OWASP London Chapter Meeting
18th May 2017

OWASP

The Open Web Application Security Project

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**

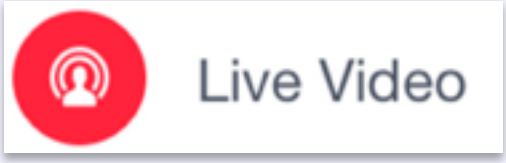
➤ "Like" **OWASPLondon** on **Facebook**

➤ Subscribe to **OWASPLondon** Channel on **YouTube**

➤ Chat with #chapter-london team owasp.Slack.com

Live Stream

OWASP
The Open Web Application Security Project



We are
LIVE STREAMING THIS EVENT:

facebook.com/OWASPLondon

Agenda

- **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

OWASP

OWASP
The Open Web Application Security Project

- 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

OWASP
The Open Web Application Security Project

- Over 160 local Chapters around the world

UK Chapters

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

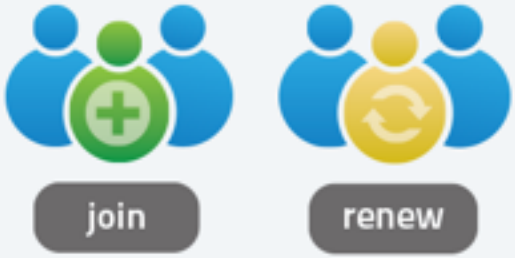
Home | Corporate Supporters | Other ways to Support OWASP | Additional Resources [edit]

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!



$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

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

Premier Members

OWASP
The Open Web Application Security Project

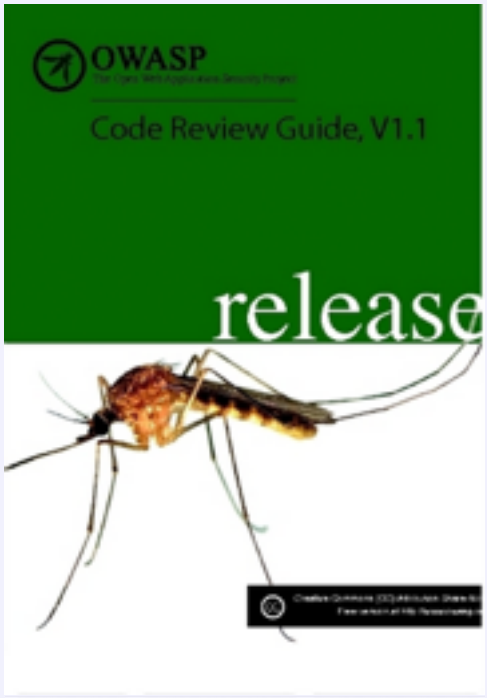
Premier members (donate $20,000/year):

