



PUBLIC

ImmuniWeb's  
WebScan API Documentation  
Version v2.0  
11<sup>th</sup> of April 2019

## Table of Contents

General Overview.....	3
Meta-information.....	5
HTTP Additional Info.....	5
HTTP headers.....	8
Content-Security-Policy.....	8
X-Powered-By.....	10
X-AspNet-Version.....	11
Content-Security-Policy-Report-Only.....	11
Access-Control-Allow Origin.....	12
Public-Key-Pins-Report-Only.....	13
Server.....	13
Strict-Transport-Security.....	14
X-Content-Type-Options.....	16
X-Frame-Options.....	16
X-XSS-Protection.....	17
Expect-CT.....	18
Expect-Staple.....	19
Feature-Policy.....	20
HTTP verbs.....	21
HTTP cookies.....	23
Internals.....	24
Error Handling.....	26
Appendix 1: List of Messages values.....	27
Appendix 3: List of Descriptions values.....	28
Appendix 4: List of Global Highlights values.....	31
Appendix 5: List of Highlights values.....	31
Appendix 6: List of Errors.....	34

## General Overview

### API Documentation and How-To

#### API Specifications

Field Name	Value
<b>Protocol</b>	HTTP/HTTPS
<b>Request Type</b>	GET
<b>URL</b>	<a href="https://www.immuniweb.com/websec/api/v1/get_result/[ustamp].html">https://www.immuniweb.com/websec/api/v1/get_result/[ustamp].html</a> - 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
<b>tested_url</b>	the URL of the domain to be tested.
<b>dnssr</b>	"true" will not show the result in the Recent tests
<b>recheck</b>	"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.
<b>follow_redirects</b>	"true" will allow the following of redirections.
<b>token</b>	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&chosen_ip=any&dnssr=off&recheck=false&follow_redirects=true&verbosity=1'
'https://www.immuniweb.com/websec/api/v1/chsec/1451425590.html'
{"debug":true,"job_id":"2a9e1f1bc92dc0c7a4bde930dff488771eea6d36988208d34163c5496227b8d c","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=2a9e1f1bc92dc0c7a4bde930dff488771eea6d36988208d34163c5496227
b8dc' 'https://www.immuniweb.com/websec/api/v1/get\_result/1451425590.html'
{"job_id":"2a9e1f1bc92dc0c7a4bde930dff488771eea6d36988208d34163c54962
27b8dc","status":"i n_progress","status_id":2,"eta":2,"message":"Your test is in
progress"}
```

**# New test (cached)**

```
$ curl -XPOST -d
'tested_url=twitter.com&chosen_ip=any&dnssr=off&recheck=false&follow_redir
ects=true&verbosity=1'
'https://www.immuniweb.com/websec/api/v1/chsec/1451425590.html'

{"test_id":"c84936eef26eeb8aaef5ffc43f38ddb91adfd90ac27fb416bd0b21fe2edb
1004","status":"tes t_cached","status_id":3,"message":"Test is cached"}
```

```
$ curl -XPOST -d
'job_id=c84936eef26eeb8aaef5ffc43f38ddb91adfd90ac27fb416bd0b21fe2edb10
04'
'https://www.immuniweb.com/websec/api/v1/get\_result/1451425590.html'
```

**# Example with error**

```
$ curl -XPOST -d
'tested_url=0.0.0.0&chosen_ip=any&dnssr=off&recheck=false&follow_redirects
=true&verbosity=1'
'https://www.immuniweb.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:

- 1- All the HTTP methods supported by the web server are properly configured.
- 2- Some HTTP headers related to security and privacy are missing or misconfigured.
- 3- 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-reportonly 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.

**X-Powered-By**

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

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

**"description":**

- Syntax: string
- Present if the 'x-powered-by' header is set
- Description: A high-level general description of the 'x-powered-by' header

**"highlight":**

- Syntax: [ value: string, bool, raw: string ]
- Always present
- Description: highlight details on the header implementation

**"raw":**

- Syntax: string
- Always present
- Description: The returned raw 'x-powered-by' header

### **X-AspNet-Version**

This section is a list of details for the 'x-aspnet-version' header. The structure is as follows:

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

#### **"highlight":**

- Syntax: [ value: string, bool, raw: string]
- Always present
- Description: highlights details on the header implementation

#### **"description":**

- Syntax: string
- Always present
- Description: a general description of the 'x-aspnet-version' header.

