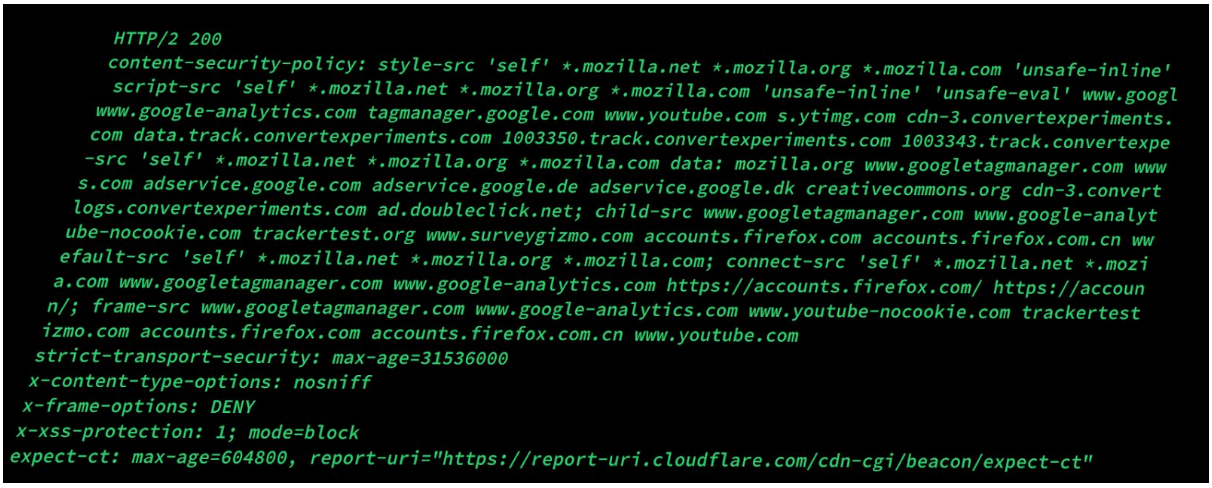
# Training - HTTP security headers



```
                HTTP/2 200
               content-security-policy: style-src 'self' *.mozilla.net *.mozilla.org *.mozilla.com 'unsafe-inline'
                script-src 'self' *.mozilla.net *.mozilla.org *.mozilla.com 'unsafe-inline' 'unsafe-eval' www.googl
             www.google-analytics.com tagmanager.google.com www.youtube.com s.ytimg.com cdn-3.convertexperiments.
            com data.track.convertexperiments.com 1003350.track.convertexperiments.com 1003343.track.convertexpe
           -src 'self' *.mozilla.net *.mozilla.org *.mozilla.com data: mozilla.org www.googletagmanager.com www
          s.com adservice.google.com adservice.google.de adservice.google.dk creativecommons.org cdn-3.convert
         logs.convertexperiments.com ad.doubleclick.net; child-src www.googletagmanager.com www.google-analyt
        ube-nocookie.com trackertest.org www.surveygizmo.com accounts.firefox.com accounts.firefox.com.cn ww
       efault-src 'self' *.mozilla.net *.mozilla.org *.mozilla.com; connect-src 'self' *.mozilla.net *.mozi
      a.com www.googletagmanager.com www.google-analytics.com https://accounts.firefox.com/ https://accoun
     n/; frame-src www.googletagmanager.com www.google-analytics.com www.youtube-nocookie.com trackertest
    izmo.com accounts.firefox.com accounts.firefox.com.cn www.youtube.com
   strict-transport-security: max-age=31536000
  x-content-type-options: nosniff
 x-frame-options: DENY
x-xss-protection: 1; mode=block
expect-ct: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
```

This is a 4-hour practical technical training for engineers on using HTTP security headers to improve client side security on the web.

**Training duration**: 4 hours (1.5h of theory / 2.5h of lab work)
**Group size**: 6 - 14
**Target audience**: web developers (backend, frontend); system administrators who work with web servers; web testers; security specialists
**Participants need**: personal laptop with a web browser and a SSH client; basic knowledge of: linux command line, HTTP protocol; HTML
**Expected outcome**: Participants are aware on available client side HTTP security controls; what protections they provide; and how to configure them. Participants have needed basics to start implementing learnings in their production applications.
**Training language**: English

# Training covers

Participants will learn about the following topics:

- CSP (Content Security Policy)
- Cookie security
- HSTS (HTTP Strict Transport Security)
- HTTPS redirects, the correct way
- Referrer Policy
- Feature Policy
- Subresource Integrity; supply chain security
- Expect-CT; Certificate Transparency
- Deprecated security headers
- XSS and browser-based protection against it

The training consists of 90 minutes of theory and 150 minutes of hands on lab work.

## Practical lab

Participants will practice applying training concepts in a real-world lab environment. The practical part will involve configuring a web page and a web server from a default insecure state to a hardened (with HTTP security headers) configuration.

The lab has interactive feedback to validate correct configuration and participants understanding of the training concepts. It also simulates numerous real-world scenarious, such as having to whitelist known good assets; or how a 3rd party vendor (CDN) compromise can affect your website -- and what to do about it.

## Backstory

As engineers and companies, we have a responsibility to keep our customers, and their data, safe. Most electronic interactions between users and companies happen on the Web, over HTTP. Engineers are usually aware and implement security checks on the server side, for example by sanitizing input - however, as HTTP is a client-server model, we should also take steps to secure the client - our user. This, however, often escapes notice.

This training aims to make web engineers aware of HTTP hardening techniques they can apply on the client, thereby increasing their applications resilience to XSS, 3rd party compromise and MitM attacks. It also gives engineers visibility into their own dependencies and user flows, and gives security analysts more visibility into attacks thrown against their website.

The biggest benefit and the reason why this training was created, is to make engineers aware of the tools available to them - so that they would actually be implemented.

## About the trainer

Ando David Roots is an engineer with over 10 years of experience in IT. With an education in IT Systems Development from the Estonian IT College, he has worked in the finance sector as a web developer, site reliability engineer and cyber security specialist. This career path gave him suitable experience to teach a training on a topic that combines all three fields. Ando currently works as a security engineer in an Estonian unicorn company.

Blog | Twitter | GitHub | LinkedIn | ando@sqroot.eu

# Feedback

Here’s what others have said about the workshop.

*“The training was enjoyable and very practical. I liked that I got interactive feedback when I solved a training exercise. The training was suitable for every level and instruction was good.”*

— Tormi Tuuling / Security Engineer / Bigbank

*”Although the topic was a bit familiar, the training was still interesting. Especially the pratical part, where you got hands on and saw in real life how important it is to implement headers correctly.”*

— Viljar Bauman / Security Engineer / Veriff

*“I would attend again. The theory and practical parts were great! 10 / 10 or technically at least an A.”*

— Bob Santos / Fullstack Developer / TransferWise

*“Made me want to SSH into my own server to immediately make changes!”*

— Bram Inniger / Software Engineer / TransferWise

*“Even though I was aware of some of these practises / headers I learned something new about all of them and how to use them in real life scenario.”*

— Karl Lääts / Fullstack Engineer / TransferWise

*“Really great training! Exactly at the level where I could understand, meaning: very detailed, but I still understood. Very cool practical part; nice challenge and competitive. Overall really good experience and would definitely recommend.”*

— Taavi Aasver / Frontend Engineer / TransferWise