W3C Workshop
Secure the Web Forward

Driving developer awareness and adoption of Web security standards & practices

September 26-28, 2023 - Virtual

Presented by W3C, OpenSSF, OWASP, OpenJS

Parsoa Khorsand

Welcome to the Workshop!

Main goal: **Secure the Web forward!**
Converge on a common understanding and draft possible next steps.
Agenda: https://www.w3.org/2023/03/secure-the-web-forward/agenda.html

- 🗣️ Presentations are a means to an end. Discussion is key!
- 🔇 Please mute when you're not speaking.
- ⏺️ Presentations **may** be recorded.
- ⏹️ Discussions will **not** be recorded.
- 📝 Notes taken in a public Google Doc under Chatham House Rule (no attribution).
- ✋ Please use “Raise hand” feature in Zoom to raise a question or comment.
- ▯ Workshop operated under W3C’s Code of Ethics and Professional Conduct.

Link to workshop agenda

Setting the Context:
Devs and Web Security Survey

- **297 developers** surveyed on MDN in May 2023
- **60%** find security aspects “Somewhat challenging” or “Very challenging”
  - 71% – Detecting security vulnerabilities
  - 69% – Understanding security threat
  - 67% – Understanding the Browser Security Model
  - 55% – Safely Integrating Third Party Services
  - 54% – Keeping Frameworks and Libraries Up-to-Date
  - 45% – HTTPS Configuration

Additional concerns raised:
staying updated with new security threats, integrating third-party code securely, the lack of cybersecurity content in formal education, regulatory compliance.

Need to get people talking to each other across silos

Workshop Topics

- How to bring the “secure software supply chain” approach to the web development community?
- Guidance for web developers who work at different levels of the stack?
- How to make web security technologies easier to use and adopt?
- How can OSS focused efforts better support web developers?
- How can OSS review processes serve as inspiration for review of new web specifications?

Possible Outcomes

- Identifying specific work on documentation that could be useful for web developers to help them make better use of existing web security technologies.
- Recommending a new WG in W3C, OpenSSF or elsewhere, or a joint task force.
- Determining what updates are needed in commonly used libraries.
- Describing potential new web features / new language features.
- Calling for updates to commonly used web standard APIs.
- Planning for collaboration between web standards and open source security initiatives.
- Planning for producing concise guidance on security issues that is aimed at web developers.

Live Session 1: Supply Chain Security

- 15:15–16:00 Paper presentations and quick Q&A
  - Software Bill of Materials for web frontends (Jan Kowalleck)
  - Establish Standards to Support Web Access to SBOM Data (Gary O'Neall)
  - Source Code Transparency (Daniel Huigens)
- 16:00–16:10 Break
- 16:10–16:55 Open discussion
- 16:55–17:00 Next steps

Live Session 2: JavaScript Security

- 15:05–15:35 Hardening JavaScript - Paper presentations and quick Q&A
  - Applying Hardened Javascript to supply chain security for a proactive approach (Zbyszek Tenerowicz)
  - JavaScript realms are used to bypass and eliminate many existing web apps security tools span A problem with a WIP solution (Gal Weizman)
- 15:35–16:10 Open discussion on hardening JavaScript
- 16:10–16:20 Break
- 16:20–16:35 Cookies - Paper presentation and quick Q&A
  - Establishing a robust long-term security model for cookies on the web (Artur Janc)
- 16:35–16:55 Open discussion
- 16:55–17:00 Next steps

Live Session 3: Developer Awareness

- 15:05–15:50 Paper presentations and quick Q&A
  - Can securing jQuery help secure the Web forward? (Tobie Langel)
  - Documentation for web security education (Florian Scholz)
  - Roadmap planning for a JavaScript security framework (Joe Sepi, Ben Sternthal)
- 15:50–16:00 Break
- 16:00–16:50 Open discussion
- 16:50–17:00 Concluding the workshop

Thanks!

Thank you for your participation!

Special thanks to the Program Committee:

- Dan Appelquist (Snyk) - chair
- Hadley Beeman (TAG)
- Harold Blankenship (OWASP)
- Jory Burson (OpenJS)
- François Daoust (W3C)
- Robin Ginn (OpenJS)
- Dominique Hazael-Massieux (W3C)
- Arnaud Le Hors (IBM)
- Christopher Robinson (Intel, OpenSSF)
- Vandana Verma Sehgal (OWASP)
- Mike West (Google)