OWASP®

IMPACT REPORT 2025

25 years
of open source security

Index

2025 key stats

A word from our Executive Director, OWASP Foundation, Inc.

2025 has been a landmark year for OWASP, marked by remarkable growth, innovation, and community engagement. Our global community remains vibrant and healthy, with contributors, chapter leaders, and project maintainers collaborating across continents to advance our mission: "No more insecure software."

> **"Our global community remains vibrant and healthy, with contributors, chapter leaders, and project maintainers collaborating across continents to advance our mission: "No more insecure software."**

Key Achievements and Initiatives

OWASP Top 10:2025 Release Candidate
This year, we unveiled the eighth edition of the OWASP Top 10, reflecting the evolving landscape of application security. The 2025 list introduces two new categories - Software Supply Chain Failures and Mishandling of Exceptional Conditions, addressing the root causes of modern software risks. These changes were driven by extensive community input and data analysis, ensuring the Top 10 remains the industry's most trusted resource for prioritizing web application security risks.

Community-Driven Impact
Our community's contributions have never been stronger. We have had many OWASP project releases in 2025, including the standardization of CycloneDX (ECMA - 424), and many releases and updates from our flagship and production projects, such as Dependency Check, Nest, BLT (Bug Logging Tool, although it does a lot more than that), Juice Shop, many new and updated Cheat Sheets, WrongSecrets, Cornucopia, and Core Rule Set.

Global Events and Education
OWASP chapters hosted hundreds of events, workshops, and conferences worldwide, including the Global AppSec Conference in Barcelona, Spain and Washington, DC in the USA in November. Many of our community leaders continue to host AppSec Days events, such as OWASP SnowFroc, AppSec Israel, AppSec Days France, OWASP Italy Day, BASC, and OWASP LASCON to mention just a few. These gatherings foster knowledge sharing, professional development, and the onboarding of new members into our community.

New Leadership and Strategic Growth
We welcomed Stacey Ebbs as our first Communications & Marketing Manager, strengthening our outreach and storytelling as we approach OWASP's 25th anniversary. Additionally, we are in the final stages of hiring a new Director of Corporate Relations, with a core focus on developing new Corporate Supporter packages, increasing the breadth of our Corporate Supporters to include enterprises, fundraising, and grants. Our Board of Directors continues to provide strategic direction, ensuring OWASP's sustainability and alignment with our core values of openness, transparency, and vendor neutrality.

Developer Enablement
The launch of the OWASP Certified Secure Software Developer (OCSD) program empowers developers to demonstrate their secure coding skills, furthering our commitment to education and professional growth.

Advancing Global Security Standards
OWASP has taken a leadership role in advocating for a unified, federated approach to global vulnerability intelligence, reflecting our commitment to innovation and international collaboration in the face of emerging cybersecurity challenges. In particular, the CycloneDX, GenAI project, and AI Exchange projects lead our efforts to standardize supply chain security, and AI.

Enhancing our European operations
In 2025, the OWASP Foundation started on a journey to create a new entity in Europe, called "OWASP Operations Europe VZW." This new entity replaces the defunct OWASP EU VZW entity, with enhanced governance, and greater ability to obtain fundraising and grants throughout Europe. We expect full operations to commence in January 2026.

I wish to thank two outgoing Directors, Avi Douglen, who was our 2024 Chair, and Diego Martins, who will continue to be involved in our new OWASP Operations Europe entity as a director. I welcome two new Board Members, Kelly Santalucia, formerly Director of Corporate Relations at OWASP Foundation, and Marisa Fagan. I look forward to meeting with the new Board at our in-person Board Summit in January 2026.

Looking Ahead
As we celebrate these achievements, we remain focused on our vision: a world where software is secure by default. Our priorities for the coming year are our extensive 25th Anniversary Celebrations. There will be 25th Anniversary events, parties in 12 major chapters throughout the world, custom swag, and more. Please keep in touch with our new website, which will launch in early 2026, and on our social media at LinkedIn, Facebook, X (formerly Twitter), Bluesky and more. As we improve our marketing, we hope to grow our membership base with enhanced membership benefits.

Operations
Looking inwards, as a non-profit, we need to keep a lid on expenses and unnecessary costs. There will be some changes in 2026, including the retirement of our association with Meetup, to be replaced by similar functionality on our website. The new functionality, which we intend to be fully complete by the end of Q1, 2026, will make it faster for people to find and attend chapter meetings.

On a purely internal operations matter, we are looking to consolidate our platforms that contain member and corporate information down to three key platforms (an association management platform for our members, a CRM for our corporate supporters and event sponsors, and Jira for service management), to better protect our community's personal information. All of these platforms feature advanced security and modern privacy controls. This consolidation of platforms also brings efficiency and financial gains.

Lastly, we're going to continue to improve our productivity by using the AI features included with the platforms we use, ensuring good AI governance with respect to security and privacy. For example, our new website is AI coded, which will allow more of our staff to keep the OWASP website up to date, without most of them needing to know how to code. We will be using AI to automate many manual workflows, which should speed up the processing of Jira tickets and allow our community to grow without further inorganic staffing growth.

Thank you to every volunteer, member, sponsor, and supporter who makes OWASP's mission possible. Together, we are building a safer future for everyone.

OWASP Projects: Built by the Community, for the World

OWASP Projects are driven by a global community of dedicated volunteers who collaborate to develop open source tools, resources, and guidance that advance software security. Project Leaders provide strategic direction, ensuring each initiative aligns with OWASP's mission and values.

With over 250 active projects and new contributions emerging regularly, the OWASP community remains at the forefront of innovation in application security.

In 2025, the momentum continued - 62 new projects were launched, alongside major updates and growth in existing efforts.

Highlights from 2025 include:

Application Security Verification Standard (ASVs)

Flagship Project

The OWASP Application Security Verification Standard (ASVs) is a flagship project and a foundational resource for building secure applications. After updates in 2019 and 2021, the team focused on improving scope, clarity, and accessibility for organizations at all maturity levels.

To accelerate progress, ASVs leaders and contributors met at the OWASP Project Summit in London in November 2024, resolving longstanding issues and refining the structure.

Building on this momentum, **ASVs Version 5.0 launched** live at OWASP Global AppSec EU in May 2025, offering expanded content, a modernized structure, and an easier entry point for new adopters.

AI Exchange | Flagship Project

In 2025, OWASP effectively set the standard for AI security, through the AI Exchange.
The Exchange was founded in 2022 by Rob van der Veer, for writing down what he learned on security and privacy of AI systems as an AI engineer, hacker and entrepreneur since the beginning of the nineties. The goal: to help security practitioners with this important new topic, trying to make it comprehensive, but simple.

Through the OWASP network, he quickly gathered a growing group of experts to continue building the body of knowledge and co-leaders Aruneesh Salhotra and Behnaz Karimi joined the project. Then Rob got involved in ISO/IEC 27090, the global standard for AI security and got elected as co-editor of prEN18282, the Security standard for the AI Act. These working groups had a hard time finding the right expertise, so Rob forged a unique liaison partnership between international standardization and the OWASP AI Exchange, allowing the material from the Exchange to be donated directly to these new standards - effectively becoming the main source.

