

OWASP London Chapter Meeting

18th May 2017



OWASP

The Open Web Application Security Project



Chapter Leaders:

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

Keeping In Touch:

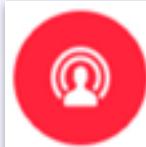
- Join the **OWASP London mailing list**
- Follow **@OWASPLondon** on Twitter
- “Like” **OWASPLondon** on Facebook
- Subscribe to **OWASPLondon** Channel on YouTube
- Chat with #chapter-london team owasp.Slack.com

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



OWASP

The Open Web Application Security Project

- **Networking, pizza & drinks**
- **Welcome and OWASP Update** - Sam Stepanyan & Sherif Mansour
- **Threat Modeling Against Payment Systems** - Dr. Grigorios Fragkos
- **Lightning Talk 1: OWASP Summit & OWASP Top 10 2017 Changes** - Dinis Cruz
----- break -----
- **Unsafe Deserialization Attacks In Java and A New Approach To Protect The JVM** - Apostolos Giannakidis
- **Lightning Talk 2: Security solutions for developers who have no time for security** - Edwin Aldridge
- **Networking & Beer** - All Bar One



- 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 160 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[™]

ups

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



London Chapter Supporters



OWASP

The Open Web Application Security Project



GOTHAM
DIGITAL SCIENCE

Quotium



netsparker



ThoughtWorks[®]

 **intelligent environments[®]**
Interact in the Digital World

skype[™]



Expedia[®]

