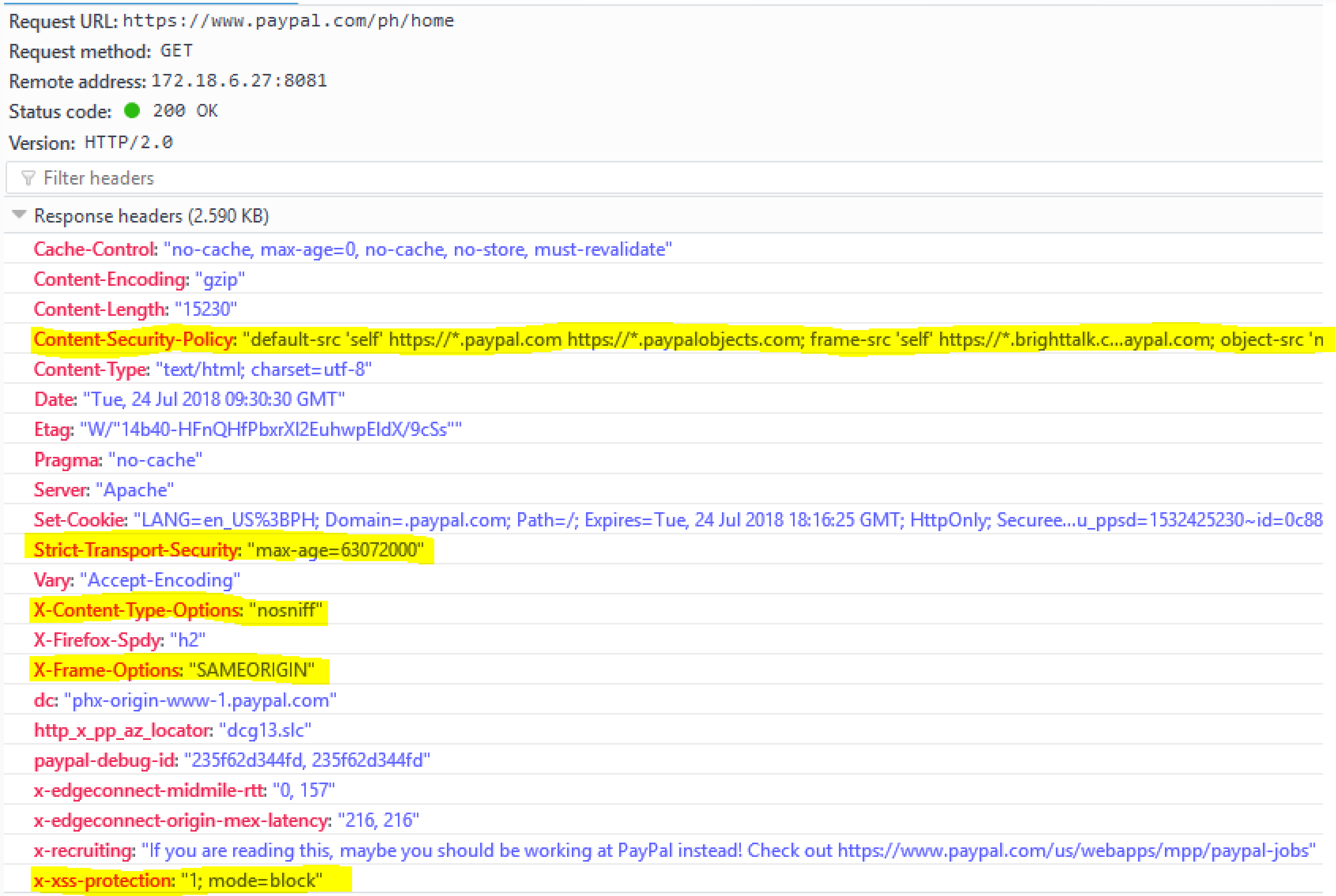
HTTP Response Headers

HTTP Response Headers



```
Request URL: https://www.paypal.com/ph/home
Request method: GET
Remote address: 172.18.6.27:8081
Status code: ● 200 OK
Version: HTTP/2.0
Filter headers
Response headers (2.590 KB)
  Cache-Control: "no-cache, max-age=0, no-cache, no-store, must-revalidate"
  Content-Encoding: "gzip"
  Content-Length: "15230"
  Content-Security-Policy: "default-src 'self' https://*.paypal.com https://*.paypalobjects.com; frame-src 'self' https://*.brighttalk.c...aypal.com; object-src 'n
  Content-Type: "text/html; charset=utf-8"
  Date: "Tue, 24 Jul 2018 09:30:30 GMT"
  Etag: "W/"14b40-HFnQHfPbxrXl2EuhwpEldX/9cSs""
  Pragma: "no-cache"
  Server: "Apache"