Next, the Exchange was adopted by SANS Institute, ISACA and EXIN, as a key resource for training. The material is open source, free of copyright and attribution, and aligns with standards - making it the perfect material for training and certification. So what started as a personal notebook from experience, turned into an OWASP flagship project with a framework of AI security threats, controls, and best practices that effectively has become the standard, and the go-to bookmark for practitioners to rely on.

owaspai.org

Core Rule Set (CRS) | Flagship Project

The OWASP Core Rule Set (CRS) project is undergoing a major modernization effort to address more than 15 years of accumulated technical debt, while positioning the project for the next decade of scalable, adaptable web application security.

CRS rules are currently written in the ModSecurity Rule Language (Seclang), a syntax shaped by constraints of the Apache era that no longer apply. As a result, rule definitions embed engine-specific configuration, limit portability across WAF implementations, and create a steep learning curve for new contributors.

The modernization effort addresses these challenges through two complementary initiatives: **seclang_parser** and **CRSLang**. Together, they provide a foundation for decoupling rule logic from execution engines, improving developer experience, and enabling broader reuse and automation across the CRS ecosystem.

seclang_parser (v0.3.2): An ANTLR4-based grammar providing canonical Seclang parsing for multiple programming languages (Go, Python). Eliminates inconsistent parsing implementations across the ecosystem.

crslang (v0.1.0): A YAML-based, WAF-agnostic rule representation built on seclang_parser. Enables bidirectional translation between Seclang and the new format, ensuring backward compatibility while opening CRS to new ecosystems like Coraza and cloud-native WAFs.

The 2025 WAF Group (CRS, Coraza & Mod Security) Dev Retreat advanced multiple strategic initiatives to improve the **quality, performance, and sustainability** of the project. Core contributors progressed foundational tooling, modernized validation workflows, and aligned on long-term release and support strategies.

Key technical outcomes included advances in **CRSLang** and the **seclang_parser**, initiation of a full **CRS linter rewrite**, and early exploration of automated self-documentation for rules. These efforts reduce contributor onboarding friction, improve portability beyond ModSecurity-specific engines, and establish a foundation for automated analysis and transformation tooling.

The retreat also strengthened tooling and quality assurance practices. A standardized performance metrics framework was established to enable consistent benchmarking across rule changes, alongside improvements

to quantitative testing methodology and CI/CD quality gates. These enhancements support better decision-making around rule complexity, performance trade-offs, and false-positive detection.

From a sustainability perspective, contributors aligned on a **Long-Term Support (LTS) release model**, targeting annual LTS releases beginning in Q1 2026, providing clearer stability and support commitments for enterprise adopters. The Dev-on-Duty program was reviewed to address changing community engagement patterns and identify more sustainable support channels.

Finally, the retreat explored **emerging technologies**, including the use of AI to improve rule explanation, documentation accessibility, and contributor onboarding. Continued work on metadata-driven lazy rule execution aims to deliver meaningful performance gains for high-traffic environments.

The combined efforts represent a strategic investment in CRS's long-term viability:

- **Portability:** Rules can now target multiple WAF engines without rewrites
- **Accessibility:** Lower barrier to entry for contributors and adopters
- **Maintainability:** Modern tooling reduces technical debt
- **Quality:** Standardized metrics enable data-driven decisions
- **Sustainability:** LTS model and community program reviews ensure project health

These initiatives position OWASP CRS to remain the industry standard for web application firewall rules while adapting to the evolving security landscape.

waf.owasp.org

CycloneDX | Flagship Project

In 2025, OWASP's work in software transparency reached major standardization milestones through Ecma International. At the 130th Ecma General Assembly in Geneva in December, 2025, **CycloneDX v1.7 was ratified as ECMA-424 (2nd Edition)**. CycloneDX v1.6 was the first version ratified in 2024. CycloneDX is the international standard for Bill of Materials supporting a broad set of use cases, including SBOM, SaaSBOM, CBOM, and AI-BOM.

The same General Assembly also approved two additional standards. **OWASP Common Lifecycle Enumeration (CLE) was ratified as ECMA-428 (1st Edition), and Package-URL (PURL) was ratified as ECMA-427 (1st Edition)**. CLE is a new standard focused on lifecycle events that affect M&A, component rebranding, and key milestones such as end-of-life and end-of-support. Package-URL is an OWASP-adjacent project and supported by multiple OWASP projects, including OWASP Dependency-Check and OWASP Dependency-Track. All three standards are advanced within Ecma Technical Committee 54, a standards effort co-designed by OWASP Foundation and Ecma International.

The Ecma General Assembly also voted in favor of moving ECMA-424 and ECMA-427 forward through the ISO/IEC JTC 1 Fast-Track process to pursue broader international adoption.

Looking ahead, development is underway for CycloneDX 2.0, which introduces a modular architecture and expands modeling to include behaviors, threats, and risks. This work aligns the broader threat modeling community behind TM-BOM, bringing together methodology authors, practitioners, and both commercial and open source tooling providers to enable a common standard for sharing threat modeling data and related intelligence.

Finally, OWASP collaborated with the Cyber Security Agency (CSA) of Singapore on a joint advisory titled "**Advisory on Software Bill of Materials and Real-time Vulnerability Monitoring for Open-Source Software and Third-Party Dependencies**", reinforcing OWASP's global impact on practical SBOM adoption and continuous vulnerability monitoring.

cyclonedx.org

csa.gov.sg

Dependency-Track | Flagship Project

In 2025 OWASP Dependency-Track saw significant investment and adoption. The project advanced **Dependency-Track v5.0**, code-named Project Hyades, which is an architectural redesign intended to support portfolios spanning millions of projects and to improve resilience and scalability for large-scale SBOM ingestion and analysis. Early alpha deployments are already demonstrating the scale the project is targeting, including environments with more than 250,000 SBOMs managed in a single Dependency-Track portfolio and sustained ingestion rates exceeding 20,000 SBOMs per hour. We expect Dependency-Track 5.0 to be released in early 2026. In parallel, the 4.x line continued strong adoption, with more than 6,000 organizations upgrading to the latest point release this year, and the project community estimating that more than 20,000 organizations run Dependency-Track in production.

GenAI Security Project | Flagship Project

In 2025, the **OWASP GenAI Security Project** solidified its role as a global leader in open-source research, guidance, and community-driven resources for securing generative AI (GenAI) systems, including Large Language Models (LLMs) and autonomous agentic applications. Originally rooted in the **OWASP Top 10 for LLM Applications**, the initiative grew into a **flagship project** with broad scope, influence, and practical outputs supporting both builders and defenders of AI systems.

Key accomplishments in 2025 included:

• **Expanded flagship research outputs:** The project continued to produce widely-adopted risk frameworks, including the updated Top 10 Risks and Mitigations for LLM and GenAI Applications, along with an evolving Agentic AI Security Top 10 addressing autonomous AI threats and guidance for secure agentic application design. These resources help developers and security teams prioritize and mitigate the most critical AI security risks.

• **Practical solution-oriented reference materials:** The release of the GenAI Security Solutions Reference Guide (Q2–Q3 2025) extended core risk taxonomies by mapping identified threats to both open-source and commercial security solutions, offering actionable pathways for securing AI systems across their operational lifecycle.

