPOST -d 'tested_url=twitter.com&choosen_ip=any&dnsr=off&recheck=false&follow_redirects=true&verbosity=1' 'https://www.htbridge.com/websec/api/v1/chsec/1451425590.html'

{"test_id":"c84936eef26eeb8aaef5ffc43f38ddb91adfd90ac27fb416bd0b21fe2edb1004","status":"test_cached","status_id":3,"message":"Test is cached"}

$ curl -XPOST -d 'job_id=c84936eef26eeb8aaef5ffc43f38ddb91adfd90ac27fb416bd0b21fe2edb1004' 'https://www.htbridge.com/websec/api/v1/get_result/1451425590.html'

 # Example with error

$ curl -XPOST -d 'tested_url=0.0.0.0&choosen_ip=any&dnsr=off&recheck=false&follow_redirects=true&verbosity=1' 'https://www.htbridge.com/websec/api/v1/chsec/1451425590.html'

The output array will be composed of the following main elements that will be detailed later in this document:

- **server_info:** containing basic server info, like IP, port, reverse DNS...
- **global_highlights**: a general overview of the test results, including the grade
- **http_cookies**: containing all information about returned cookies
- **http_headers**: containing all information about returned http headers
- **http_verbs**: containing all information about allowed http verbs

- **internals**: contains internal information such as city, country, server IP…
- **http_additional_info**: details if the server supports content_encoding, waf etc:
- **third_party_content**: containing all the third-party content
    - **protocol_negotiation:** contains information about npn and alpn
    - **content_encoding:** contains information about encoding of http content
    - **waf:** contains information about WAF presence
    - **sri:** contains information about subresource integrity
    - **blacklist**: contains list of all services listing hostname as spam or similar
    - **cryptojacking**: containing all detected cryptojacking scripts
    - **hosting_provider**: contains information about server hosting location
    - **dirlist**: containing some of detected directory listings enabled
    - **is_it_phishing**: containing lists that listed this domain as malware
    - **viewstate**: containing information about bad ViewState implementation

Meta-information

Global highlights is an array of text that holds a general overview of the test results. A returned integer will correspond to three highlights:

0 - All the HTTP methods supported by the web server are properly configured.

1 - Some HTTP headers related to security and privacy are missing or misconfigured.

2 - All cookies sent by the web application have secure flags and attributes.

The structure is as follows:

Syntax: [global_highlight: string, highlight: int]

HTTP Additional Info

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

Syntax:

{blacklist: [], protocol_negotiation: {npn: [string, protocol: string, alpn: bool, content_encoding: [string], waf: [] … }

"blacklist":

• Syntax: [string, string]

• Always present

• Description: array of servers that listed servers IP as spam

"content_encoding":

• Syntax: [string]

• Always present

• Description: the content encoding format

"protocol_negotiation":

• Syntax: { npn: [string, string], alpn: bool }

• Present if the server supports the next protocol negotiation extension

• Description: the protocol negotiation supported by the server

The following are boolean values represent the next protocol negotiation configuration present inside the protocol negotiation section

"npn"

• Syntax: [string, string, tag: bool]

• Present if the server supports the next protocol negotiation extension

• Description: values containing the protocol negotiation types

The following details the subresource integrity configuration.

"sri":

• Syntax: [{tag: string, calculated_hash: string, error: bool, hash_type: string, location: string, original_hash: string, original_html: string, suggested _html: string}]

• Always present

• Description: details of the subresource integrity configuration

The following is an array of details concerning the web application firewall

"waf":

• Syntax: string or []

• Present if the server has a web application firewall

• Description: details of a web application firewall implementation

The following is an array of details concerning the cryptojacking malware detection

"cryptojacking":

• Syntax: [{ 'url': string, 'ip': string, 'pattern': string, 'country': string, 'city': string, 'country_code': string}]