 **empiric**

J.P.Morgan

The Telegraph

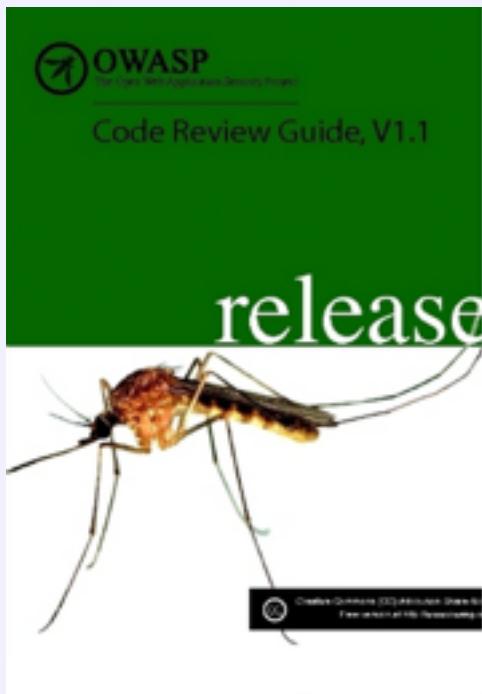
 **worldpay**

OWASP Books



OWASP

The Open Web Application Security Project

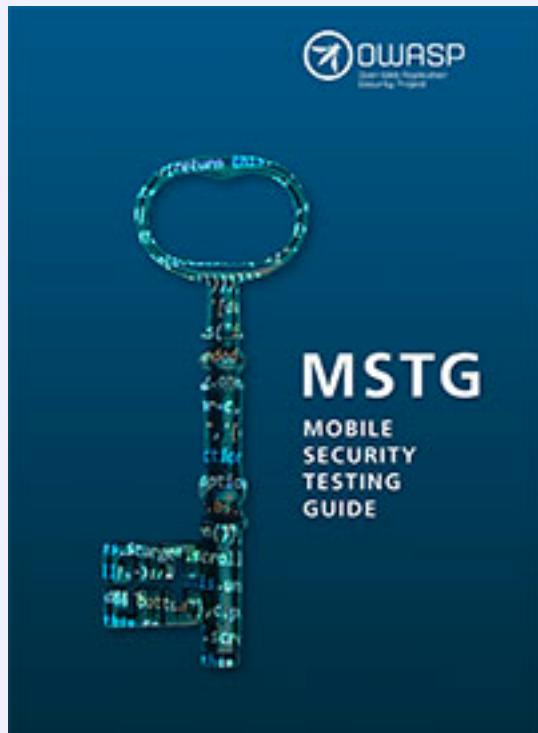


Standards and Guidelines



OWASP

The Open Web Application Security Project



OWASP Tools - ZAP



OWASP

The Open Web Application Security Project

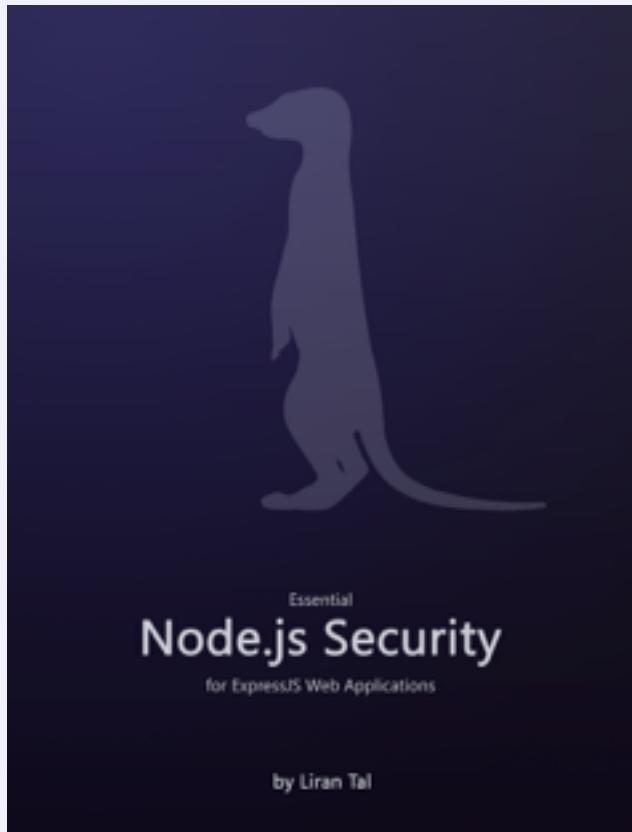
The screenshot shows the OWASP ZAP interface. The top menu bar includes 'File Edit View Analyse Report Tools Online Help' and the status 'Sun Dec 8, 5:37 PM'. The title bar says 'Untitled Session - OWASP ZAP'. The left sidebar lists 'Sites' with a tree view of a target application at 'http://192.168.147.133'. A context menu is open over a selected item 'GET: index.php?name=username'. The menu options include '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', and 'Generate anti-CSRF test FORM'. Below the tree view are sections for 'Processed' and 'Method' requests, showing various HTTP methods and their URLs. The main central area displays the 'Welcome to the OWASP Zed Attack Proxy (ZAP)' message, instructions to enter a URL and press 'Attack', and a progress bar indicating 'Not started'. It also includes a note about using the browser or automated tests while proxying. At the bottom, tabs for 'Scan', 'Spider', 'Forced Browse', 'Fuzzer', 'Params', 'Http Sessions', 'WebSockets', 'Ajax Spider', and 'Output' are visible, along with a progress bar for current scans and a table for flagged items.

FREE eBook



OWASP

The Open Web Application Security Project



Essential Node.js Security for ExpressJS Web Applications

*Hands-on and abundant with
source code for a practical guide to
Securing Node.js web applications.*

