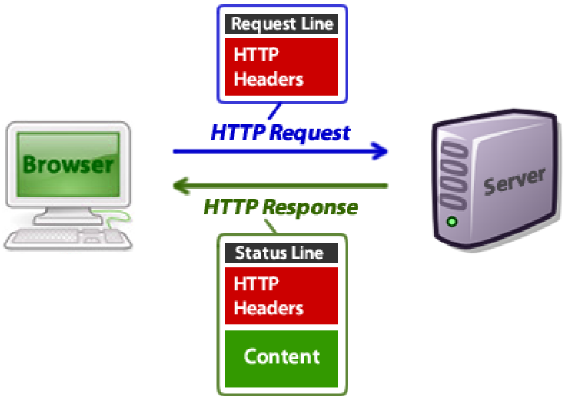
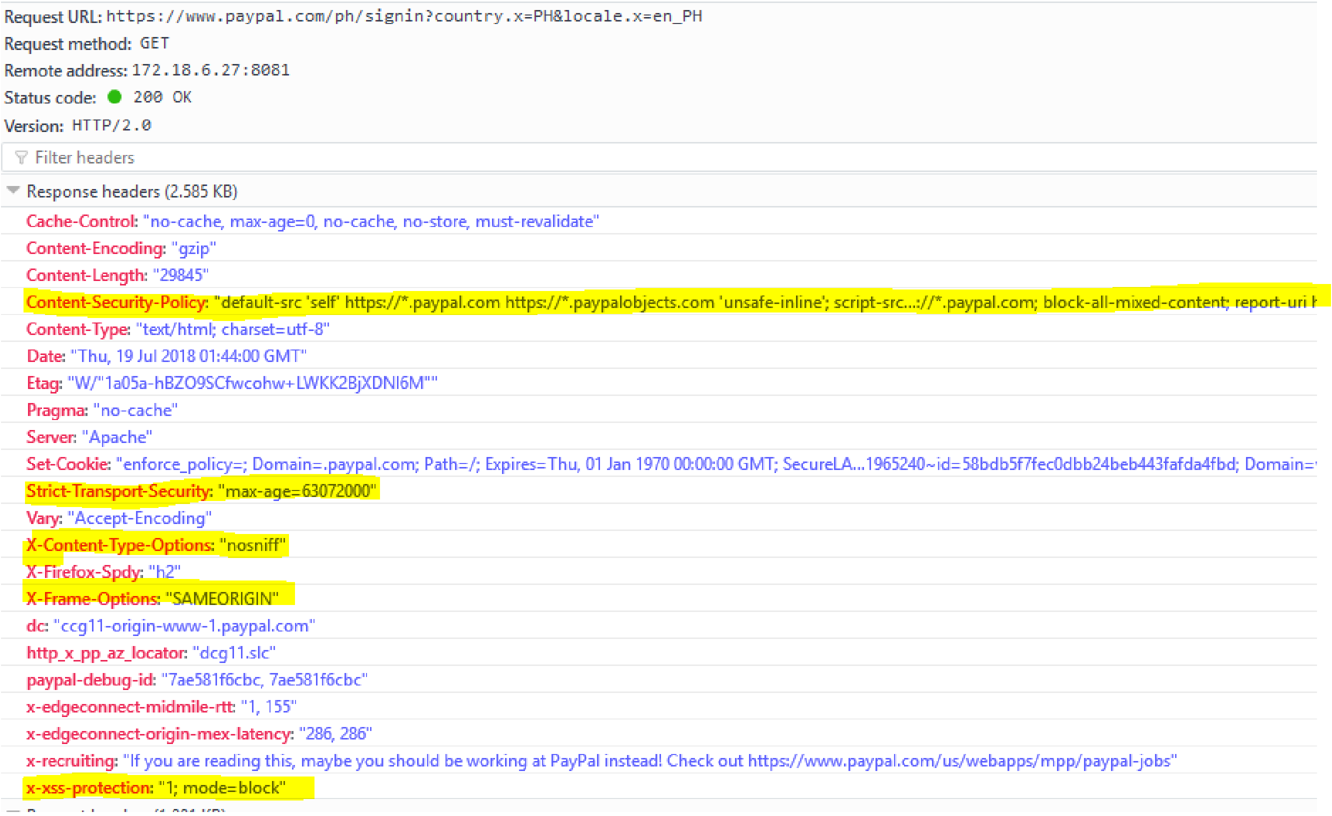
la1HTTP headers:

- Allows client and the server to pass additional information with the request or reponse
- They carry information about the client browser, the requested page, the server and more.

