**X-Frame-Options** :

* + DENY：不允许被任何页面嵌入；
  + SAMEORIGIN：不允许被本域以外的页面嵌入；
  + ALLOW-FROM uri：不允许被指定的域名以外的页面嵌入（Chrome现阶段不支持）；

**X-XSS-Protection** :

* + 0：禁用XSS保护；
  + 1：启用XSS保护；
  + 1; mode=block：启用XSS保护，并在检查到XSS攻击时，停止渲染页面（例如IE8中，检查到攻击时，整个页面会被一个#替换）；

**X-Content-Type-Options** :   
互联网上的资源有各种类型，通常浏览器会根据响应头的Content-Type字段来分辨它们的类型。例如：”text/html”代表html文档，”image/png”是PNG图片，”text/css”是CSS样式文档。然而，有些资源的Content-Type是错的或者未定义。这时，某些浏览器会启用MIME-sniffing来猜测该资源的类型，解析内容并执行。   
例如，我们即使给一个html文档指定Content-Type为”text/plain”，在IE8-中这个文档依然会被当做html来解析。利用浏览器的这个特性，攻击者甚至可以让原本应该解析为图片的请求被解析为**[JavaScript](http://lib.csdn.net/base/javascript" \o "JavaScript知识库" \t "http://blog.csdn.net/beckham1984/article/details/_blank)**。

* + nosniff : 禁用浏览器的类型猜测

**X-Content-Security-Policy** :   
[Content Security Policy](http://www.w3.org/TR/CSP/)，简称CSP。顾名思义，这个规范与内容安全有关，主要是用来定义页面可以加载哪些资源，减少XSS的发生。

指令示例：

| **指令** | **指令值示例** | **说明** |
| --- | --- | --- |
| default-src | ‘self’ cnd.a.com | 定义针对所有类型（js、image、css、web font，ajax请求，iframe，多媒体等）资源的默认加载策略，某类型资源如果没有单独定义策略，就使用默认的。 |
| script-src | ‘self’ js.a.com | 定义针对JavaScript的加载策略。 |
| style-src | ‘self’ css.a.com | 定义针对样式的加载策略。 |
| img-src | ‘self’ img.a.com | 定义针对图片的加载策略。 |
| connect-src | ‘self’ | 针对Ajax、WebSocket等请求的加载策略。不允许的情况下，浏览器会模拟一个状态为400的响应。 |
| font-src | font.a.com | 针对Web Font的加载策略。 |
| object-src | ‘self’ | 针对<object>、<embed>或<applet>等标签引入的flash等插件的加载策略。 |
| media-src | media.a.com | 针对audio>或<video>等标签引入的html多媒体的加载策略。 |
| frame-src | ‘self’ | 针对frame的加载策略。 |
| sandbox | allow-forms | 对请求的资源启用sandbox（类似于iframe的sandbox属性）。 |
| report-uri | /report-uri | 告诉浏览器如果请求的资源不被策略允许时，往哪个地址提交日志信息。 特别的：如果想让浏览器只汇报日志，不阻止任何内容，可以改用Content-Security-Policy-Report-Only头。 |

指令值示例：

| **指令** | **指令示例** | **说明** |
| --- | --- | --- |
|  | img-src | 允许任何内容。 |
| ‘none’ | img-src ‘none’ | 不允许任何内容。 |
| ‘self’ | img-src ‘self’ | 允许来自相同来源的内容（相同的协议、域名和端口）。 |
| data | img-src data | 允许data:协议（如base64编码的图片）。 |
| www.a.com | img-src img.a.com | 允许加载指定域名的资源。 |
| \*.a.com | img-src \*.a.com | 允许加载a.com任何子域的资源。 |
| [https://img.com](https://img.com/) | img-src [https://img.com](https://img.com/) | 允许加载img.com的https资源（协议需匹配）。 |
| https: | img-src https: | 允许加载https资源。 |
| ‘unsafe-inline’ | script-src ‘unsafe-inline’ | 允许加载inline资源（例如常见的style属性，onclick，inline js和inline css等等）。 |
| ‘unsafe-eval’ | script-src ‘unsafe-eval’ | 允许加载动态js代码，例如eval()。 |