#### **"raw":**

- Syntax: string
- Always present
- Description: The returned raw 'x-aspnet-version' header

### **Content-Security-Policy-Report-Only**

This section is a list of details for the content-security-policy report-only header. The structure is as follows:

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

#### **"highlight":**

- Syntax: [ value: string, bool, raw: string]
- Always present
- Description: highlights details on the header implementation

**"description":**

- Syntax: string
- Always present
- Description: a general description of the 'content-security-policy-report-only' header.

**"raw":**

- Syntax: string
- Always present
- Description: The returned raw 'content-security-policy-report-only' header

**Access-Control-Allow Origin**

Details the CORS response headers 'Access-Control-Allow Origin' implementation. The structure is as follows:

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

**"highlight":**

- Syntax: [ value: string, bool, raw: string]
- Always present
- Description: highlights details on the header implementation

**"description":**

- Syntax: string
- Always present
- Description: a general description of the 'Access-Control-Allow Origin' header.

**"raw":**

- Syntax: string
- Always present
- Description: The returned raw 'Access-Control-Allow Origin' header

### **Public-Key-Pins-Report-Only**

This section is a list of details for the 'public-key-pins-report-only' header. The structure is as follows:

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

#### **"highlight":**

- Syntax: [ value: string, bool, raw: string]
- Always present
- Description: highlights details on the header implementation.

#### **"description":**

- Syntax: string
- Always present
- Description: a general description of the 'public-key-pins-report-only' header.

#### **"raw":**

- Syntax: string
- Always present
- Description: The returned raw 'public-key-pins-report-only' header.

### **Server**

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



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

**"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-row":**

- 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
<b>1</b>	Sets the URI that browsers should use as the base URI
<b>2</b>	Forces browsers to block HTTP content in an HTTPS page
<b>3</b>	Sets the list of sources that can be included in frames or iframes
<b>4</b>	Sets the list of servers that browsers are allowed to connect to, for instance with WebSockets
<b>5</b>	Sets the list of sources where browsers are allowed to get every resource from, if not specified in another directive
<b>6</b>	Ensures that a resource will disown its opener when navigated to
<b>7</b>	Sets the list of sources where browsers are allowed to get fonts from
<b>8</b>	Sets the list of destinations where browsers are allowed to submit forms to
<b>9</b>	Sets the list of domains that are allowed to include this website into a frame or an iframe
<b>10</b>	Deprecated and replaced by child-src. Sets the list of sources that can be included in frames or iframes
<b>11</b>	Sets the list of sources where browsers are allowed to get images from
<b>12</b>	Sets the list of sources where browsers are allowed to get application manifest from
<b>13</b>	Sets the list of sources where browsers are allowed to get media from, such as videos, audio...
<b>14</b>	Sets the list of sources where browsers are allowed to get plugin content from
<b>15</b>	Sets the list of plugins that browsers can use for this website
<b>16</b>	Forces browsers what to send in Referer HTTP header
<b>17</b>	Similar to X-XSS-Protection header, forces browsers to enable or disable heuristic XSS protection
<b>18</b>	Sets the URL where browsers will report any violation to the policy
<b>19</b>	Sets which group should be used to report violations to
<b>20</b>	Instructs the client to require the use of Subresource Integrity for scripts or styles on the page
<b>21</b>	Forces browsers to enable or disable some sandboxing features
<b>22</b>	Sets the list of sources where browsers are allowed to get scripts from
<b>23</b>	Sets the list of sources where browsers are allowed to get style sheets from
<b>24</b>	Forces browsers to use HTTPS to download every resources
<b>25</b>	Sets the list of sources where browsers can load as worker
<b>26</b>	Forces browsers not to send Referer header
<b>27</b>	Forces browsers not to send Referer header when downgrading from HTTPS to HTTP
<b>28</b>	Forces browsers to only send hostname in Referer header
<b>29</b>	Forces browsers to only send hostname in Referer header when switching to another website

<b>30</b>	Forces browsers to send hostname and webpage in Referer header
<b>31</b>	Forces browsers to disable heuristic protection against reflected XSS attacks
<b>32</b>	Forces browsers to block server's response when heuristic protection detects an XSS
<b>33</b>	Forces browsers to filter XSS payload from server's response when detected by heuristic protection. This can introduce vulnerabilities
<b>34</b>	Instructs the client to require the use of Subresource Integrity verification for externally loaded scripts
<b>35</b>	Instructs the client to require the use of Subresource Integrity verification for externally loaded stylesheets
<b>36</b>	Allows browsers to submit forms that are contained in the page
<b>37</b>	Allows the page to access data, like cookies stored from the same origin
<b>38</b>	Allows browsers to execute scripts from the page
<b>39</b>	Allows content to access data, like cookies, set by the top-level context
<b>40</b>	Allows content to access the Pointer Lock API to interact with the mouse pointer
<b>41</b>	Allows content to spawn popups
<b>42</b>	Allows browsers to execute unsafe inline scripts
<b>43</b>	Allows browsers to execute unsafe JavaScript eval() function
<b>44</b>	Allows browsers to execute scripts that are dynamically loaded from other scripts
<b>45</b>	Allows browsers to execute inline scripts specified by following sha256 directives without

