26th January 2017

OWASP

The Open Web Application Security Project

Agenda

OWASP
The Open Web Application Security Project

- **Networking, snacks & drinks**
- **Welcome and OWASP Update** - Sam Stepanyan & Sherif Mansour
- **Identities Exposed - How Design Flaws in Authentication Solutions May Compromise Your Privacy** - David Johansson
- **Lightning Talk: Introducing OWASP Summit 2017** - Francois Raynaud, Dinis Cruz

  ——————— break —— snacks—drinks——————-
- **OWASP-SAMM Maturity Models -** Dinis Cruz
- **Networking & Beer**

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

OWASP

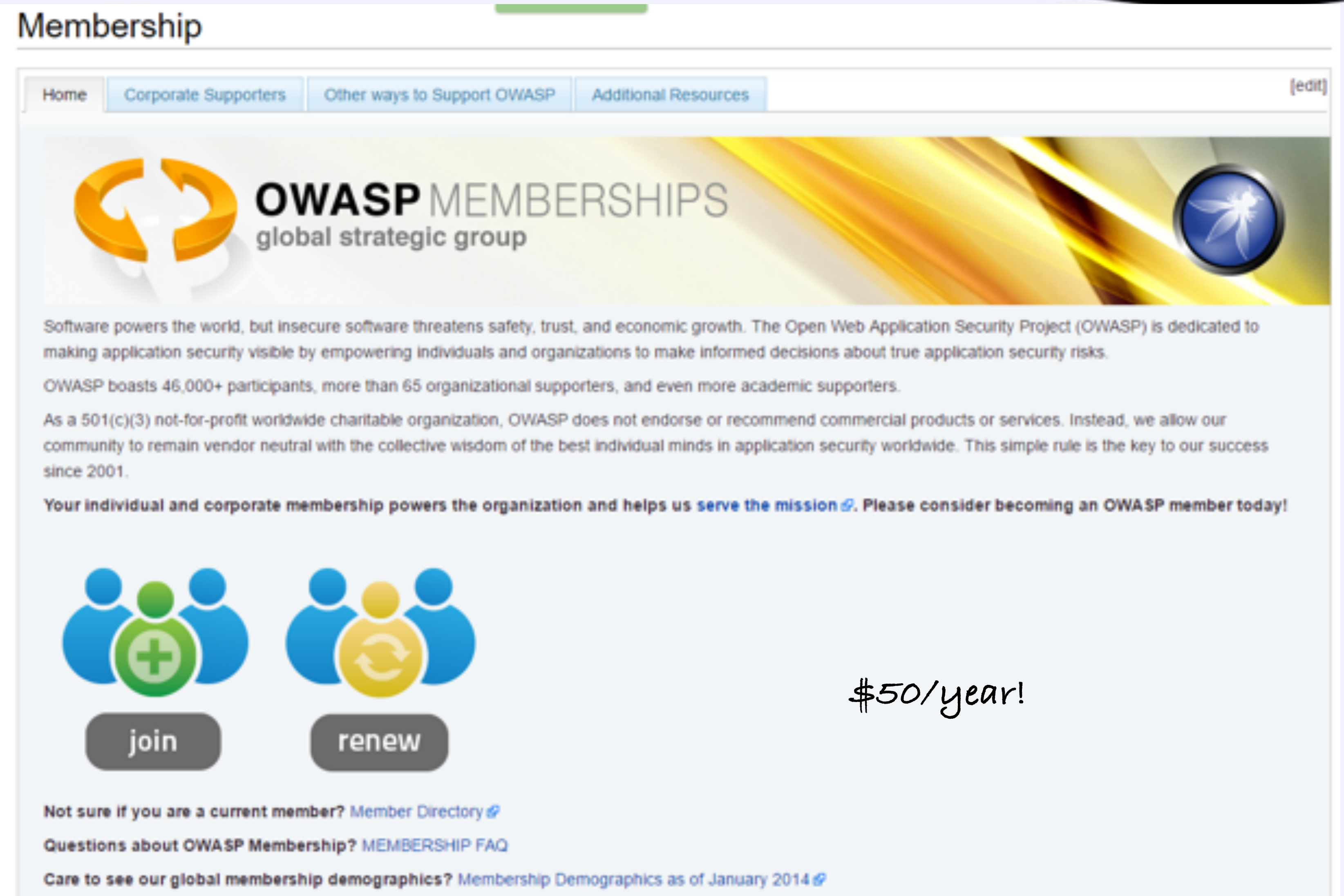
OWASP
The Open Web Application Security Project

