

OWASP London Chapter Meeting

27th July 2017



OWASP

The Open Web Application Security Project

JUST EAT



OWASP

The Open Web Application Security Project

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!



OWASP

The Open Web Application Security Project

Join The OWASP London Mailing List:

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



Follow us on Twitter
[@owasplondon](https://twitter.com/owasplondon)



“Like” us on Facebook
<https://www.facebook.com/OWASPLondon>



Slack: [#chapter-london](https://owasp.slack.com)



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:

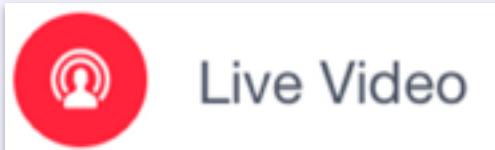
28 September 2017

Live Stream



OWASP

The Open Web Application Security Project



We are
LIVE STREAMING THIS EVENT:

facebook.com/OWASPLondon



Agenda



OWASP

The Open Web Application Security Project

- **Networking, pizza & drinks**
- **Welcome and OWASP Update** - Sam Stepanyan & Sherif Mansour
- **So you thought you were safe using AngularJS? Think again!** - Lewis Ardern
- **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)



OWASP

The Open Web Application Security Project

- 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



OWASP

The Open Web Application Security Project

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](#)



OWASP

The Open Web Application Security Project

- 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

accenture

acunetix

ARXAN
Protecting the App Economy[®]

ASPECT SECURITY
Application Security Experts

ASTECH SECURITY

BLACK DUCK

black hat
USA 2016

BROCADE

ca
technologies

CHECKMARX

Digital
BUILDING SECURITY IN

CIPHERTECHS

CLOUDFLARE

distil
networks

Cobalt

FICO

HUAWEI

CONTRAST
SECURITY

FORTINET

IMMUNIO

Credit Karma

Fraunhofer

IMPERVA

cybozu

GoSECURE
Information Builders

GOTHAM
DIGITAL SCIENCE

intelligent environments

Johnson Controls

jscrambler

nccgroup
Cybersecurity. Business resilience.

netsparker

netSPI
RISK COMPLIANCE SECURITY

NETSUITE

NowSecure

oneconsult
Holistic cyber security consultancy

OPTIV

ORACLE

Panasonic

PARASOFT

POSITIVE TECHNOLOGIES

Rakuten

RAPID7

SCHUBERG
PHILIS

SECU YOUR SITE

SCSK

söoryen
technologies

Security Compass

springcm

Twistlock

WhiteHat
SECURITY

SECURITY INNOVATION

SIG
Software Improvement Group

SYNOPSYS
Silicon to Software[™]



SMARTRAC

tCell.io
VERACODE

SECURING THE SOFTWARE THAT POWERS YOUR WORLD.

ThoughtWorks

verizon
digital media services

Virsec

Premier Members



OWASP

The Open Web Application Security Project

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



Signal Sciences





OWASP

The Open Web Application Security Project

VERACODE



GOTHAM
DIGITAL • SCIENCE

Quotium

netsparker
web application security scanner

intelligent
environments[®]
Interact in the Digital World

Expedia[®]

