The Next 25 Years

Andrew van der Stock
Executive Director
OWASP Foundation, Inc.

Thank You to Our Sponsors and Hosts!

Without them, this Conference couldn't happen.

Andrew van der Stock

Executive Director, OWASP Foundation
Former Board member 2015-2018

OWASP Top 10 co-leader
Former OWASP ASVS co-leader
Former OWASP DevGuide leader

AppSec since 1998
Cats


No more insecure software

To be the global open community that powers secure software through education, tools, and collaboration

As the world's largest non-profit organization concerned with software security, OWASP:

Supports the building of impactful projects

Develops & nurtures communities through events and chapter meetings worldwide

Provides educational publications & resources

Enable developers to write better software, and security professionals to make the world's software more secure.

NBSIR 76-1041

Security Analysis and Enhancements of Computer Operating Systems

Institute for Computer Sciences and Technology
National Bureau of Standards
Washington, D. C. 20234

April, 1976

Final Report

U S. DEPARTMENT OF COMMERCE
NATIONAL BUREAU OF STANDARDS

n	26 lower-case letters	36 lower-case letters and digits	62 alpha-numeric characters	95 printable characters	all 128 ASCII characters
1	30 msec.	40 msec.	80 msec.	120 msec.	160 msec.
2	800 msec.	2 sec.	5 sec.	11 sec.	20 sec.
3	22 sec.	58 sec.	5 min.	17 min.	44 min.
4	10 min.	35 min.	5 hrs.	28 hrs.	93 hrs.
5	4 hrs.	21 hrs.	318 hrs.	112 days	500 days
6	107 hrs.	760 hrs.	2.2 yrs.	29 yrs.	174 yrs.

One has to conclude that it is no great matter for someone with access to a PDP-11 to test all lower-case alphabetic strings up to length five and, given access to the machine for, say, several weekends, to test all such strings up to six characters in length. By using such a program against a collection of actual encrypted passwords, a substantial fraction of all the passwords will be found.

Evolution of the OWASP Top 10

2003

A1	**Unvalidated parameters**
A2	Broken access control
A3	Broken authentication and session management
A4	Cross Site Scripting (XSS) Flaws
A5	Buffer overflows
A6	Command Injection Flaws
A7	Error Handling Problems
A8	Insecure use of cryptography
A9	Remote administration flaws
A10	Web and application server misconfiguration

Evolution of the OWASP Top 10

2004

A1	**Unvalidated input**
A2	Broken access control
A3	Broken authentication and session management
A4	Cross Site Scripting (XSS) Flaws
A5	Buffer overflows
A6	Injection Flaws
A7	Improper Error Handling
A8	Insecure storage
A9	Denial of service
A10	Insecure configuration management

Evolution of the OWASP Top 10

2007

A1	**Cross site scripting (XSS)**
A2	Injection Flaws
A3	Malicious File Execution
A4	Insecure Direct Object Reference
A5	Cross Site Request Forgery (CSRF)
A6	Information Leakage and Improper Error Handling
A7	Broken authentication and session management
A8	Insecure cryptographic storage
A9	Insecure communication
A10	Failure to restrict URL access

Evolution of the OWASP Top 10

2010

A1	**Injection**
A2	Cross Site Scripting (XSS)
A3	Broken Authentication and Session Management
A4	Insecure Direct Object References
A5	Cross Site Request Forgery (CSRF)
A6	Security Misconfiguration
A7	Insecure Cryptographic Storage
A8	Failure to Restrict URL Access
A9	Insufficient Transport Layer Protection
A10	Unvalidated Redirects and Forwards

Evolution of the OWASP Top 10

2013

A1	**Injection**
A2	Broken Authentication and Session Management
A3	Cross Site Scripting (XSS)
A4	Insecure Direct Object References
A5	Security Misconfiguration
A6	Sensitive Data Exposure
A7	Missing Function Level Access Control
A8	Cross Site Request Forgery (CSRF)
A9	Using Known Vulnerable Components
A10	Unvalidated Redirects and Forwards

Evolution of the OWASP Top 10

2017

A1	**Injection**
A2	Broken Authentication
A3	Sensitive Data Exposure
A4	XML External Entities (XXE)
A5	Broken Access Control
A6	Security Misconfguration
A7	Cross Site Scripting (XSS)
A8	Insecure Deserialization
A9	Using Components with Known Vulnerabilities
A10	Insufficient Logging and Monitoring

