24th November 2016

OWASP

The Open Web Application Security Project

Agenda

OWASP

The Open Web Application Security Project

- **Networking, pizza and beer**
- **Welcome and OWASP Update** - Sam Stepanyan & Sherif Mansour
- **OWASP ZAP Jenkins Plugin Demo & Walkthrough -** Goran Sarenkapa
- **PCI - The View From The Bridge - Jeremy King**
- *——————— break —— beer—pizza————————-*
- ***JSON Hijacking - Gareth Hayes***
- ***myBBC Security Council - What It Means To You*** *- Shane Kelly*
- **Networking & Beer**

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

OWASP

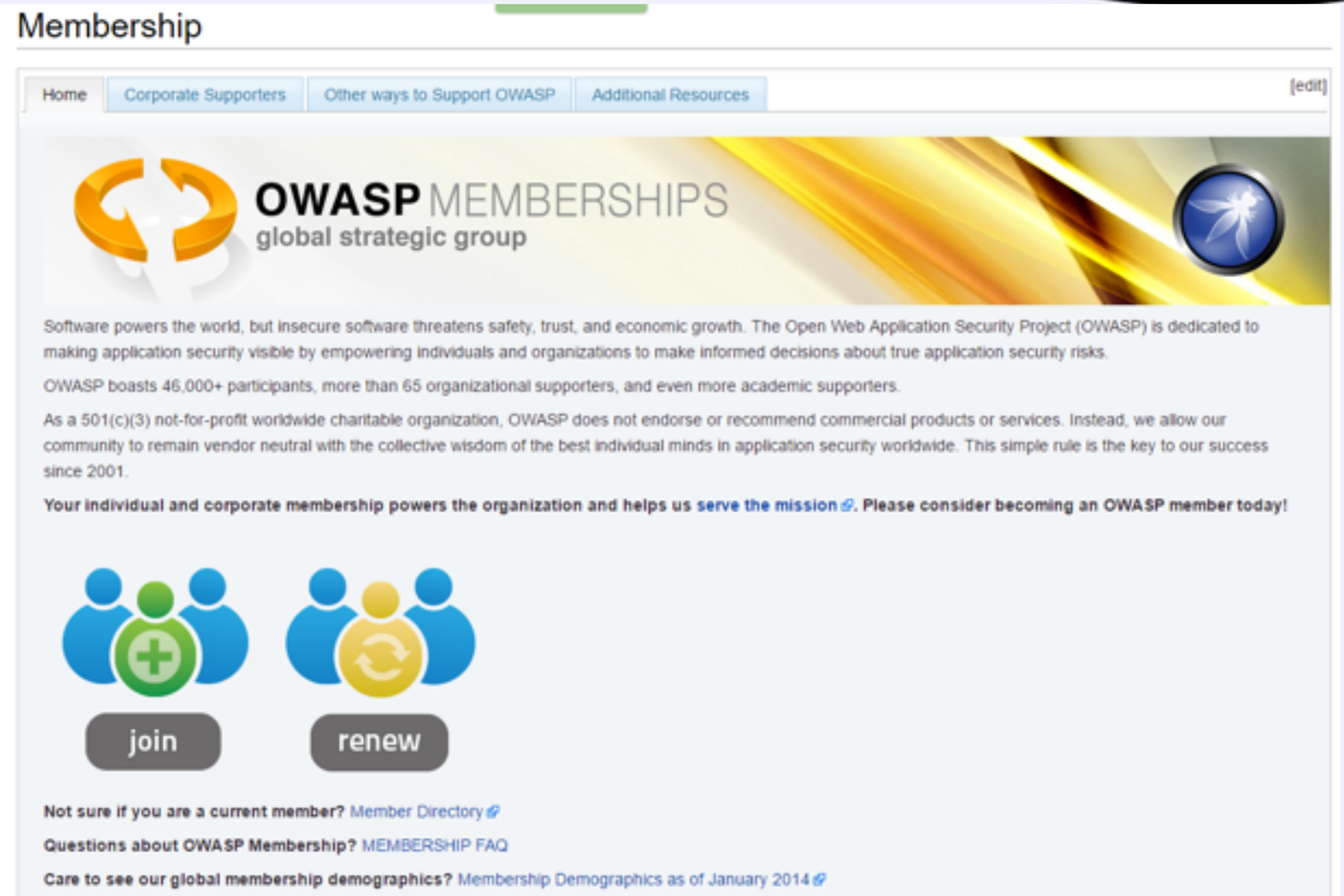
OWASP
The Open Web Application Security Project

- 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
- Provide free tools, guidance, documentation

Become a Member

We are all VOLUNTEERS! (45,000 worldwide)

Membership



Membership

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!

Not sure if you are a current member? Member Directory

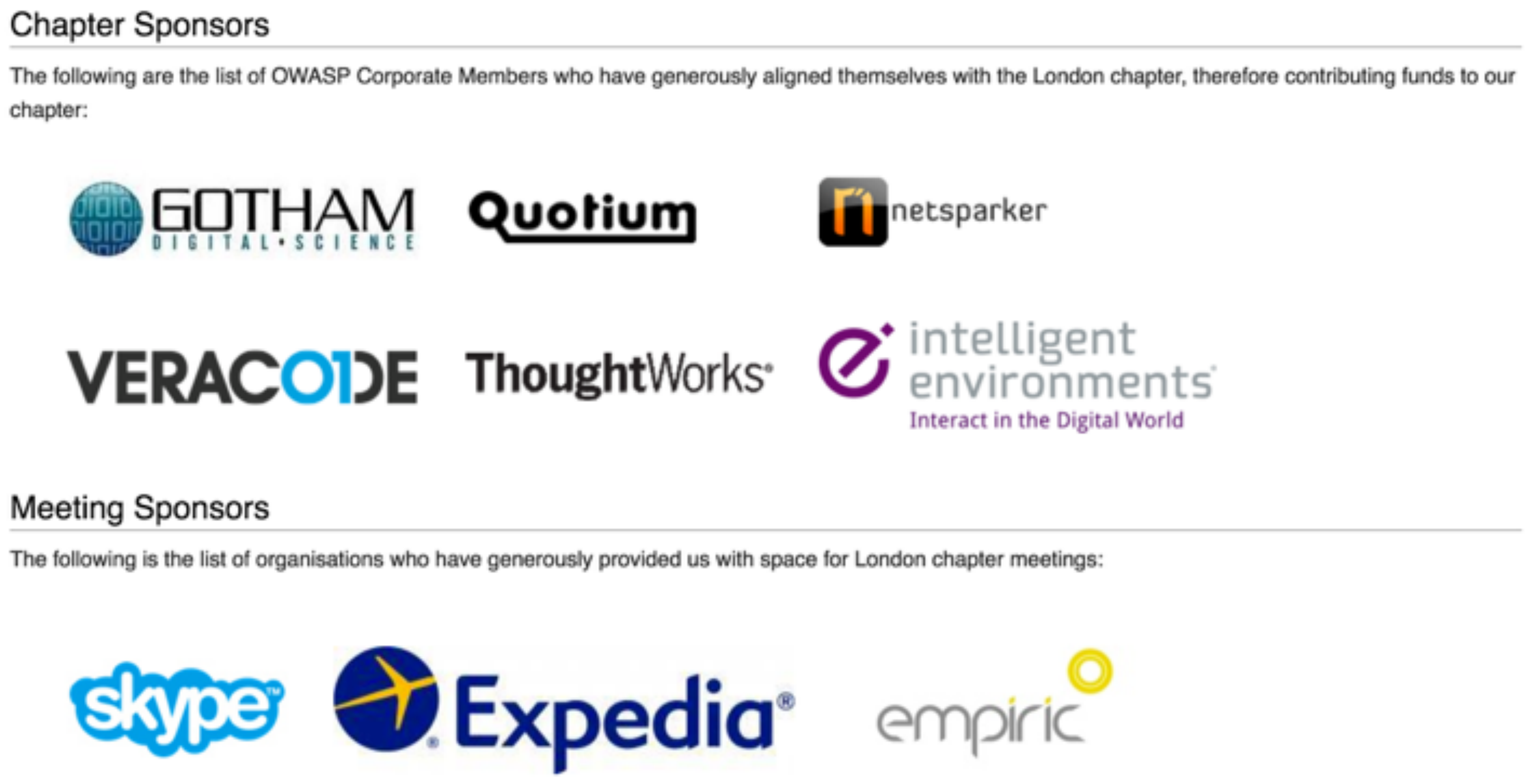
Questions about OWASP Membership? MEMBERSHIP FAQ

Care to see our global membership demographics? Membership Demographics as of January 2014

London Chapter Supporters

OWASP
The Open Web Application Security Project

Thanks to our sponsors! It is Thanksgiving!