kiuwan

skypeTM

The Telegraph

empiric

J.P.Morgan

worldpay

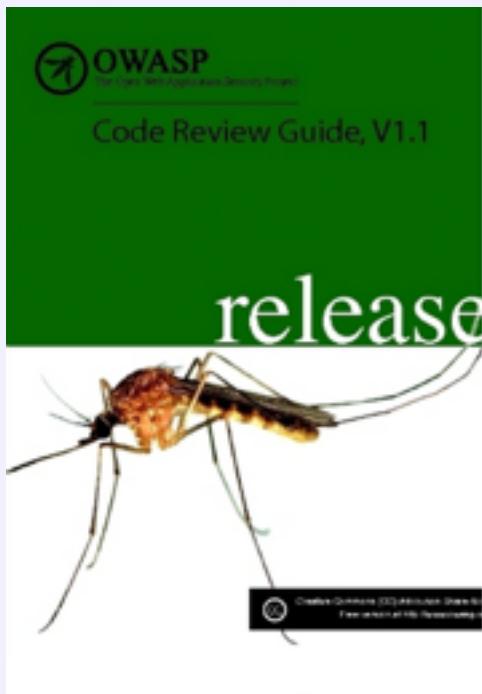
JUST EAT

OWASP Books



OWASP

The Open Web Application Security Project

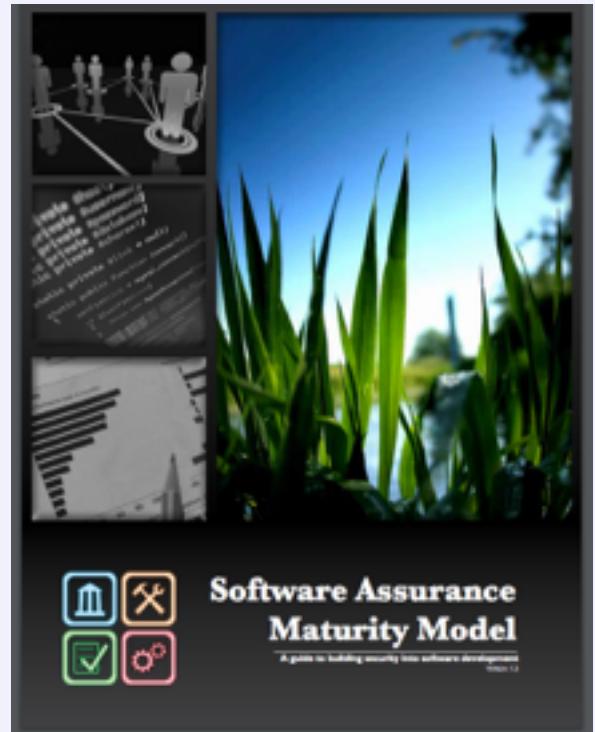
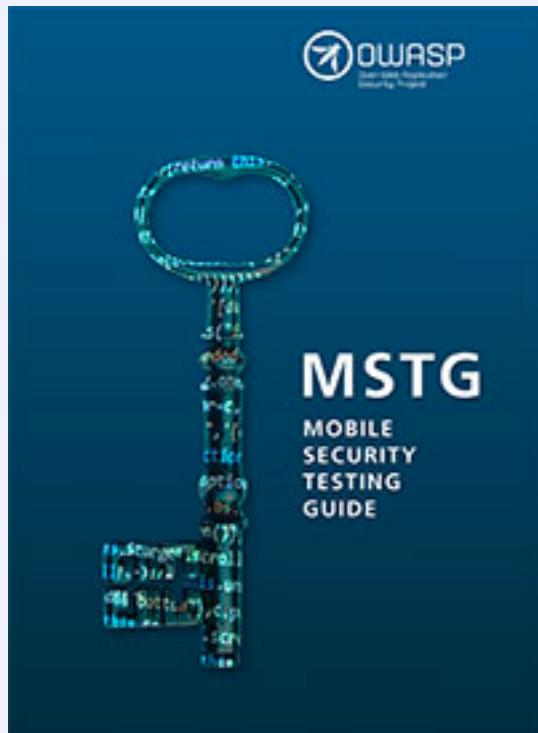


Standards and Guidelines



OWASP

The Open Web Application Security Project



OWASP Top 10 2017 RC



OWASP

The Open Web Application Security Project



OWASP

The Open Web Application Security Project

OWASP Top 10 - 2017 rc1

The Ten Most Critical Web Application Security Risks

Release Candidate

Comments requested per instructions within

release



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



OWASP

The Open Web Application Security Project

Sun Dec 8, 5:37 PM Untitled Session - OWASP ZAP

File Edit View Analyse Report Tools Online Help

Standard mode Back Forward Stop Reload Home

Sites

http://192.168.147.133

- GET:mutilidae
- # GET:robots.txt
- M mutilidae
 - M GET:index.php?page
 - M GET:set-up-database.php
 - P GET:index.php?ds.page
 - M GET:index.php
- GET:index.php?name=username
- M GET:favicon
- M GET:fav
- M documents
- M images
- M POST:in
- M GET:in
- M GET:in
- M POST:in
- M POST:in

