```
# Set regular mime types.
AddType application/pgp-keys .asc
AddType image/jpeg           .jpg
AddType image/png            .png
AddType text/html            .html

# I have only one xml file, and that one is an atom feed.
AddType application/atom+xml .xml

# The correct mime type for woff is 'application/font-woff', but for woff2 it is
# 'font/woff2'. For png it is 'image/png', so I am going with consistency here,
# even though it is not standard. Browsers understand anyway.
AddType font/woff  .woff
AddType font/woff2 .woff2

# Set encoding and language.
DefaultLanguage en-GB
AddDefaultCharset UTF-8
AddCharset UTF-8 .html
AddCharset UTF-8 .xml

# Allow caching of static resources.
ExpiresActive on
ExpiresByType image/png            "access plus 1 month"
ExpiresByType image/jpeg           "access plus 1 month"

# The feed is not updated that often, but when it is, the changes should be
# visible as soon as possible. Trade latency for bandwith.
ExpiresByType application/atom+xml "access plus 6 hours"

# Because I subset fonts for every page specifically, a change in the page
# likely causes a change in the font. (I optimize for initial page load, because
# most visitors only visit one page.) The only use case for caching then, is
# when you hit the back button on the browser, or when you are surfing. I assume
# nobody stays on my site for longer than two hours in one session, so that is
# the time to cache.
ExpiresByType text/html            "access plus 2 hours"
ExpiresByType font/woff            "access plus 2 hours"
ExpiresByType font/woff2           "access plus 2 hours"

# Enable strict transport security with a max age of 180 days
# Enable strict transport security with a max age of 120 days.
Header set Strict-Transport-Security "max-age=10368000" env=HTTPS

# Disable loading stuff from other domains to mitigate XSS attacks. (I have a
# static stite anyway, but it doesn't hurt either, except maybe for the extra
# header bytes.)
Header set Content-Security-Policy: "default-src 'none'; font-src 'self'; img-src 'self';
style-src 'unsafe-inline'"

# Do not list directory contents.
Options -MultiViews -Indexes

# Pages should not end in a trailing slash.
DirectorySlash Off

RewriteEngine On

# Redirect insecure connections to the https version. There are some downsides
# to this (downgrading man in the middle attacks, etc.), but I've allowed the
# insecure version for over a year (with a rel=canonical link pointing to the
# secure version, and updating all links within my control), and I am still
# seeing significant amounts of insecure traffic, so I think that this is best
# in the end.
RewriteCond %{HTTP_HOST} !=beta.ruudvanasseldonk.com
RewriteCond %{HTTPS} off
RewriteRule ^ https://ruudvanasseldonk.com%{REQUEST_URI} [R=301,L]

# Redirect anything that ends in a slash to the page without slash.
RewriteBase /
RewriteRule ^(.*)\/$ $1 [R=301,L]

# Internally, the document for /foo/bar is at /foo/bar/index.html.
RewriteRule ^([\w\d\/-]+)$ $1/index.html [T=text/html]

# Do not serve files with .gz extension with a gzip mime type, but instead
# make .gz set the encoding to gzip.
RemoveType .gz
AddEncoding gzip .gz

# Serve gzipped files if the browser accepts them and if a non-empty .gz file
# exists for the requested file. All html and xml files have a corresponding
# .gz file.
RewriteCond %{HTTP:Accept-Encoding} gzip
RewriteCond %{REQUEST_FILENAME}\.gz -s
RewriteRule ^(.*)$ $1.gz [L]
```