Chapter Sponsors

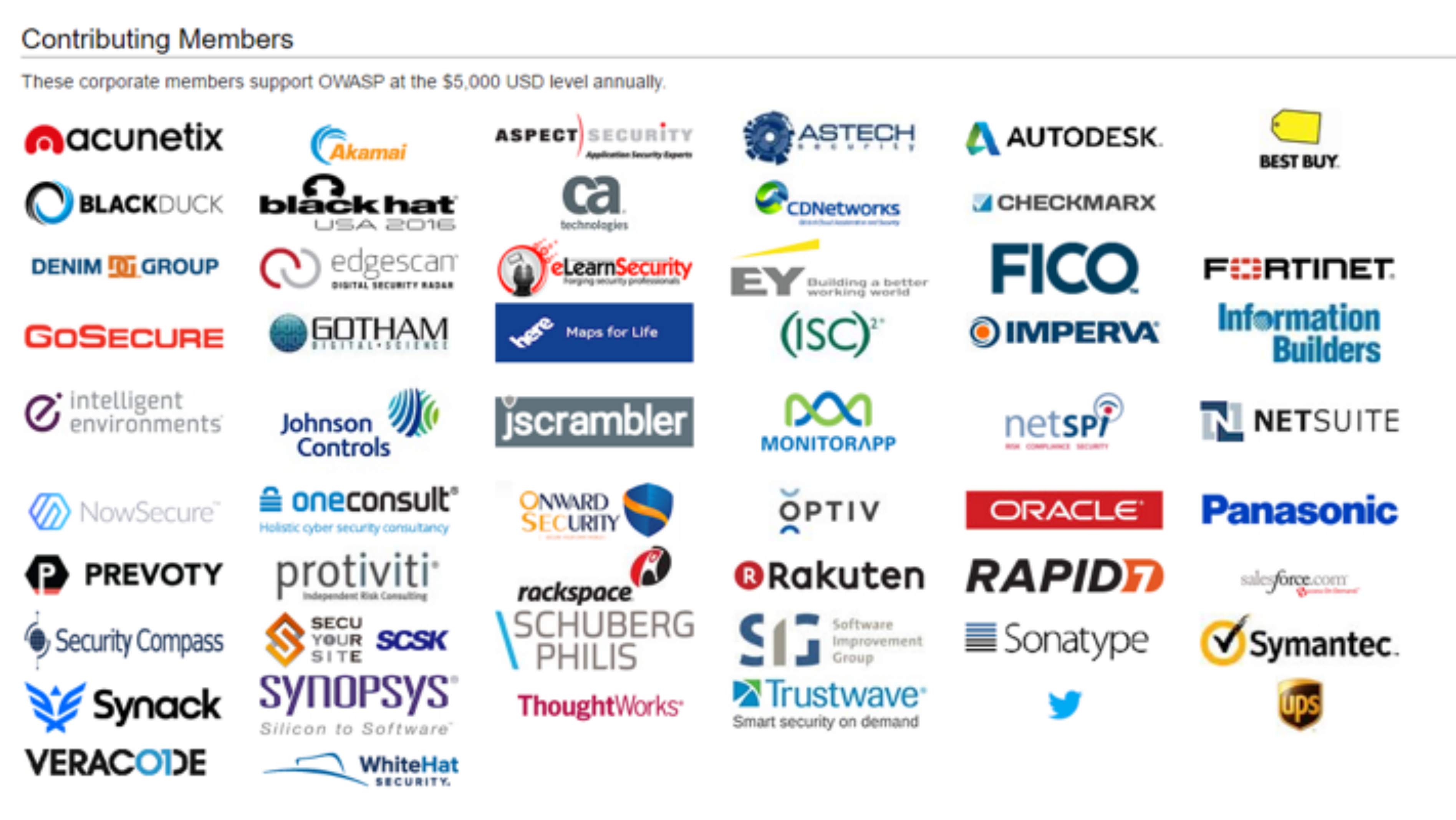
The following are the list of OWASP Corporate Members who have generously aligned themselves with the London chapter, therefore contributing funds to our chapter:

Meeting Sponsors

The following is the list of organisations who have generously provided us with space for London chapter meetings:

OWASP Corporate Members

OWASP
The Open Web Application Security Project

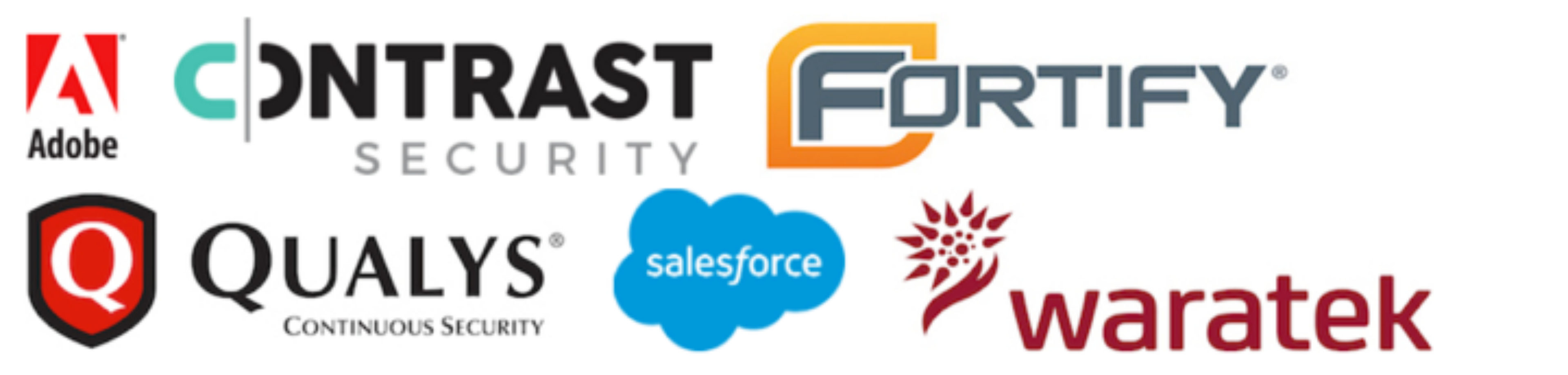


Contributing Members

These corporate members support OWASP at the $5,000 USD level annually.