Response Headers: Headers with additional information about the response and a component of a network packet that is sent by the web server to a web browser or a client machine in response to a HTTP request.

Or simply put HTTP headers is used to control how the web browser should render a page blalbalbalbalba





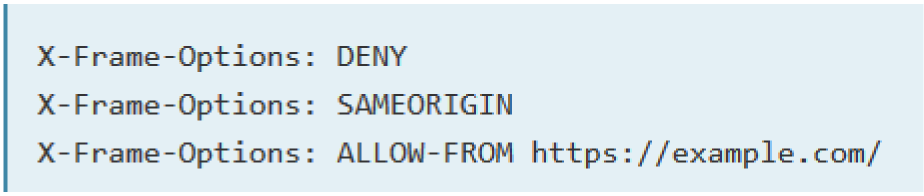
```
Request URL: https://www.paypal.com/ph/signin?country.x=PH&locale.x=en_PH
Request method: GET
Remote address: 172.18.6.27:8081
Status code: ● 200 OK
Version: HTTP/2.0
Filter headers
Response headers (2.585 KB)
  Cache-Control: "no-cache, max-age=0, no-cache, no-store, must-revalidate"
  Content-Encoding: "gzip"
  Content-Length: "29845"
  Content-Security-Policy: "default-src 'self' https://*.paypal.com https://*.paypalobjects.com 'unsafe-inline'; script-src...://*.paypal.com; block-all-mixed-content; report-uri h
  Content-Type: "text/html; charset=utf-8"
  Date: "Thu, 19 Jul 2018 01:44:00 GMT"
  Etag: "W/"1a05a-hBZO9SCfwcohw+LWKK2BjXDNI6M""
  Pragma: "no-cache"
  Server: "Apache"
  Set-Cookie: "enforce_policy=; Domain=.paypal.com; Path=/; Expires=Thu, 01 Jan 1970 00:00:00 GMT; SecureLA...1965240~id=58bdb5f7fec0dbb24beb443fafda4fbd; Domain=
  Strict-Transport-Security: "max-age=63072000"
  Vary: "Accept-Encoding"
  X-Content-Type-Options: "nosniff"
  X-Firefox-Spdy: "h2"
  X-Frame-Options: "SAMEORIGIN"
  dc: "ccg11-origin-www-1.paypal.com"
  http_x_pp_az_locator: "dcg11.slc"
  paypal-debug-id: "7ae581f6cbc, 7ae581f6cbc"
  x-edgeconnect-midmile-rtt: "1, 155"
  x-edgeconnect-origin-mex-latency: "286, 286"
  x-recruiting: "If you are reading this, maybe you should be working at PayPal instead! Check out https://www.paypal.com/us/webapps/mpp/paypal-jobs"
  x-xss-protection: "1; mode=block"
```

- **X-Frame-Options** – HTTP response header can be used to indicate whether or not a browser should be allowed to render a page in a <frame>, <iframe> or <object>.

  The header, when set by website owner, declares its preferred framing policy: values of `DENY`, `SAMEORIGIN`, or `ALLOW-FROM` *`origin`* will prevent any framing, framing by external sites

  Clickjacking is an attack that tricks a web user into clicking a button, a link or a picture, etc. that the web user didn't intend to click, typically by overlaying the web page with a (typically transparent) iframe. The user thinks he is clicking the link on the legitimate page, but actually clicks an unseen overlaid link or button.

  Directives for X-Frame-Options:



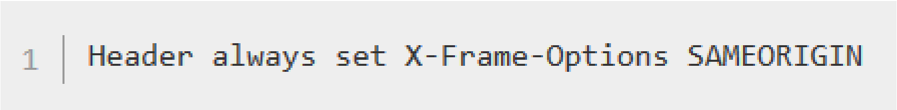
```
X-Frame-Options: DENY
X-Frame-Options: SAMEORIGIN
X-Frame-Options: ALLOW-FROM https://example.com/
```

DENY: The page cannot be displayed in a frame, regardless of the site attempting to do
SAMEORIGIN: The page can only be displayed in a frame on the same origin as the page itself
ALLOW-FROM: Page can only be displayed in a frame on the specified origin

.