- 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
- All meetings are free to attend (*free beer included)

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!

$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

London Chapter Supporters

GOTHAM DIGITAL SCIENCE

Quotium

netsparker

VERACODE

ThoughtWorks

intelligent environments
Interact in the Digital World

skype

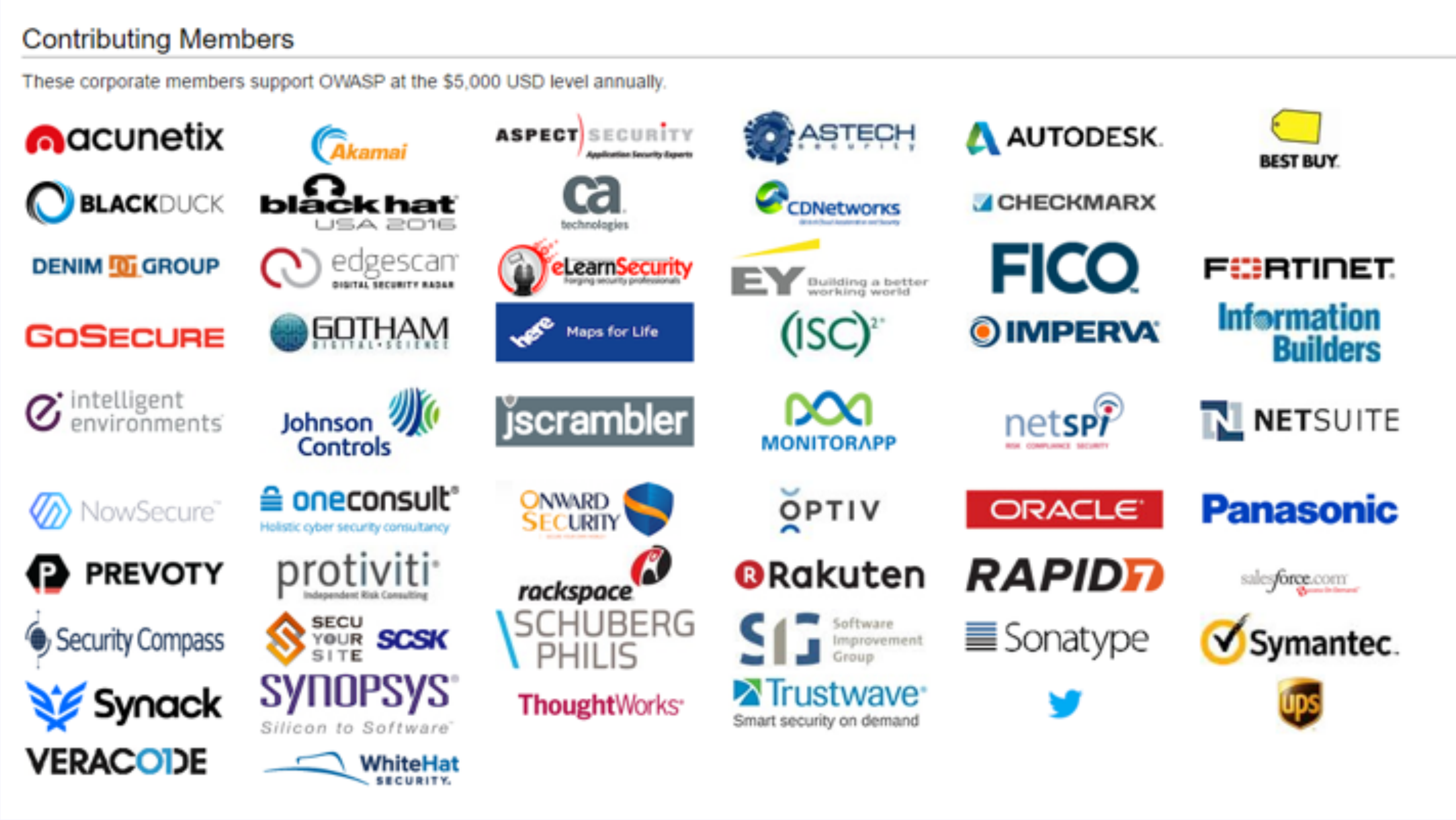
Expedia

empiric

J.P.Morgan

OWASP Corporate Members

OWASP
The Open Web Application Security Project

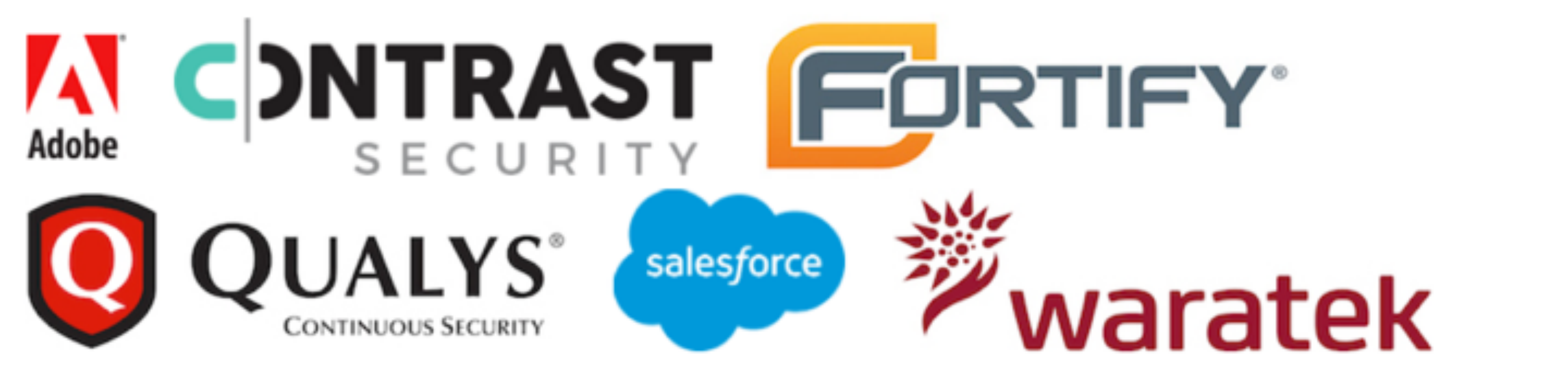


Contributing Members

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

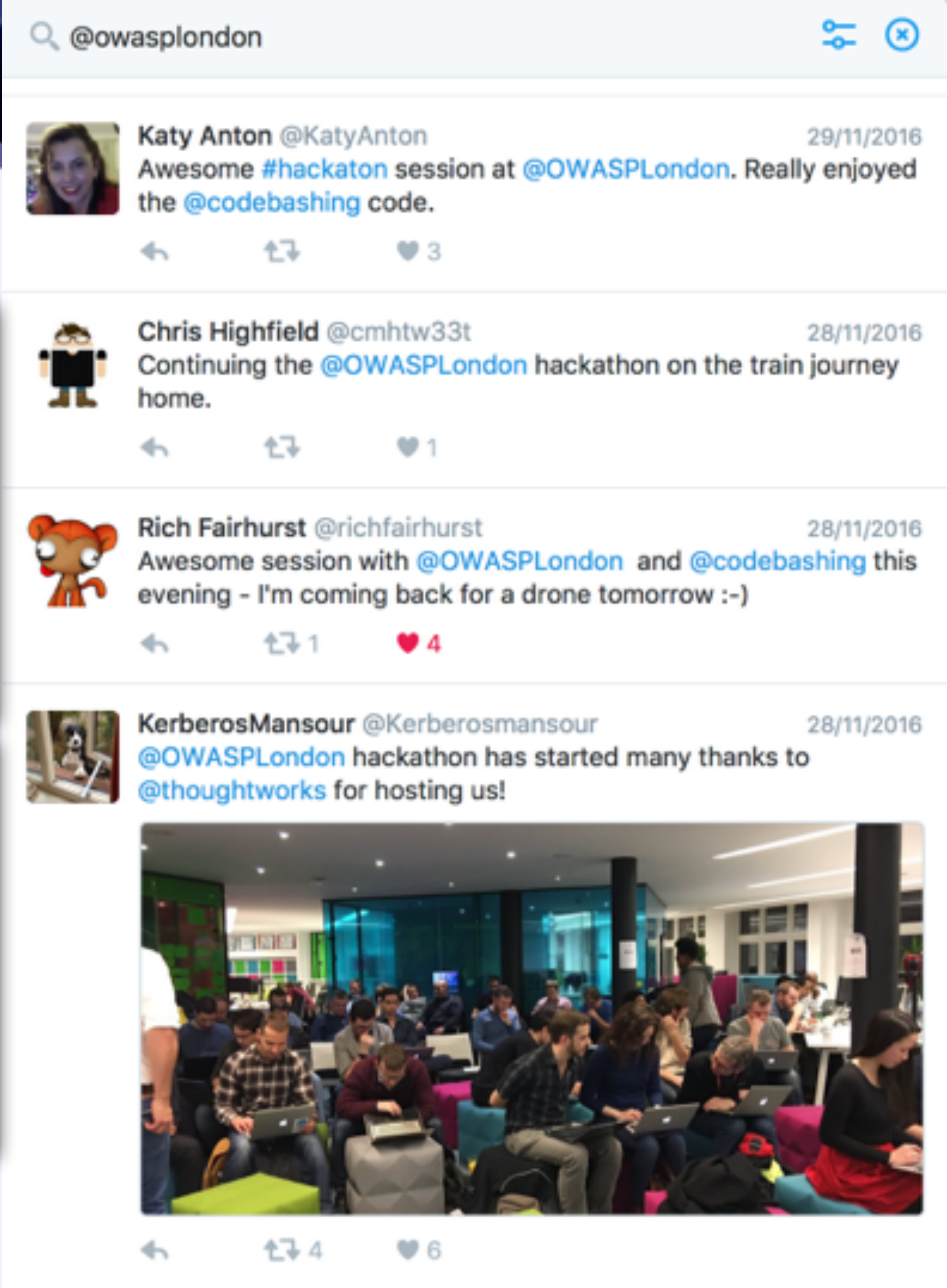
Premier Members

Premier members



Hackathon & CTF Tournament