London Chapter Supporters

OWASP
The Open Web Application Security Project

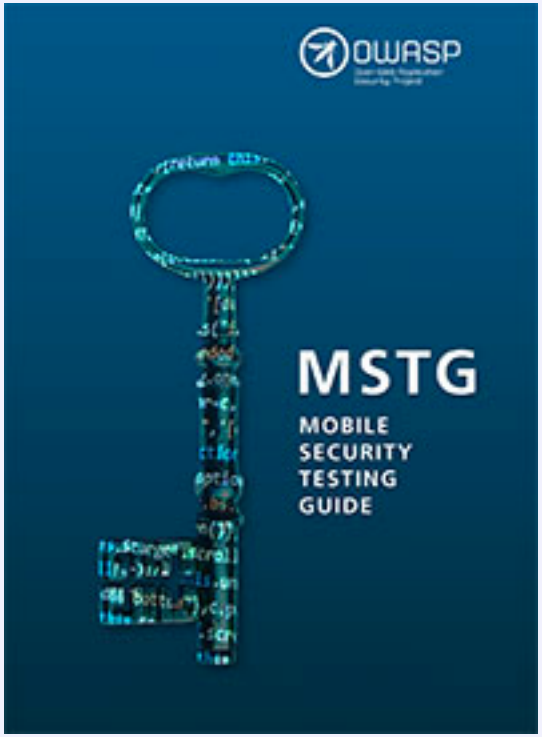
OWASP Books

OWASP
The Open Web Application Security Project



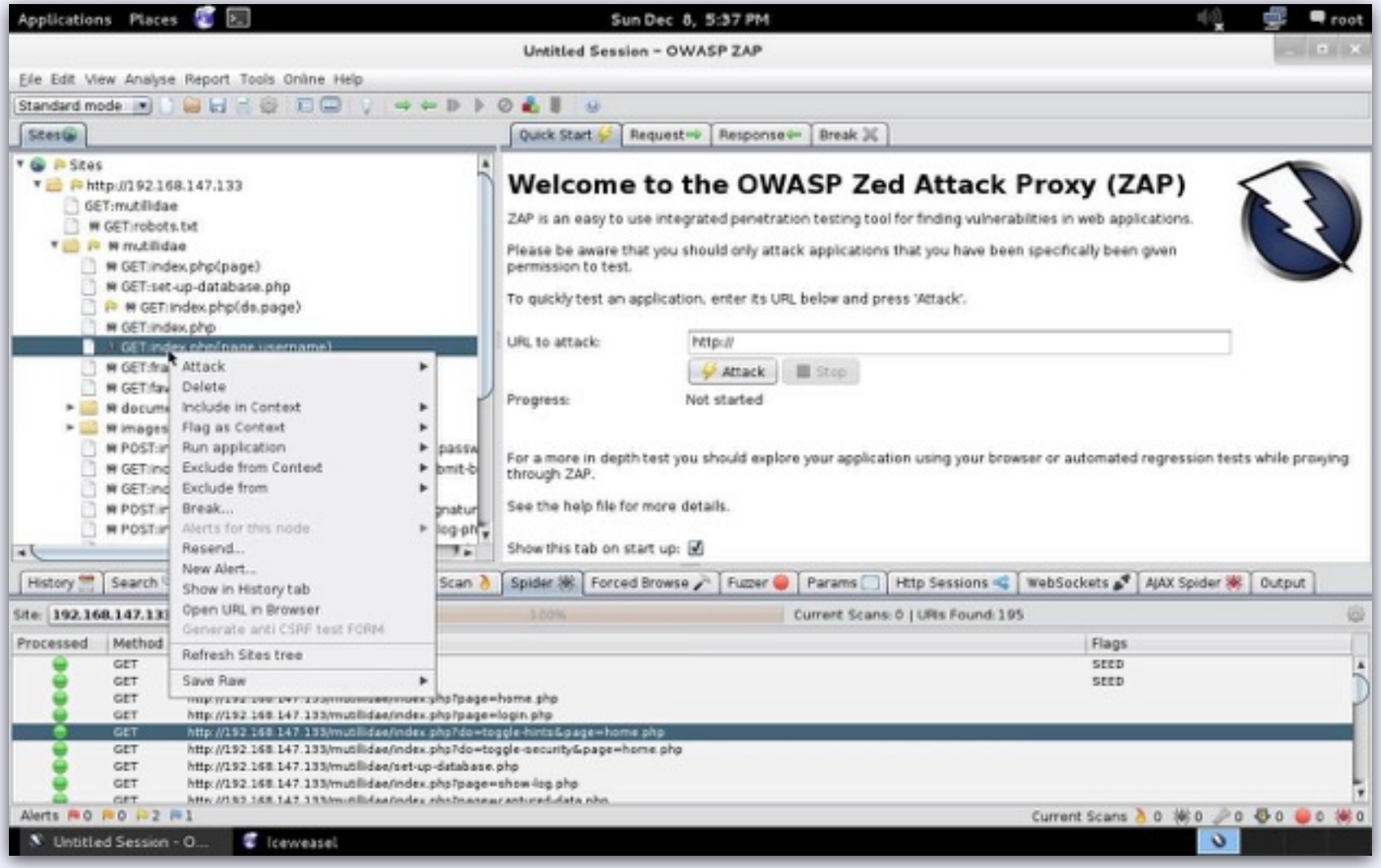
Standards and Guidelines

OWASP
The Open Web Application Security Project



