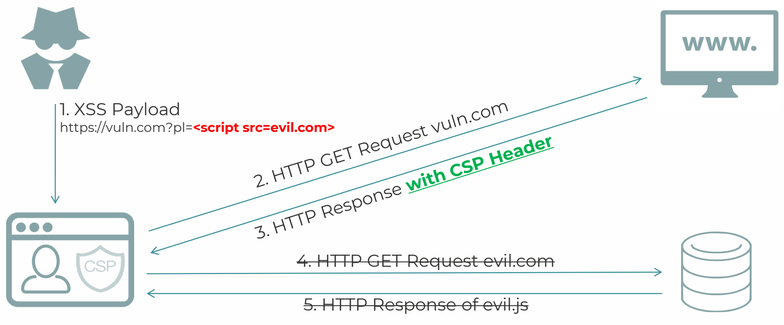
12 Angry Developers
A Qualitative Study on Developers' Struggles with CSP

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

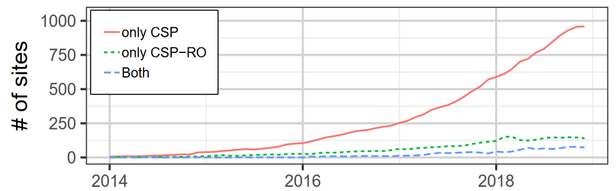
What is a Content Security Policy (CSP)?



XSS is one of the most prevalent issues in the Web[2]
A correct CSP can effectively mitigate the effect of XSS.

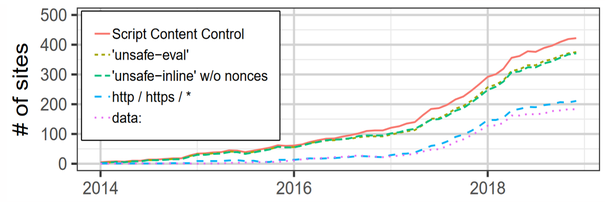
Previous Work on CSP Deployment [3]

Longitudinal evolution of deployment CSPs within the historically Top 10k visited sites:

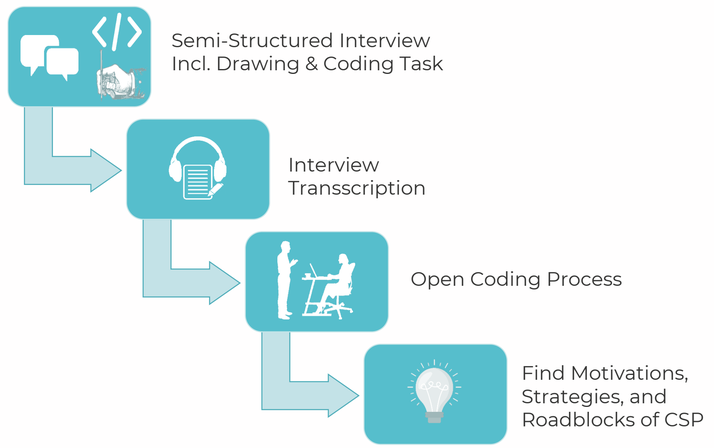


→ Not many sites are deploying a CSP...

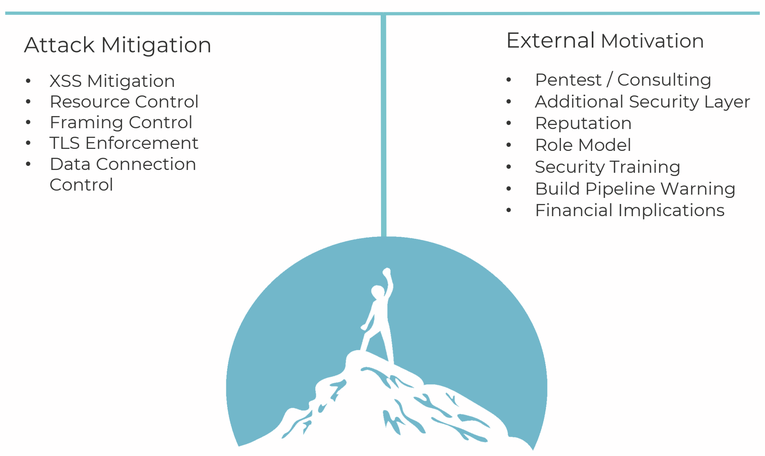
... and those who do, misconfigure it. ←