OWASP
The Open Web Application Security Project



@owasplondon

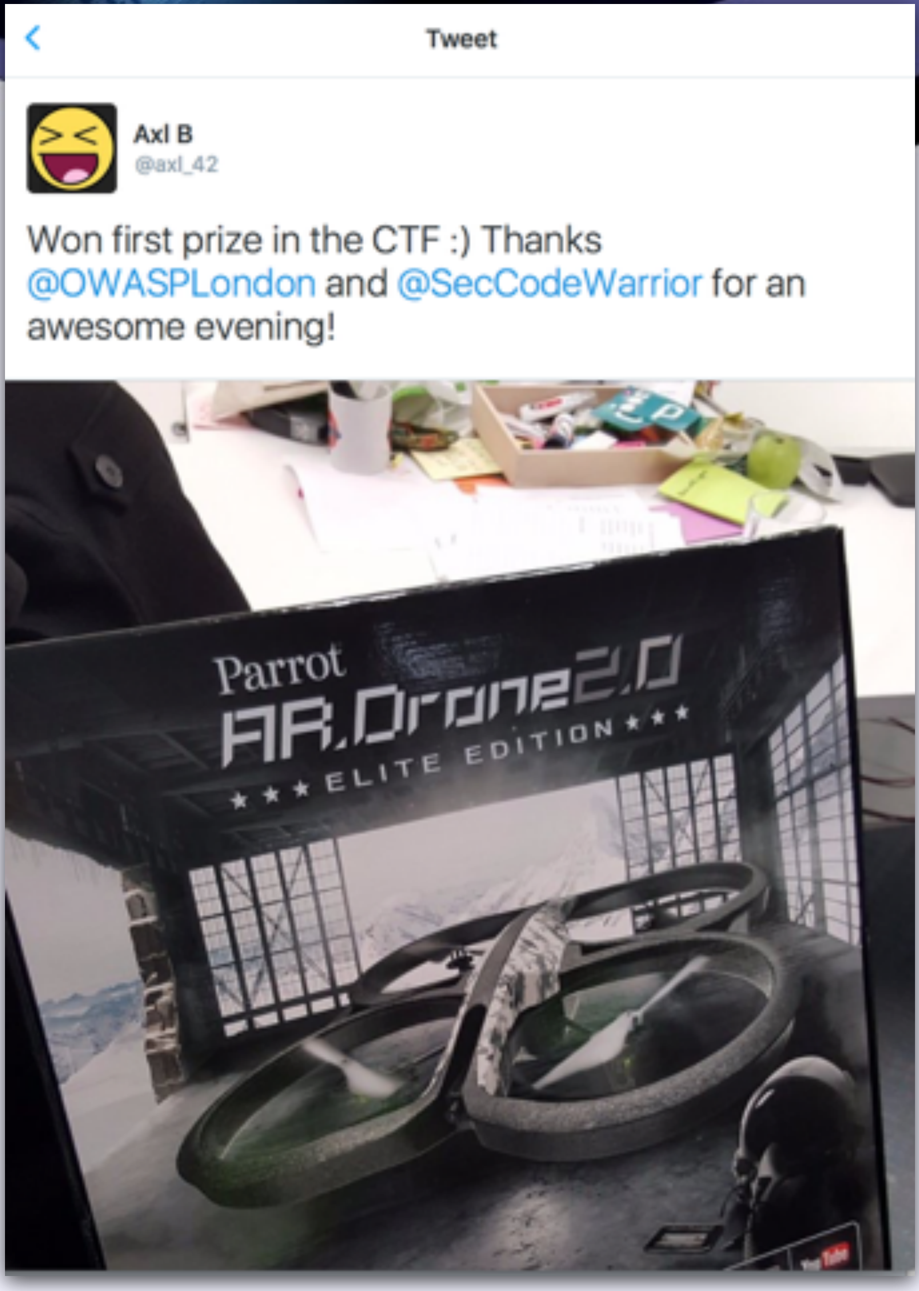
Katy Anton @KatyAnton 29/11/2016
Awesome #hackaton session at @OWASPLondon. Really enjoyed the @codebashing code.
3

Chris Highfield @cmhtw33t 28/11/2016
Continuing the @OWASPLondon hackathon on the train journey home.
1

Rich Fairhurst @richfairhurst 28/11/2016
Awesome session with @OWASPLondon and @codebashing this evening - I'm coming back for a drone tomorrow :-)
1 4

KerberosMansour @Kerberosmansour 28/11/2016
@OWASPLondon hackathon has started many thanks to @thoughtworks for hosting us!
4 6

Hackathon Prizes



Axl B
@axl_42

Won first prize in the CTF :) Thanks @OWASPLondon and @SecCodeWarrior for an awesome evening!