	allowing all inline scripts
<b>46</b>	Used to allow browsers developers to hardcode enforcement of usage of HTTPS only for this website
<b>47</b>	Used to enforce the use of HTTPS on subdomains of your website
<b>48</b>	Sets the time browsers must enforce the use of HTTPS to browse the website
<b>49</b>	Sets the time browsers must record the allowed pins
<b>50</b>	Sets the pins that browsers must record
<b>51</b>	Used to record the same pins for other subdomains of your website
<b>52</b>	Sets a URL where browsers should submit any mismatch between pins and certificate chain
<b>53</b>	HTTP-Strict-Transport-Security (HSTS) header forces browsers to browse the website in HTTPS
<b>54</b>	HTTP-Public-Key-Pinning (HPKP) header prevents Man-In-The-Middle attacks against the website by whitelisting allowed certificates in the trust chain
<b>55</b>	X-Frame-Options header specifies whether the website should allow itself to be framed, and from which origin.
<b>56</b>	Blocking framing helps defend against attacks such as Clickjacking
<b>57</b>	X-XSS-Protection defines how browsers should enforce cross-site scripting protection

<b>58</b>	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.
<b>59</b>	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
<b>60</b>	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
<b>61</b>	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
<b>62</b>	Referrer-Policy HTTP header governs which referrer information, sent in the Referer header, should be included with requests made
<b>63</b>	Sets the maximum lifetime of the cookie using a date
<b>64</b>	Sets the maximum lifetime of the cookie using a time in seconds
<b>65</b>	Sets the domains where browsers should send this cookie too
<b>66</b>	Sets the path of the application where the cookie should be sent
<b>67</b>	Prevents browsers to send the cookie over an insecure connection
<b>68</b>	The attribute is not expected to have a value
<b>69</b>	Prevents client-side scripts from accessing the cookie value.
<b>70</b>	Prevents client-side scripts to access the cookie by telling browsers to only transmit the cookie over HTTP(S)
<b>71</b>	The SameSite attribute helps mitigating CSRF attacks
<b>72</b>	Prevents CSRF attacks by not sending the cookies when the request comes from another website.
<b>73</b>	The value disables protection when using potentially read-only HTTP methods like GET
<b>74</b>	The value enables CSRF protection when using every HTTP Methods
<b>75</b>	The __Host- prefix disables the ability to alter the cookie
<b>76</b>	Disables browser ability to detect content type by analyzing it and allows to prevent XSS for example
<b>77</b>	Forces browsers to enable heuristic protection against reflected XSS attacks
<b>78</b>	Forces browsers to block server's response when heuristic protection detects an XSS
<b>79</b>	Sets an URL where browsers can report detected XSS

<b>80</b>	Forces browsers to disable heuristic protection against reflected XSS attacks. Make sure your web application is XSS free
<b>81</b>	Disables client-side protection
<b>All cookies sent by the web application have secure flags and attributes</b>	
<b>Test results are over one-week-old, click "Refresh" to update the results</b>	