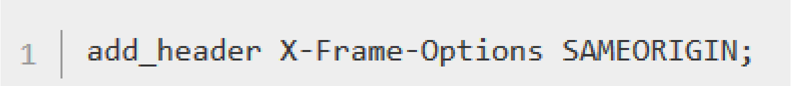
Implementing X-Frame on different site's configuration

Apache:



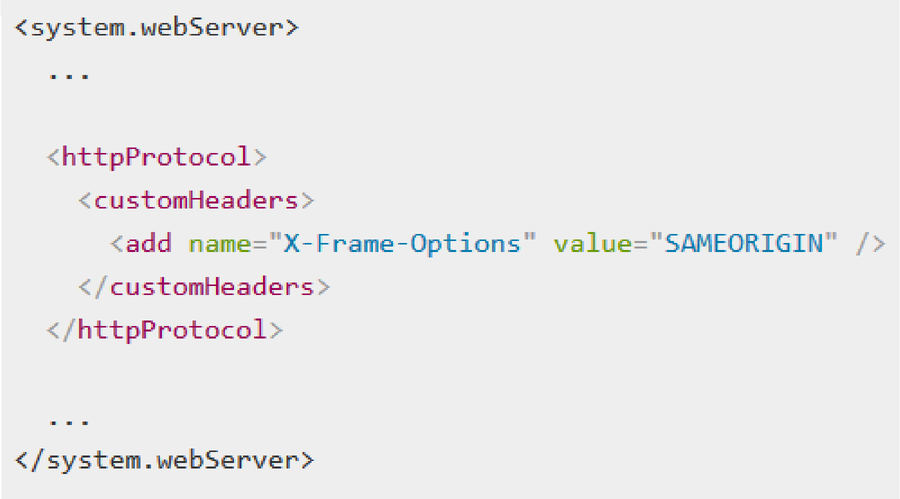
```
Header always set X-Frame-Options SAMEORIGIN
```

nginx:



```
add_header X-Frame-Options SAMEORIGIN;
```

Microsoft IIS:



```
<system.webServer>
  ...

  <httpProtocol>
    <customHeaders>
      <add name="X-Frame-Options" value="SAMEORIGIN" />
    </customHeaders>
  </httpProtocol>

  ...
</system.webServer>
```

https://security.stackexchange.com/questions/167081/how-to-add-x-frame-options-header-to-a-simple-html-file

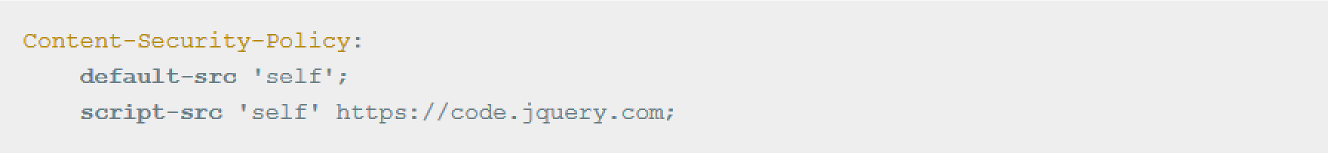
- **Content-Security-Policy** – added layer of security that helps to detect and mitigate certain types of attacks

  A security standard introduced to help prevent XSS and other content injection attacks, it achieves this by restricting sources of content loaded by the user agent to those only allowed by site operator

  To enable CSP, configure web server to return the Content-Security-Policy HTTP header

  Using CSP: To configure CSP, just add the Content-Security-Policy HTTP header to a web page.

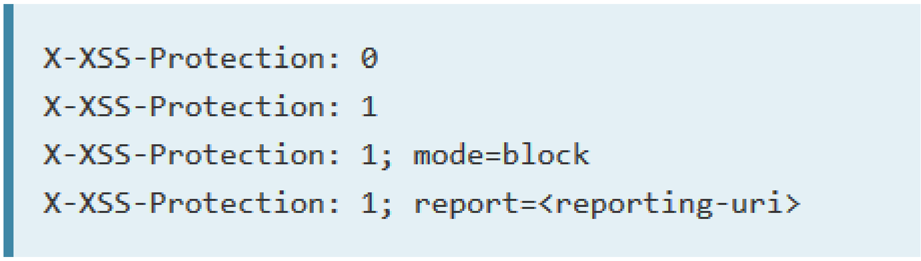
  Implementing CSP: Define lists of allowed origins for the all of the type of resources that your site utilizes.



```
Content-Security-Policy:
    default-src 'self';
    script-src 'self' https://code.jquery.com;
```

https://hacks.mozilla.org/2016/02/implementing-content-security-policy/
https://stackoverflow.com/questions/28715989/how-to-implement-content-security-policy

