



OWASP London Chapter Meeting 27th July 2017



OWASP

The Open Web Application Security Project

JUST EAT



Chapter Leaders:

- Sam Stepanyan (@securestep9)
- Sherif Mansour (@kerberosmansour)

Chapter Events:

- Chapter Meetings at least once every 2 months
- Hackathon & CTF - once a year
- Workshops - launching in August - hopefully monthly!

Staying in Touch
OWASP London



Join The OWASP London Mailing List:

<http://lists.owasp.org/mailman/listinfo/owasp-london>



Follow us on Twitter
@owasplondon



“Like” us on Facebook

<https://www.facebook.com/OWASPLondon>



Slack: owasp.slack.com #chapter-london



Watch us on YouTube: [YouTube.com/OWASPLondon](https://www.youtube.com/OWASPLondon)

Visit OWASP London Chapter webpage

<https://www.owasp.org/index.php/London>

OWASP London
Provisional Dates of
future meetings:

28 September 2017

Live Stream



OWASP

The Open Web Application Security Project



Live Video

**We are
LIVE STREAMING THIS EVENT:**

[facebook.com/OWASPLondon](https://www.facebook.com/OWASPLondon)



Agenda



- **Networking, pizza & drinks**
- **Welcome and OWASP Update** - Sam Stepanyan & Sherif Mansour
- **So you thought you were safe using AngularJS? Think again!** - Lewis Arden
- **Lightning Talk: OWASP Summit 2017 Outcomes** - ~~Dinis Cruz~~ Sherif Mansour
- break -----
- **Introducing the OWASP ModSecurity Core Rule Set (CRS) 3.0**
- Dr. Christian Folini
- **Wrap up**
- **Networking & Beer** - The Viaduct Tavern



- We are a Global not-for-profit charitable organisation
- Focused on **improving the security** of software
- Vendor-Neutral Community
- **Collective Wisdom of the Best Minds in Application Security Worldwide**
- We collaboratively develop and provide **free** tools, guidance, standards
- All meetings are free to attend (*free beer included)

Worldwide



- Over 200 local Chapters around the world





OWASP

The Open Web Application Security Project

- Belfast
- Birmingham
- Bristol
- Cambridge
- Leeds
- **London**
- Manchester
- Newcastle
- Royal Holloway (inactive)
- Scotland
- Sheffield
- Suffolk



Become a Member



We are all **VOLUNTEERS!** (45,000 worldwide)



Membership



OWASP

The Open Web Application Security Project

Membership

[Home](#) [Corporate Supporters](#) [Other ways to Support OWASP](#) [Additional Resources](#)

[\[edit\]](#)



OWASP MEMBERSHIPS

global strategic group



Software powers the world, but insecure software threatens safety, trust, and economic growth. The Open Web Application Security Project (OWASP) is dedicated to making application security visible by empowering individuals and organizations to make informed decisions about true application security risks.

OWASP boasts 46,000+ participants, more than 65 organizational supporters, and even more academic supporters.

As a 501(c)(3) not-for-profit worldwide charitable organization, OWASP does not endorse or recommend commercial products or services. Instead, we allow our community to remain vendor neutral with the collective wisdom of the best individual minds in application security worldwide. This simple rule is the key to our success since 2001.

Your individual and corporate membership powers the organization and helps us [serve the mission](#). Please consider becoming an OWASP member today!



join



renew

\$50/year!

Not sure if you are a current member? [Member Directory](#)

Questions about OWASP Membership? [MEMBERSHIP FAQ](#)

Care to see our global membership demographics? [Membership Demographics as of January 2014](#)

Member Benefits



- ➔ Support Ethics & Principles of the OWASP Foundation
- ➔ Underscore your awareness of Application Security
- ➔ Increase your value, knowledge and expand your skills, network with professionals who share similar concerns, interests and goals, collaborate on projects
- ➔ Get exclusive discounts on AppSecEU/USA and many other Global CyberSecurity Conferences & events
- ➔ Donate to your local Chapter and Projects \$50/year!
- ➔ Get an @owasp.org email address
- ➔ **VOTE** on issues that shape direction of OWASP community

OWASP Member



OWASP

The Open Web Application Security Project



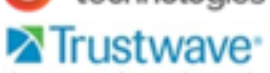
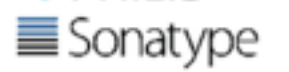
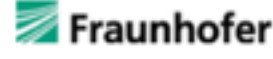
**If you are a member already
- collect this sticker from the
Chapter Leaders**