OWASP Tools - ZAP

OWASP
The Open Web Application Security Project



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

Go Secure Coding Practices Free eBook

OWASP
The Open Web Application Security Project

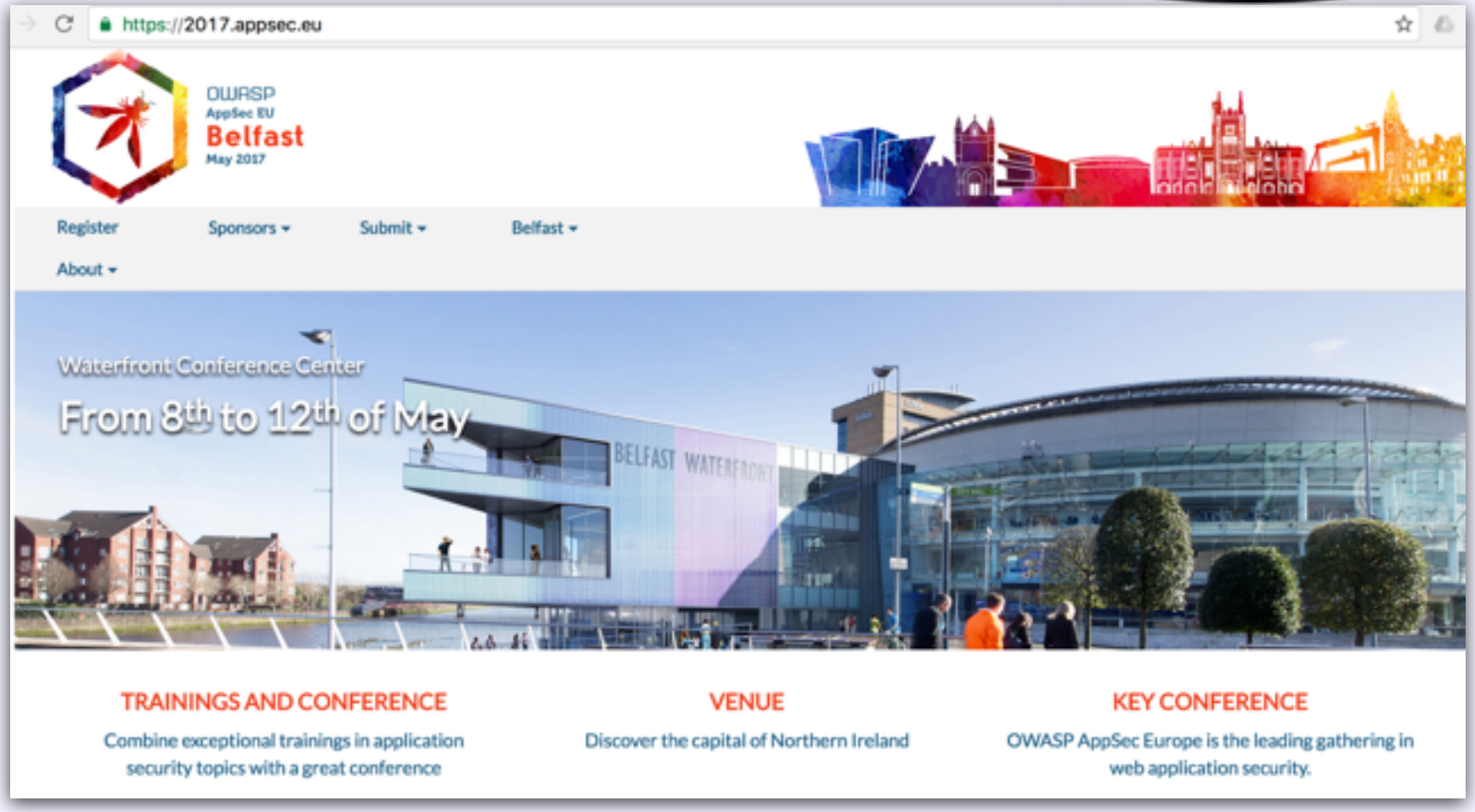
Go Language -
Web Application Secure Coding Practices