  Set-Cookie: "LANG=en_US%3BPH; Domain=.paypal.com; Path=/; Expires=Tue, 24 Jul 2018 18:16:25 GMT; HttpOnly; Securee...u_ppsd=1532425230~id=0c88
  Strict-Transport-Security: "max-age=63072000"
  Vary: "Accept-Encoding"
  X-Content-Type-Options: "nosniff"
  X-Firefox-Spdy: "h2"
  X-Frame-Options: "SAMEORIGIN"
  dc: "phx-origin-www-1.paypal.com"
  http_x_pp_az_locator: "dcg13.slc"
  paypal-debug-id: "235f62d344fd, 235f62d344fd"
  x-edgeconnect-midmile-rtt: "0, 157"
  x-edgeconnect-origin-mex-latency: "216, 216"
  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"
```

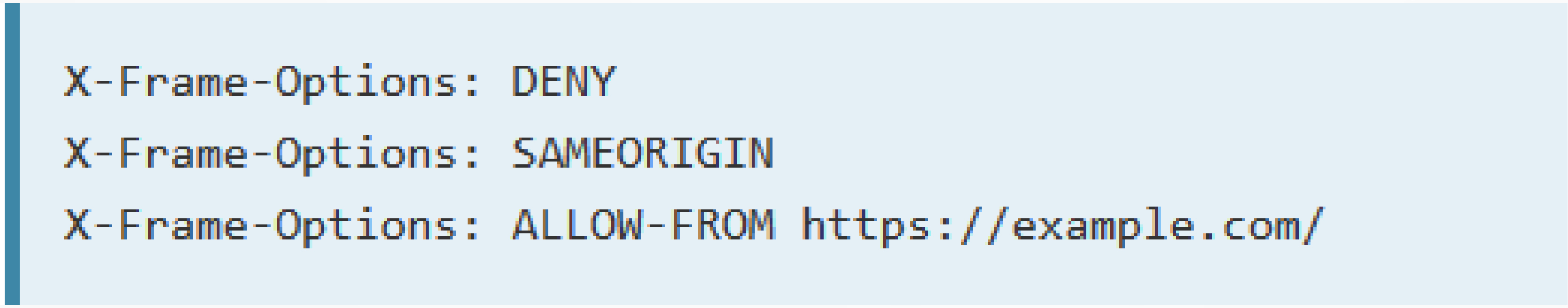
HTTP Response Headers

- X-Frame-Options
- Content Security Policy
- X-XSS-Protection
- X-Content Type Options
- Strict-Transport-Security

