Security options, headers, ciphers, and TLS settings.

==========

Security Options and Headers

SSL/TLS Settings

Define SSL certificate in vhost:

```
ssl_certificate /etc/nginx/ssl/your-domain.com.crt;
ssl_certificate_key /etc/nginx/ssl/your-domain.com.key;
```

Enable TLS 1.2 and 1.3:

```
ssl_protocols TLSv1.2 TLSv1.3;
```

Force usage of ciphers in order of most secure to least:

```
ssl_prefer_server_ciphers on;
```

Define SSL ciphers for nginx to use:

```
ssl_ciphers 'ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256';
```

==========

Headers

HSTS

HTTP Strict Transport Security (HSTS) is a web security policy mechanism that helps to protect websites against man-in-the-middle attacks such as protocol downgrade attacks and cookie hijacking.. It allows web servers to declare that web browsers (or other complying user agents) should only interact with it using secure HTTPS connections, and never via the insecure HTTP protocol.

HSTS can be enabled globally in the nginx.conf file, or on a per site bases.

```
add_header Strict-Transport-Security "max-age=63072000; includeSubdomains;"
```

X-Content-Type-Options

Prevents MIME-sniffing attacks where browsers may override the declared content type of a resource.

`nosniff`: Instructs the browser not to sniff the MIME type and to use the content type as declared in the `Content-Type` header.

```
add_header X-Content-Type-Options "nosniff" always;
```

X-Frame-Options

Prevents clickjacking attacks by controlling whether your site can be embedded in a frame or iframe.

`DENY`: Prevents any site from framing your content.

`SAMEORIGIN`: Allows framing only from the same origin.

```
add_header X-Frame-Options "DENY" always;
```


X-XSS-Protection

Enables the Cross-Site Scripting (XSS) filter built into modern web browsers.

`1; mode=block`: Activates the XSS filter and instructs the browser to block the response if an XSS attack is detected.

```
add_header X-XSS-Protection "1; mode=block" always;
```


Referrer-Policy

Controls how much referrer information is included with requests.
`no-referrer-when-downgrade`: Sends the full URL as a referrer to requests going to the same origin or a less secure destination (HTTP to HTTPS).

```
add_header Referrer-Policy "no-referrer-when-downgrade" always;
```

==========
==========

Revision #5
Created 2024-06-17 14:15:55 UTC by Daniel
Updated 2024-06-23 22:48:32 UTC by Daniel