- **X-XSS-Protection –** is a response header and a feature available only to Internet Explorer, Google Chrome and Safari, it stops pages from loading when they detect reflected cross-site scripting attacks.



```
X-XSS-Protection: 0
X-XSS-Protection: 1
X-XSS-Protection: 1; mode=block
X-XSS-Protection: 1; report=<reporting-uri>
```

0 – Disables XSS-Protection
1 – Enables XSS filtering, the browser will sanitize the page or will remove the unsafe parts but will still render the page
1; mode=block – Enable XSS filtering but the browser will prevent the page from loading if an attack is detected
1; report=<reporting-uri> (Chrome) – If a XSS attack is detected, the browser will report a violation by using the CSP *report-ui* directive to send a report

https://stackoverflow.com/questions/9090577/what-is-the-http-header-x-xss-protection

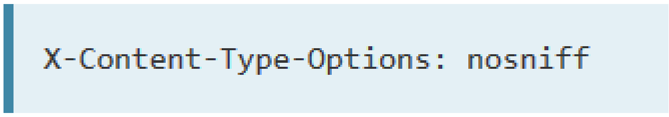
- **X-Content Type Options –** is a marker used by the server to indicate that the MIME types advertised in the Content-Type headers should not be changed and be followed. T

  Content-Type – used to indicate the media type of the resource

  Mime Sniffing is the practice of some web browsers(primarily Internet Explorer), to inspect the files we upload or download so as to deduce the file format(.txt, .html, .asp, etc.) of the file.

  For example, an HTML file can be faked as a JPG file by providing incorrect headers.
  When a web application allows users to upload an image and only checks the file extension, the user can upload an image.jpg that actually contains HTML code.

  This is a security feature that helps prevent attacks based on MIME-type confusion.



```
X-Content-Type-Options: nosniff
```

nosniff: Blocks a request if the request type is

- "style" and the MIME type is not "text/css"

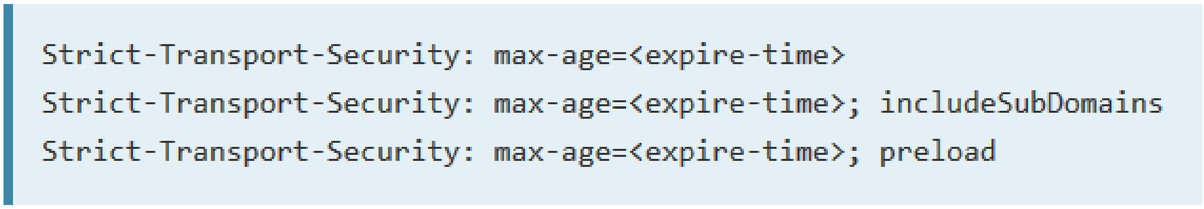
- **Strict-Transport-Security** – response header that lets a website tell browsers that it should only access using HTTPS instead of HTTP

  Inform web browsers how to handle its connection through a response header or HSTS forces browsers or application to use HTTPS if its only available. Even if someone just types "www" or http://

  HSTS addresses following threats:

  - User bookmarks or manually types http://example.com and is subject to a man-in-the-middle attack
    - HSTS automatically redirects HTTP requests to HTTPS for the the target domain
  - Web Application that is intended to be purely HTTPS inadvertently contains HTTP links or serves content over HTTP
    - HSTS automatically redirects HTTP requests to HTTPS for the target domain
  - A man-in-the-middle attacker attempts to intercept traffic from a victim user using an invalid certificate and hopes the user will accept the bad certificate
    - HSTS will not allow a user to override the invalid certificate message

  Directives for HSTS



```
Strict-Transport-Security: max-age=<expire-time>
Strict-Transport-Security: max-age=<expire-time>; includeSubDomains
Strict-Transport-Security: max-age=<expire-time>; preload
```

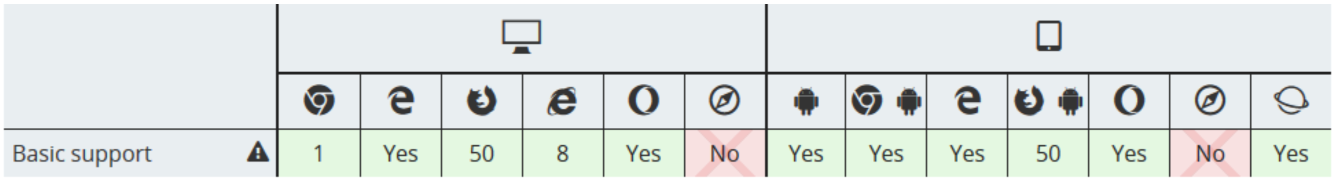
  <expire-time> - Time in seconds, browser should remember that a site is only to be accessed using HTTPS.

  includeSubDomains – rule applies to all of the site's subdomains

  preload – Browsers will never connect to the domain using an insecure connection.

