IT Igloo

Linux for everyone

How to configure HTTP Strict Transport Security (HSTS) on Apache & NGINX

What is HTTP Strict Transport Security (HSTS)?

HTTP Strict Transport Security (HSTS) is a security policy which is necessary to protect secure HTTPS websites against downgrade attacks. It also aids protection against cookie hijacking. It allows web servers to declare that web browsers should only interact with it using secure HTTPS connections, and never via the insecure HTTP protocol.

What are the requirements for HSTS?

A minimum of Apache 2.2.22 and NGINX 1.1.19 is required for HSTS.

Implications of turning on HSTS?

Turning on HSTS is actually a simple process. However, don't underestimate the implications of turning it on!

Firstly, HSTS is a time based system. What this means is that when you enable it you decide how long you are prepared to guarantee that your site will be served over HTTPS. It is advised that this is set to a long time. At least 6 months or longer is recommended.

How does HSTS work?

When a compatible HSTS browser contacts a HSTS enabled web server, it looks for a special HTTP header. This header states that the web client should only ever talk to the server over a HTTPS connection.

In addition there is a max-age value associated with the header that allows the browser to know that the server administrator is guaranteeing that the site should only be accessed over HTTPS for at least that time. This max-age value should be a long time. At least 6 months is recommended, but several years are possible.

Once a web browser has been to the site once and received the header it will remember that the site should only be accessed over HTTPS for the duration of the max-age value. This value is reset every time the site is accessed.

How do I configure HSTS on Apache?

1. Enable the Apache Headers Module.

```
a2enmod headers
```

2. Add the additional header to the HTTPS VirtualHost directive. Max-age is measured in seconds.

```
<VirtualHost *:443>
    # Guarantee HTTPS for 1 Year including Sub Domains
    Header always set Strict-Transport-Security "max-age=31536000;
includeSubDomains"
```

Please note that this header is only valid on a HTTPS VirtualHost.

You should probably add a server-side redirect to upgrade non-https connections the first time the site is accessed. Add this to the non-HTTP VirtualHost.

```
<VirtualHost *:80>
  [...]
  ServerName example.com
  Redirect permanent / https://example.com/
```

How do I configure HSTS on NGINX?

Enabling HSTS on NGINX is even simpler. Add the following to the server block of your HTTPS configuration.

```
add_header Strict-Transport-Security max-age=31536000;
```

Testing your site

Go to SSL Labs Test Site. The output will tell you if you have everything correct.

https://ssllabs.com/ (https://ssllabs.com/)

That's it… Enjoy the rest of your day.

One comment

1. Pingback: Configuring HSTS & OCSP Stapling | IT Igloo