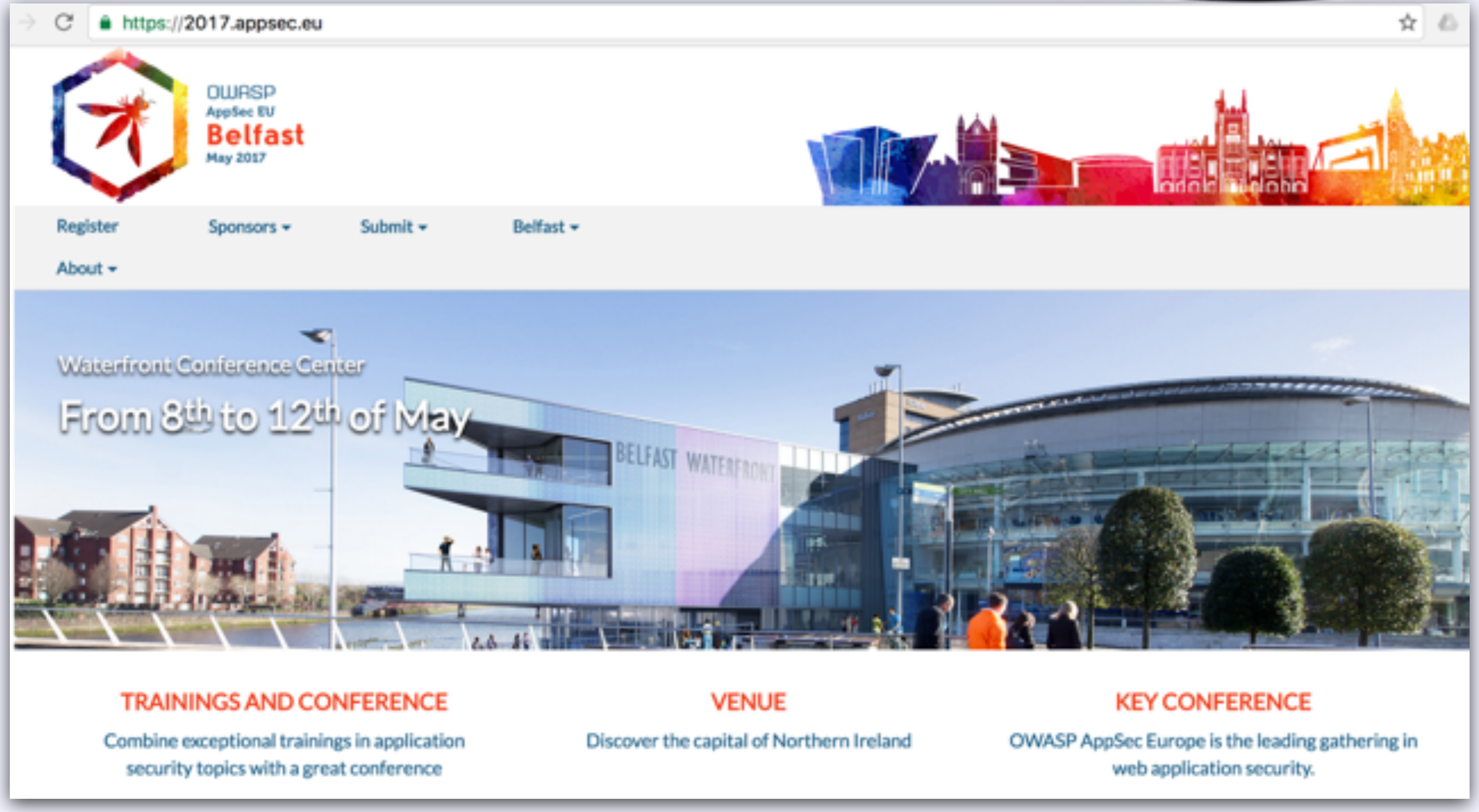
Premier Members

Premier members



AppSec Europe 2017

OWASP
The Open Web Application Security Project



https://2017.appsec.eu

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

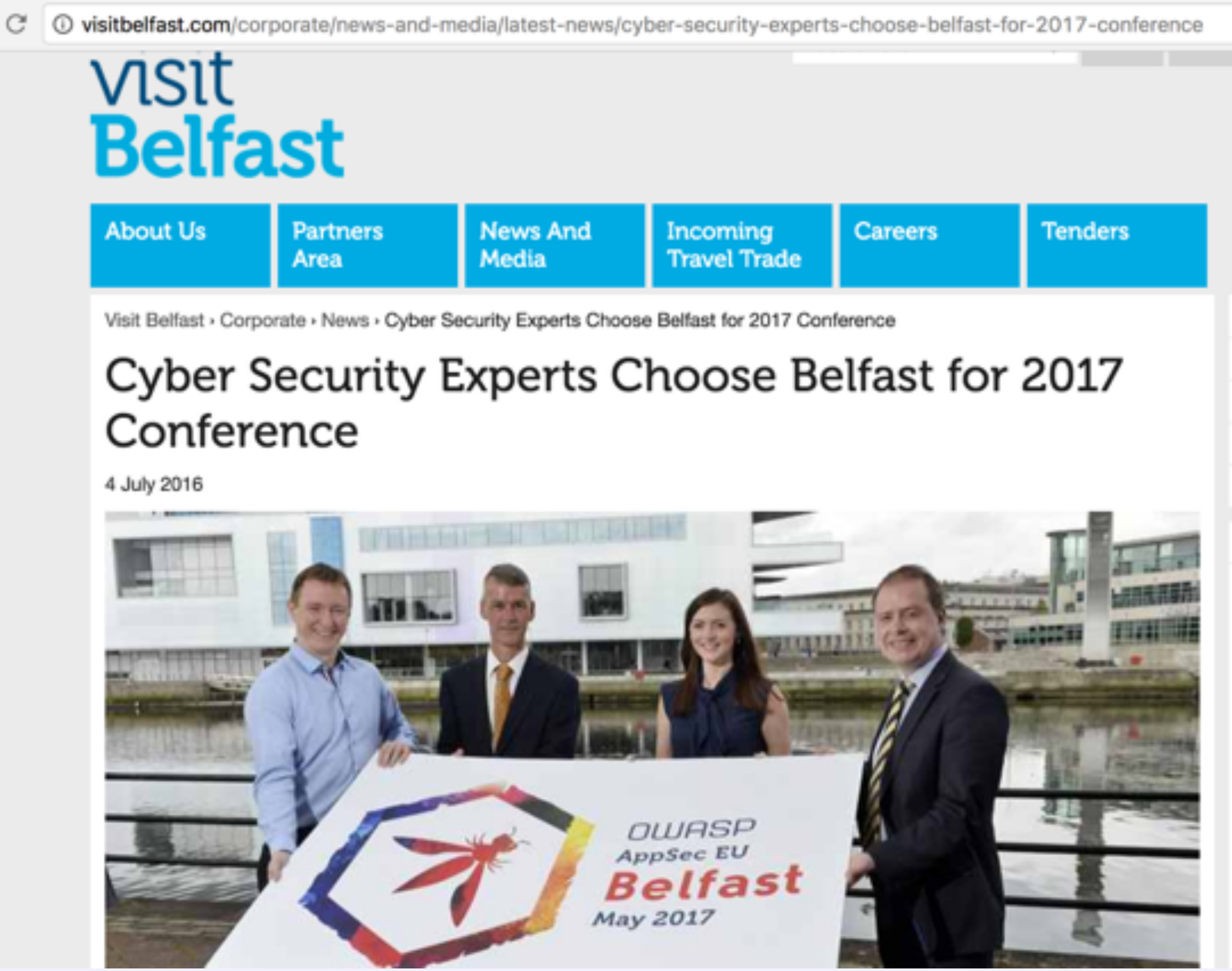
KEY CONFERENCE

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

8-12 May 2017, Belfast
Northern Ireland

Belfast,Belfast!

OWASP
The Open Web Application Security Project



visitbelfast.com/corporate/news-and-media/latest-news/cyber-security-experts-choose-belfast-for-2017-conference

visit Belfast

Visit Belfast › Corporate › News › Cyber Security Experts Choose Belfast for 2017 Conference