* 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

AppSec Europe 2017

OWASP
The Open Web Application Security Project



8-12 May 2017, Belfast
Northern Ireland

OWASP JuiceShop

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.

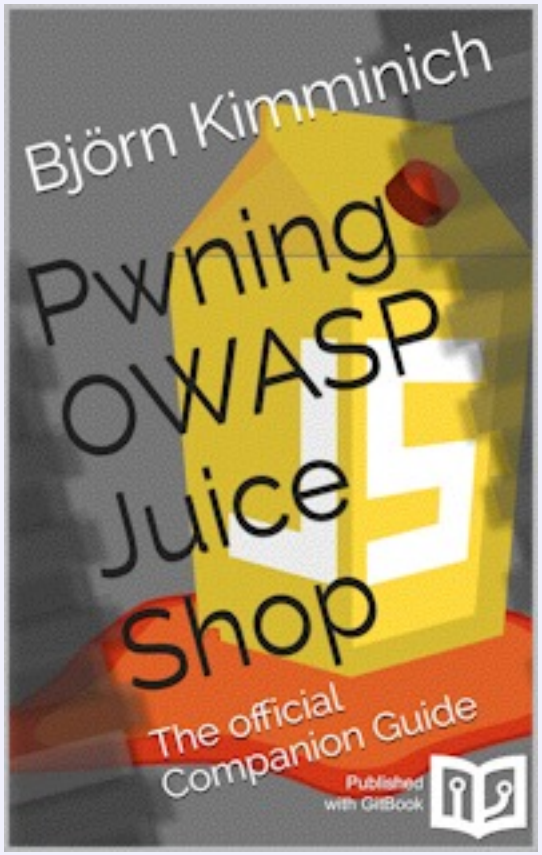
Description

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!