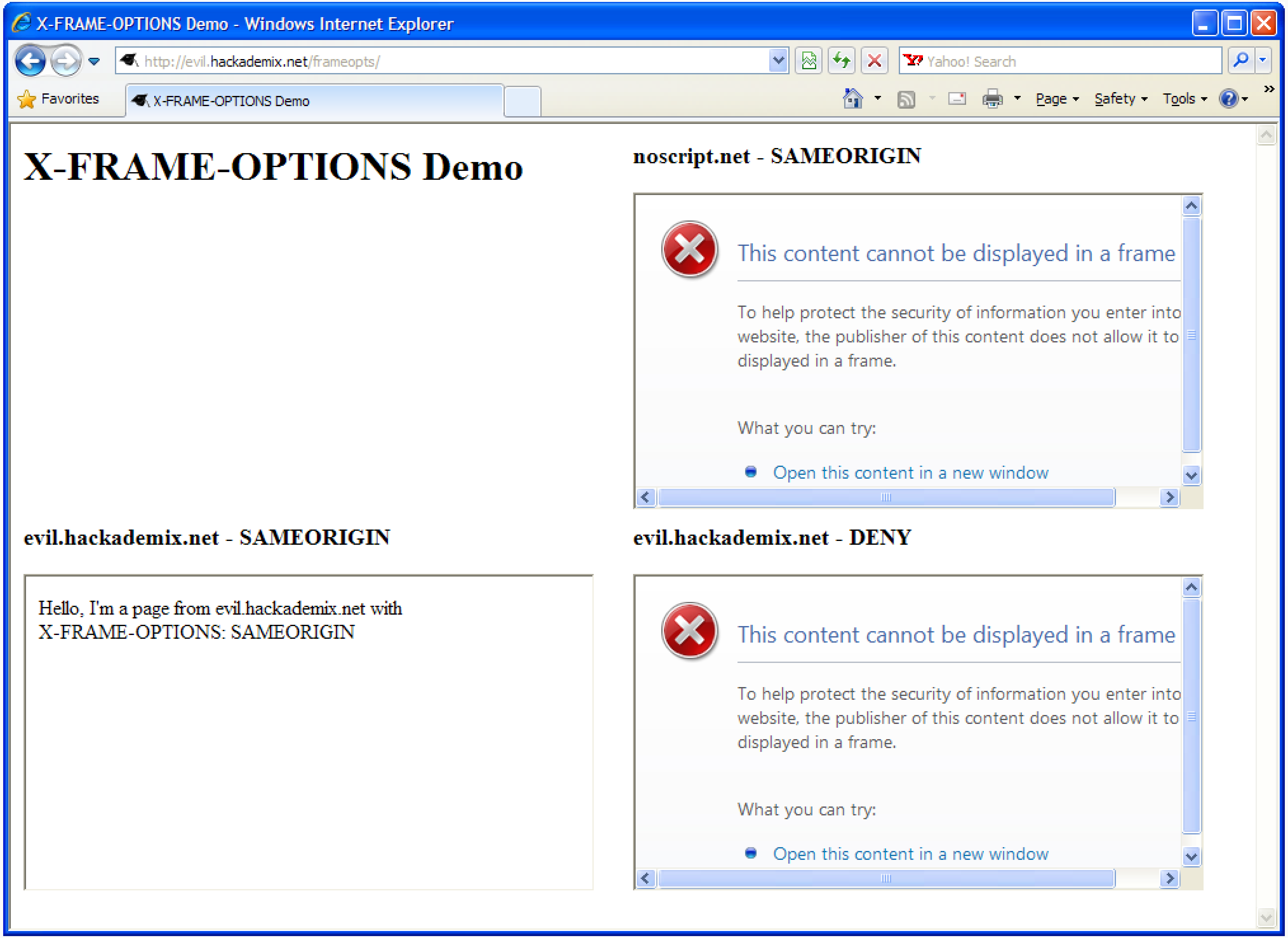
X-Frame Options

- used to indicate whether or not a browser should be allowed to render a page in <frame>, <iframe> or <object>

- X-Frame Options Directives



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


X-FRAME-OPTIONS Demo - Windows Internet Explorer
http://evil.hackademix.net/frameopts/
Yahoo! Search
Favorites
X-FRAME-OPTIONS Demo
Page
Safety
Tools

X-FRAME-OPTIONS Demo

noscript.net - SAMEORIGIN

This content cannot be displayed in a frame

To help protect the security of information you enter into website, the publisher of this content does not allow it to displayed in a frame.

What you can try:

- Open this content in a new window

evil.hackademix.net - SAMEORIGIN

Hello, I'm a page from evil.hackademix.net with X-FRAME-OPTIONS: SAMEORIGIN

evil.hackademix.net - DENY

This content cannot be displayed in a frame

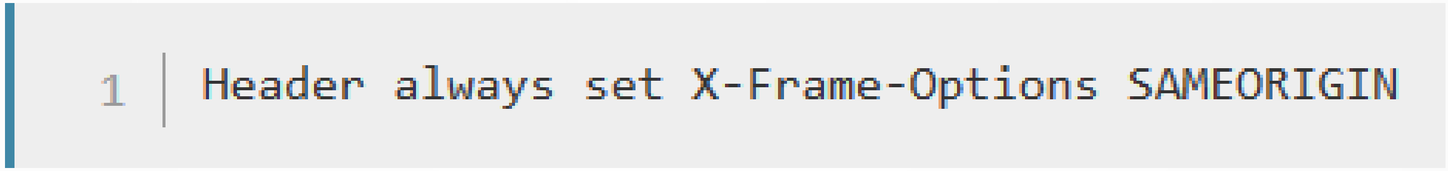
To help protect the security of information you enter into website, the publisher of this content does not allow it to displayed in a frame.

