

# HACKATHON PROJECT BRIEF

## FAIR Software Security Assistant

*Automating vulnerability screening and policy enforcement for FAIR-based WordPress repositories.*

Presented by






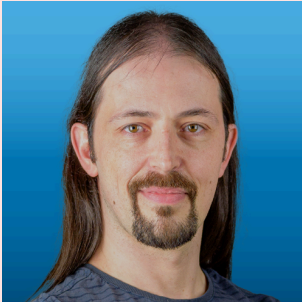
### Project Description

Hosting providers adopting or recommending the FAIR Package Manager need to maintain secure, reliable WordPress repositories at scale. The FAIR Software Security Assistant automates security screening using vulnerability intelligence data from Patchstack, enabling hosting providers and end users to efficiently manage their repositories to maintain security without manual auditing overhead.

This open-source tool will automatically cross-reference packages against Patchstack's comprehensive vulnerability database to ensure synchronized repositories show the latest security information for each package. Hosting providers can apply customizable security policies to manage package approval workflows, ensuring only verified software reaches customer sites.

Proposed key features include automated vulnerability scanning by Patchstack, configurable risk-based approval workflows, compliance reporting, and audit trails. By combining FAIR's decentralized architecture with Patchstack's security intelligence, the tool will empower hosting providers to exercise enhanced control over their WordPress software supply chain to lower risk and improve security. Not only will this enable blocking installation of vulnerable packages, but as an added benefit, end users can opt in to auto-update patches for vulnerable packages that have already been installed.

## Project Leads

	<b>Carrie Dils</b> <i>Project co-lead</i> WordPress Developer & LinkedIn Learning Instructor FAIR TSC Co-chair		<b>Brent Toderash</b> <i>Project co-lead</i> Project Director at Modern Earth & AspirePress Project Manager FAIR TSC Member
	<b>Elliot Taylor</b> <i>Project co-lead</i> Head of Engineering at Patchstack		<b>Alain Schlessler</b> <i>Project mentor</i> Principal Architect at Yeast

## Hackathon Goals 🎯

The project will deliver a working, minimum viable product that addresses hosting provider security workflows.

### Primary MVP Deliverables

- A repository monitoring system that provides current vulnerability labels to FAIR aggregators or end users & verifies the label before installing new/updated packages.
- Security analysis engine integrating Patchstack's vulnerability database for on-the-fly scanning.
- Basic policy engine for risk-based package approvals (approve/flag/block workflows).
- Minimal dashboard to visualize repository security status and flagged packages.

### Stretch Goals

- Compliance reporting and audit trail generation
- Advanced policy configuration interface
- Integration documentation for hosting control panels
- Containerization for deployment
- Managed Vulnerability Disclosure Program (mVDP) integration
- End-user (WordPress site admin) dashboard access to tools & controls

Teams can focus on different components based on expertise: backend API integration, frontend dashboard development, security policy engine, or hosting platform integration.

## Skillsets Needed 🎓

- Full-stack developers with API integration experience
- Frontend developers and UI/UX designers
- Security engineers and DevOps professionals
- WordPress and PHP developers
- System administrators with hosting infrastructure knowledge
- Backend developers experienced with data processing and automation

## Target Audience 🗣️

- Cloud hosting providers and managed WordPress hosting companies
- Enterprise IT teams managing WordPress deployments
- FAIR repository maintainers
- WordPress agencies managing multiple client sites
- DevOps and infrastructure teams implementing FAIR

## Hashtags #

#CloudFest #CloudFestUSA #CFHack #Security #Distributed #WordPress #FAIR #Patchstack  
#OpenSource

## Questions?



**Carole Olinger**

***Head of CloudFest Hackathon***

✉️ [carole@cloudfest.com](mailto:carole@cloudfest.com)