• **Actionable guidance for next-generation AI systems:** Complementing risk taxonomies, the project published resources like the Securing Agentic Applications Guide 1.0, providing practical recommendations for designing, developing, and deploying secure agentic AI systems - a rapidly emerging class of autonomous AI capabilities.

• **Ongoing thought leadership and community engagement:** Through the OWASP GenAI blog, the project highlighted topical incidents, research collaborations, and ecosystem partnerships that advanced understanding of real-world AI security challenges and fostered cross-sector collaboration.

Underpinning these outputs was the project's collaborative global community, drawing contributions from hundreds of security practitioners, researchers, and organizations. By making all research and tools openly accessible under permissive licenses, the GenAI Security Project continues to empower practitioners, policymakers, and developers with practical frameworks that bridge academic research and operational practice.

As generative AI becomes increasingly embedded across industries and software ecosystems, OWASP's GenAI Security Project is shaping how the global security community identifies, prioritizes, and mitigates emerging AI-specific risks — ensuring that innovation is matched by a foundation of secure, responsible deployment.

Software Assurance Maturity Model (SAMM)

Flagship Project

The SAMM community remained vibrant throughout 2025, with monthly calls bringing together practitioners, contributors, and adopters to discuss practical usage, updates, and roadmap topics.

SAMM User Days, held in Barcelona and Washington, DC, showcased real-world adoption, case studies, and deep dives into applying SAMM across diverse organizational contexts

Education and enablement efforts included in-person training at dozens of OWASP Chapter events worldwide, as well as a 5-hour online SAMM course, broadening access to structured AppSec maturity education. Regular SAMM-focused podcasts shared practitioner experiences, lessons learned, and insights on software security maturity. Overall, SAMM continues to serve as a practical, vendor-neutral framework, bridging theory and real-world implementation while maintaining strong community engagement and lasting educational impact.

owaspsamm.org

Top 10 | Flagship Project

The OWASP Top 10 is one of OWASP's oldest flagship projects. The Top 10 is a standard awareness document whose purpose is to provide developers, security teams, and decision-makers with a shared language and understanding of the most critical application security risks, helping them focus limited effort on the issues with the greatest real-world impact.

By combining large-scale vulnerability data with community input, the **OWASP Top 10 2025 edition highlights systemic, root-cause weaknesses such as access control, misconfigurations, software supply chain failures, and poor error handling, reflecting how modern applications are built and attacked.**

Its main contribution is to raise the global minimum bar for security development by guiding training, testing priorities, and policy baselines across the industry, while serving as an entry point that organizations can extend into deeper frameworks such as OWASP ASVs and OWASP SAMM for comprehensive application security programs.

owasp.org

OWASP EKS Goat

The OWASP EKS Goat hands-on training reached a global audience in 2025, helping practitioners safely explore AWS EKS security risks. Sessions were delivered at Black Hat Europe (London, 4,500+ attendees), OWASP AppSec Days Singapore (participants from 14+ countries), BSides Bangalore (1,200+ attendees), and Seasides Conference Goa (1,000+ attendees), covering Kubernetes privilege escalation, IAM-to-RBAC abuse, cluster hardening, and real-world attack/defense scenarios.

As the only OWASP project focused on EKS security, EKS Goat provides a deliberately vulnerable environment for hands-on learning and has seen growing adoption, with security teams, SREs, and developers leveraging it to understand and mitigate cloud-native threats.

Production Projects

OWASP WrongSecrets

2025 was the **year of speed** for OWASP WrongSecrets: we upgraded the application to a CDS based container distribution, which allowed our low-end, hobbyist implementation (Heroku Dyno) to perform at a 190 RPS instead of 60, tripling the speed of the application, while remaining very low on resource utilization.

Next, we upgraded the code-base to leverage the best out of Co-Pilot, enabling much quicker challenge development, automated previews on pull-requests, and many improved Q/A steps.

WrongSecrets has seen a wider adoption throughout the year, including many trainings and courses at colleges/universities where OWASP WrongSecrets is used as curriculum and course material.

owasp.org

Lab Projects

OWASP Nest

OWASP Nest is a comprehensive, community-first platform built to enhance collaboration and contribution across the OWASP community. Acting as a central hub, it helps users discover chapters and projects, find contribution opportunities, and connect with like-minded individuals based on their interests and expertise.

Community Growth and Engagement

OWASP Nest continued to grow organically in 2025, attracting new contributors and mentors while strengthening collaboration across the OWASP community.

Standardized OWASP Schema and Automated Data Population

OWASP Nest designed and implemented a unified metadata schema with automated data population to ensure standardized information for all OWASP chapters and projects.

Transparency Report for 2025 Board Candidates

OWASP Nest delivered a structured transparency report outlining each candidate's OWASP contributions, leadership experience, and communication activity to support informed board elections.

REST API v0 and Multi-Language SDKs

OWASP Nest released REST API v0 alongside official Go, Python, and TypeScript SDKs to enable reliable programmatic access to OWASP Nest data.

Contributor Sponsorship Program Launch

The OWASP Nest Sponsorship Program launched in 2025, distributing over $1,000 USD to recognize and support impactful contributor efforts.

nest.owasp.org

OWASP Nettacker

OWASP Nettacker Receives OpenAI Open Source Fund Grant

In April 2025, OWASP Nettacker was selected as a recipient of the first OpenAI Codex Open Source Fund grants, recognizing the importance of community-driven security tooling. The grant provided the OWASP Nettacker Project team with $10,000 in OpenAI API credits and direct access to the Codex coding agent.

OWASP Nettacker is an automated network penetration testing platform designed to help security professionals and organizations scan their networks, identify their assets and vulnerabilities, assess exposure, and strengthen defenses. By making offensive security capabilities more structured and repeatable, the project supports defenders in proactively improving organizations' environments before threats can be exploited.

The selection of Nettacker is significant external validation from one of the world's leading AI organizations. The grant is significant not only as support for Nettacker itself, but also as a broader signal that open source cybersecurity projects are becoming essential to digital public infrastructure. For OWASP, this recognition reinforces the value of practical, globally accessible open source tools that empower researchers, practitioners, and organizations of all sizes to improve their security posture.

owasp.org

Incubator Projects

OWASP AI Vulnerability Scoring System (AIVSS)

OWASP AI Vulnerability Scoring System (AIVSS) launched in June 2025 to provide a **standardized framework for assessing AI-specific security vulnerabilities**, addressing gaps that traditional CVSS cannot cover.

Key 2025 Milestones: The project kicked off in June with the OWASP Top 10 for Agentic AI. By July, AIVSS v0.5 was released for community review, receiving strong global feedback. In November, the project was showcased at OWASP Global AppSec USA 2025 in Washington, DC and was also highlighted on the OWASP Spotlight video series on YouTube. Community engagement extended through January 2026, with AIVSS v1.0 on track for publication before RSA 2026. The team expanded to include Tim Marple (formerly Google/OpenAI) as Co-Lead, joined by Ken Huang, Michael Bargury, Vineeth Sai Narajala, and Bhavya Gupta. A 9-member Expert Review Board ensures rigorous guidance.

Community & Industry Impact: Collaborations with CMU SEI, FIRST, CERT, and OWASP GenAI Security Project, plus co-chairing the Cloud Security Alliance AI Safety Working Group, strengthened adoption and alignment.

