

# Poster on previously published paper: 12 Angry Developers – A Qualitative Study on Developers' Struggles with CSP

## **Title:**

12 Angry Developers – A Qualitative Study on Developers' Struggles with CSP

## **Authors:**

Sebastian Roth, Lea Gröber, Michael Backes, Katharina Krombholz, Ben Stock

## **Venue:**

ACM SIGSAC Conference on Computer and Communications Security (CCS) 2021

## **PDF Link:**

<https://publications.cispa.saarland/3463/1/roth2021usable.pdf>

## **Abstract:**

The Web has improved our ways of communicating, collaborating, teaching, and entertaining us and our fellow human beings. However, this cornerstone of our modern society is also one of the main targets of attacks, most prominently Cross-Site Scripting (XSS). A correctly crafted Content Security Policy (CSP) is capable of effectively mitigating the effect of those Cross-Site Scripting attacks. However, research has shown that the vast majority of all policies in the wild are trivially bypassable.

To uncover the root causes behind the omnipresent misconfiguration of CSP, we conducted a qualitative study involving 12 real-world Web developers. By combining a semi-structured interview, a drawing task, and a programming task, we were able to identify the participant's misconceptions regarding the attacker model covered by CSP as well as roadblocks for secure deployment or strategies used to create a CSP.