Evolution of the OWASP Top 10

A1	**Broken Access Control**
A2	Cryptographic Failures
A3	Injection
A4	Insecure Design
A5	Security Misconfiguration
A6	Vulnerable and Outdated Components
A7	Identification and Authentication Failures
A8	Software and data integrity failures
A9	Security Logging and Monitoring failures
A10	Server Side Request Forgery (SSRF)

2021

OWASP:
The first nearly 25 years

Humble but ambitious beginnings

Started by three people in Mark Curphey's apartment in September 2001

"In short the project aims to help everyone build more secure web applications and web services."

- First Website December 2001
    - SSL available after 2011

Owasp

OPEN WEB APPLICATION SECURITY PROJECT

Home

OFFICIAL LAUNCH

We are extremely pleased to finally officially launch OWASP, the "Open Web Application Security Project". For those that have been following the site and mailing list for the last 8 weeks you'll be a part of the 250,000 web hits, and this will be nothing new; but given our new technical committee it made sense to re-launch the efforts with some basic work already done.

In short the project aims to help everyone build more secure web applications and web services. We will be covering a wide range of related work over the coming years and have initially defined two areas to concentrate on.

Attack Components - The Application Security Attack Components project was started as an attempt to create common language and definitions for which much of the other work planned at OWASP can later benefit. When describing security issues in web applications or when attempting to model security it is very easy to describe the same issue in many different ways, seemingly creating new problems. When analyzing problems described on Bugtraq it is evident that most problems are variants of common issues, but applied to different applications or systems using different parameters or targets. The aim is definitely not to build the biggest list of problems or describe attacks like Nimda or Code Red; but to document the underlying primary attack components that are used in attacks so people can learn to avoid developing them and others can learn to test for them.

We have a good initial start although focused on mainly external attack black-box type issues. The current list can be found here.With our new team we hope to flesh out this list to include internal "with knowledge" attacks as well as cryptographic issues and any other classes we need to include. The work is scheduled to take place in December of this year.

Testing Framework - As with any emerging technology like web application security where there is a lack of documented knowledge and experience, it is hard to know how to be sure that security has been implemented correctly; protecting the application, the data and the user. As in the early days of network security some people would have you believe application security is a black art. If you ask a security vendor to conduct an application security review today, it could consist of anything from a consultant pressing "scan now" on an automated tool designed to find holes in operating systems, to a full blown line by line code review. What is the correct way to test security of web applications and web services? The Web Application Security Testing Framework is setting out to produce an industry standard blueprint for how to methodically test the security of all web applications and web services. The work is likely to include modelling security attacks (maybe in XML) and is likely to use "Attack Trees" to define paths of attack. The framework will be open to all and will be extensible to be able to be used in all web applications scenarios. It will discuss the difference between white-box testing and black box testing, describe tool and techniques as well as describe how to conduct tests, analyze results, fix problems and report findings. The framework will help everyone build more secure web applications and web services. One ultimate goal that has been put forward is to also produce a web service where all users can download sets of known or experimental attacks (and possibly build them online) for import into reference tools either developed by the project or commercial tools. The specifications would be published and made freely available. The web service effectively would de-couple the current situation where commercial tools have both knowledge and techniques, thus making the security knowledge available to everyone and the tools stand on the merit of the tools themselves. This idea will depend on funding, probably from the government.

NEW OWASP TECHNICAL COMMITTEE

The Technical Committee is made up of renowned application security experts who ensure that the work and ideas produced by the project are technically sound. These people have a wealth of experience and knowledge and will be guiding much of the direction of the work in various areas. As well as participating on the mailing list the technical committee has a monthly conference call to discuss progress. They are the OWASP technical think tank!

- **Elias Levy**
  - probably best known as the long-time moderator of Bugtraq at securityfocus.com and author of "Smashing the Stack for Fun and Profit"
- **Chris Wysopal**
  - formerly with the L0pht and heads up the @Stake Application Security Center of Excellence.
- **John Viega**
  - wrote 'the' book on "Building Secure Software" and is author of RATS (Rough Auditing Tool for Security) as well as hundreds of articles and several other books. John is the CTO of Secure Software.
- **Greg Hoglund**
  - well known for his work on buffer overflows and his Black Hat presentations, as well a respected developer of security and fault injection software at ClicktoSecure.