Tools & Resources: The open-source AIVSS Calculator democratizes AI security assessment, while the Contributor Risk Ranking Survey ensures v1.0 reflects real-world priorities.

OWASP EKS Goat

OWASP EKS Goat is a hands-on AWS EKS security lab that teaches real-world attack and defense techniques for AWS managed Kubernetes clusters. As the only OWASP project focused on EKS security, EKS Goat provides a deliberately vulnerable environment for hands-on learning and has seen growing adoption, with security teams, SREs, and developers leveraging it to understand and mitigate cloud-native threats.

The OWASP EKS Goat hands-on training reached a global audience in 2025, helping practitioners safely explore AWS EKS security risks. Sessions were delivered at Black Hat Europe (London, 4,500+ attendees), OWASP AppSec Days Singapore (participants from 14+ countries), BSides Bangalore (1,200+ attendees), and Seasides Conference Goa (1,000+ attendees), covering Kubernetes privilege escalation, IAM-to-RBAC abuse, cluster hardening, and real-world attack/defense scenarios.

OWASP Framework for Integrating Application Security into Software Engineering (FIASSE)

FIASSE (pronounced /feiz/ like 'phases of the moon') is a lightweight framework that adapts to your existing software development processes. FIASSE provides a model and principles to create truly securable software by focusing on core software qualities and promoting fundamental Software Engineering capabilities. This makes your security efforts more effective, sustainable, and integrated with the development team.

FIASSE does not intend to replace existing security assurance advice like OWASP PSCF, OWASP SAMM, OWASP ASVs, etc. Instead, it aims to complement other projects by providing a developer-centric framework. It does this by providing a structured approach to securing code through engineering practices.

Launched in 2025, the Framework for Integrating Application Security into Software Engineering (FIASSE) **which is a vendor-neutral approach to embedding security directly into the software engineering discipline**, is now entering the 3rd Project deliverable phase, publish FIASSE and SSEM specifications, including their core attributes and integration strategies, for expected release Q3 2026.

OWASP Spotlight Series

The OWASP Project Spotlight is a dedicated video series that highlights individual OWASP open-source projects, bringing awareness to the breadth and depth of work produced by the community. Each episode focuses on a specific project — explaining its motivation, core purpose, how it works, and ways for community members to contribute. This format makes complex tools and initiatives more accessible to developers, security practitioners, and prospective contributors alike.

owasp.org

Projects at Events

Hackathon

In May 2025, OWASP & Ecma hosted an IETF-style **Hackathon** in Barcelona, a collaborative working session focused on advancing the **Transparency Exchange API (TEA) specification** — the next evolution in secure software supply chain communication. The event brought together open-source leaders, implementers, and security practitioners to test and refine the first beta of the TEA specification in real-world conditions.

Instead of a traditional competition, the hackathon was structured as a **hands-on collaborative workshop**, where participants from both open source and commercial projects worked directly with the TEA Beta 1 specification and tooling, validating cross-implementation interoperability and providing actionable feedback that will shape future development of the transparency standard. This format emphasized OWASP's commitment to **practical collaboration, open standards development, and community-driven impact** in the software supply chain security space.

OWASP Project Demo Lab

In 2025, OWASP introduced the **Projects Demo Lab** at Global AppSec events, strengthening the connection between community innovation and real-world application security practice.

The Demo Lab provides a dedicated space for OWASP Projects to be demonstrated live, enabling attendees to engage directly with Project Leaders and contributors while exploring how open-source tools and frameworks are applied across the software development lifecycle.

By moving beyond theory and into practical implementation, the Projects Demo Lab:

- Increased **visibility** of active OWASP Projects
- Enabled **direct knowledge transfer** between maintainers and practitioners
- Reinforced OWASP's commitment to **vendor-neutral, community-driven solutions**
- **Supported adoption** of open standards and open-source security tooling

The addition of the Projects Demo Lab reflects OWASP's ongoing investment in creating meaningful pathways from open-source contribution to operational security impact. It also provides Project Leaders with a scalable platform to showcase innovation, gather feedback, and grow contributor communities.

As Global AppSec continues to evolve, the Projects Demo Lab plays a key role in ensuring that OWASP events remain practitioner-focused, community-led, and grounded in real-world security outcomes.

Projects represented:

- ASVs Nuclei
- Cornucopia
- Cumulus,
- DefectDojo
- GSoc Mentor Meetup
- Juice Shop
- KubeFIM
- GenAI Security Project
- OWASP Secure Developer Certification
- OWASP Top 10
- SAMM
- Sunshine for CycloneDX
- Web Application Honeypot

OWASP x DEFCON Community

In August 2025, OWASP brought its community-driven mission to DEFCON 33, one of the world's largest and most influential hacker and security gatherings. OWASP's presence reinforced our commitment to open collaboration, practical learning, and empowering builders, defenders, and researchers in the global application security ecosystem.

Across multiple days, OWASP's presence at DEFCON enabled:

- **Direct practitioner engagement** through demos, workshops, and candid discourse
- **Real-time knowledge transfer** between project contributors and global security attendees
- **Amplification of open-source security tools** in an environment rich with offensive and defensive learning
- **Community** building through inclusive spaces that fostered collaboration, mentorship, and new contributor relationships

The DEFCON experience highlights how OWASP continues to expand its impact beyond traditional conference stages—creating spaces for hands-on exploration, community exchange, and practical skill building that resonate with both seasoned professionals and emerging practitioners alike.

Projects represented:

- Amass
- ASVs
- Cheat Sheet Series
- Coraza
- Core Rule Set
- Cornucopia
- Cumulus
- Juice Shop
- GenAI Security Project
- Mod Security
- Security Champions Guide
- SAMM

Chapters

Our Local Chapters are all about people, bringing app security pros together in a space that's free, open, and welcoming to everyone. From hands-on training to practical talks and networking, there's something for everyone to learn and share.

It's incredible to see how chapters keep growing and thriving, creating meetups and events that make the AppSec community feel connected no matter where you are in the world.

42 New chapters set up in 2025 & **822** Chapter Meetings

New chapter Spotlight

Tirana Chapter was established in 2025 with its first chapter meeting in November

“I wanted to set up the OWASP Tirana chapter because Albania and the Western Balkans deserve a strong, open, and collaborative cybersecurity community. My goal is to create a space where engineers, students, and professionals can come together to share knowledge, challenge each other, and raise the security culture across the region. OWASP Tirana is not just about education; it’s about fostering innovation in our local tech ecosystem, empowering the next generation of builders, and connecting our talent with global best practices. I believe our region shouldn’t only adopt security standards we should contribute to shaping them.”

Kreshnik Rexha - Tirana Chapter Leader

New chapter Spotlight

Canberra Chapter.

As the nation's capital, Canberra sits on the front line of global cyber threats. With its concentration of government, critical infrastructure, and national institutions, application security is a critical foundation of cyber resilience. The chapter plays an important role in education, awareness, and enabling the adoption of good application security practices across the community.
The chapter is intentionally inclusive, bringing together developers, cyber teams, operations, and business leaders. If we continue to work in isolation, we will collectively fail. By working together, we reduce friction, build empathy, and form meaningful partnerships across disciplines. The chapter exists to support and grow the local application security community by passing the torch to the next generation, sharing real - world experience, and enabling secure software development that is worthy of trust. OWASP Canberra will be built around the community, not the other way around.

