**Application Security**

Application Security covers security risks posed to an organization's application users through HTTP headers, which are sent with all communication to and from users and the app and contain information about the messages, including how to receive them, and how recipients should respond.

If configured correctly, these headers can help prevent malicious behavior, such as [man-in-the-middle](http://en.wikipedia.org/wiki/Man-in-the-middle_attack) and [cross-site scripting](http://en.wikipedia.org/wiki/Cross-site_scripting) attacks.

**What headers are required for HTTP/1.0 and HTTP/1.1?**

**Required Headers**

|  |  |  |
| --- | --- | --- |
| **HTTP Header Name** | **Required for** | **Documentation** |
| Content-Security-Policy | HTTP/1.1 and HTTP/1.0 | [W3C Content Security Policy](http://www.w3.org/TR/CSP2/) |
| Strict-Transport-Security (HTTPS only) | HTTP/1.1 and HTTP/1.0 | [HTTP Strict Transport Security (HSTS)](http://tools.ietf.org/html/rfc6797) |
| X-Content-Type-Options | HTTP/1.1 and HTTP/1.0 | [IE8 Security Part VI: Beta 2 Update](http://blogs.msdn.com/b/ie/archive/2008/09/02/ie8-security-part-vi-beta-2-update.aspx) |
| Expires | HTTP/1.0 | [Hypertext Transfer Protocol (HTTP/1.1): Caching](http://tools.ietf.org/html/rfc7234) |
| X-Frame-Options | HTTP/1.0 | [HTTP Header Field X-Frame-Options](http://tools.ietf.org/html/rfc7034) |
| Cache-Control | HTTP/1.1 | [Hypertext Transfer Protocol (HTTP/1.1): Caching](http://tools.ietf.org/html/rfc7234) |

**Optional Headers**

|  |  |  |
| --- | --- | --- |
| **HTTP Header Name** | **Optional for** | **Documentation** |
| Access-Control-Allow-Origin | HTTP/1.0 and HTTP/1.1 | [W3C Cross Origin Resource Sharing](http://www.w3.org/TR/access-control/#access-control-allow-origin-response-header) |
| Set-Cookie | HTTP/1.0 and HTTP/1.1 | [HTTP State Management Mechanism](http://tools.ietf.org/html/rfc6265) |
| X-XSS-Protection | HTTP/1.0 and HTTP/1.1 | [IE8 Security Part IV: The XSS Filter](http://blogs.msdn.com/b/ie/archive/2008/07/02/ie8-security-part-iv-the-xss-filter.aspx) |

**Recommended values:**   
  
X-Content-Type-Options = "nosniff".  
Strict-Transport-Security = "max-age=31536000; includeSubDomains; preload".  
Cache-Control = "private, no-cache, no-store, max-age=0"  
Omit if not sure: Content-Security-Policy" = "default-src 'none'; script-src 'self'; connect-src 'self'; img-src 'self'; style-src 'self';".

**Reference Link:**

[**https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/**](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/)