Apache - Configuring HTTP Strict Transport Security

To configure the Apache webserver to use HTTP Strict Transport Security (HSTS), the following steps can be taken.

Activating HSTS headers

To have Apache transfer the HSTS headers we need to add the headers module to the configuration (/etc/apache2/httpd.conf):

```
LoadModule headers_module modules/mod_headers.so
```

Configure headers per website

Configure the header settings per website that uses SSL, the configuration file can normally be found in `/etc/apache2/sites-enabled/`

.

To have the Strict-Transport-Security header settings configured for a timespan of 2 years, the following line should be added to the configuration:

```
<VirtualHost *:443>
...
Header always set Strict-Transport-Security "max-age=63072000; includeSubDomains"
...
</VirtualHost>
```

Adding the includeSubDomains argument makes that the browser will connect to other subdomains on this domain too. Removing this option makes that only the visited domain is always accessed via HTTPS, but this is not advised.

After reloading the Apache configuration this header is presented to every visitor with an expirationtime of 63072000 seconds (2 years). Be careful to only add this configuration option to the HTTPS (:443) vhost, and not in the HTTP (:80) version.

For the configuration of HSTS you'll need an SSL certificate.