## Appendix 4: List of Global Highlights values

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

## Appendix 5: List of Highlights values

<b>ID</b>	<b>Value</b>
<b>1</b>	The header is properly set
	unsafe-url policy will leak origins and paths from TLS-protected resources to insecure origins
<b>2</b>	This header is deprecated and will not work in modern browsers. Use Content-SecurityPolicy HTTP header instead
<b>3</b>	Content-Security Policy is enforced
<b>4</b>	This directive should have a value
<b>5</b>	The header contains empty directive(s) that should have a value
	The header value is invalid
<b>6</b>	The header contains unknown directive(s)
<b>7</b>	The header contains unknown value(s)
<b>8</b>	The directive is not expected to have a value
<b>9</b>	The header contains directive(s) that have a value while they should not
<b>10</b>	The header is properly set
<b>11</b>	The directive is expected to have a single value
<b>12</b>	The header contains directive(s) that have several values while only one was expected
<b>13</b>	Some directives have an unknown value
<b>14</b>	Some directives have an invalid value
<b>15</b>	Some directives have value considered as unsafe
<b>16</b>	Some directives have values that are too permissive, like wildcards
<b>17</b>	Some values were not recognized
<b>18</b>	Header max-age value is short
<b>19</b>	The header is properly set. Any dangerous XSS content will be escaped.
<b>20</b>	Report URL does not seem to be valid
<b>21</b>	The header contains unknown value(s)
<b>22</b>	The XSS Protection is disabled, even if it's enabled in the client's browser
<b>23</b>	This directive will be ignored as protection is disabled
<b>24</b>	Allow-From directive contains an invalid URL
<b>25</b>	Allow-From directive must be followed by one URL
<b>26</b>	X-AspNet-Version header advertises the ASP.Net version running on the server
<b>27</b>	Webserver does not send detailed information about its ASP.NET version
<b>28</b>	Webserver does not send detailed information about its version
<b>29</b>	The header contains duplicate directive(s)
<b>30</b>	The header is disabled due to max-age value
<b>31</b>	The header contains directive(s) that have a value while they should not
<b>32</b>	Unknown directive
<b>33</b>	This directive is mandatory and is missing. Header must be ignored by browsers
<b>34</b>	Mandatory directive is missing
<b>35</b>	Because of a syntax error, header must be ignored by browsers
<b>36</b>	A cookie must start with the following: 'name=value'. The cookie must be ignored.



<b>37</b>	A cookie must start with the following: 'name=value
<b>38</b>	The cookie name is empty, the cookie must be ignored
<b>39</b>	Some values do not have attribute name associated.
<b>40</b>	The value does not have attribute name associated
<b>41</b>	Some values are invalid.
<b>42</b>	The attribute is expected to have a value.
<b>43</b>	Some attributes are set twice
<b>44</b>	The value should be a domain name
<b>45</b>	The cookie has an invalid path
<b>46</b>	The path is invalid, browsers will use default path instead
<b>47</b>	The value enables CSRF protection when using every HTTP Methods
<b>48</b>	The value is unknown, enforcing Strict policy for SameSite attribute
<b>49</b>	The cookie contains unknown attributes
<b>50</b>	The attribute is unknown
<b>51</b>	The cookie has the Secure flag set and will only be sent over a secure connection
<b>52</b>	The cookie name contains the __Secure- prefix, making sure it can't be altered using non secure protocols
<b>53</b>	The cookie name contains the __Secure- prefix but has been set using HTTP, it will be ignored
<b>54</b>	The cookie name contains the __Secure- prefix but does not have the secure flag set, it will be ignored
<b>55</b>	The cookie has the Secure flag set and will only be sent over a secure connection
<b>56</b>	The cookie name contains the __Host- prefix, making impossible to alter it from subdomains
<b>57</b>	The cookie name contains the __Host- prefix but does not have the secure flag set, it will be ignored
<b>58</b>	The cookie has the Secure flag set and will only be sent over a secure connection
<b>59</b>	The cookie name contains the __Host- prefix but does have the domain flag set, it will be ignored
<b>60</b>	The cookie name contains the __Host- prefix but does not have the path flag set to /, it will be ignored
<b>61</b>	The cookie has neither Secure nor HttpOnly flags set, make sure it does not store sensitive information
<b>62</b>	The cookie has the following attributes set: Secure attribute; HttpOnly attribute

## Appendix 6: List of Errors

<b>error_id</b>	<b>error</b>
<b>1</b>	You have performed N tests in the last 3 minutes. The system is currently busy, please try again a bit later.
<b>2</b>	You have performed N tests in the last 24 hours. The system is currently busy, please try again a bit later.
<b>3</b>	Sorry, our systems are very busy now, we are working on the issue. Please try again in a few minutes.
<b>4</b>	You reached the limit of N concurring running tests. Please wait until at least one of them is finished.
<b>5</b>	Sorry, your API key is invalid or has expired. Please double-check it or contact us.
<b>6</b>	Test is forbidden
<b>7</b>	The domain name cannot be resolved
<b>9</b>	The domain name does not exist
<b>10</b>	An error has occurred while checking DNS records of domain
<b>11</b>	Invalid IP address
<b>12</b>	Error with token. Our API has changed, please take look at documentation at <a href="https://www.immuniweb.com/websec/#api">https://www.immuniweb.com/websec/#api</a>
<b>13</b>	We could not conduct the requested test because a timeout occurred
<b>14</b>	Arbitrary error from engine
<b>16</b>	Domain name was resolved in an invalid IP address
<b>17</b>	An error occurred while encoding results
<b>18</b>	Test does not exist
<b>19</b>	Too many downloads of PDF
<b>20</b>	Not logged in