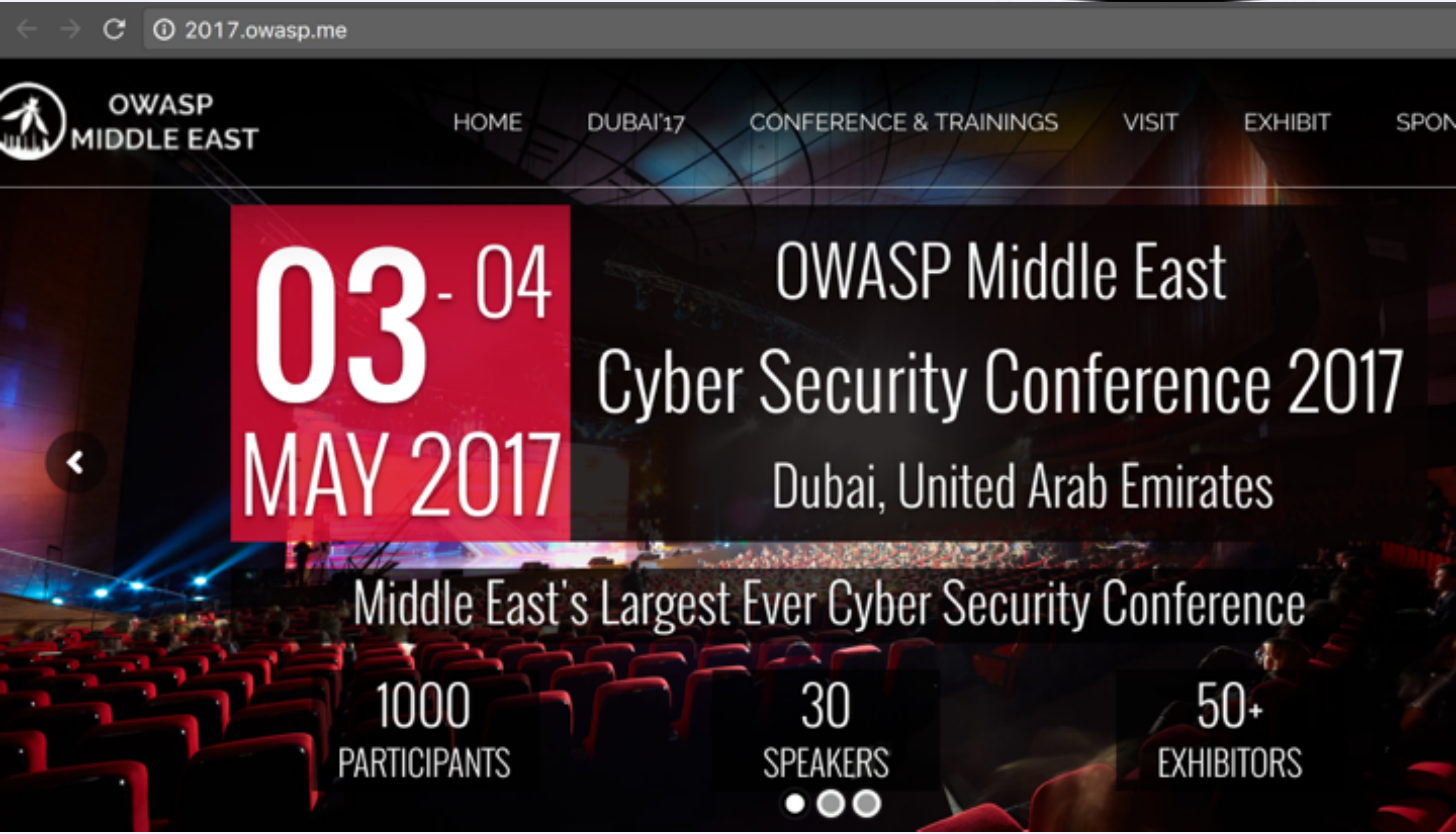
Cyber Security Experts Choose Belfast for 2017 Conference

4 July 2016

AppSecEurope 2017 - Call For Papers is OPEN! Submit your proposals!

OWASP MiddleEast 3-4 May 2017

OWASP
The Open Web Application Security Project



03 - 04 MAY 2017

OWASP Middle East

Cyber Security Conference 2017

Dubai, United Arab Emirates

Middle East's Largest Ever Cyber Security Conference

1000 PARTICIPANTS

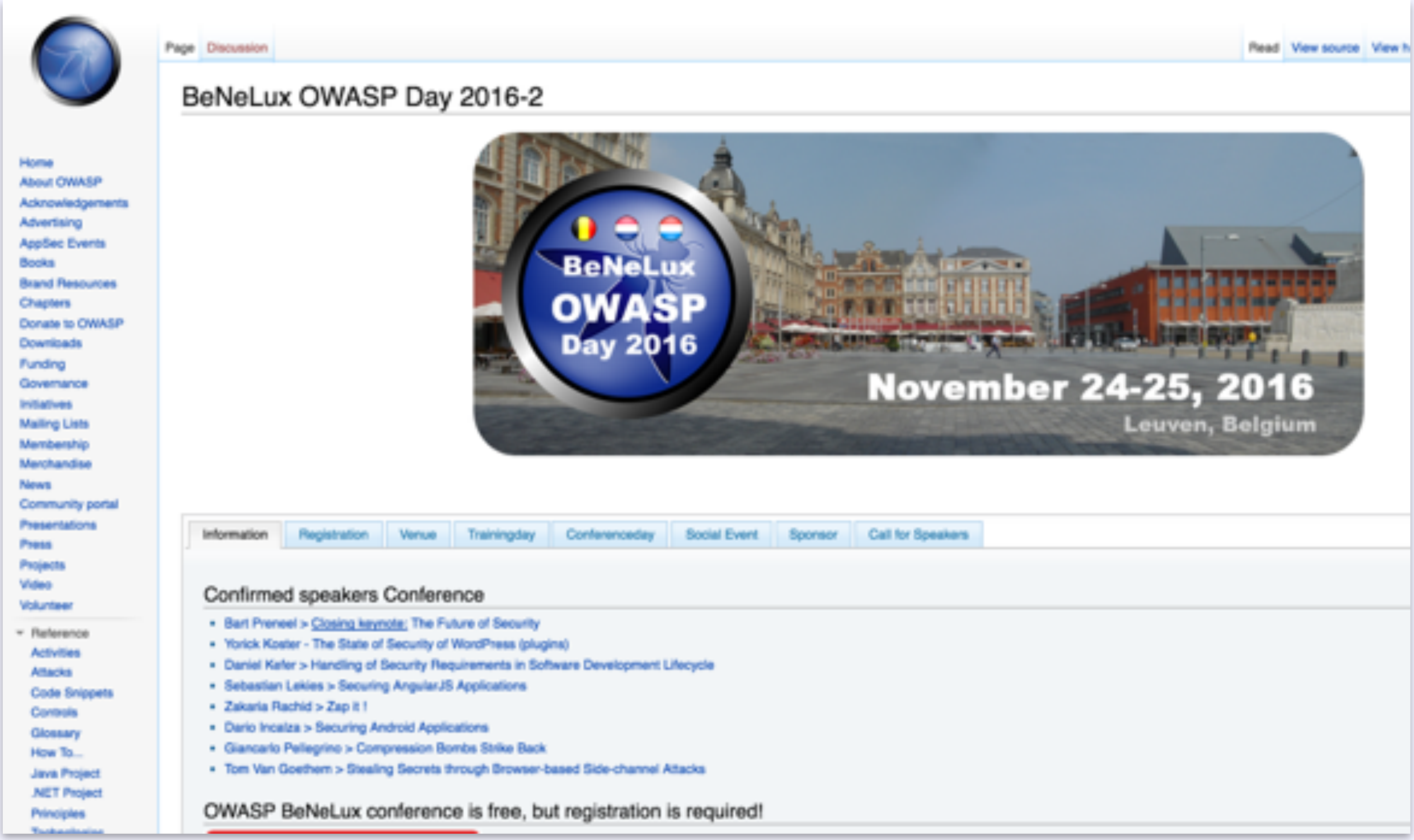
30 SPEAKERS

50+ EXHIBITORS

OWASP BeNeLux Days

OWASP
The Open Web Application Security Project

Leuven Belgium



Page | Discussion | Read | View source | View h

Home
About OWASP
Acknowledgements
Advertising
AppSec Events
Books
Brand Resources
Chapters
Donate to OWASP
Downloads
Funding
Governance
Initiatives
Mailing Lists
Membership
Merchandise
News
Community portal
Presentations
Press
Projects
Video
Volunteer

- Reference
  - Activities
  - Attacks
  - Code Snippets
  - Controls
  - Glossary
  - How To...
  - Java Project
  - .NET Project
  - Principles

BeNeLux OWASP Day 2016-2

BeNeLux OWASP Day 2016

November 24-25, 2016

Leuven, Belgium

Information | Registration | Venue | Trainingday | Conferenceday | Social Event | Sponsor | Call for Speakers