OWASP Corporate Members



OWASP

The Open Web Application Security Project



Premier Members

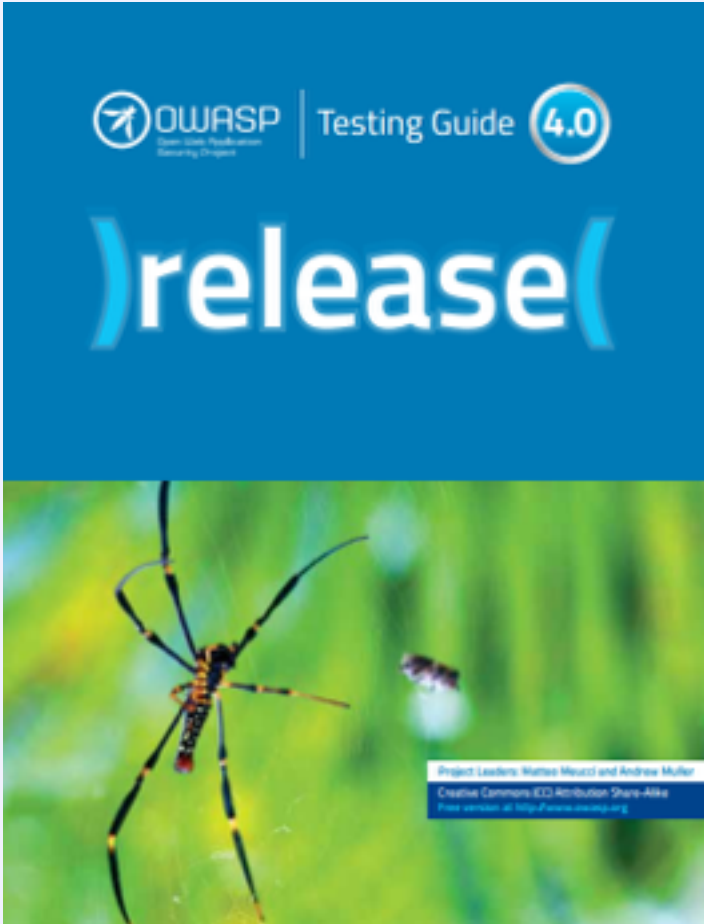


Premier members (donate \$20,000/year):

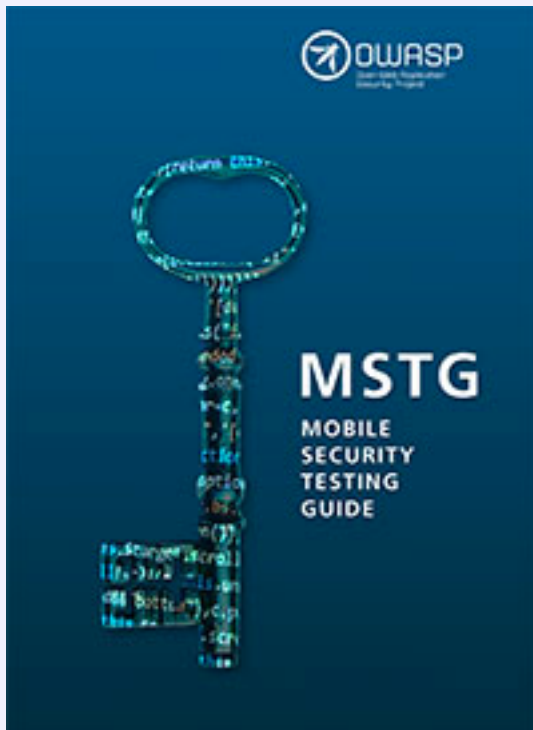




OWASP Books



Standards and Guidelines



OWASP Top 10 2017 RC



OWASP Top 10 – 2013 (Previous)	OWASP Top 10 – 2017 (New)
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References - Merged with A7	A4 – Broken Access Control (Original category in 2003/2004)
A5 – Security Misconfiguration	A5 – Security Misconfiguration
A6 – Sensitive Data Exposure	A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control - Merged with A4	A7 – Insufficient Attack Protection (NEW)
A8 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards - Dropped	A10 – Underprotected APIs (NEW)

- RC1 of the OWASP Top 10 2017 has been **rejected**
- A1, A2, A3, A4, A5, A6, A8, A9 have been left untouched by consensus view
- Requirement to choose two additional items
- Appeal for data and opinion is open until August 25, 2017 (github.com/OWASP/Top10)
- The new OWASP Top 10 2017 is to be released late November 2017.