OWASP WEBSLEUTH

WebSleuth is an early release of a concept tool which will become part of the Testing Framework Toolkit. We hope to have a complete suite of open source tools including source code analyzers which support the Testing Framework and help people secure their web applications. Released under the OWASP open source license, WebSleuth allows you to manually browse a web application, intercepting traffic and being able to modify it in the fly in real-time, exploring security. This allows you to change cookies, generate raw HTTP requests, parse HTML and client-side JavaScripts, as well as automatically parsing comments and forms for known issues. The next release due this week will incorporate the ability to test for cross-site scripting in all web forms.

It works over HTTP and SSL without having to use a proxy. The application is not cross platform and only runs on Win32 as it make extensive use of the Internet Explorer object. The lead developer David Zimmer is always looking for feedback and ways to improve the tool.

Download from our Framework Tools section.

NEWS UPDATES

OWASP Foundation

Founded April 2004 by Jeff Williams and Dave Wichers

- Non-stock membership organization
- IRS 501 (c) (3)
- Deliberately kept small
- First full-time employee wasn't until 2011
- Currently, six staff and one contractor

First appointed Board 2007

First elected Board 2011

Revised Certificate of Incorporation and Bylaws 2024

Community

2001 – 2019

Listman mail lists

2019–

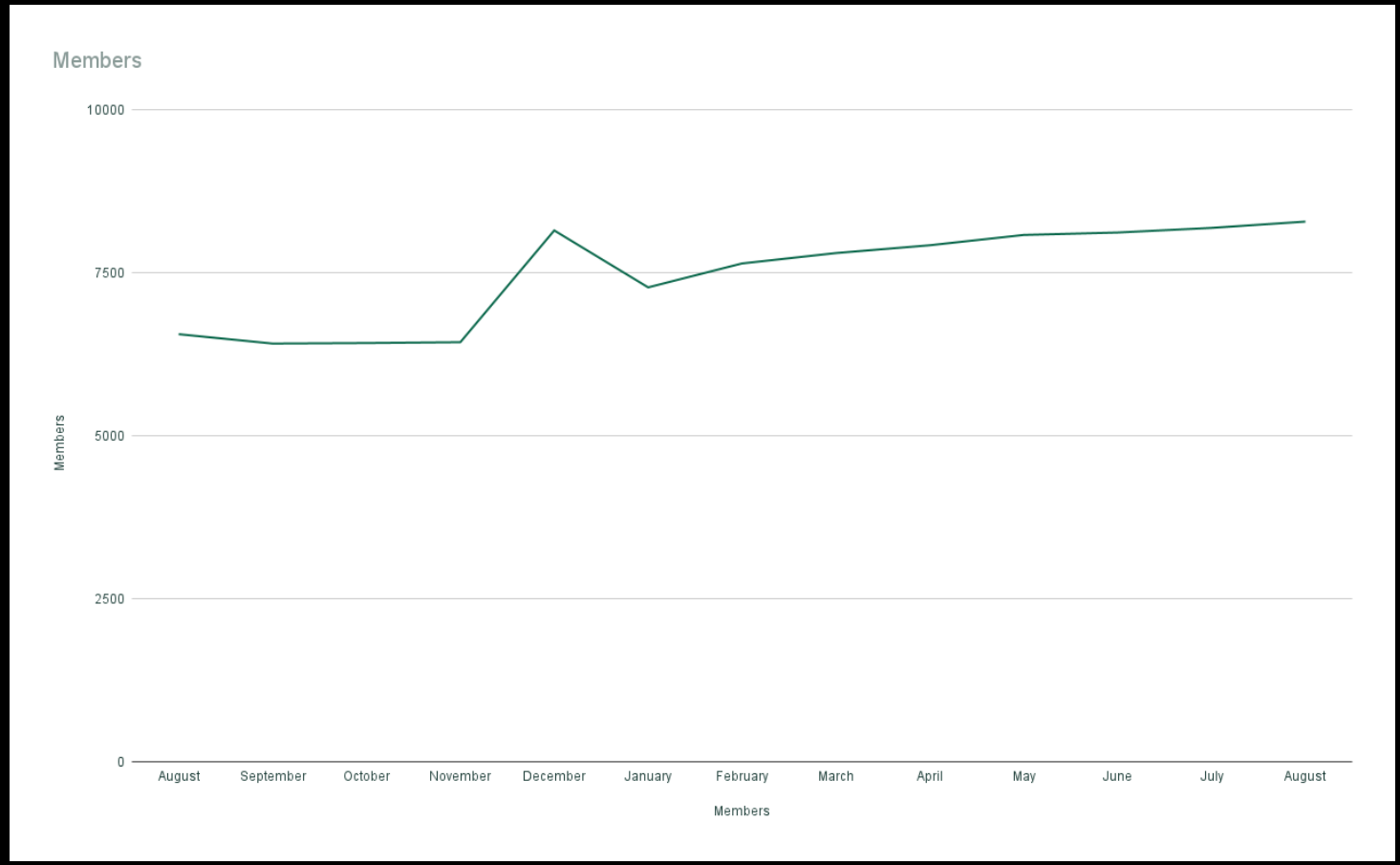