What you can try:

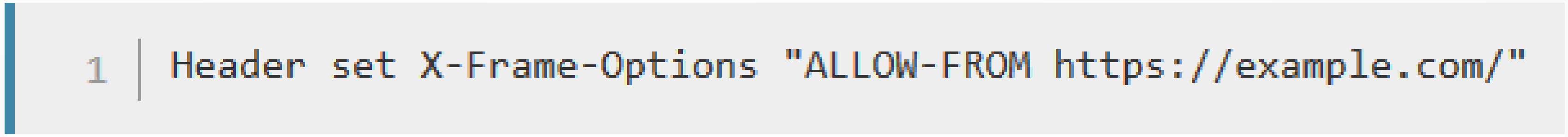
- Open this content in a new window

X-Frame Options Configuration

- Apache:

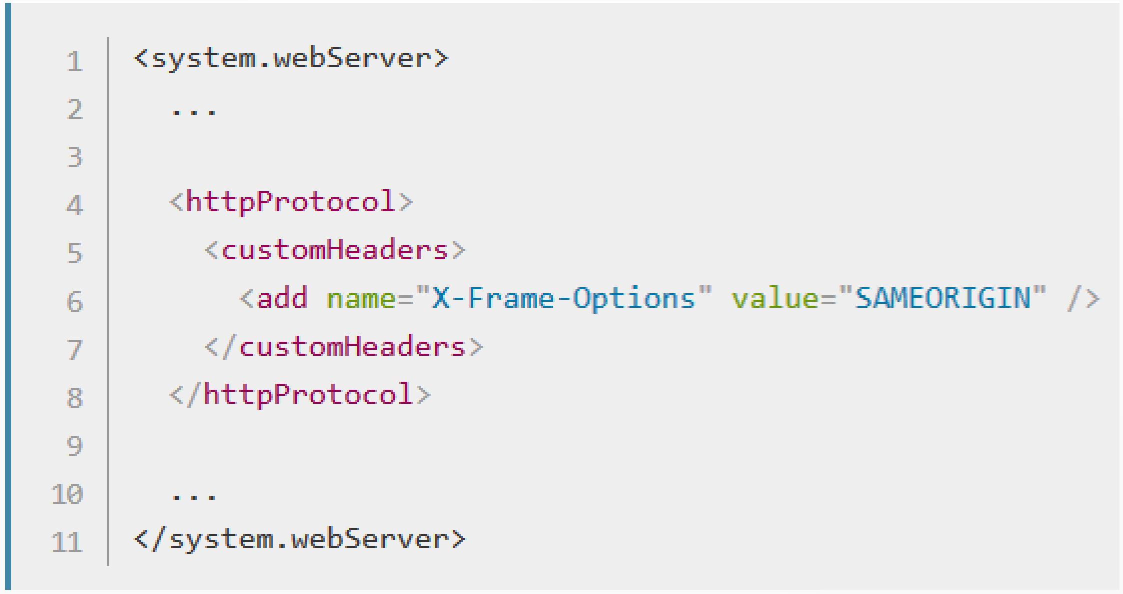


```
Header always set X-Frame-Options SAMEORIGIN
```



```
Header set X-Frame-Options "ALLOW-FROM https://example.com/"
```

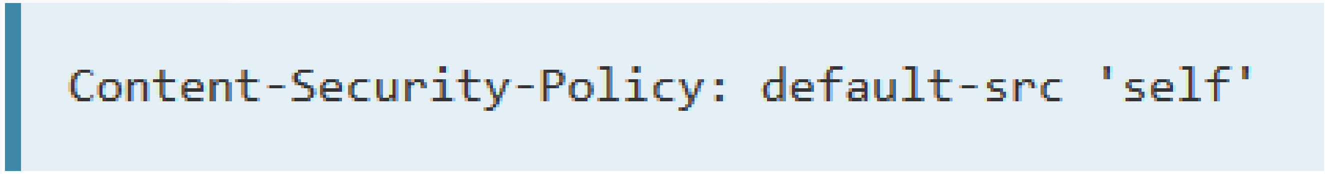
- Microsoft IIS:



