# HSTS Header "richtig" setzen

Viele nginx-User haben HTTP und HTTPS in einem server-Block zusammengefasst. Trägt man dort nun den add_header Code ein, wird er auch für beide Protokolle ausgeliefert:

```
add_header Strict-Transport-Security "max-age=31536000; includeSubDomains; preload";
```

Das ist eigentlich falsch, da laut RFC 6797 der HSTS Header nicht über unverschlüsseltes HTTP gesendet werden soll.

Auf jeden Fall RFC konform ist diese Lösung und es lassen sich damit auch Port 80 und 443 zusammenfassen:

```
map $scheme $hsts_header {
    https "max-age=31536000; includeSubDomains; preload";
}

server {
    listen  80;
    listen  443 ssl;

    add_header Strict-Transport-Security $hsts_header;
}
```

---

Revision #1
Created 2021-05-05 07:00:08 UTC by magenbrot
Updated 2021-05-05 07:00:30 UTC by magenbrot