Google Groups

2015–

Slack

Members

- First members 2006
  - $100 USD per year
- Now 8339 members
- Leaders as members



First chapters

First chapters August 2004

Quickly spread all over the world

- Los Angeles
- Boston
- San Antonio
- London
- Panama City
- Austria
- Atlanta
- Washington DC
- Toronto
- Switzerland
- Rochester, New York
- New York City
- Ireland
- San Francisco
- Sydney

Now

279
Chapters

First projects

- First projects:
  - Testing Framework
  - Attack Components
  - WebSleuth
  - XML Data Exchange
- Developer Guide 1.0 2002
- OWASP Top 10 1.0 Jan 2003

Now

345 Projects

- Flagship
- Production
- Lab
- Incubator

OWASP Amass

OWASP Application Security Verification Standard (ASVS)

OWASP Cheat Sheet Series

OWASP CycloneDX

OWASP Defectdojo

OWASP Dependency-Check

OWASP Dependency-Track

OWASP Juice Shop

OWASP Mobile Application Security

OWASP CRS

OWASP OWTF

OWASP SAMM

OWASP Security Shepherd

OWASP Top Ten

First events

Now

100+ Events

- Lisbon
- San Francisco
- Singapore

- AppSec EU 2025
- AppSec USA (DC)
- AppSec NZ 2025

OWASP SnowFROC

OWASP BASC

OWASP AppSec Days PNW

OWASP AppSec Days Spain

OWASP AppSec Days Panama

OWASP German Day

OWASP AppSec Days Virtual India

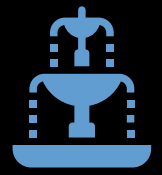
OWASP BeNeLux

OWASP Lascon

... and many more!


The road to 2026
Achievable Hairy Audacious Goals

Agile all the things



OWASP Projects are often stuck in the waterfall and on-prem age

Projects consumable by developers

Align with current development practices (cloud, CI/CD)