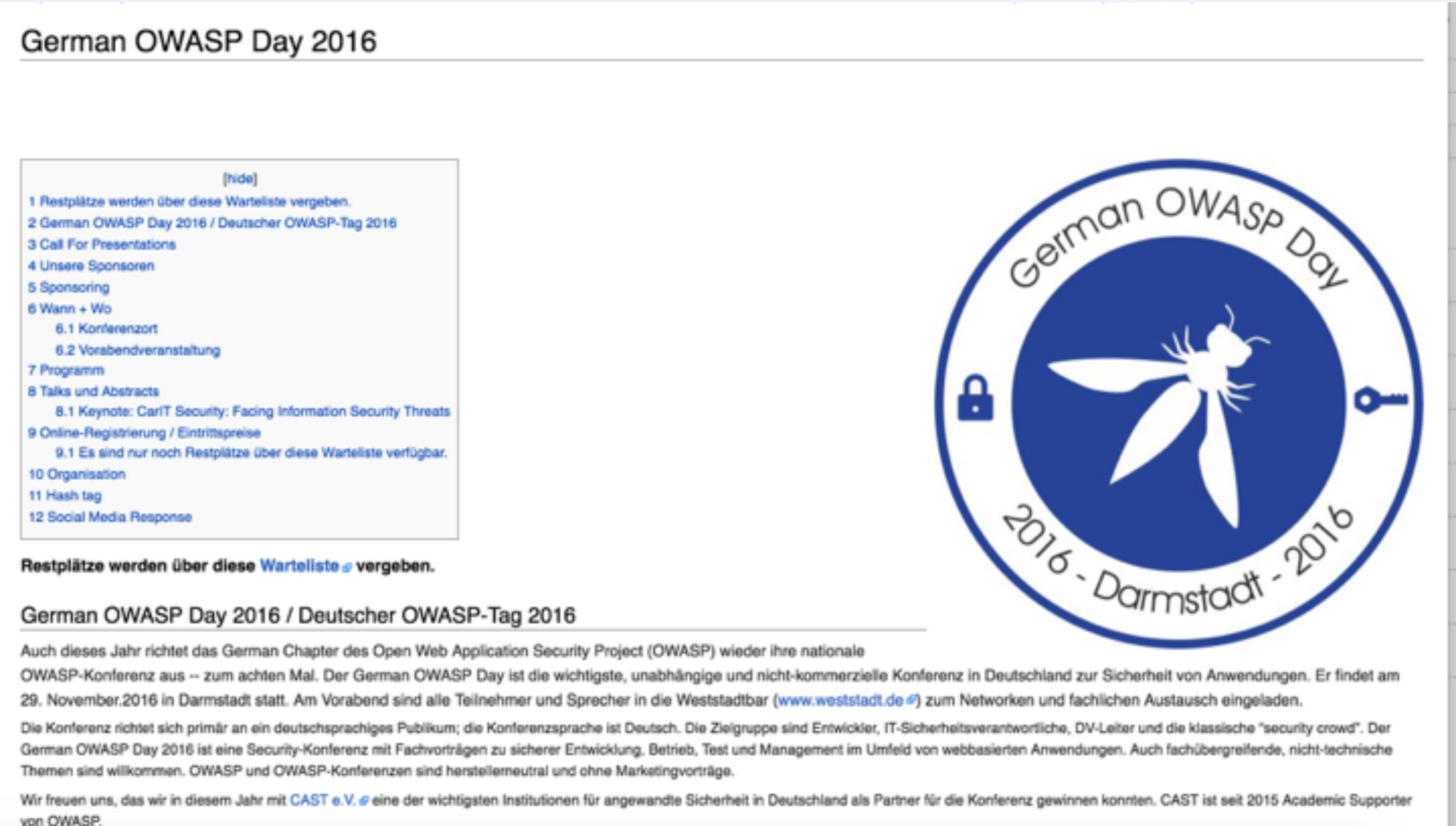
Confirmed speakers Conference

- Bart Preneel > Closing keynote: The Future of Security
- Yorick Koster - The State of Security of WordPress (plugins)
- Daniel Kefer > Handling of Security Requirements in Software Development Lifecycle
- Sebastian Lekies > Securing AngularJS Applications
- Zakaria Rachid > Zap it !
- Dario Incalza > Securing Android Applications
- Giancarlo Pellegrino > Compression Bombs Strike Back
- Tom Van Goethem > Stealing Secrets through Browser-based Side-channel Attacks

OWASP BeNeLux conference is free, but registration is required!

28-29 November Darmstadt

OWASP
The Open Web Application Security Project



German OWASP Day 2016

[hide]

Restplätze werden über diese Warteliste vergeben.

German OWASP Day 2016 / Deutscher OWASP-Tag 2016

Auch dieses Jahr richtet das German Chapter des Open Web Application Security Project (OWASP) wieder ihre nationale OWASP-Konferenz aus -- zum achten Mal. Der German OWASP Day ist die wichtigste, unabhängige und nicht-kommerzielle Konferenz in Deutschland zur Sicherheit von Anwendungen. Er findet am 29. November.2016 in Darmstadt statt. Am Vorabend sind alle Teilnehmer und Sprecher in die Weststadtbar (www.weststadt.de) zum Networken und fachlichen Austausch eingeladen.

Die Konferenz richtet sich primär an ein deutschsprachiges Publikum; die Konferenzsprache ist Deutsch. Die Zielgruppe sind Entwickler, IT-Sicherheitsverantwortliche, DV-Leiter und die klassische "security crowd". Der German OWASP Day 2016 ist eine Security-Konferenz mit Fachvorträgen zu sicherer Entwicklung, Betrieb, Test und Management im Umfeld von webbasierten Anwendungen. Auch fachübergreifende, nicht-technische Themen sind willkommen. OWASP und OWASP-Konferenzen sind herstellerneutral und ohne Marketingvorträge.

Wir freuen uns, das wir in diesem Jahr mit CAST e.V. eine der wichtigsten Institutionen für angewandte Sicherheit in Deutschland als Partner für die Konferenz gewinnen konnten. CAST ist seit 2015 Academic Supporter von OWASP.

28th November 2016 - Secure Development Workshop & Hackathon

29th November 2016 - CTF Competition (with Prizes!)