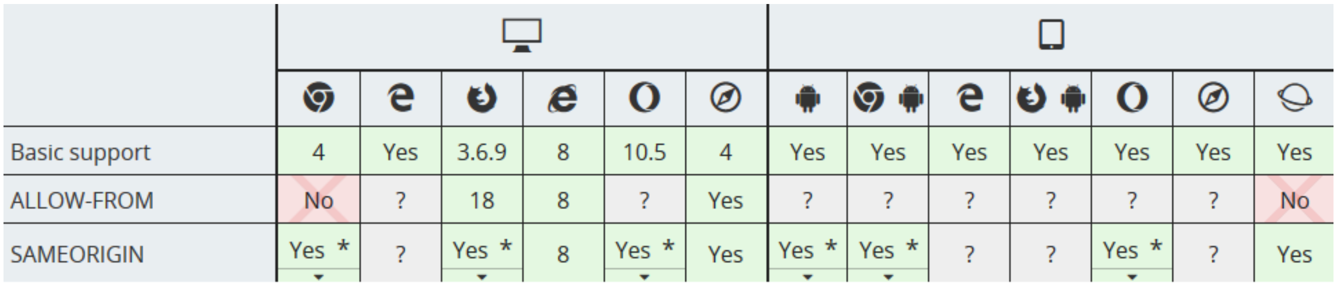
Supported Browsers:

X-Content-Type Options



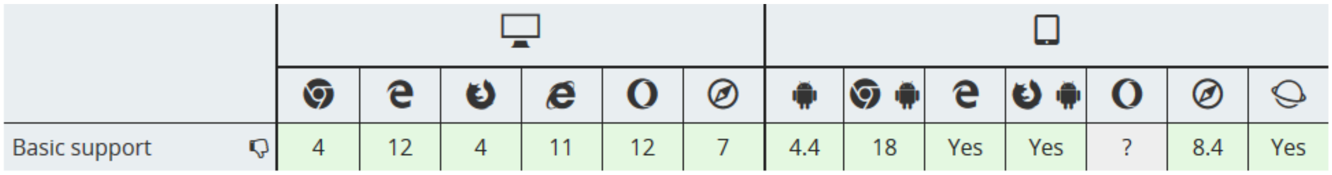
	🖥						📱						
Basic support ⚠	1	Yes	50	8	Yes	No	Yes	Yes	Yes	50	Yes	No	Yes

X-Frame-Options



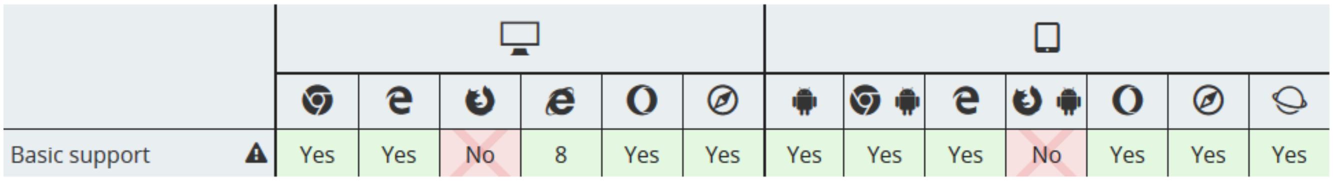
	🖥						📱						
Basic support	4	Yes	3.6.9	8	10.5	4	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ALLOW-FROM	No	?	18	8	?	Yes	?	?	?	?	?	?	No
SAMEORIGIN	Yes *	?	Yes *	8	Yes *	Yes	Yes *	Yes *	?	?	Yes *	?	Yes

Strict Transport Security (HSTS)



	🖥						📱						
Basic support 👎	4	12	4	11	12	7	4.4	18	Yes	Yes	?	8.4	Yes

X-XSS-Protection



	🖥						📱						
Basic support ⚠	Yes	Yes	No	8	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes