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)? Previous Work on CSP Deployment [3] What have we Done? [1] Longitudinal evolution of deployment CSPs within the Semi-Structured Interview historically Top 10k visited sites: Incl. Drawing & Coding Task www. only CSP sites → Not many | 1. XSS Payload sites are https://vuln.com?pl=<script src=evil.com> deploying a Interview CSP... **#** 250 Transscription 2014 2016 2018 Open Coding Process 4. HTTP GET Request evil.com -Script Content Control ... and those \leftarrow 5. HTTP Response of evil.is who do. --'unsafe-inline' w/o nonces misconfigur Find Motivations. XSS is one of the most prevalent issues in the Web^[2] Strategies, and A correct CSP can effectively mitigate the effect of XSS. Roadblocks of CSP **Motivations to deploy CSP Strategies for CSP Deployment Roadblocks for CSP Deployment** Developer Application External Motivation Attack Mitigation Browsers Pentest / Consulting XSS Mitigation Additional Security Layer Resource Control Framing Control Reputation Solving Deployment TLS Enforcement Role Model Strategies

CSP Complexity

Knowledge Gaps

Conceptual Issues

Engineering Effort

Company

Different Dev Teams

Consequences

Financial

Security is secondary

[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)

Security Training

Build Pipeline Warning

Financial Implications

Data Connection

Control

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

· Inline Code

3rd Parties

少分

Framework

Third Parties

Support

Legacy Code

[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)

Externalize code

inline)

Use nonces / hashes

• Use fallbacks (unsafe-

Self-host script assets

Change functionality

Remove dependencies

Browser behaviour

Insufficient Reports

Information Sources

Lack of bigger

Misleading claims

picture

False Positive Reports



Initial

Deployment

 Report-Only vs. Enforcement Restrictive or Lax starting CSP

Tools (generated CSP)

Principles

Report-Only

In-the-field Testing

Integral Dev. Part

Iterative Deployment

One or Mutiple CSPs

Functionality > Security