nccgroup

ThoughtWorks®

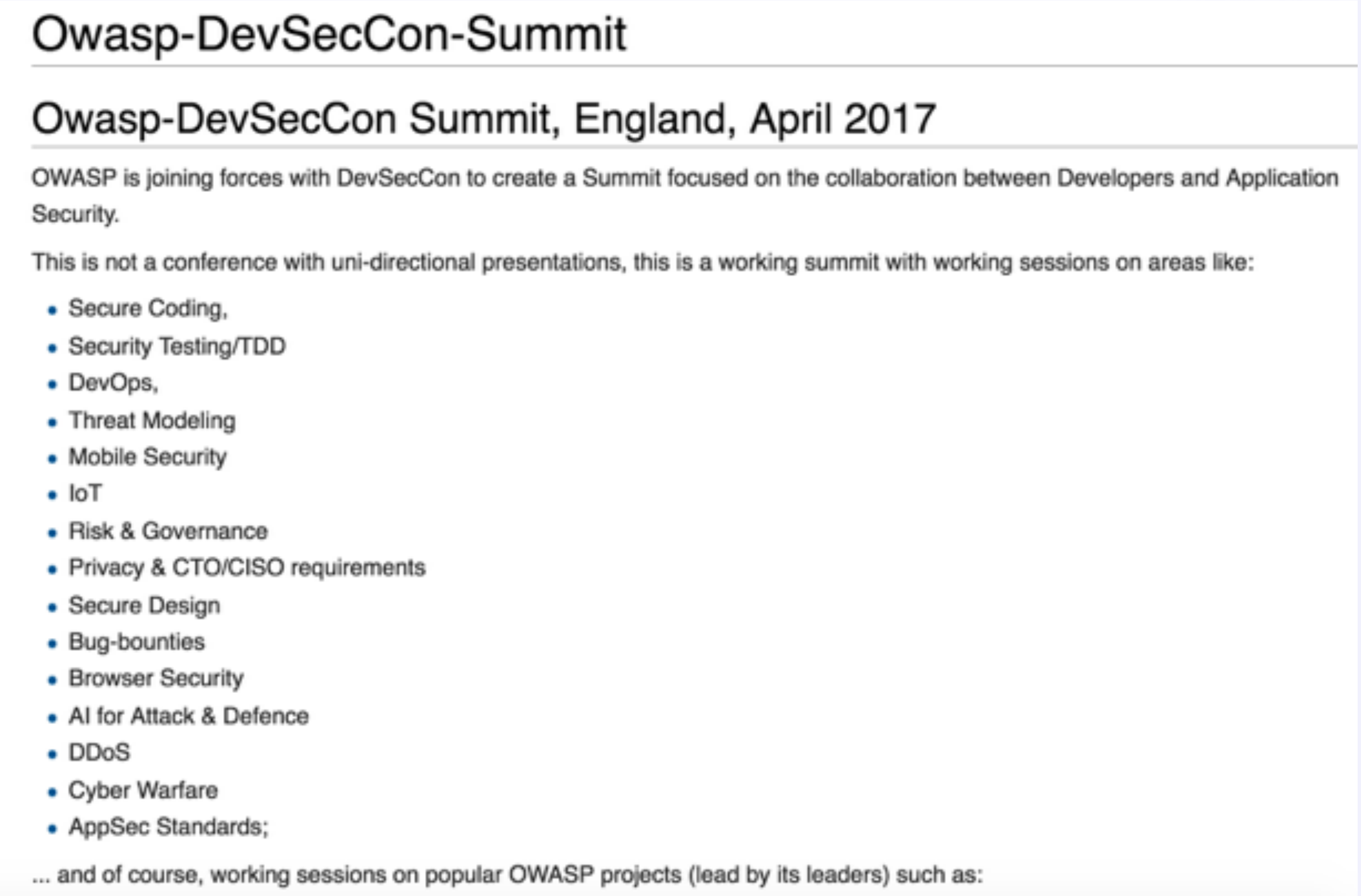
Pen Test Partners

>_codebashing

Veracode

SECURE CODE WARRIOR

DevSecCon Summit Planned



Owasp-DevSecCon-Summit

Owasp-DevSecCon Summit, England, April 2017

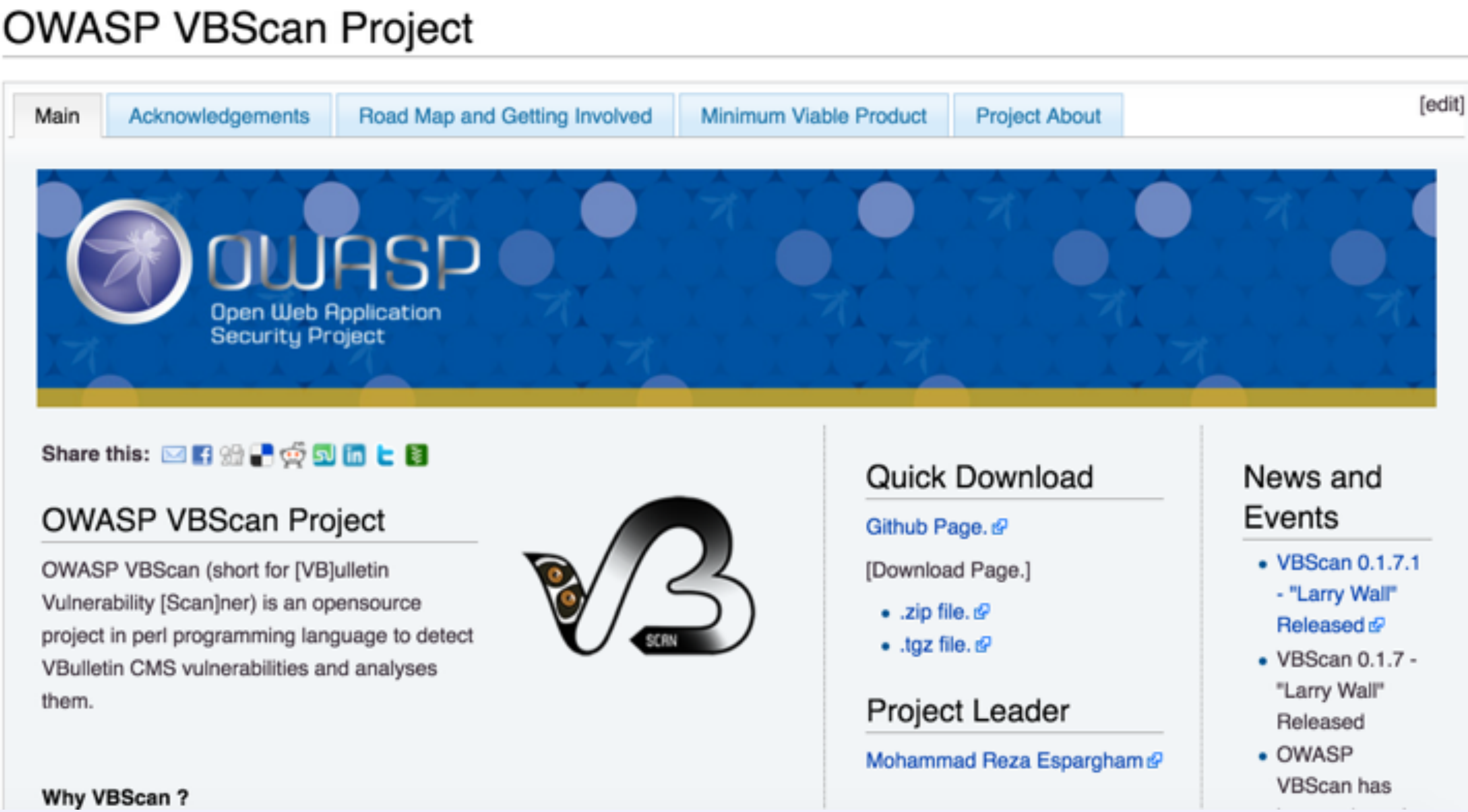
OWASP is joining forces with DevSecCon to create a Summit focused on the collaboration between Developers and Application Security.

This is not a conference with uni-directional presentations, this is a working summit with working sessions on areas like:

- Secure Coding,
- Security Testing/TDD
- DevOps,
- Threat Modeling
- Mobile Security
- IoT
- Risk & Governance
- Privacy & CTO/CISO requirements
- Secure Design
- Bug-bounties
- Browser Security
- AI for Attack & Defence
- DDoS
- Cyber Warfare
- AppSec Standards;

... and of course, working sessions on popular OWASP projects (lead by its leaders) such as:

VBScan Projects



OWASP VBScan Project

Share this:

OWASP VBScan Project

OWASP VBScan (short for [VB]ulletin Vulnerability [Scan]ner) is an opensource project in perl programming language to detect VBulletin CMS vulnerabilities and analyses them.

Why VBScan ?

Quick Download

Github Page.

[Download Page.]

- .zip file.
- .tgz file.