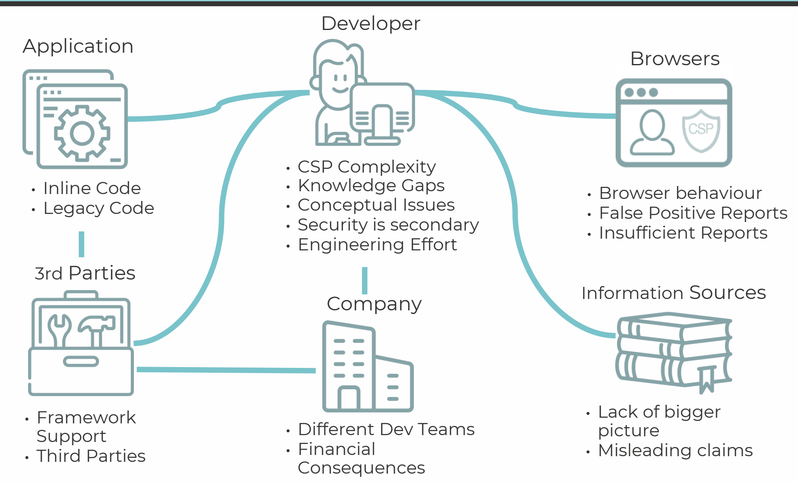
What have we Done? [1]



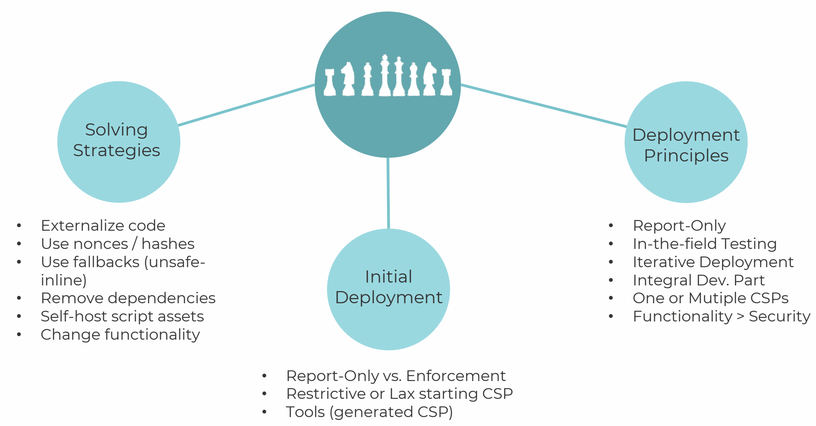
Motivations to deploy CSP



Roadblocks for CSP Deployment



Strategies for CSP Deployment



[1] 12 Angry Developers – A Qualitative Study on Developers' Struggles with CSP
Sebastian Roth, Lea Gröber, Michael Backes, Katharina Krombholz, and Ben Stock
Conference on Computer and Communications Security (CCS '21)

[2] OWASP Top 10 Web Application Security Risks
Online at: https://owasp.org/www-project-top-ten/
Open Web Application Security Project (OWASP)

[3] Complex Security Policy? – A Longitudinal Analysis of Deployed Content Security Policies
Sebastian Roth, Timothy Barron, Stefano Calzavara, Nick Nikiforakis, and Ben Stock
Network and Distributed System Security Symposium (NDSS '20)

CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY