v2.0.7-tls12-100p

trimstray

# NGINX HARDENING CHEATSHEET

HOWTO: A+ with all 100%’s on SSL Labs and Mozilla Observatory

**The following rules are security-oriented but blindly deploying of some of them (e.g. CSP) will broke the most of web apps!**

## Hide Nginx version number

```
server_tokens off;
```

## Hide Nginx server signature

```
more_clear_headers 'Server';
```

## Use min. 4096-bit private key

```
$ openssl -genrsa -out example.com.key 4096
$ certbot certonly -d example.com --rsa-key-size 4096
```

## Keep only TLS 1.2

```
ssl_protocols TLSv1.2;
```

## Use only strong ciphers for TLS 1.2

```
ssl_ciphers "ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES256-SHA384";
```

## Use more secure ECDH Curves

```
ssl_ecdh_curve secp521r1:secp384r1:prime256v1;
```

## Enable DNS CAA ( On your DNS service that supports CAA Policy )

```
your.domain. CAA 0 issue "certificate-authority"
```

**Keep NGINX up-to-date!**

Do not follow guides just to get 100% of something. Think about what you actually do at your server!

## Enable OCSP Stapling

```
ssl_stapling on;
ssl_stapling_verify on;
ssl_trusted_certificate ssl/inter-CA-chain.pem
resolver 1.1.1.1 8.8.8.8 valid=300s;
resolver_timeout 5s;
```

## Force all connections over TLS

```
return 301 https://$host$request_uri;
```

## Defend against the BEAST attack

```
ssl_prefer_server_ciphers on;
```

## HTTP Strict Transport Security

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

## Disable HTTP compression

```
gzip off;
# Only for private resources when using TLS.
```

## Reduce XSS risks (Content-Security-Policy)

```
add_header Content-Security-Policy "default-src 'none'; script-src 'self'; connect-src 'self'; img-src 'self'; style-src 'self';" always;
```

Based on **trimstray/nginx-admins-handbook**

## Control the behavior of the Referer header (Referrer-Policy)

```
add_header Referrer-Policy "no-referrer";
```

## Provide clickjacking protection (X-Frame-Options)

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

## Prevent some categories of XSS attacks (X-XSS-Protection)

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

## Prevent Sniff Mimetype (X-Content-Type-Options)

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

## Deny the use of browser features (Feature-Policy)

```
add_header Feature-Policy "geolocation 'none'; midi 'none'; notifications 'none'; push 'none'; sync-xhr 'none'; microphone 'none'; camera 'none'; magnetometer 'none'; gyroscope 'none'; speaker 'none'; vibrate 'none'; fullscreen 'none'; payment 'none'; usb 'none';";
```