Project Leader

Mohammad Reza Espargham

News and Events

- VBScan 0.1.7.1 - "Larry Wall" Released
- VBScan 0.1.7 - "Larry Wall" Released
- OWASP VBScan has

OWASP Mobile AppSec

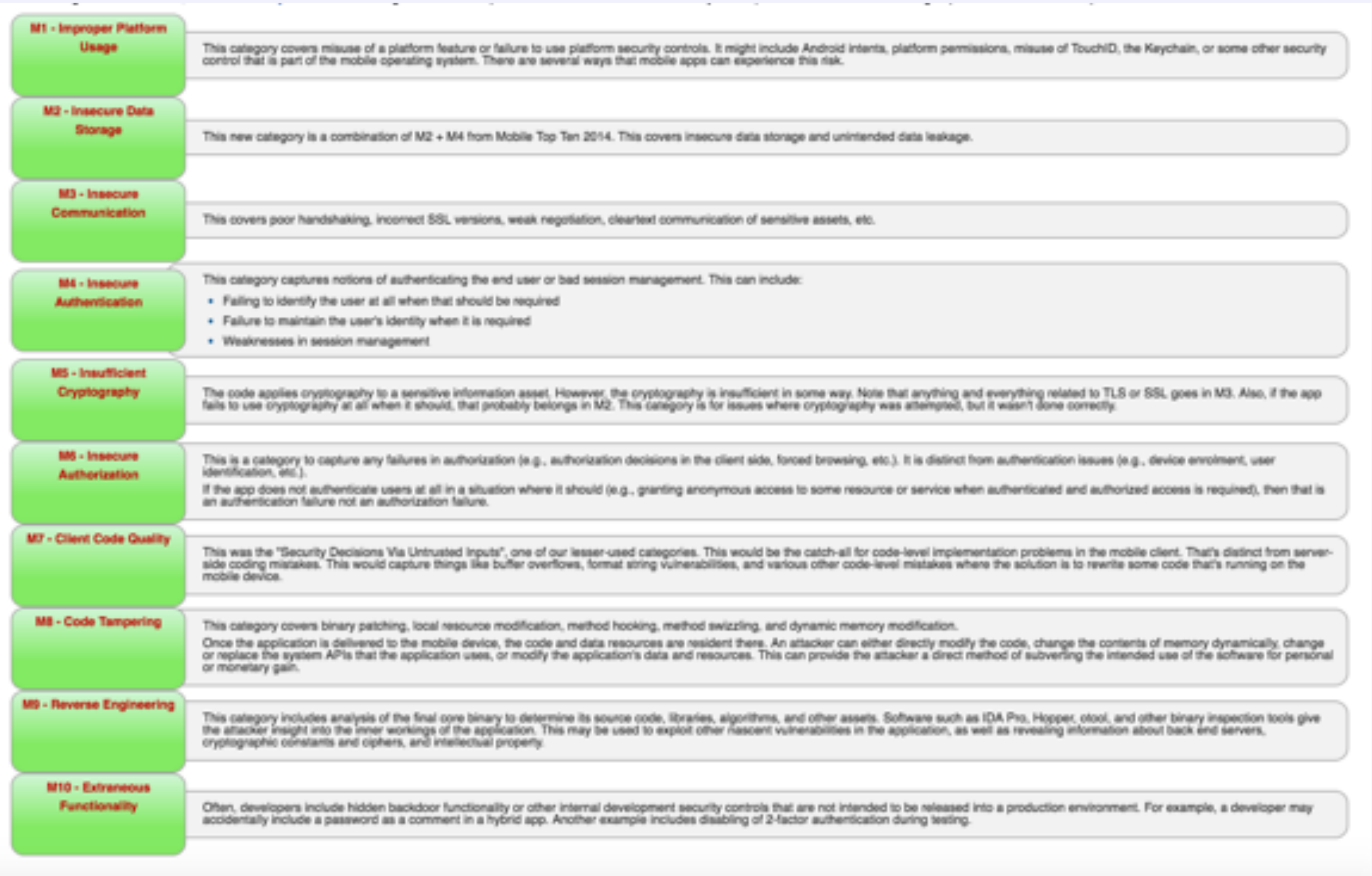
OWASP
Open Web Application Security Project

Standard 0.9 beta

Mobile AppSec Verification

OWASP Mobile Top 10 RC

OWASP Mobile Top 10 2016 - Release Candidate



M1 - Improper Platform Usage

This category covers misuse of a platform feature or failure to use platform security controls. It might include Android intents, platform permissions, misuse of TouchID, the Keychain, or some other security control that is part of the mobile operating system. There are several ways that mobile apps can experience this risk.

M2 - Insecure Data Storage

This new category is a combination of M2 + M4 from Mobile Top Ten 2014. This covers insecure data storage and unintended data leakage.

M3 - Insecure Communication

This covers poor handshaking, incorrect SSL versions, weak negotiation, cleartext communication of sensitive assets, etc.

M4 - Insecure Authentication

This category captures notions of authenticating the end user or bad session management. This can include:

- Failing to identify the user at all when that should be required
- Failure to maintain the user's identity when it is required
- Weaknesses in session management

M5 - Insufficient Cryptography

The code applies cryptography to a sensitive information asset. However, the cryptography is insufficient in some way. Note that anything and everything related to TLS or SSL goes in M3. Also, if the app fails to use cryptography at all when it should, that probably belongs in M2. This category is for issues where cryptography was attempted, but it wasn't done correctly.

M6 - Insecure Authorization

This is a category to capture any failures in authorization (e.g., authorization decisions in the client side, forced browsing, etc.). It is distinct from authentication issues (e.g., device enrolment, user identification, etc.).

If the app does not authenticate users at all in a situation where it should (e.g., granting anonymous access to some resource or service when authenticated and authorized access is required), then that is an authentication failure not an authorization failure.

M7 - Client Code Quality

This was the "Security Decisions Via Untrusted Inputs", one of our lesser-used categories. This would be the catch-all for code-level implementation problems in the mobile client. That's distinct from server-side coding mistakes. This would capture things like buffer overflows, format string vulnerabilities, and various other code-level mistakes where the solution is to rewrite some code that's running on the mobile device.

M8 - Code Tampering

This category covers binary patching, local resource modification, method hooking, method swizzling, and dynamic memory modification.

Once the application is delivered to the mobile device, the code and data resources are resident there. An attacker can either directly modify the code, change the contents of memory dynamically, change or replace the system APIs that the application uses, or modify the application's data and resources. This can provide the attacker a direct method of subverting the intended use of the software for personal or monetary gain.