OWASP Tools - ZAP

A screenshot of the OWASP Zed Attack Proxy (ZAP) web application. The window title is "Untitled Session - OWASP ZAP". The interface includes a menu bar (File, Edit, View, Analyse, Report, Tools, Online, Help), a toolbar with "Standard mode" and various icons, and a "Sites" tree on the left. The main pane displays a "Welcome to the OWASP Zed Attack Proxy (ZAP)" message. Below the message is a "URL to attack" input field containing "http://", with "Attack" and "Stop" buttons. A "Progress" indicator shows "Not started". At the bottom, a table lists processed requests with columns for "Processed", "Method", and "Flags".

Applications Places Sun Dec 8, 5:37 PM root

Untitled Session - OWASP ZAP

File Edit View Analyse Report Tools Online Help

Standard mode

Sites

Quick Start Request Response Break

Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

Please be aware that you should only attack applications that you have been specifically given permission to test.

To quickly test an application, enter its URL below and press 'Attack'.

URL to attack:

Progress: Not started

For a more in depth test you should explore your application using your browser or automated regression tests while proxying through ZAP.

See the help file for more details.

Show this tab on start up:

Scan Spider Forced Browse Fuzzer Params Http Sessions WebSockets AJAX Spider Output

100% Current Scans: 0 | URIs Found: 195

Processed	Method	Flags
<input checked="" type="checkbox"/>	GET	SEED
<input checked="" type="checkbox"/>	GET	SEED
<input checked="" type="checkbox"/>	GET	
<input checked="" type="checkbox"/>	GET	
<input checked="" type="checkbox"/>	GET	
<input checked="" type="checkbox"/>	GET	
<input checked="" type="checkbox"/>	GET	
<input checked="" type="checkbox"/>	GET	
<input checked="" type="checkbox"/>	GET	
<input checked="" type="checkbox"/>	GET	
<input checked="" type="checkbox"/>	GET	

Alerts 0 0 0 2 1

Current Scans 0 0 0 0 0 0 0 0 0 0

Untitled Session - O... Iceweasel



OWASP Juice Shop Project

Main Acknowledgements Road Map and Getting Involved

LAB medium level projects

OWASP Juice Shop Tool Project

The most trustworthy online shop out there. ([dschadow](#))

OWASP Juice Shop is an intentionally insecure webapp for security trainings written entirely in Javascript which encompasses the entire [OWASP Top Ten](#) and other severe security flaws.

Description

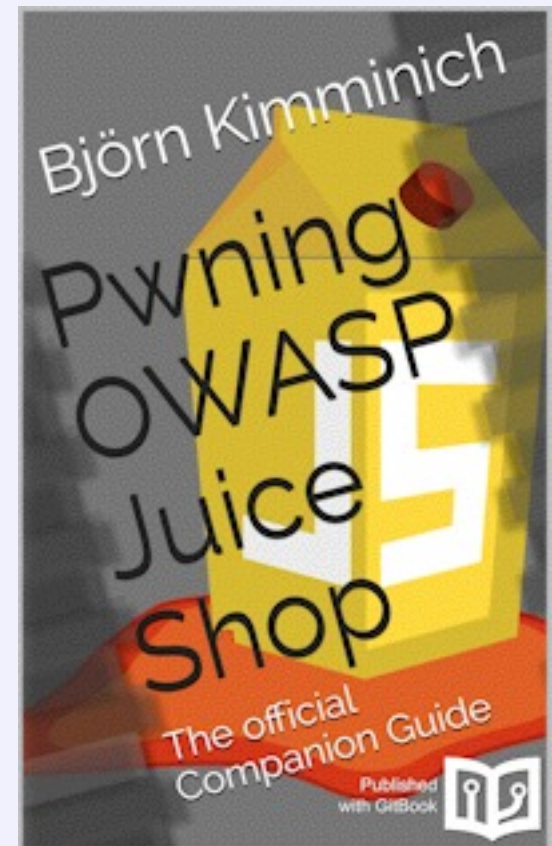


Juice Shop is written in Node.js, Express and AngularJS. It was the first application written entirely in JavaScript listed in the [OWASP VWA Directory](#).

The application contains more than 30 challenges of varying difficulty where the user is supposed to exploit the underlying vulnerabilities. The hacking progress is tracked on a score board. Finding this score board is actually one of the (easy) challenges!