<https://bit.ly/freenodejsbook>



OWASP

The Open Web Application Security Project

The Go Language Guide Web Application Secure Coding Practices



Go Language - Web Application Secure Coding Practices

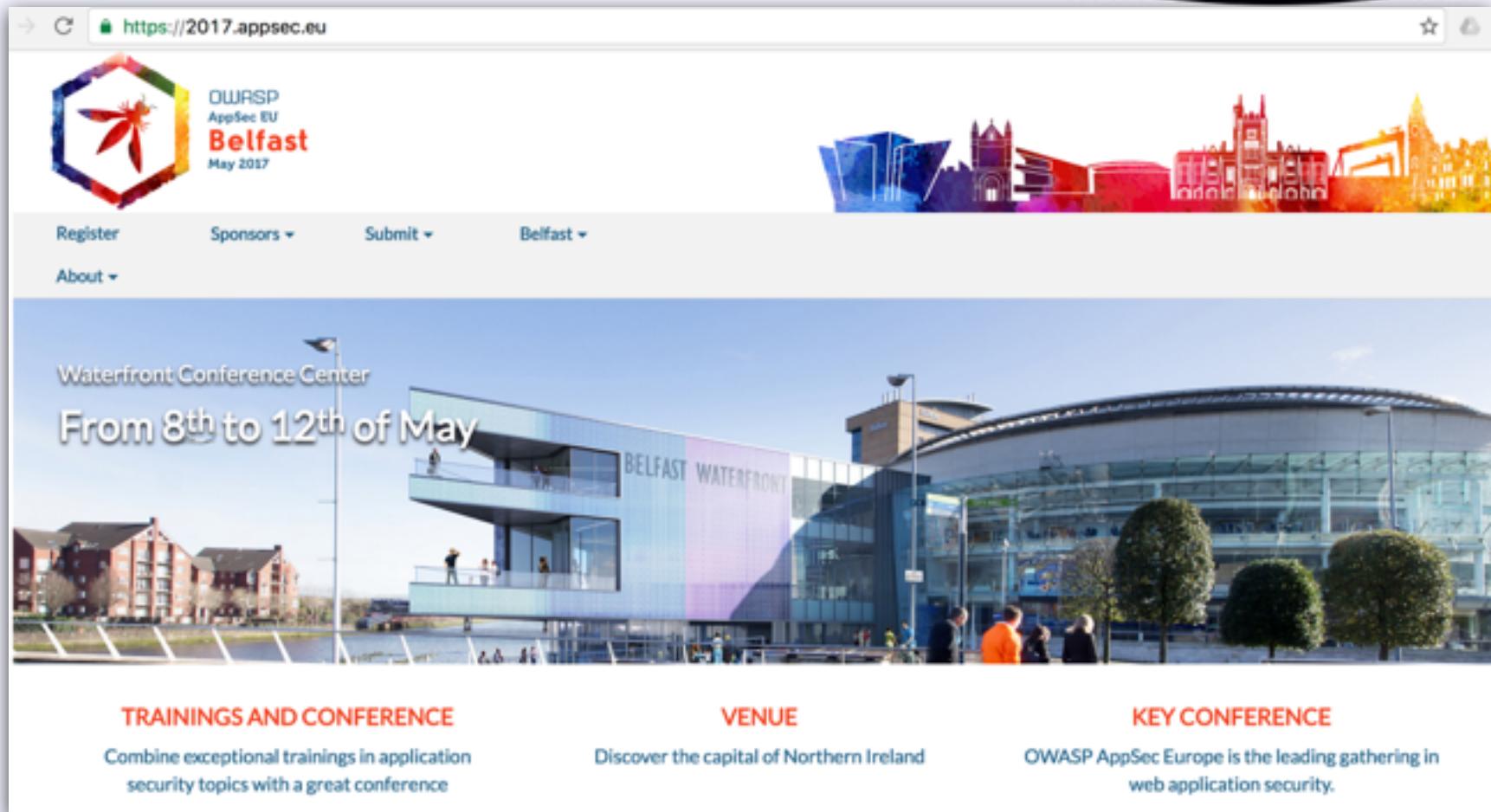
- * Avoid common mistakes
- * Hands-on detail on ...
- * how to code in Go securely
- * Donated by CheckMarx
- * Hosted on GitBook
- * You can contribute, not just read

<https://bit.ly/go-scp>



OWASP

The Open Web Application Security Project



A screenshot of the official website for OWASP AppSec Europe 2017. The URL in the browser bar is <https://2017.appsec.eu>. The page features the OWASP logo and the title "OWASP AppSec EU Belfast May 2017". A navigation bar includes links for Register, Sponsors, Submit, Belfast, and About. A large banner image shows the Belfast Waterfront Conference Center. Text on the banner reads "Waterfront Conference Center" and "From 8th to 12th of May". Below the banner, three sections provide information: "TRAININGS AND CONFERENCE", "VENUE", and "KEY CONFERENCE".

https://2017.appsec.eu

OWASP AppSec EU Belfast May 2017

Register Sponsors Submit Belfast About

Waterfront Conference Center
From 8th to 12th of May

TRAININGS AND CONFERENCE
Combine exceptional trainings in application security topics with a great conference

VENUE
Discover the capital of Northern Ireland

KEY CONFERENCE
OWASP AppSec Europe is the leading gathering in web application security.