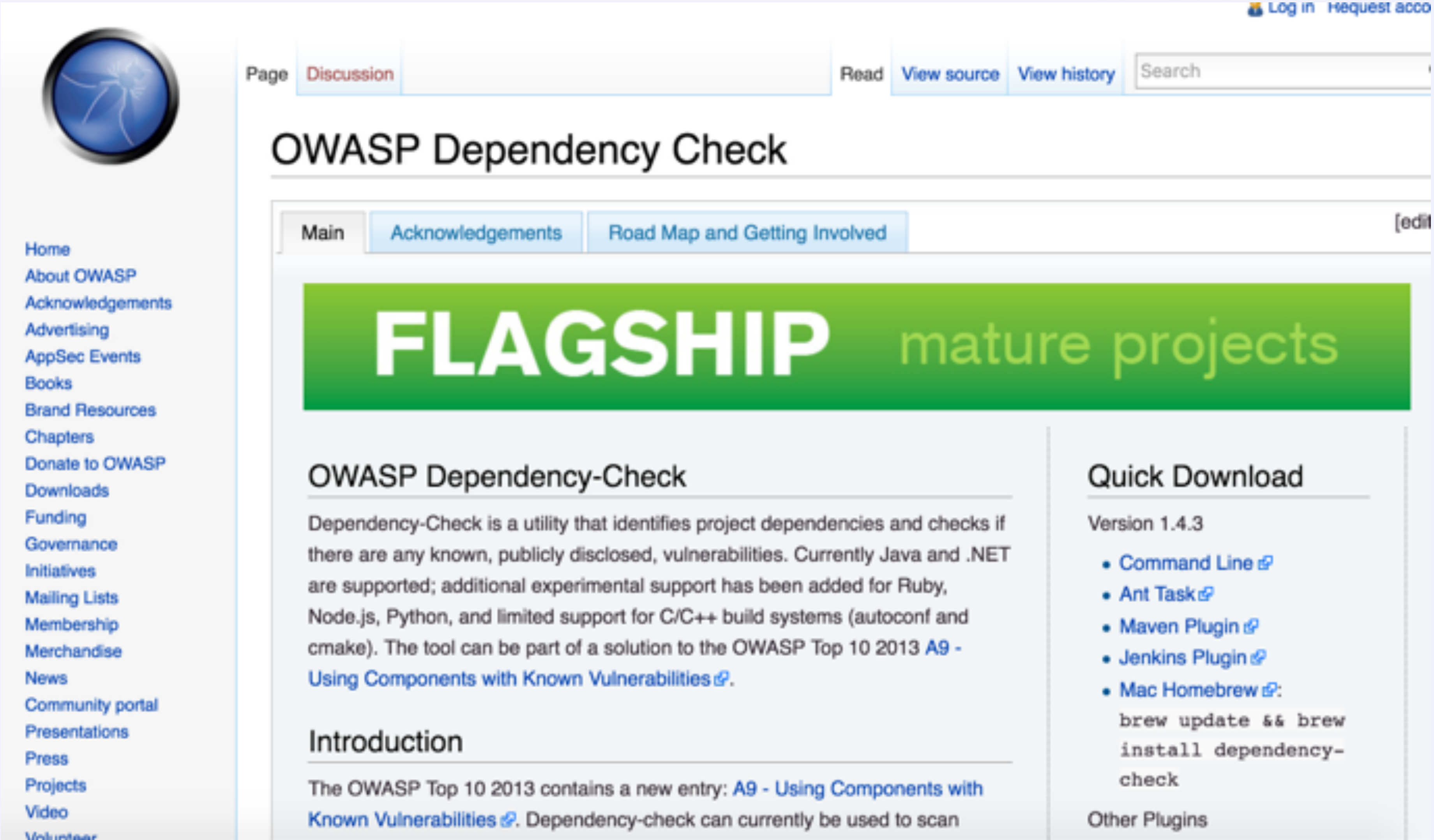
M9 - Reverse Engineering

This category includes analysis of the final core binary to determine its source code, libraries, algorithms, and other assets. Software such as IDA Pro, Hopper, otool, and other binary inspection tools give the attacker insight into the inner workings of the application. This may be used to exploit other nascent vulnerabilities in the application, as well as revealing information about back end servers, cryptographic constants and ciphers, and intellectual property.

M10 - Extraneous Functionality

Often, developers include hidden backdoor functionality or other internal development security controls that are not intended to be released into a production environment. For example, a developer may accidentally include a password as a comment in a hybrid app. Another example includes disabling of 2-factor authentication during testing.

Dependency Check



OWASP Dependency Check

OWASP Dependency-Check

Dependency-Check is a utility that identifies project dependencies and checks if there are any known, publicly disclosed, vulnerabilities. Currently Java and .NET are supported; additional experimental support has been added for Ruby, Node.js, Python, and limited support for C/C++ build systems (autoconf and cmake). The tool can be part of a solution to the OWASP Top 10 2013 A9 - Using Components with Known Vulnerabilities.

Introduction

The OWASP Top 10 2013 contains a new entry: A9 - Using Components with Known Vulnerabilities. Dependency-check can currently be used to scan

Quick Download

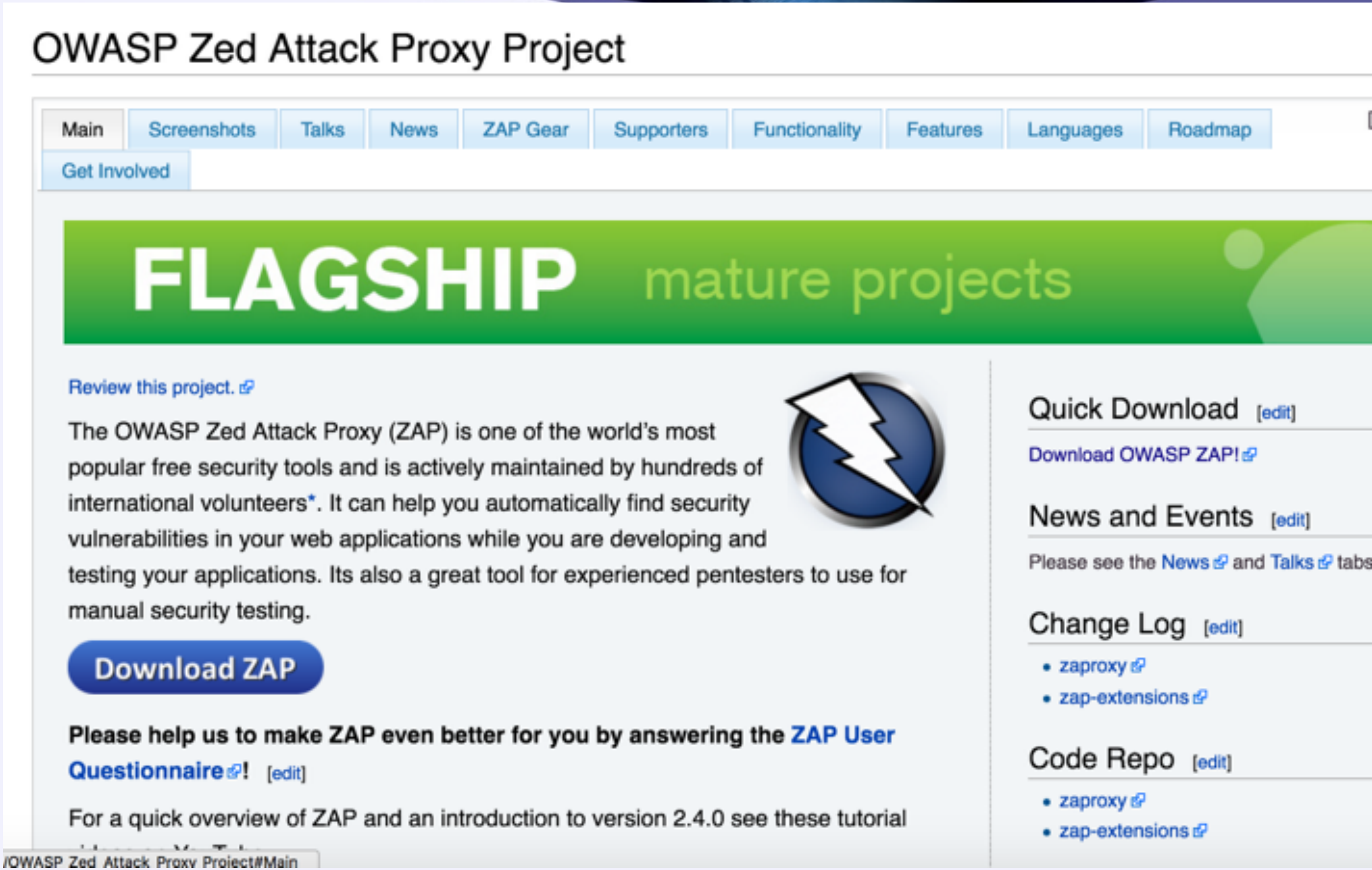
Version 1.4.3

- Command Line
- Ant Task
- Maven Plugin
- Jenkins Plugin
- Mac Homebrew:

```
brew update && brew
install dependency-
check
```

Other Plugins

OWASP ZAP



OWASP Zed Attack Proxy Project

FLAGSHIP mature projects

Review this project.

The OWASP Zed Attack Proxy (ZAP) is one of the world's most popular free security tools and is actively maintained by hundreds of international volunteers*. It can help you automatically find security vulnerabilities in your web applications while you are developing and testing your applications. Its also a great tool for experienced pentesters to use for manual security testing.

Please help us to make ZAP even better for you by answering the ZAP User Questionnaire! [edit]

For a quick overview of ZAP and an introduction to version 2.4.0 see these tutorial

Quick Download [edit]

Download OWASP ZAP!

News and Events [edit]

Please see the News and Talks tabs

Change Log [edit]

- zaproxy
- zap-extensions

Code Repo [edit]

- zaproxy
- zap-extensions

Staying in Touch
OWASP London

OWASP
The Open Web Application Security Project

Keep in Touch – get informed about future events:

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

owasp.slack.com #chapter-london

Visit OWASP London Chapter webpage

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

OWASP London
Save The Dates of Future meetings:

26th January 2017

Present Your Talk

OWASP

The Open Web Application Security Project

Call For Speakers For Future Events

Do you have a great Web 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:

- Jeremy King
- Gareth Hayes
- Goran Sarenkapa
- Shane Kelly

Hosts for this event

- Empiric

- Attendees (you!)