• Present if the server has a cryptojacking malware

• Description: details of a cryptojacking malware implementation

The following is an array of details concerning the directory listing enabled detection

"dirlist":

• Syntax: [string, string …] or []

• Present if the server has a directory listing enabled

• Description: details of a directory listing enabled implementation

The following is an array of details concerning the domain presence in phishing blacklists detection

"is_it_phishing":

• Syntax: [string, string …] or []

• Present if the server has a presence in phishing blacklists

• Description: details of a phishing blacklists detection implementation

The following is an array of details concerning the domain presence in hosting provider detection

"hosting_provider":

• Syntax: string or []

• Present if system detected where is server hosted

• Description: details of a hosting provider detection implementation

HTTP headers

This section lists the returned security related http headers and relevant information regarding them. It is composed of the following main subsections.

- **Content-Security-Policy**: implementation details of the observed content-security policy
- **Content-Security-Policy-Report-Only**: details of the observed content-security-policy-report-only header implementation
- **Public-Key-Pins:** details of the observed public-key-pins implementation
- **Public-Key-Pins-Report-Only**: details of the observed public-key-pins-report-only header implementation
- **Referrer-Policy:** details of the observed referrer-policy header
- **Server:** details of the observed server header implementation
- **Strict-Transport-Security:** details of the observed hsts implementation,
- **X-Content-Type-Options:** details of the observed x-content-type options header implementation
- **X-Frame-Options**: details of the observed x-frame-options header implementation
- **X-XSS-Protection**: details of the observed x-xss-protection header implementation
- **X-Powered-By**: details of the observed x-powered-by header implementation
- **X-AspNet-Version**: details of the observed x-aspnet-version header implementation
- **Access-Control-Allow-Origin**: details of the observed access-control-allow-origin header implementation
- **Expect-CT**: details of the observed expect-ct header implementation
- **Expect-Staple**: details of the observed expect-staple header implementation
- **Feature-Policy**: details of the observed feature-policy header implementation

The structure is as follows:

Syntax: {Server: { description: string } }

Description: each http header contains its own list that details its implementation details, such as directives and highlights.

Content-Security-Policy

This section is a list of content-security policy directive information. It contains the following sections:

block-all-mixed-content: contains detailed information regarding the returned block-all-mixed content directive.

colored-raw: a representation of the returned results

default-src: contains detailed information regarding the returned default-src directive

description: an overview of the content-security-policies purpose

highlight: an overview of the returned content-security-policies implementation

raw: the raw returned content-security-policy

report-uri: contains detailed information regarding the returned report-uri directive

The structure is as follows:

Syntax: {Server: { description: string }, directive: {string}}

Description: each directive has its own list with entries regarding implementation details and descriptions.

"block_all_mixed_content":

• Syntax: {description: string, tag: int}

• Present if this directive is present

• Description: set to 'true' if the 'block-all-mixed-content' directive is present

"colored_raw":

• Syntax: { description: string, tag: int}

• Always present

• Description: a representation of the returned results

"default-src":

• Syntax: [{value: string, description: string, tag: int}]

• Present if this directive is present

• Description: each found 'default-src' domain value will be populated with the appropriate message string. The description field will describe the directive.

"highlight":

• Syntax: [value: string, tag: int]

• Always present

• Description: A high-level overview of the implementation, each integer will correspond to a highlight of the implementation.

"report-uri":

• Syntax: { description: string, tag: int}

• Present if the 'report-uri' directive is present

• Description: the description field will describe the function of the directive.

Public-Key-Pins

This Public-Key-Pins section provides details on the returned public-key-pins implementation with all relevant directives. The structure is as follows:

Syntax: [colored_raw: { }, enforced: bool}, highlight: [bool], max-age: int, description: string pin-sha256:{}, description: string }

Description: the 'enforced' value will be set to 'true' if the header is present, with other values present in the list corresponding to directives.