8-12 May 2017, Belfast
Northern Ireland



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

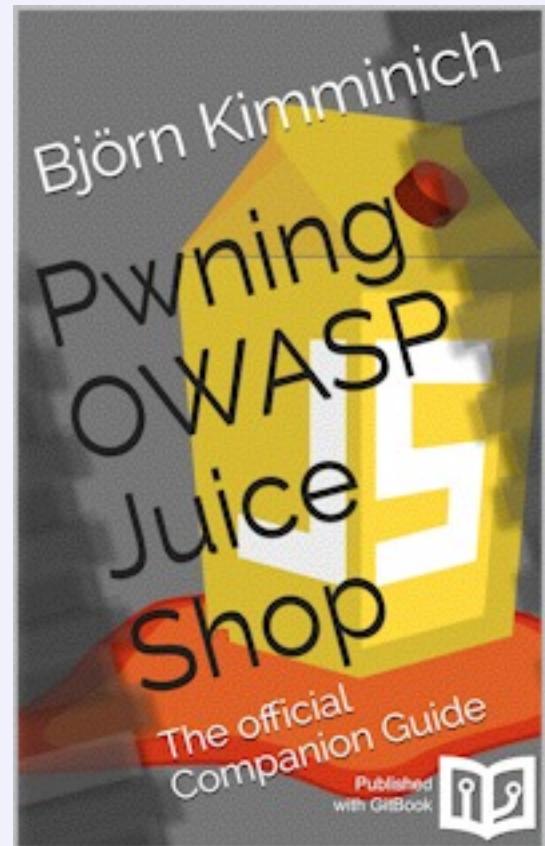


Juice Shop is written in Node.js, Express and AngularJS. It was the first application written entirely in JavaScript listed in the [OWASP VWA Directory](#).

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 v3.1.0](#)
- * [juice-shop-ctf v1.1.0](#)





OWASP

The Open Web Application Security Project

A screenshot of a web browser window. The address bar shows "https://threatdragon.org/login". The page content is the Threat Dragon login screen, featuring a large orange header with the text "Threat Dragon" and a cartoon dragon illustration. The main text on the page reads "Welcome! Threat Dragon is a free, open-source threat modeling tool from OWASP. It can be used as a standalone desktop app for Windows, MacOS and Linux or as a web application. We think the desktop app is great, but if you choose the online version you get to unleash the awesome power of GitHub on your threat models! Obviously, to do this you need to log in first...". A "Login with GitHub" button is visible at the bottom right.



Welcome!

Threat Dragon is a free, open-source threat modeling tool from OWASP. It can be used as a standalone desktop app for Windows, MacOS and Linux or as a web application. We think the desktop app is great, but if you choose the online version you get to unleash the awesome power of GitHub on your threat models! Obviously, to do this you need to log in first...



Login with GitHub

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



Creative Commons (CC) Attribution Share-Alike
Free version at <https://www.owasp.org>

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)

Please send comments:
OWASP-TopTen@lists.owasp.org

Comments recommending changes to the items listed in the Top 10 should include a complete suggested list of 10 items, along with a rationale for any changes



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



OWASP

The Open Web Application Security Project



BSides London 2017

Biggest Community-Driven
InfoSec Conference

07.June.2017

IEC Conference Centre
47 Lillie Road London
SW6 1UD

WE WILL BE THERE!