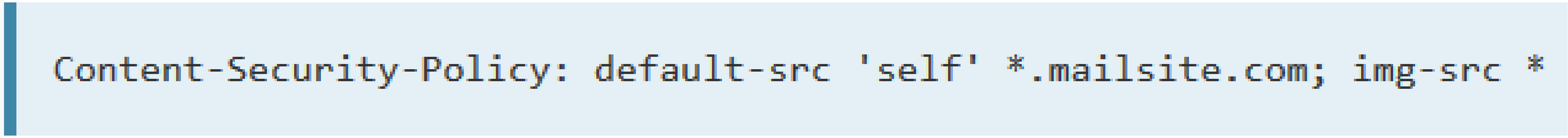
```
<system.webServer>
  ...

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

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

Content Security Policy

- Added layer of security that helps to detect and mitigate certain attacks like XSS and Data Injection Attacks



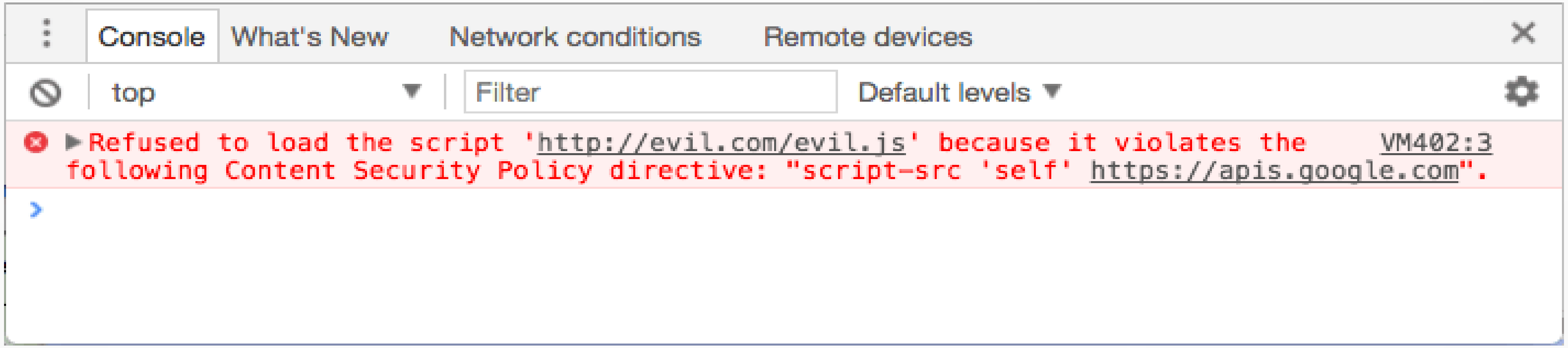
```
Content-Security-Policy: default-src 'self'
```



```
Content-Security-Policy: default-src 'self' *.mailsite.com; img-src *
```

Content Security Policy

```
Content-Security-Policy: script-src 'self' https://apis.google.com
```

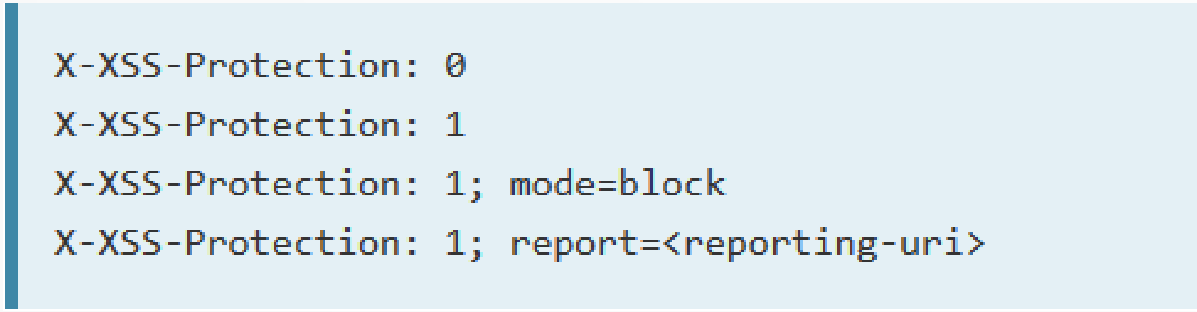