Apart from the hacker and awareness training use case, pentesting proxies or security scanners can use Juice Shop as a "guinea pig"-application to check how well their tools cope with Javascript-heavy application frontends and REST APIs.

- * [juice-shop v4.2.0](#)
- * [juice-shop-ctf v1.2.0](#)





GLOBAL OWASP WASPY AWARDS 2017



Best Community Supporter (3 way tie):

- Dinis Cruz
- Jeremy Long
- Nicole Becher

Best Mission Outreach:

- Mark Miller

Best Innovator

- Seba Deleersnyder

Girl Hacker?



OWASP

The Open Web Application Security Project



- Learn more about AppSec
- Participate & Contribute in OWASP as Members and Leaders
- Speak at OWASP events and AppSec conferences
- Make Connections with like-minded women locally & globally
- Develop Thought Leadership
- Train and mentor all interested women in AppSec
- Grow Your Career

Women In AppSec



OWASP

The Open Web Application Security Project



OWASP WIA

@OWASPWIA

OWASP Foundation Women in AppSec
(WIA): owasp.org/index.php/Wome...

Tanya Janca - WIA Chair
OWASP Ottawa Chapter Leader
@shehackspurple





OWASP

The Open Web Application Security Project



[HOME](#) [CALL FOR PAPERS](#) [SCHEDULE](#) [SPEAKERS](#) [SPONSORS](#) [ABOUT](#) [REGISTRATION](#)

OWASP
AppSec USA



ORLANDO

2017

APPSEC USA 2017

September 19th - 22nd 2017 | Orlando, FL

[REGISTER](#)

All Day DevOps



OWASP

The Open Web Application Security Project

All Day DevOps 2017

[Home](#)

[Sponsors](#)

[Supporters](#)

[Register](#)

All Day DevOps 2017

24 Hours. 96 Sessions. Live Online.

Join us on October 24, 2017



2017 Global Board of Directors Election

[hide]

- 1 2017 Global Board of Directors Election
 - 1.1 About OWASP
 - 1.2 Election Timeline**
 - 1.3 Global Board of Directors Primary Responsibilities
 - 1.4 Eligibility Requirements for Board Candidates
 - 1.5 Call for Questions
 - 1.6 Honorary Membership
 - 1.7 Who Can Vote?
 - 1.8 How Do I Vote?
 - 1.9 Have additional questions about the OWASP Membership?
 - 1.10 Election FAQ
 - 1.11 Communications

- Home
- About OWASP
- Acknowledgements
- Advertising
- AppSec Events
- Books
- Brand Resources
- Chapters
- Donate to OWASP
- Downloads
- Funding
- Governance
- Initiatives
- Mailing Lists
- Membership

Candidates announced - August 7, 2017
Interviews: August 9 - September 1, 2017
Voting opens - October 9, 2017
Voting closes - October 31, 2017
Results Published - November 7, 2017



Questions for Candidates:

Anonymous | 06/06/2017



What kind of action plan do you have in mind to help motivate the participation of Developers into OWASP community?

Anonymous | 09/06/2017



What accomplishments related to OWASP Foundation's mission have you demonstrated in the last (5) years?

Anonymous | 30/06/2017



What is your strategy to keep chapters active and motivated with OWASP and keep having meetings and organize local events?



Call For Speakers For Future Events

Do you have a great Application Security Related Talk?

3 Tracks:

- **Breakers**
- **Defenders**
- **Builders**

Submit the abstract of your talk and your bio to:

owasplondon @ owasp .org



- [ABOUT](#)
- [WORKING SESSIONS](#)
- [PARTICIPANTS](#)
- [VENUE](#)
- [SPONSORS](#)
- [SUMMIT ORGANIZATION](#)

[BUY TICKET](#)

OWASP SUMMIT 2017

12-16 JUNE 2017, LONDON

Talk Time!



OWASP

The Open Web Application Security Project

- Lewis Arden
- Sherif Mansour
- Dr. Christian Folini

Thank You!



Speakers:

- Lewis Arden
- ~~Dinis Cruz~~ Sherif Mansour
- Christian Folini

All slides will be published on [OWASP.ORG](https://www.owasp.org) and video recordings will be on OWASP London YouTube channel in a few days

Hosts for this event

- **JUST EAT**
JUST EAT

- **Attendees (you!)**

Pub Time!



- **Networking and Drinks at:**
- **The Viaduct Tavern**
- **26 Newgate Street, EC1A 7AA**