Khaled Sefian - Canberra Chapter Leader

Community

Community is at the heart of who we are and what makes OWASP special. Our members, volunteers, and contributors create the projects, events, and environments where we can all thrive, feel welcome, and make meaningful contributions to our mission of improving software security.

With **5,220 members in 2025**, and a goal to grow even further in 2026, here's what our community has to say about OWASP and the impact it has on them.

"OWASP projects provide me with the required frameworks and guidance to secure applications through the development lifecycle including security culture and education (projects such as ASVs, MASVs, WSTG, Nettacker, Web Goat, Cheat sheets and OWASP Top 10).

OWASP events provide an opportunity to know and understand the emerging technology in applications (such as AI, firmware such as IoT, low-code/No-code), changes in the threat landscape (such as advanced threat vectors like dependencies of third party code, Actions), and the various ways to address applicable threats (such as Threat Modelling, OWASP Top 10, Secure Headers and Security RAT).

Absence of OWASP would mean re-inventing the wheel and lack of uniformity to secure applications."

Shruti Kulkarni

5,220 members in 2025

"Becoming an OWASP member allows me to actively contribute to the global direction of application security, specifically threat modelling, while connecting with a community of industry leaders who share the same passion. Membership strengthens my work in threat modelling and secure-by-design by giving me access to related OWASP projects that will bring opportunities to collaborate, speak, and influence best practices in those fields."

Paul Spruce

"My experience with OWASP truly began when I joined my local chapter. Through volunteering and meaningful connections, I grew as a cybersecurity professional and discovered how important it is to share knowledge and help others learn."

Luciano Balmaceda

Community Partnership

We're stronger together

In a move that speaks directly to the power of open collaboration, OWASP partnered with InfoSecMap, a community-first project dedicated to making InfoSec events and resources more accessible, global, and inclusive.

At its core, OWASP is a community-driven force building free, open resources for anyone who cares about building safer software. InfoSecMap, meanwhile, has been quietly but impactfully connecting the dots across the global InfoSec ecosystem by mapping events, from major conferences to CTFs and local meetups, along with communities and other useful resources, without pay-to-play marketers getting in the way.

This partnership is more than symbolic. It's strategic.

Together, we're working to:

- Expand access to global InfoSec events and resources
- Amplify historically underrepresented voices & geographies in cybersecurity
- Improve community visibility and knowledge sharing across borders

This collaboration is rooted in the belief that open source should also mean open access - and we're building the infrastructure to make that real.

Visit the all new OWASP hub at **infosecmap.com/owasp** to find the latest from OWASP Chapters, Events, and Community

What does OWASP mean to you?

> **OWASP to me is an organization that helps people to write secure code, that is a thriving community where everyone is trying their best to actually create better software and a better community for secure software design.**

Johan Sydseter

> **OWASP means Passionate people with security mindset coming together to save the world.**

Ashwini Siddhi

> **I've always remembered something Jeff Williams once said. As our first board leader, he put it perfectly: People may come to us for the tools, but they stay because of the people.**

Sebastien Deleersnyder

> OWASP always has been for me a lot of things along this magical road. I've been using OWASP material for a long time, and from there I learned about the community, so OWASP first for me means community. It's been enriching all the materials, my courses, and everything I've been doing for the last 15 years. I started by just teaching others how to read the material, then how to use it. From there, I fell in love with the tooling, and nowadays I use it every day. I've made a lot of friends, and that's also what it means to me - it means community, it means friendships, and working toward common goals, getting things done. I stay because my work is giving back to the community that I love, so it means a lot to me.

Felipe Zipitría

> OWASP is the most important organization in the world if we talk about application security. Why, because all these methodologies, good practices, standards, guidelines and tools help everyone who works in the world of application security to make the digital world more secure, and I think this is the leading organization in application security.

Max Alejandro Gómez Sánchez Vergaray

> Security and privacy through Community.

Kim Wuyts

> OWASP means open source. It means standards. It means reference points for application security. But mostly community!

Petra Vukmirovic

> OWASP is all about community. These global events bring everyone together, giving us the chance to meet people we've previously only known online, reconnect with friends, catch up, network, and work together to build more secure software.

Josh Grossman

> OWASP means Spearheading security for applications.

Paul Horton

Engage & Amplify

When we can't meet in person at chapter meetups or events, online platforms are the next best thing. We continue to grow our online engagement through social media as a way to stay connected and share the OWASP mission. In 2026, we will focus on expanding our reach, diversifying our content, and exploring new and creative ways to engage with the community.

A big part of this growth is thanks to the community sharing their content for us to amplify on the foundation.

287,464
Followers

214,000
Followers

4,494
Followers

2,253
Followers

Events

From **Global AppSec conferences** and **AppSec Days** to **Chapter meetings**, OWASP events energize the community and ignite a passion for application security. They blend world-class training, inspiring keynotes, and hands-on learning to create experiences that spark ideas, build skills, and bring security professionals together from around the world.

Fueled by the enthusiasm and dedication of our global community, OWASP events are truly unmatched, born from passion, powered by volunteers, and driven by a shared mission to elevate and transform the security industry.

Conferences hosted in 2025

Global AppSec EU 2025 (Barcelona)
Global AppSec USA 2025 (Washington, D.C)
AppSec Days Bangalore
AppSec Days France
Appsec Days Singapore
AppSec Days Uruguay
AppSec Days Israel
BASC
BeNeLux
German OWASP Day
Italy Day
LASCON
SnowFROC

Global AppSec EU Stats

1010 Overall Ticket sales

810 Conference Ticket sales

180 Training Ticket sales

90% of attendees rated the conference a 4 or 5 out of 5

Global AppSec USA Stats

936 Overall Ticket sales

770 Conference Ticket sales

127 Training Ticket sales

> **In the past few years, we have (re)organized the Events Committee, creating a core team of 6 members that closely collaborate with the OWASP organization to improve Global Appsec events, and where needed, help out in local events. We have recruited an experienced and engaged team of Track Leaders, who each have built a dependable team of reviewers. We refreshed how reviews are done, both for training and presentations, and raised the amount of guidance available to new and prospective presenters. As well, new activities ("Meet The Mentor", "How To Write a CfP", Puppy Room) and soon Pods have been introduced, to raise the value of the event for attendees. We have further ideas and plans, and are looking forward to the events of the 25th anniversary to be of further service to OWASP membership.**

Izar Tarandach - Events Committee Chair

Corporate Supporters

Our Corporate Supporters are essential to the OWASP community. Their support helps power our mission to make software security better for everyone.

Through their contributions, OWASP can grow its programs, share knowledge worldwide, and support a global community of practitioners. In return, supporters gain meaningful visibility across our channels, connecting with 500,000+ followers, millions of monthly site visitors, and thousands of OWASP members.

In 2025 we had 84 Corporate supporter help contribute to our mission.