```
Refused to load the script 'http://evil.com/evil.js' because it violates the        VM402:3
following Content Security Policy directive: "script-src 'self' https://apis.google.com".
```

X-XSS Protection

- Is a response header and a feature available only to IE, Chrome and Safari. It stops pages from loading when they detect reflected cross site scripting attacks.

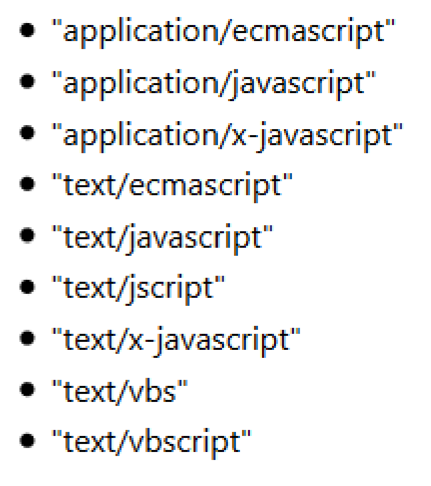
- X-XSS Directives



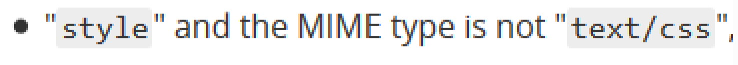
```
X-XSS-Protection: 0
X-XSS-Protection: 1
X-XSS-Protection: 1; mode=block
X-XSS-Protection: 1; report=<reporting-uri>
```

X-Content Type Options