"colored-raw":

• Syntax: [{ }]

• Always present

• Description: a representation of the returned results

"description":

• Syntax: {description: string}

• Present if public-key-pins is set

• Description: A general description of the Public-Key-Pins header

"enforced":

• Syntax: {tag: bool}

• Always present

• Description: Set to 'true' if the header is enforced

"highlight":

• Syntax: {value: string, tag: bool}

• Always present

• Description: A boolean value indicating is the header is correctly set

"max-age":

• Syntax: {value: string, description: string, tag: int}

• Present if the cookie has the 'max-age' attribute set

• Description: The max-age value will be returned if present

"pin-sha256":

• Syntax: {value: string, description: string, tag: int}

• Present if the cookie has the ''pin-sha256" attribute set

• Description: Implementation details of the returned 'pin-sha256' header

"report-uri":

• Syntax: { value: string, description: string, tag: int}

• Present if the cookie has the 'report-uri' attribute set

• Description: Implementation details of the returned 'report-uri' header

Referrer-Policy

This section is a list of details for the referrer-policy header, there is a string 'raw' that returns the raw header, and a highlight array will be returned detailing an overview of the implementation.

The structure is as follows:

{raw: string, colored-raw: [], description: string, highlight: [bool, raw: string], same-origin: string}

"colored-raw":

• Syntax: [ ]

• Always present

• Description: a representation of the returned results

"description":

• Syntax: string

• Always present

• Description: A high-level general description of the 'referrer-policy' header

"highlight":

• Syntax: [value: string, tag: bool]

• Always present

• Description: highlights details on the returned referrer-policy implementation.

"raw":

• Syntax: string

• Present if the referrer-policy header is set

• Description: The returned raw 'referrer-policy' header

"same-origin":

• Syntax: string

• Present if the referrer-policy has the 'same-origin' directive

• Description: This is returned if the 'same-origin' directive is present

Server

This section is a list of details for the server header, the structure is as follows:

This section is a list of details for the referrer-policy header, there is a string 'raw' that returns the raw header, and a highlight array will be returned detailing an overview of the implementation.

The structure is as follows:

{description: "String", highlight: bool, raw: string }

"description":

• Syntax: string

• Always present

• Description: A high-level general description of the 'server' header

"highlight":

• Syntax: [value: string, bool, raw: string]

• Present if the header is set

• Description: highlights details on the server header implementation

"raw":

• Syntax: string

• Always present

• Description: The returned raw server header

Strict-Transport-Security

This section is a list of details for the strict-transport-security header. 'Enforced' will be set to 'true' if the header is present. The list will contain values populated by the observed strict-transport security implementation. The structure is as follows:

{raw: string, enforced: bool highlight: [bool], includeSubdomains: {description: string
max-age: string, description: string}, preload: {description: string}}

"raw":

• Syntax: string

• Always present

• Description: The returned raw strict transport security header directives

"colored-raw":

• Syntax: []

• Always present

• Description: a representation of the returned results

"description":

• Syntax: string

• Always present

• Description: A high-level general description of the 'strict-transport-security' header

"enforced":

• Syntax: bool

• Always present

• Description: set to 'true' if the header is present

"highlight":

• Syntax: [value: string, tag: bool]

• Present if the header is set

• Description: highlights details on the strict-transport-security implementation

"includeSubdomains":

• Syntax: {description: string, tag: int}

• Present if the 'includeSubdomains' directive is set

• Description: A high-level general description of the 'includeSubdomains' directive

"max-age":

• Syntax: {value: int, description: string, tag: int}

• Present if the 'max-age' directive is set

• Description: A high-level general description of the 'max-age' directive

"preload":

• Syntax: {description: string, tag: int}

• Present if the 'preload' directive is set

• Description: A high-level general description of the 'preload' directive

X-Content-Type-Options

This section is a list of details for the x-content-type options header, the structure is as follows:

{raw: "String", highlight: [string]}

"description":