Here is what a few had to say:

> **Partnering with OWASP globally has been a natural fit for Aikido Security's developer-first mission. These events bring together the AppSec experts who inspire the innovations behind our unified code, cloud, and runtime platform. The depth of discussions and shared passion for secure software make every stop, from Barcelona to Washington DC and beyond, worth returning to.**

Michiel Denis, Aikido Security

> **Understanding and connecting with the AppSec community is crucial to our success as an application security platform. There's nowhere better than OWASP events - from meetups to global conferences - for engaging directly with practitioners and leaders in genuine conversations. Partnering with OWASP is a key part of our strategy.**

Jenn Gile, Head of Community at Endor Labs

> **Sponsoring OWASP Global AppSec events has been a consistently positive experience. The events are well organized, attract an engaged security community, and create meaningful opportunities for knowledge sharing and networking. Our participation has also led to valuable connections that support our broader business growth.**

Paula Alfaro - SecureFlag

A word from the Chairman of the Board

Governance & Structure

We spent a significant portion of this year doing the often unseen but essential work of governance.

We reviewed and refined board policies, clarified director responsibilities, strengthened conflict-of-interest and anti-trust safeguards, and modernized our approach to elections and board operations. These are not glamorous tasks, but they are foundational. They ensure that OWASP remains credible, transparent, and resilient as it continues to grow globally.

What matters most to me is that we approached these changes deliberately, with respect for our history and with an eye toward sustainability.

Operational Progress

This year also marked steady progress operationally.

We received regular financial reporting, improved visibility into cash flow and receivables, and continued to professionalize how the foundation manages its resources. That discipline gives us flexibility. It allows us to support projects, chapters, events, and staff with confidence rather than reaction.

We also saw forward movement on long-standing initiatives like the website redesign, marketing strategy alignment, and major milestone planning, including preparations for OWASP's 25th anniversary.

Community & Global Perspective

One of OWASP's greatest strengths is its global reach, and this board leaned into that.

We heard perspectives from across regions, supported initiatives like international training days, and remained mindful that decisions made at this table ripple outward to chapters, project leaders, and volunteers worldwide.

This year reminded us that global governance requires listening just as much as leading.

> **"This year was not about a single headline initiative. It was about maturity. About strengthening how we govern, how we decide, and how we serve the community that trusts us."**

Board Culture & Transitions

I also want to acknowledge the culture of this board.

We didn't always agree, and that's a good thing. But we consistently showed respect, curiosity, and a shared commitment to the mission. We debated hard issues thoughtfully and kept the organization's best interests at the centre of those discussions.

As we've seen today, this year also includes meaningful transitions. Board service is finite by design, and the willingness of leaders to step in, serve fully, and then step aside responsibly is a sign of a healthy organization.

Looking Ahead

As we move into the next year, we do so with clearer structures, stronger foundations, and renewed momentum.

The work ahead will require focus, discipline, and collaboration, but this board has demonstrated that it can meet those demands. My confidence in this group, and in OWASP's future, is stronger than ever before.

About the OWASP Foundation Global Board

The OWASP Foundation Global Board consists of seven elected members who serve two-year terms. Each fall, the membership participates in the election of new leadership. The Board typically meets monthly, with meetings open to the public, and follows a standard agenda that is recorded for transparency. The Global Board provides strategic direction for the Foundation, establishes policies, oversees the annual budget, and defines governance and leadership roles.

Our 2025 Board Members:

Ricardo Griffith
Chair

Steve Springett
Vice Chair

Harold Blankenship
Treasurer

Avi Douglen
Member at Large

Ashwini Siddhi
Member at Large

Diego Martins
Member at Large

Sam Stepanyan
Secretary

Balance Sheet | As of December 31, 2025

	TOTAL
Assets	
Current Assets	
Bank Accounts	
Bill.com Money Out Clearing	-152.52
Chase Checking-5767	753,605.75
Chase Checking-9635	2,986.00
Chase Savings-1751	536,515.69
Citizens Checking 4011	15,385.45
Citizens Money Market -2008	207,948.28
GlueUp Clearing Account	0.00
Total Bank Accounts	**$1,516,288.65**
Accounts Receivable	
Accounts Receivable	369,133.64
Accounts Receivable (A/R) - AUD	0.00
Accounts Receivable (A/R) - EUR	17,127.92
Accounts Receivable (A/R) - GBP	18,253.11
Accounts Receivable (A/R) - SGD	431.50
Total Accounts Receivable	**$404,946.17**
Other Current Assets	
2 month CD Acct #1170	175,655.59
3 month CD Acct #3862	175,040.47
3 month CD Acct #3863	175,040.47
Due from Eventbrite	22,769.76
Due from OWASP Europe VZW	0.00
PayPal - EUR	-104.93
PayPal - PLN	0.00
PayPal - SGD	0.00
PayPal - USD	64,662.87
Stripe Clearing	1,990.25
Suspense Payments	0.00
Undeposited Funds	7,500.00
Total Other Current Assets	**$622,554.48**
Total Current Assets	**$2,543,789.30**
Fixed Assets	
Equipment	0.00
Accumulated Depreciation	0.00
Equipment	0.00
Total Equipment	**0.00**
Total Fixed Assets	**$0.00**

Balance Sheet | As of December 31, 2025

Other Assets	
Due from Employee	1,582.53
Prepaid Expense	263,990.33
Total Other Assets	**$265,572.86**
Total Assets	**$2,809,362.16**
Liabilities and Equity	
Liabilities	
Current Liabilities	
Accounts Payable	
Accounts Payable	19,247.53
Accounts Payable (A/P) - AED	0.00
Accounts Payable (A/P) - AUD	0.00
Accounts Payable (A/P) - CAD	0.00
Accounts Payable (A/P) - CHF	0.00
Accounts Payable (A/P) - EUR	16,266.28
Accounts Payable (A/P) - GBP	21.95
Accounts Payable (A/P) - ILS	0.00
Accounts Payable (A/P) - INR	457.67
Accounts Payable (A/P) - JPY	0.00
Accounts Payable (A/P) - NOK	0.00
Accounts Payable (A/P) - SGD	402.71
Accounts Payable (A/P) - UYU	0.00
Affiliate - Accounts Payable	0.00
Total Accounts Payable	**$36,396.14**
Credit Cards	
Amex-Plum Card	-0.30
Commerce Credit Card	3,083.48
Total Credit Cards	**$3,083.18**
Other Current Liabilities	
Accrued Liabilities	0.00
Deferred Revenue	68,358.86
EU Tax Liability	128,973.00
US Tax Liability	12,847.64
Total Other Current Liabilities	**$210,179.50**
Total Current Liabilities	**$249,658.82**
Total Liabilities	**$249,658.82**

Balance Sheet | As of December 31, 2025

Equity	
Affiliate - Net Assets	0.00
Opening Bal Equity	0.00
Restricted net assets	0.00
Retained Earnings	2,440,853.90
Net Income	118,849.44
Total Equity	**$2,559,703.34**
Total Liabilities and Equity	**$2,809,362.16**