- Instructs the browsers to disable content or MIME sniffing.
- Browser will refuse to load the styles and scripts in case they have an incorrect MIME-type.

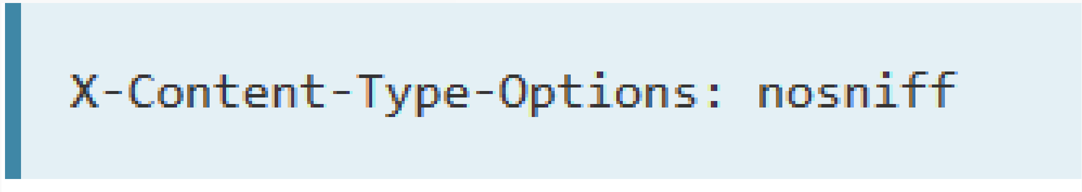


- "application/ecmascript"
- "application/javascript"
- "application/x-javascript"
- "text/ecmascript"
- "text/javascript"
- "text/jscript"
- "text/x-javascript"
- "text/vbs"
- "text/vbscript"



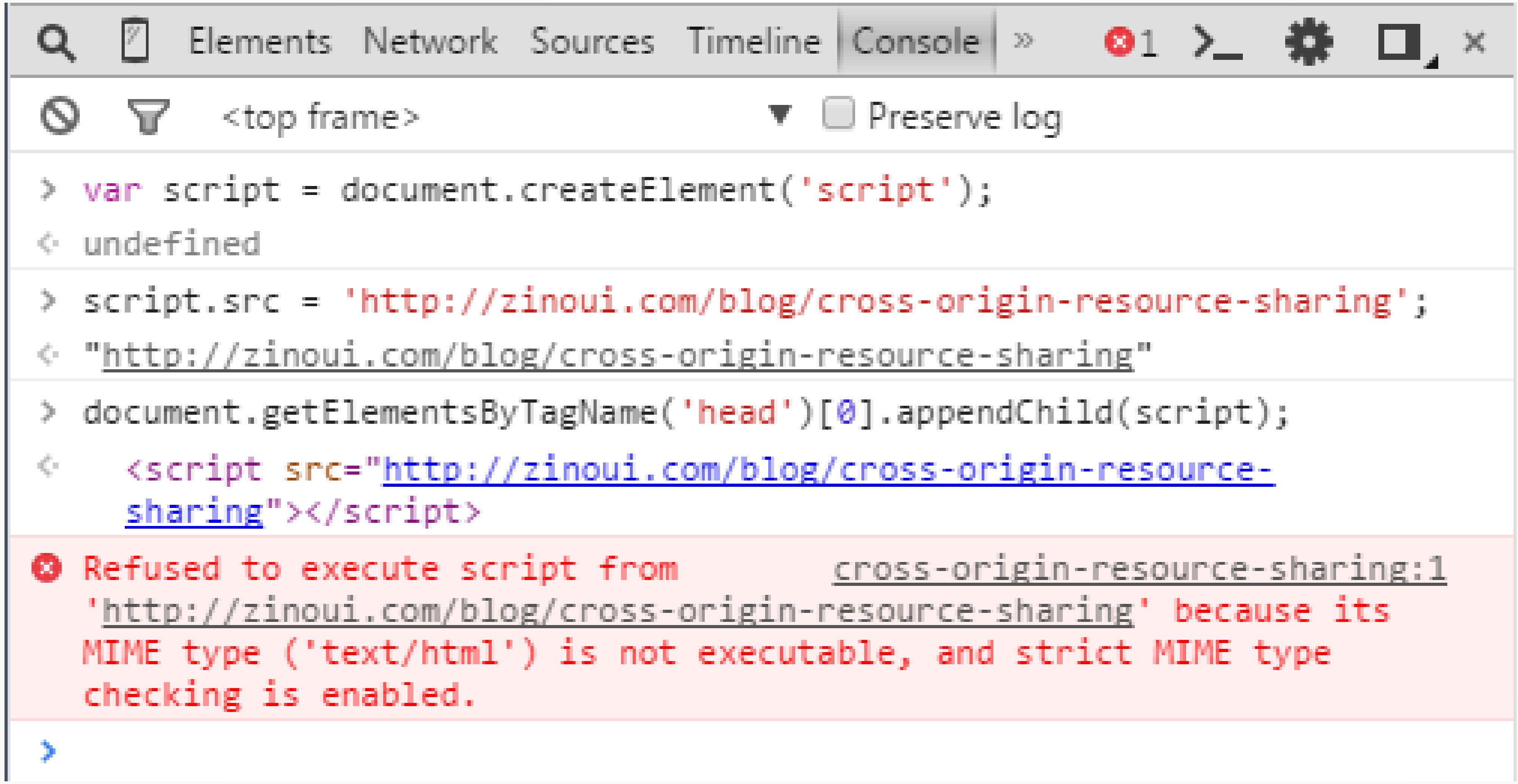
- "`style`" and the MIME type is not "`text/css`",

- Nosniff Directive



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

X-Content Type Options

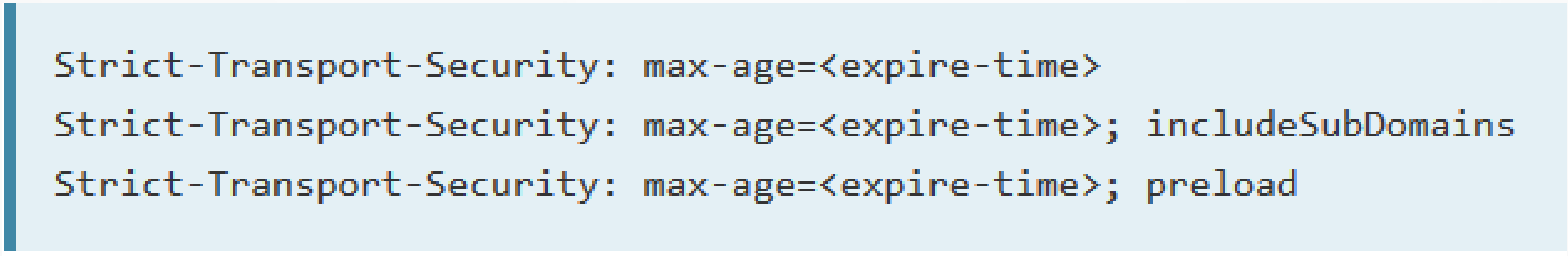


