v1.0.0

trimstray

NGINX HARDENING CHECKLIST

HOWTO: A+ with all 100%'s on SSL Labs

Hide Nginx version number

```
server_tokens off;
```

Hide Nginx server signature

```
more_set_headers "Server: Unknown";
```

Use only 4096-bit private keys

```
# openssl genrsa -out domain.com.key 4096
# certbot certonly -d domain.com --rsa-key-size 4096
```

Keep only TLS 1.2 (+ TLS 1.3)

```
ssl_protocols TLSv1.2;
```

Use only strong ciphers

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

Use more secure ECDH Curve

```
ssl_ecdh_curve X25519:prime256v1:secp521r1:secp384r1;
```

These guidelines provides recommendations for very restrictive setup.

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

Use strong Key Exchange

```
# openssl dhparam -dsaparam -out /etc/nginx/dh.pem 4096

ssl_dhparam /etc/nginx/dh.pem;
```

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 compression

```
gzip off;
```

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-quick-reference**

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;
```