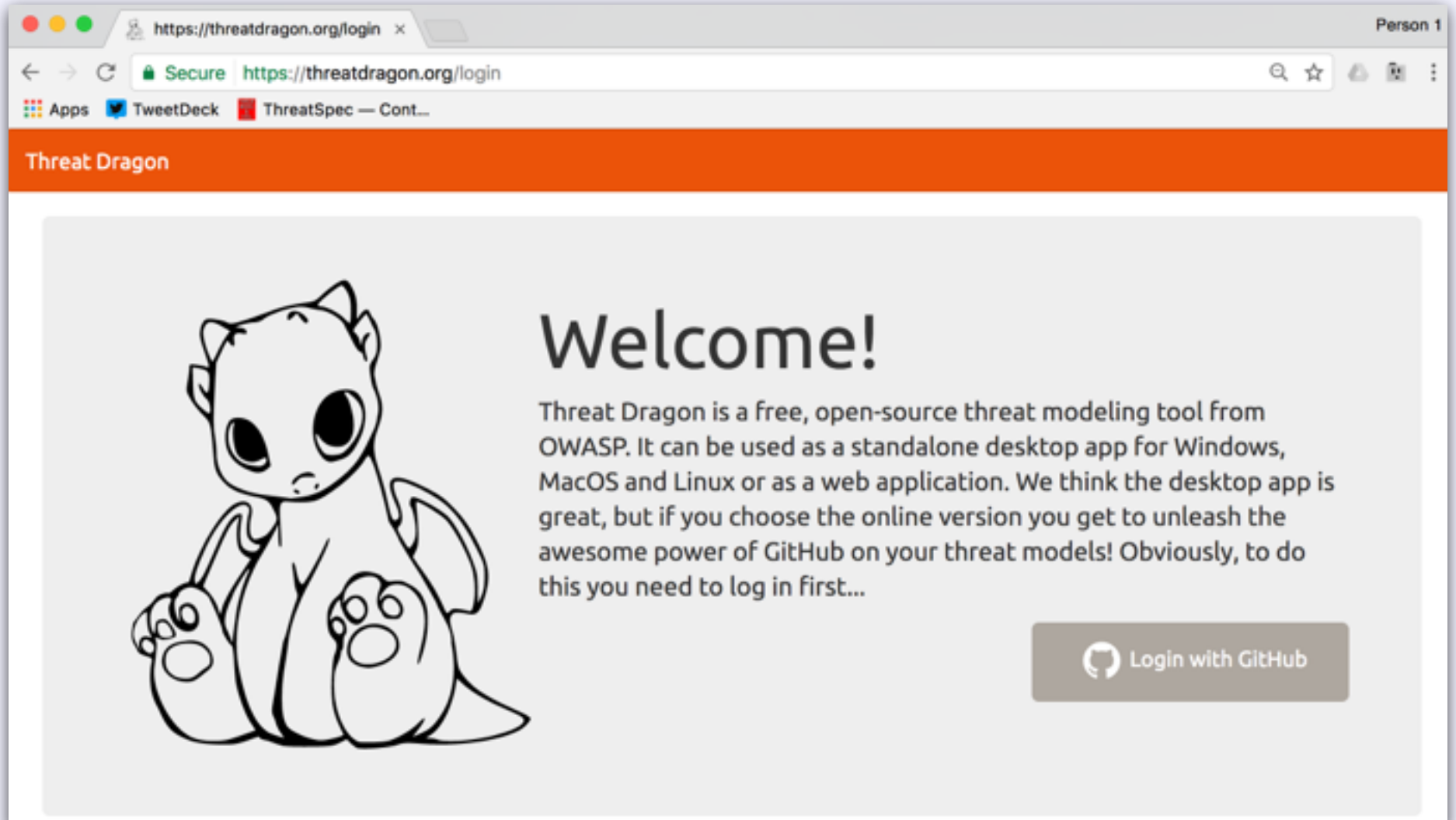
Apart from the hacker and awareness training use case, pentesting proxies or security scanners can use Juice Shop as a "guinea pig"-application to check how well their tools cope with Javascript-heavy application frontends and REST APIs.

* juice-shop v3.1.0
* juice-shop-ctf v1.1.0



OWASP Threat Dragon

OWASP
The Open Web Application Security Project



OWASP Top 10 2017 RC

OWASP
The Open Web Application Security Project

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 Summit 2017

OWASP
The Open Web Application Security Project

BSides London 2017

Biggest Community-Driven InfoSec Conference

07.June.2017

ILEC Conference Centre
47 Lillie Road London
SW6 1UD

WE WILL BE THERE!

BSIDES Athens

OWASP
The Open Web Application Security Project

InfoSec Europe 2017

OWASP
The Open Web Application Security Project

AppSecUSA 2017

OWASP
The Open Web Application Security Project

All Day DevOps

OWASP
The Open Web Application Security Project

All Day DevOps 2017

Home Sponsors Supporters Register

Keynote Intro

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

Staying in Touch
OWASP London

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

"Like" us on Facebook
https://www.facebook.com/OWASPLondon

Watch us on YouTube**: YouTube.com/OWASPLondon**

Slack: owasp.slack.com #chapter-london

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

OWASP London
Provisional Dates of future meetings:

27th July 2017

Present Your Talk

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**

worldpay

- **Attendees (you!)**

Pub Time!

OWASP
The Open Web Application Security Project

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