• Syntax: { value: string, tag: int}

• Always present

• Description: A high-level general description of the 'x-content-type-options' header

"highlight":

• Syntax: [value: string, tag: bool]

• Always present

• Description: Indicates whether the 'x-content-type-options' header is correctly set

"nosniff":

• Syntax: string

• Present if the 'nosniff' directive is present

• Description: A high-level general description of the 'nosniff' directive

"raw":

• Syntax: string

• Present if the 'x-content-type options' header is set

• Description: The returned raw 'x-content-type-options' header

X-Frame-Options

This section is a list of details for the x-fame-options header, the structure is as follows

{raw: "String", highlight: [string], colored-raw: []}

"description":

• Syntax: string

• Present if the 'x-frame-options' header is set

• Description: A high-level general description of the 'x-frame-options' header

"colored-raw":

• Syntax: []

• Always present

• Description: a representation of the returned results

"highlight":

• Syntax: [string]

• Always present

• Description: Indicates whether the 'x-frame-options' header is correctly set

"raw":

• Syntax: string

• Always present

• Description: The returned raw 'x-frame-options' header

X-XSS-Protection

This section is a list of details for the x-xss-protection header, a value of '1' indicates that the directive is correctly informing the browser to implement heuristic protection. The structure is as follows:

{raw: string, highlight: string, 1: string, colored_raw: [], description: string, highlight: [string], mode=block: string}

"description":

• Syntax: string

• Present if the 'x-xss-protection' header is set

• Description: A high-level general description of the 'x-xss-protection' directive

"colored-raw":

• Syntax: []

• Always present

• Description: a representation of the returned results

"highlight":

• Syntax: [string]

• Always Present

• Description: Indicates whether the 'x-xss-protection' header is correctly set

"mode=block":

• Syntax: string

• Present if the 'mode=block' directive is set

• Description: A general high-level description of the 'mode=block' directive.

"raw":

• Syntax: string

• Always present

• Description: The returned raw 'x-xss-protection' header

Expect-CT

This section is a list of details for the expect-ct header. Expect-CT allows a site to determine if they are ready for the upcoming Chrome requirements and/or enforce their CT policy. The structure is as follows:

{raw: string, highlight: string, colored_raw: [], description: string, highlight: [string]}

"description":

• Syntax: string

• Present if the ‘expect-ct’ header is set

• Description: A high-level general description of the 'expect-ct' header

"colored-raw":

• Syntax: []

• Always present

• Description: a representation of the returned results

"highlight":

• Syntax: [string]

• Always Present

• Description: Indicates whether the 'expect-ct' header is correctly set

"raw":

• Syntax: string

• Always present

• Description: The returned raw 'expect-ct' header

Expect-Staple

This section is a list of details for the expect-staple header. Expect-Staple allows a site to determine if they are ready for the upcoming Chrome requirements and/or enforce their OCSP policy. The structure is as follows:

{raw: string, highlight: string, colored_raw: [], description: string, highlight: [string]}

"description":

• Syntax: string

• Present if the 'expect-staple' header is set

• Description: A high-level general description of the 'expect-staple' header

"colored-raw":

• Syntax: []

• Always present

• Description: a representation of the returned results

"highlight":

• Syntax: [string]

• Always Present

• Description: Indicates whether the 'expect-staple' header is correctly set

"raw":

• Syntax: string

• Always present

• Description: The returned raw 'expect-staple' header

Feature-Policy

This section is a list of details for the feature-policy header. 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.). The structure is as follows:

{raw: string, highlight: string, colored_raw: [], description: string, highlight: [string]}

"description":

• Syntax: string

• Present if the 'feature-policy' header is set

• Description: A high-level general description of the 'feature-policy' header

"colored-raw":

• Syntax: []

• Always present

• Description: a representation of the returned results

"highlight":

• Syntax: [string]

• Always Present

• Description: Indicates whether the 'feature-policy' header is correctly set

"raw":

• Syntax: string

• Always present

• Description: The returned raw 'feature-policy' header

HTTP verbs

This section details the servers allowed http verbs.