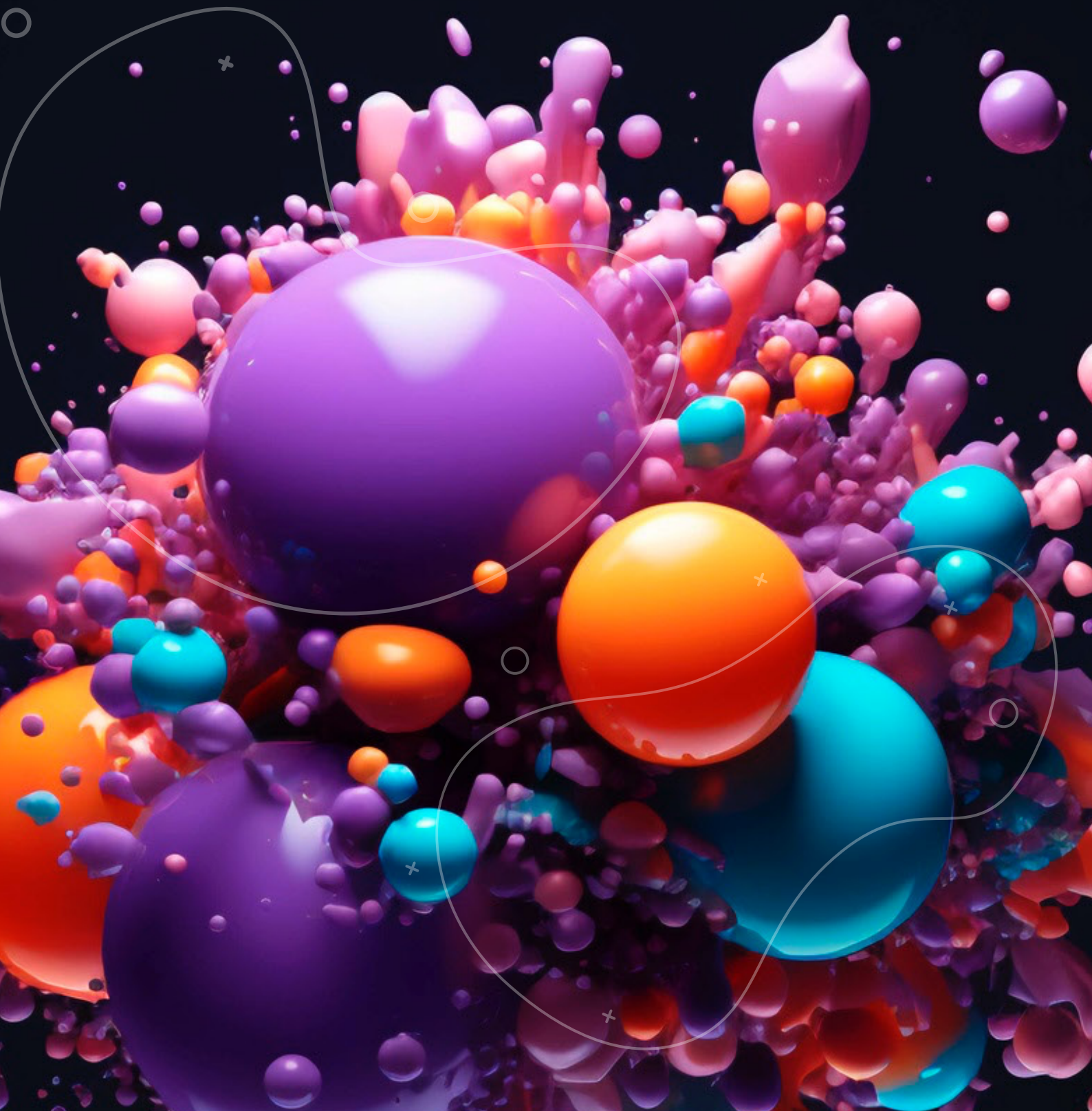
Profit and Loss | January - December 2025

	TOTAL
Income	
Conference Income	
Registrations	936,619.00
Sponsorships	1,997,066.69
Training	478,120.53
Total Conference Income	**3,411,806.22**
Donations	
Corporate Supporters	346,867.88
Fundraising	105.13
General Donations	40,223.04
Local Chapter	3,727.48
Project Income	572.76
Projects Donations	500,719.58
Total Project Income	**501,292.34**
Total Donations	**892,215.87**
Membership Income	
Individual	236,283.53
Total Membership Income	**236,283.53**
Miscellaneous Income	36,265.08
Uncategorized Income	18,000.00
Total Income	**$4,594,570.70**
Gross Profit	**$4,594,570.70**
Expenses	
Community Outreach	
Community Outreach Travel	1,946.38
Outreach	409.48
Shipping & Postage	6,883.94
Swag	30,516.82
Total Community Outreach	**39,756.62**
Conference Expenses	
Audio & Video	371,419.31
Conference Expenses	148,438.17
Conference Travel	138,137.07
Contractor Expenses	424.47
Copying & Printing	6,846.36
Fees - Registration	24,924.22
Food & Beverages	752,263.93
Graphic Design	12,934.25
Insurance	6,251.66
Lead Scanners, Lanyards, & Badges	25,206.86

Marketing	15,081.90
Miscellaneous	20,708.36
Office Supplies & Equipment	4,123.51
Photography	4,591.87
Postage & Shipping	463.63
Signage	12,246.61
Speakers	1,979.06
Speakers Gifts	9,181.89
Swag	22,956.93
Tax Compliance	9,071.93
Training	249,731.01
Venue	465,220.26
Total Conference Expenses	**2,302,203.26**
General & Admin - Operations	
Awards and Member Benefits	1,353.40
Bank & Credit Card Fees	32,207.97
Contractor Expenses	2,299.28
Employee Recognition	1,062.68
Marketing, Communications, and Advertising	907.67
Merchant Fees	54,886.80
Miscellaneous Expenses	-66.50
Office Supplies & Equipmen	687.47
tOWASP Insurance	34,041.74
Phone Expenses	1,410.76
Professional Development	2,377.99
Relocation Expenses	12,817.55
Shipping & Postage	1,592.39
Software, Internet, Dues, & Subscriptions	206,305.77
Tax Compliance - EU	18,441.76
Tax Compliance - US	1,013.43
Travel	
Board Travel	54,839.75
Staff Travel	3,583.70
Total Travel	**58,423.45**
Total General & Admin - Operations	**429,763.61**
Local Chapter Expenses	
Meeting Expenses	90,786.57
Meetup	16,253.10
Other Chapter Expenses	54.51
Your Membership	
Total Local Chapter Expenses	**1107,094.188**

Personnel & Payroll	
Benefits	89,962.23
Gross Wages	965,910.28
Payroll Processing Fee	11,116.31
Payroll Taxes	98,021.30
PEO Admin & HR fees	13,282.25
Tech Allowance	1,757.42
Workers Comp	55,031.78
Total Personnel & Payroll	**1,235,081.57**
Professional Fees	
Accounting - EU	16,504.62
Accounting - US	105,840.00
Legal	42,640.38
Total Professional Fees	**164,985.00**
Project Expenses	
Other Expenses	24,508.08
Project Expenses	89,542.22
Project Travel	35,910.59
Services (UI/UX, Graphics, Translations & Marketing/Media)	62,061.15
Shipping Cost	1,102.14
Summits	20,159.64
Swag	12,245.74
Technology	17,556.30
Total Project Expenses	**263,085.86**
Total Expenses	**$4,541,970.10**
Net Operating Income	**$52,600.60**
Other Income	
Interest Income	24,360.48
Other Income	58,051.84
Total Other Income	**$82,412.32**
Other Expenses	
Unrealized Gain or Loss	0.00
Exchange Rate Gain/Loss	5,542.12
One time write offs - Bad Debt Expense	10,621.36
Total Other Expenses	**$16,163.48**
Net Other Income	**$66,248.84**
Net Income	**$118,849.44**

Awards 2025



WASPY awards

Each year, countless individuals devote their time and talent to advancing the OWASP mission. Some are well known within the community, while many others make significant contributions behind the scenes. These awards are designed to recognize those who fly under the radar, passionate contributors who volunteer their time to strengthen OWASP and improve the cybersecurity landscape, yet often do so without public recognition.