Developer Outreach

WE NEED TO SPEAK AT DEVELOPER CONFERENCES

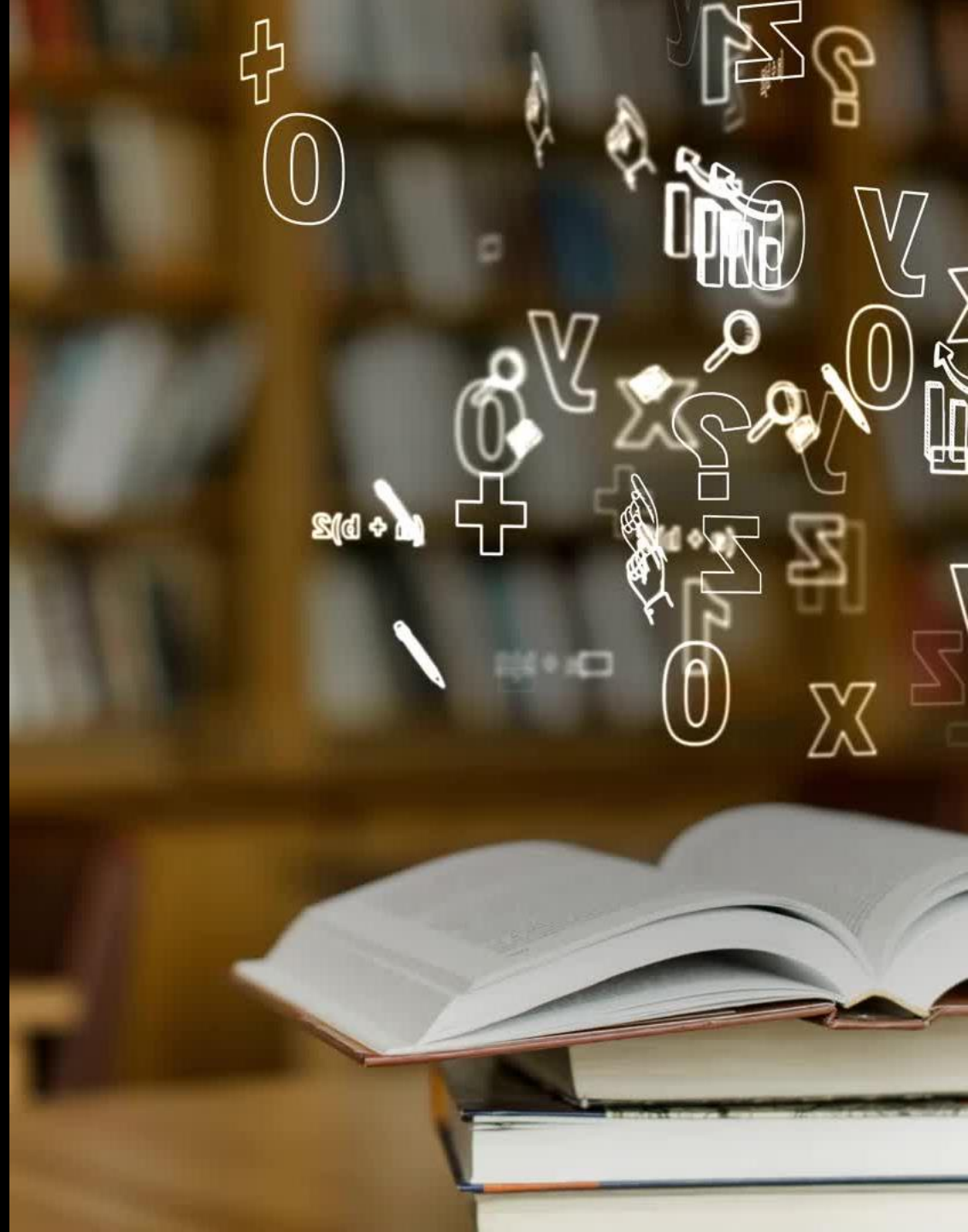
WE NEED TO TRAIN AT DEVELOPER CONFERENCES

WE NEED BOOTHS AT DEVELOPER CONFERENCES

OWASP IS SKIPPING RSA, BLACK HAT, AND DEFCON

Education

Academic basis for our field
Open Tertiary Curriculum and Syllabus
Open Industry Curriculum
Open Textbooks



Chapters in every large city

If you live in a city with more than one million population

… and you don’t have a chapter

START ONE!

Wellington

Mexico City, Osaka, Kinshasa, Chicago, Ho Chi Minh City

Larger events

- Events are OWASP's primary fundraiser
- 2000+ attendees for AppSec US/EU

- Modernizing CFP/CFT process
- Moving to Sessionize
- Need more review volunteers!

Corporate Supporters

- Banks
- Large organizations with a development function
- FinTech Startups

The next 25 years

A Call to Action!

Like it or not, the future is AI

AI is good, but it’s not perfect.

Not everything is a Kiwi

Humans cannot outsource responsibility to AI

Get involved!

OWASP is YOU!

Become a member!

owasp.org > Join

AppSec: The Next Generation

We need to attract the best and brightest developers to the application security field

High School Career Paths

Industry re-training

Certification

Project Fill the Gaps

- Create the future!
- Scale us!

- Framework security
- Architecture
- Agile security
- AppSec as developers

Volunteer for a project!

owasp.org > Projects > Browse all projects


Start a project!
owasp.org > Projects > Create a project

Funding for the next level

Grants for projects

Giving Tuesday December 3
- Matching donations!
- Donate!

Become a corporate supporter!