"GET":

• Syntax: string

• Always present

• Description: A general high-level description of the 'GET' http verb

"POST":

• Syntax: string

• Always present

• Description: A general high-level description of the 'POST' http verb

"HEAD":

• Syntax: string

• Present if the 'HEAD' http verb is supported

• Description: A general high-level description of the 'HEAD' http verb

"OPTIONS":

• Syntax: string

• Present if the 'OPTIONS' http verb is supported

• Description: A general high-level description of the 'POST' http verb

"TRACE":

• Syntax: string

• Present if the 'TRACE' http verb is supported

• Description: A general high-level description of the 'TRACE' http verb

"TRACK":

• Syntax: string

• Present if the 'TRACK' http verb is supported

• Description: A general high-level description of the 'TRACK' http verb

"PUT":

• Syntax: string

• Present if the 'PUT' http verb is supported

• Description: A general high-level description of the 'PUT' http verb

"CONNECT":

• Syntax: string

• Present if the 'CONNECT' http verb is supported

• Description: A general high-level description of the 'CONNECT' http verb

"PATCH":

• Syntax: string

• Present if the 'PATCH' http verb is supported

• Description: A general high-level description of the 'PATCH' http verb

"DELETE":

• Syntax: string

• Present if the 'DELETE' http verb is supported

• Description: A general high-level description of the 'DELETE' http verb

HTTP cookies

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

Syntax: [{colored_raw: [{}] domain: {description: string, value: string}, highlight: bool, httponly: {description: string, value: string}, max_age {description: string, value: string}, path: {description: string, value: string}, secure: {description: string, value: string}]

Description: the boolean values represent different states of attributes, the description field provides information on the attribute, and the value field displays the set value of the attribute.

"colored-raw":

• Syntax: {description: string, tag: int}

• Always present

• Description: a representation of the returned results

"domain":

• Syntax: {value: string, tag: int}

• Present if the domain attribute is set

• Description: the 'domain' attribute returned from the cookie

"expires":

• Syntax: { description: string, value: string, tag: int}

• Always present

• Description: the 'expires' attribute returned from the cookie

"highlight":

• Syntax: { value: string, tag: int}

• Always present

• Description: Set to 0 if the cookie has the 'Secure' and 'HttpOnly' attributes set

"httponly":

• Syntax: { description: string, value: string, tag: int}

• Present if the cookie has the 'httponly' attribute set

• Description: Set to true if the 'httponly' flag is present

"max-age":

• Syntax: { description: string, value: string, tag: int}

• Present if the cookie has the 'max-age' attribute set

• Description: the 'max-age' attribute returned from the cookie

"path":

• Syntax: { description: string, value: string, tag: int}

• Present if the cookie has the 'path' attribute set

• Description: the 'path' attribute returned from the cookie

"secure":

• Syntax: { description: string, value: string, tag: int}

• Present if the cookie has the 'secure' attribute set

• Description: the 'secure' attribute returned from the cookie

Internals

This section details internal details.

"alternate_url":

• Syntax: string

• Always present

• Description: A high-level general description of the 'x-xss-protection' directive

"can_index":

• Syntax: bool

• Always present

• Description: Set to 'true' if the result can be indexed

"city":

• Syntax: string

• Always present

• Description: the city of the tested service

"country":

• Syntax: string

• Always present

• Description: the country of the tested server

"description":

• Syntax: string

• Always present

• Description: A description of the free service

"description_twitter":

• Syntax: string

• Always present

• Description: A description of the twitter results

"grade_norm":

• Syntax: string

• Always present

• Description: the grade of the test

"landing_url":

• Syntax: string

• Always present

• Description: the landing url

"server_ip":

• Syntax: string

• Always present

• Description: the IP address of the tested server

"title":