The 2025 WASPY award Winners

Chapter Person of the Year

John DiLeo

John is a Lifetime Member of OWASP, having first joined in 2014, while living and working in Kansas City, Missouri. He has been active in the New Zealand Chapter since moving to Auckland in late 2017.

John took on a leadership role in the New Zealand Chapter in April 2018, restarting the Auckland Meetup, which he led until May 2024, when he moved to Hamilton. Once settled there, John launched the Hamilton Meetup, which is now going strong.

John became Chair of the annual OWASP New Zealand Day conference in 2019, keeping it going through COVID lockdowns, border closures, and travel bans. This year, he is coaching his successor, so he can 'retire' as conference chair after his seventh. John helped organize the student-focused security.ac.nz event in 2019 and 2022. He also organizes OWASP Training Day events around New Zealand.

Beyond the chapter, John has been a member of the OWASP SAMM Project's core team since 2018, has been part of the Chapters and Education and Training Committees, and has founded a number of small OWASP projects.

Event Person of the Year

Jim Manico

Jim Manico has been deeply involved in the OWASP community for more than two decades, beginning his volunteer journey in 2003. Over the years, he has taken on a wide range of leadership and hands-on roles.

Global Governance
Elected to OWASP's Global Board of Directors (2011 – 2014), where he helped shape the foundation's strategic direction, fundraising model, and community-driven governance.

OWASP Cheat Sheet Series (2009 - present)
Co-founder and long-time project manager, coordinating dozens of security cheat sheets that distil complex topics into actionable, developer-friendly guidance.

OWASP Application Security Verification Standard (ASVs) & Artificial Intelligence Security Verification Standard (AISVS)
Core contributor and project manager, ensuring that both standards remain technically rigorous, developer-centric, and mapped to modern threat landscapes.

Regular contributor to other flagship initiatives, including the OWASP Top Ten and Proactive Controls.

Community Building & Education
A frequent keynote speaker and trainer at AppSec USA, AppSec EU, and dozens of local OWASP chapters, Jim has delivered hundreds of secure-coding workshops worldwide, championing open knowledge and evidence-based practices.

Recognition. Honored with OWASP's Lifetime Achievement Award (2023) for sustained, high-impact service—a testament to his belief in the foundation's mission of "making software security visible, so that individuals and organizations can make informed decisions.

A true believer in OWASP's open, vendor-neutral ethos, Jim remains an active contributor, mentor, and evangelist - continuing to advance the state of software security through community-driven standards, education, and tooling.

Project Person of the Year

Jannik Hollenbach

Jannik joined OWASP around 2017 after being introduced to the Juice Shop project at university. He then became a regular contributor to the Juice Shop project and created the MultiJuicer project to enable people to run trainings and workshops with Juice Shop. He is now a project lead for both the OWASP Juice Shop and OWASP secureCodeBox projects.

OWASP Distinguished Lifetime Award

OWASP values the dedication of our volunteer community, whose ongoing efforts play a vital role in advancing our mission and strengthening our leadership in application security. The OWASP Distinguished Lifetime Award is presented by the Board to recognize individuals who have made exceptional, long-term contributions to the organization.

Our 2025 recipients were:

Seba Deleersnyder

Sebastien (Seba) Deleersnyder, co-founder and CTO of Toreon, combines software engineering expertise with a passion for holistic product security. After earning his Master's in Software Engineering from the University of Ghent, he became a driving force in the security community as founder of the Belgian OWASP chapter, OWASP Foundation Board member, and co-founder of BruCON, Belgium's annual security conference. His leadership of OWASP SAMM and decade-long role as a highly-rated Black Hat trainer have significantly impacted global software security.

Christian Folini

When Christian Folini made his debut at the OWASP AppSec conference in Milan in 2007, he quickly found himself invited to share his insights on a panel discussing the emerging PCI DSS Web Application Firewall (WAF) requirements.

Over the years, he has evolved into a cornerstone of the open-source WAF community. As the author of the second edition of the ModSecurity Handbook, he is one of the go-to experts for all things rule language. Folini introduced groundbreaking concepts such as the OWASP CRS Paranoia Levels and the notion of strict siblings.

His innovative spirit led to the design of the CRS plugin architecture and the inception of the CRS dev-on-duty program. Moreover, Folini played a key role in transitioning ModSecurity to become a part of the OWASP Foundation. Beyond his contributions to OWASP, Christian Folini is a member of the steering committee for the Swiss National Cyber Strategy. He is also the public face of the Swiss Cyber Storm conference and continues to shape the cybersecurity landscape both in Switzerland and on a global level.

Josh Grossman

Outside of his day job as an AppSec practitioner, Josh has been involved with OWASP in many different roles. This includes serving as a co-leader of the Israel chapter (and co-organizing the legendary AppSecIL conference), serving as a member of the events committee, and also working as a co-leader of the OWASP ASVs project.

Andrew van der Stock

Andrew is well known throughout the OWASP community for his hard work on several key OWASP projects, including the OWASP Top Ten and the OWASP ASVs. He has also served the community in leadership roles, representing OWASP on the Global Board of Directors from 2015 to 2018 and serving as the Foundation's Executive Director since 2020.

Board Member updates

Steve Springett
Chair

Ricardo Griffith
Vice Chair

Harold Blankenship
Treasurer

Sam Stepanyan
Member at Large

Ashwini Siddhi
Member at Large

Kelly Santalucia
Member at Large

Marisa Fagan
Secretary

What's next?

A look ahead to our 25th Anniversary

We've got an exciting year ahead, packed with celebrations, special events, exclusive swag, and plenty more. Be sure to follow our social channels and check our website so you don't miss a thing!

We want all of you to celebrate with us.
Let's make this anniversary year one to remember!

Save the dates

Global AppSec EU
Vienna
June 22-26, 2026

Global AppSec USA
San Francisco
November 2-6, 2026

OWASP 25th Anniversary Virtual Conferences
Feb 24th 2026
September 21st 2026

OWASP London Training Days
Feb 25th -28th 2026

And many more!

Ways you can get involved in 2026:

Become a Member for just

$50 a year!

Membership →

Join a Chapter and meet your local community

Join a chapter →

Contribute to a project and become part of the movement

Go to projects →

Make a donation, a little really does go a long way in helping create and maintain this amazing community

Donate →

Become a corporate supporter and play a vital role in supporting the foundation's mission

Supporter →

Join us at one of our many events happening throughout 2026

Go to events →

→

Contribute to Content Creation – We're aiming to create even more amazing content this year, social posts, videos, collateral, swag, the sky's the limit! Keep an eye out for content capture forms coming your way in 2026 so you can be featured and help share your story with the community.

→

Spread the word - Help us share our message and promote OWASP through online engagement or just good old-fashioned word of mouth!

OWASP®

IMPACT REPORT 2025

25 years
Of open source security

owasp.org