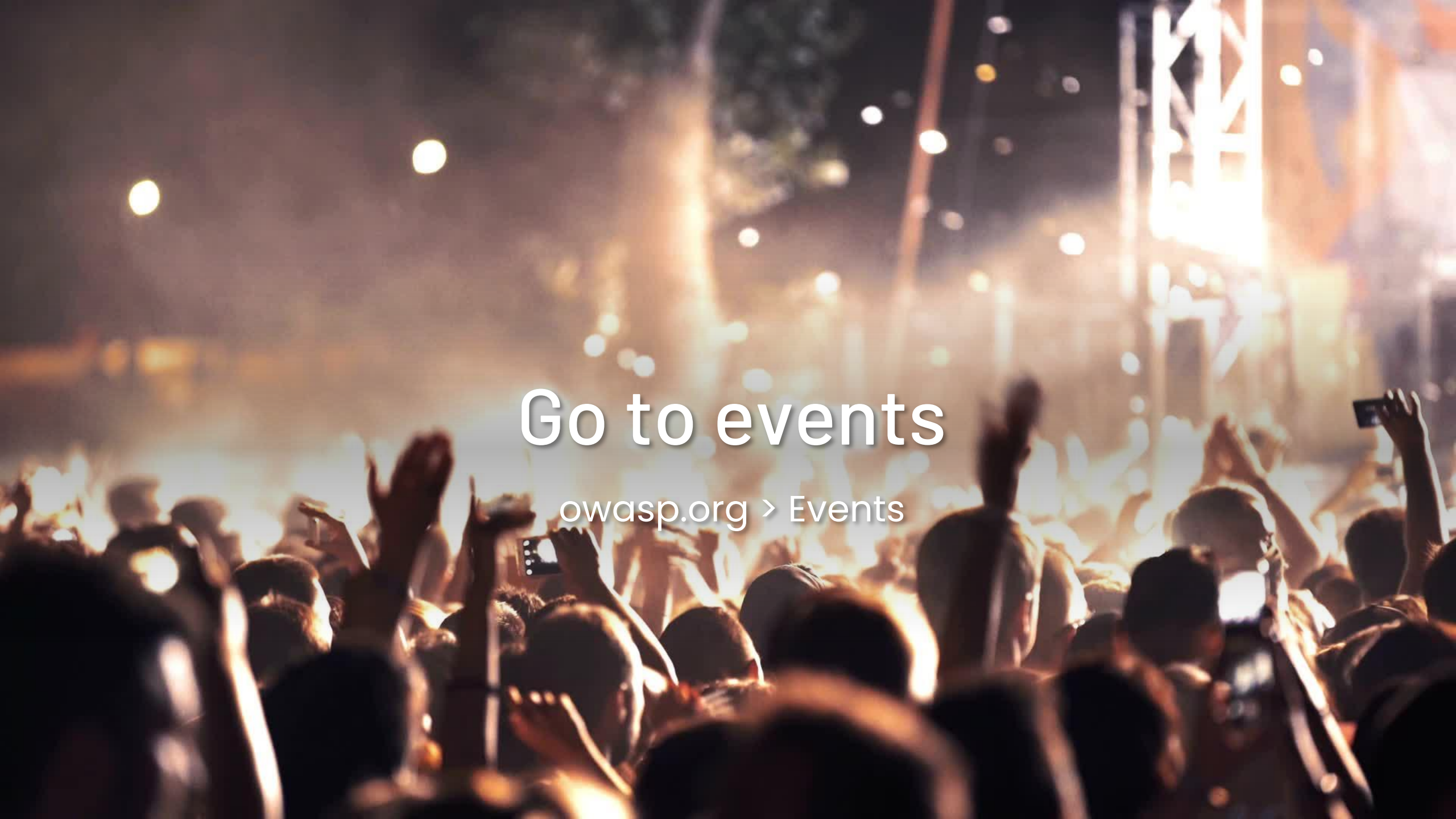
Go to your chapter!

owasp.org > Chapters > Find a local chapter

Meetup.com > Search your nearby area for OWASP

Start a chapter!

owasp.org > Chapters > Start a local chapter


Go to events
owasp.org > Events

One more thing...


13

Thank you!

andrew.vanderstock@owasp.com

@vanderaj ← most platforms