• Syntax: string

• Always present

• Description: the official title of the test

"title_twitter":

• Syntax: string

• Always present

• Description: the official title of the test to be displayed on twitter

Error Handling

Possible error messages which system can return are:

The domain name cannot be resolved.
An error has occurred while checking DNS records of domain.
Invalid IP address.
Error with token. Our API has changed, please take look at documentation.
API key is not valid. Please double check it.
You have performed N tests in the last 3 minutes. The system is currently busy, please try again later.
You have performed N tests in the last 24 hours. The system is currently busy, please try again later.
System is very busy now, please try again later.

You reached the limit of N total running tests. Wait for one to finish, then retry.

An error occured while testing server configuration, server become unreachable during the test.

Appendix 1: List of Messages values

ID	Value
1	The Referer 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 header 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 3: List of Descriptions values

ID	Value
1	Sets the URI that browsers should use as the base URI
2	Forces browsers to block HTTP content in an HTTPS page
3	Sets the list of sources that can be included in frames or iframes
4	Sets the list of servers that browsers are allowed to connect to, for instance with WebSockets
5	Sets the list of sources where browsers are allowed to get every resource from, if not specified in another directive
6	Ensures that a resource will disown its opener when navigated to

7	Sets the list of sources where browsers are allowed to get fonts from
8	Sets the list of destinations where browsers are allowed to submit forms to
9	Sets the list of domains that are allowed to include this website into a frame or an iframe
10	Deprecated and replaced by child-src. Sets the list of sources that can be included in frames or iframes
11	Sets the list of sources where browsers are allowed to get images from
12	Sets the list of sources where browsers are allowed to get application manifest from
13	Sets the list of sources where browsers are allowed to get media from, such as videos, audio...
14	Sets the list of sources where browsers are allowed to get plugin content from
15	Sets the list of plugins that browsers can use for this website
16	Forces browsers what to send in Referer HTTP header
17	Similar to X-XSS-Protection header, forces browsers to enable or disable heuristic XSS protection
18	Sets the URL where browsers will report any violation to the policy
19	Sets which group should be used to report violations to
20	Instructs the client to require the use of Subresource Integrity for scripts or styles on the page
21	Forces browsers to enable or disable some sandboxing features
22	Sets the list of sources where browsers are allowed to get scripts from
23	Sets the list of sources where browsers are allowed to get style sheets from
24	Forces browsers to use HTTPS to download every resources
25	Sets the list of sources where browsers can load as worker
26	Forces browsers not to send Referer header
27	Forces browsers not to send Referer header when downgrading from HTTPS to HTTP
28	Forces browsers to only send hostname in Referer header
29	Forces browsers to only send hostname in Referer header when switching to another website
30	Forces browsers to send hostname and webpage in Referer header
31	Forces browsers to disable heuristic protection against reflected XSS attacks
32	Forces browsers to block server's response when heuristic protection detects an XSS
33	Forces browsers to filter XSS payload from server's response when detected by heuristic protection. This can introduce vulnerabilities
34	Instructs the client to require the use of Subresource Integrity verifiction for externally loaded scripts
35	Instructs the client to require the use of Subresource Integrity verifiction for externally loaded stylesheets
36	Allows browsers to submit forms that are contained in the page
37	Allows the page to access data, like cookies stored from the same origin
38	Allows browsers to execute scripts from the page
39	Allows content to access data, like cookies, set by the top-level context
40	Allows content to access the Pointer Lock API to interact with the mouse pointer
41	Allows content to spawn popups
42	Allows browsers to execute unsafe inline scripts
43	Allows browsers to execute unsafe JavaScript eval() function
44	Allows browsers to execute scripts that are dynamically loaded from other scripts
45	Allows browsers to execute inline scripts specified by following sha256 directives without