OWASP

The Open Web Application Security Project



Security BSides Athens 2017

Saturday, 24th June 2017



BSides Athens 2017

Event Details

Sponsors

CFP

Tickets

Venue

Extras

Contact

bsidesath.gr > Home

Sunday, 14 May 2017

Welcome

Security BSides Athens will be held in Athens for the second time in 2017 and more specifically on:

Saturday, 24 June 2017

Security BSides is a community-driven framework for building events by and for information security community members. These events are already happening in major cities all over the world! We are responsible for organizing an independent **BSides-Approved** event for Athens, Greece.

The idea behind the Security BSides events is to organise a free Information Security conference where professionals, experts, researcher, and InfoSec enthusiasts come together to discuss

Who is organising this event?

•The short answer to this is **YOU**. This is what makes these events so successful and a unique experience. Security BSides events are organized:

..by the community, for the community

•Behind the scenes to drive the event are a number of people, professionals in the area of Information Security, who decided to take the first steps and bring this global event in Greece.

•Our sponsors, our volunteers, our community supporters, our speakers, our delegates and more importantly **you**. Support this initiative to have a Security BSides event in Athens.

[Join Us](#)

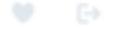
Tweets by @BSidesAth



BSides Athens
@BSidesAth



Tracks Schedule is now online! Tracks 1 & Track 2 have talks, Track 3 has the workshop.
Download our mobile app, for real-time updates.



12 May



BSides Athens
@BSidesAth





OWASP

The Open Web Application Security Project

infosecurity[®]

EUROPE

06-08 JUNE 2017 OLYMPIA, LONDON.
EVERYONE & EVERYTHING YOU NEED TO KNOW ABOUT INFORMATION SECURITY

[Register to Attend](#) [Book to Exhibit](#)

[About](#) [Visit](#) [Exhibit](#) [Find Exhibitors 2017](#) [Conference](#) [Media](#) [Infosecurity Week](#) [Blog](#) [My Event](#)

1.7K 121

INFOSECURITY EUROPE 2017 IS SET TO WELCOME OVER 18,000 INDUSTRY PROFESSIONALS

Be part of the future of the infosecurity industry

REGISTER NOW



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, which includes the text "OWASP AppSec USA" above a stylized blue wasp icon inside a circle. Below this, the word "ORLANDO" is written in large, bold, blue letters, followed by "2017" in smaller orange letters. A horizontal line separates this from the title "APPSEC USA 2017". At the bottom, the text "September 19th - 22nd 2017 | Orlando, FL" is displayed, followed by a large orange button with the word "REGISTER" in white capital letters.

All Day DevOps



OWASP

The Open Web Application Security Project

All Day DevOps 2017

[Home](#) [Sponsors](#) [Supporters](#)

[Register](#)



A large, semi-transparent watermark image of a man's face in profile, facing left, with his mouth open as if speaking. In front of his face, there is a professional microphone on a stand. The background of the entire slide is a dark blue gradient.

All Day DevOps 2017

24 Hours. 96 Sessions. Live Online.

Join us on October 24, 2017



OWASP

The Open Web Application Security Project

- Before introducing the keynote speaker, let's remember some vulnerabilities with own logos..



Logos



OWASP

The Open Web Application Security Project



@drgfragkos



OWASP

The Open Web Application Security Project



Dr Grigorios “Greg” Fragkos

Talk Time!



OWASP

The Open Web Application Security Project

- Dr Grigorios “Greg” Fragkos
- Dinis Cruz
- Apostolos Giannakidis
- Edwin Aldridge



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>



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



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

Visit OWASP London Chapter webpage
<https://www.owasp.org/index.php/London>

OWASP London
Provisional Dates of
future meetings:

27th July 2017



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

Thank You!



OWASP

The Open Web Application Security Project

Speakers:

- Dr Grigorios Fragkos
- Dinis Cruz
- Apostolos Giannakidis
- Edwin Aldridge

All slides will be published on
OWASP.ORG and video
recordings will be on OWASP
London YouTube channel in a
few days

Hosts for this event

- WorldPay



- Attendees (you!)



OWASP

The Open Web Application Security Project

- Networking and Drinks at:
- All Bar One: 103 Cannon Street
- The Cannick Tapps

