Change HTTP header settings using .htaccess file

First step, if you do not already have a .htaccess file created in the root directory of the affected domain name document. To do this, refer to the following:

How to create .htaccess file?

If the file already exists, you can edit it as described below:

- Creating and editing a file via FTP
- Creating and editing a file via SSH

WHAT IS THE HTTP HEADER?

The HTTP header is part of an HTTP request or response. This determines the operating parameters of the HTTP transaction. For more information, see the following link:

List of HTTP header fields

The .htaccess file can be used to modify or complement the HTTP response header.

CHARSET HEADER

The .htaccess file can use the following to force the header of a given content type. The charset header specifies the document's character encoding. You can add the header without the meta tag:

```
<IfModule mod_headers.c>
   AddDefaultCharset UTF-8
   AddDefaultCharset ISO-8859-2
</IfModule>
```

CONTENT-LANGUAGE HEADER

In the .htaccess file, you can set a language header as follows. You can add the header without the meta tag:

```
<IfModule mod_headers.c>
   DefaultLanguage hu-hu
</IfModule>
```

CACHE-CONTROL HEADER

Cache-Control is one of the most common headers used for websites. This determines how long the file is stored in your browser

For example, if you set 5 minutes in the Cache-Control header, the visitor's browser downloads the page and then caches it for 5 minutes. After 5 minutes, the page must be retrieved from the server.

For example:

In the following example, we set the web page to be stored for 5 minutes by visitors browsers.

```
<IfModule mod_headers.c>
   Header set Cache-Control "max-age=300, public"
</IfModule>
```

Syntax

max-age is set in seconds.

The caching policy may be "public", "private" or "no-store".

USE 'VARY' HTTP HEADERS FOR MOBILE PAGES

The following Google article describes the use of Vary headers for mobile pages:

- The Vary HTTP Header

SEURITY

CONTENT-SECURITY-POLICY

Content-Security-Policy header helps reduce XSS risks. For more details, see the following pages:

- https://content-security-policy.com/

STRICT-TRANSPORT-SECURITY (HSTS)

Specifies that browsers will only communicate over HTTP instead of HTTPS. For more details, see the following pages:

- https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
- https://www.owasp.org/index.php/HTTP_Strict_Transport_Security_Cheat_Sheet

Enable the following content in the .htaccess file:

```
<IfModule mod_headers.c>
   Header add Strict-Transport-Security "max-age=31415926;includeSubDomains;"
</IfModule>
```

You can testing the following command:

```
curl -I https://example.com
```

The output looks like this:

```
[server]$ curl -I https://example.com
HTTP/1.1 200 OK
Date: Tue, 05 Jun 2018 20:05:52 GMT
Server: Apache
Last-Modified: Tue, 05 Jun 2018 16:26:52 GMT
ETag: "2f9-56de78493cbc8"
Accept-Ranges: bytes
Content-Length: 761
Strict-Transport-Security: max-age=31415926;includeSubDomains;
Content-Type: text/html
```

The command output shows the Strict-Transport-Security header

---

Revision #2
Created 24 October 2023 14:40:43 by Judit Pásztor
Updated 26 October 2023 10:23:22 by Judit Pásztor