	allowing all inline scripts
46	Used to allow browsers developers to hardcode enforcement of usage of HTTPS only for this website
47	Used to enforce the use of HTTPS on subdomains of your website
48	Sets the time browsers must enforce the use of HTTPS to browse the website
49	Sets the time browsers must record the allowed pins
50	Sets the pins that browsers must record
51	Used to record the same pins for other subdomains of your website
52	Sets a URL where browsers should submit any mismatch between pins and certificate chain
53	HTTP-Strict-Transport-Security (HSTS) header forces browsers to browse the website in HTTPS
54	HTTP-Public-Key-Pinning (HPKP) header prevents Man-In-The-Middle attacks against the website by whitelisting allowed certificates in the trust chain
55	X-Frame-Options header specifies whether the website should allow itself to be framed, and from which origin.
56	Blocking framing helps defend against attacks such as Clickjacking
57	X-XSS-Protection defines how browsers should enforce cross-site scripting protection
58	X-Content-Type-Options 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.
59	Content-Security-Policy (CSP) allows the definition of allowed sources for each type of content, helping to defend against XSS attacks. It also allows the ability to define several browser behaviors, such as sandbox enforcement, to the value to be sent in the HTTP Referer header
60	HTTP-Public-Key-Pinning (HPKP) header prevents Man-In-The-Middle attacks against the website by whitelisting allowed certificates in trust chain. Report-Only allows for testing without enforcement meaning that your website will remain reachable if HPKP is not correctly configured
61	Content-Security-Policy (CSP) allows to define allowed sources for each type of content, helping to defend against XSS attacks for example. It also allows to define several browsers behaviors, like sandbox enforcement, or value to send in Referer HTTP header. Report-Only allows for testing without enforcement meaning that your website will remain reachable if the header is incorrectly configured
62	Referrer-Policy HTTP header governs which referrer information, sent in the Referer header, should be included with requests made
63	Sets the maximum lifetime of the cookie using a date
64	Sets the maximum lifetime of the cookie using a time in seconds
65	Sets the domains where browsers should send this cookie too
66	Sets the path of the application where the cookie should be sent
67	Prevents browsers to send the cookie over an insecure connection
68	The attribute is not expected to have a value
69	Prevents client-side scripts from accessing the cookie value.
70	Prevents client-side scripts to access the cookie by telling browsers to only transmit the

	cookie over HTTP(S)
71	The SameSite attribute helps mitigating CSRF attacks
72	Prevents CSRF attacks by not sending the cookies when the request comes from another website.
73	The value disables protection when using potentially read-only HTTP methods like GET
74	The value enables CSRF protection when using every HTTP Methods
75	The __Host- prefix disables the ability to alter the cookie
76	Disables browser ability to detect content type by analyzing it and allows to prevent XSS for example
77	Forces browsers to enable heuristic protection against reflected XSS attacks
78	Forces browsers to block server's response when heuristic protection detects an XSS
79	Sets an URL where browsers can report detected XSS
80	Forces browsers to disable heuristic protection against reflected XSS attacks. Make sure your web application is XSS free
81	Disables client-side protection
All cookies sent by the web application have secure flags and attributes	
Test results are over one-week-old, click "Refresh" to update the results	

Appendix 4: List of Global 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 and 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 5: List of 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-Security-Policy 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
	The header value is invalid
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 has the Secure flag set and will only be sent over a secure connection
56	The cookie name contains the __Host- prefix, making impossible to alter it from subdomains
57	The cookie name contains the __Host- prefix but does not have the secure flag set, it will be ignored
58	The cookie has the Secure flag set and will only be sent over a secure connection
59	The cookie name contains the __Host- prefix but does have the domain flag set, it will be ignored
60	The cookie name contains the __Host- prefix but does not have the path flag set to /, it will be ignored
61	The cookie has neither Secure nor HttpOnly flags set, make sure it does not store sensitive information
62	The cookie has the following attributes set: Secure attribute; HttpOnly attribute