Attack Delete Include in Context Flag as Context Run application Exclude from Context Exclude from Break... Alerts for this node Resend... New Alert... Show in History tab Open URL in Browser Generate anti CSRF test FORM Refresh Sites tree Save Raw

http://192.168.147.133/mutilidae/index.php?page=home.php
http://192.168.147.133/mutilidae/index.php?page=login.php
http://192.168.147.133/mutilidae/index.php?do=toggle-hints&page=home.php
http://192.168.147.133/mutilidae/index.php?do=toggle-security&page=home.php
http://192.168.147.133/mutilidae/set-up-database.php
http://192.168.147.133/mutilidae/index.php?page=show-log.php
http://192.168.147.133/mutilidae/index.php?name=username&id=data.nhn

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 been given permission to test.

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

URL to attack:

Attack Stop

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

Current Scans: 0 | URLs Found: 195

Flags
SEED
SEED

Alerts 0 0 2 1

Untitled Session - O... Iceweasel Current Scans 0 0 0 0 0 0 0 0 0 0



OWASP

The Open Web Application Security Project

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

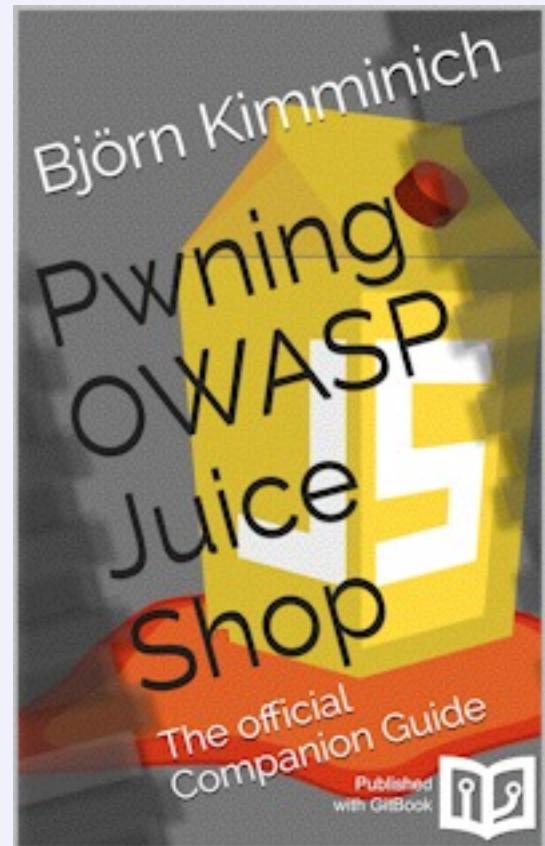


Juice Shop is written in Node.js, Express and AngularJS. It was the first application written entirely in JavaScript listed in the [OWASP VWA Directory](#).

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](#)





OWASP

The Open Web Application Security Project

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

The screenshot shows the homepage of the AppSecUSA 2017 conference website. At the top, there is a navigation bar with links: HOME, CALL FOR PAPERS, SCHEDULE, SPEAKERS, SPONSORS, ABOUT, and REGISTRATION. To the left of the main content area, there is a small blue circular icon with a white wasp and a small orange arrow pointing upwards. The main content features the OWASP AppSec USA logo at the top, followed by a large blue circular logo with a wasp in the center. Below this is the text "ORLANDO" in large blue letters and "2017" in smaller orange letters. A horizontal line separates this from the text "APPSEC USA 2017". At the bottom, it says "September 19th - 22nd 2017 | Orlando, FL" and a large orange button with the word "REGISTER" in white capital letters.

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](#)



A large, semi-transparent background image shows a person from the side, wearing headphones and speaking into a professional microphone. The image has a blue and white color palette.

All Day DevOps 2017

24 Hours. 96 Sessions. Live Online.

Join us on October 24, 2017



Page Discussion

Read

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](#)

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

1

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

Anonymous | 09/06/2017

0

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

Anonymous | 30/06/2017

0

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



OWASP

The Open Web Application Security Project

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



OWASP

The Open Web Application Security Project

[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!



OWASP

The Open Web Application Security Project

Speakers:

- Lewis Arden
- ~~Dinis Cruz~~ Sheriff 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!)



OWASP

The Open Web Application Security Project

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