```
> var script = document.createElement('script');
< undefined
> script.src = 'http://zinoui.com/blog/cross-origin-resource-sharing';
< "http://zinoui.com/blog/cross-origin-resource-sharing"
> document.getElementsByTagName('head')[0].appendChild(script);
<   <script src="http://zinoui.com/blog/cross-origin-resource-
    sharing"></script>
⊗ Refused to execute script from          cross-origin-resource-sharing:1
  'http://zinoui.com/blog/cross-origin-resource-sharing' because its
  MIME type ('text/html') is not executable, and strict MIME type
  checking is enabled.
>
```

Strict-Transport Security

- Response header that lets a website tell browsers that it should only access using HTTPS instead of HTTP

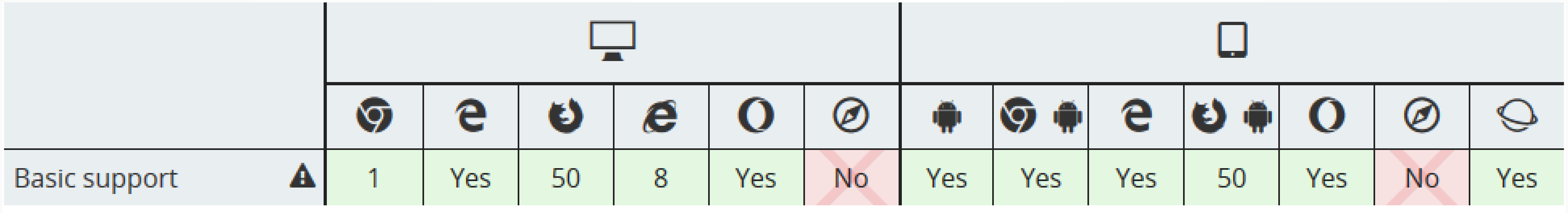
- HSTS Directives



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

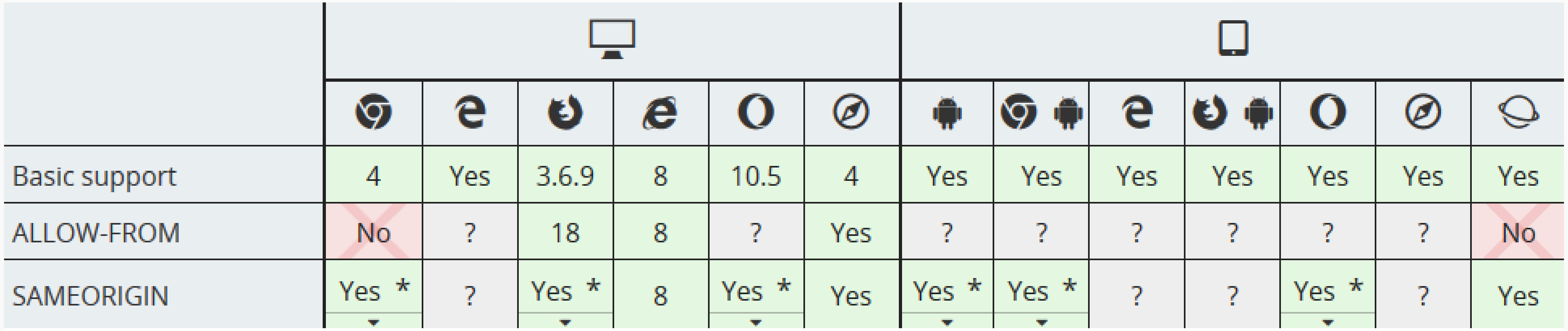
Supported Browsers

- X-Content-Type Options



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

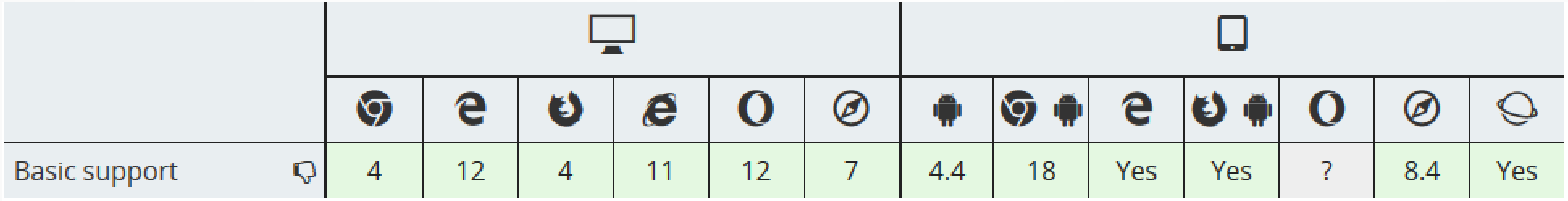
- X-Frame Options



	🖥						📱						
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

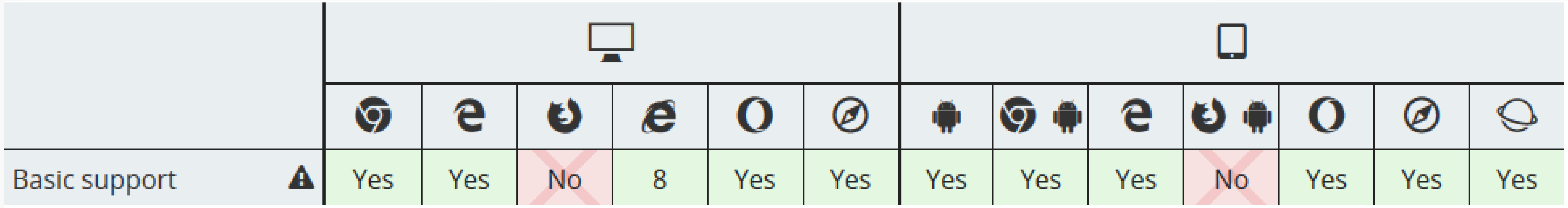
Supported Browsers

- Strict Transport Security



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

- X-XSS-Protection



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