Hackathon Sponsors Needed

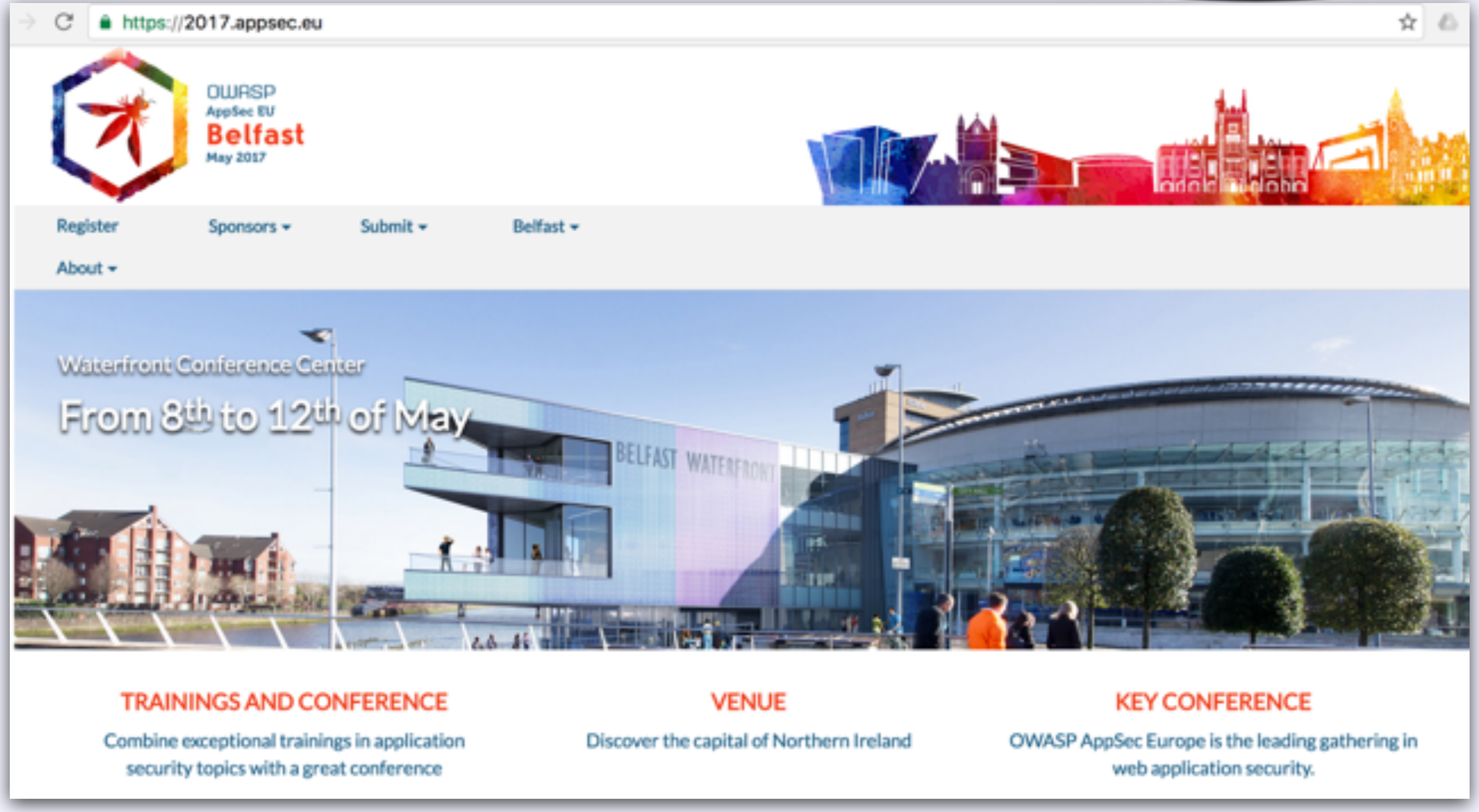
There will be a Hackathon this year - need hosting sponsors!

Tomas Zezula @TomasZezula 29/11/2016

Exciting challenge with an amusing twist at the end. Thanks for organising @OWASPLondon #CTF

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

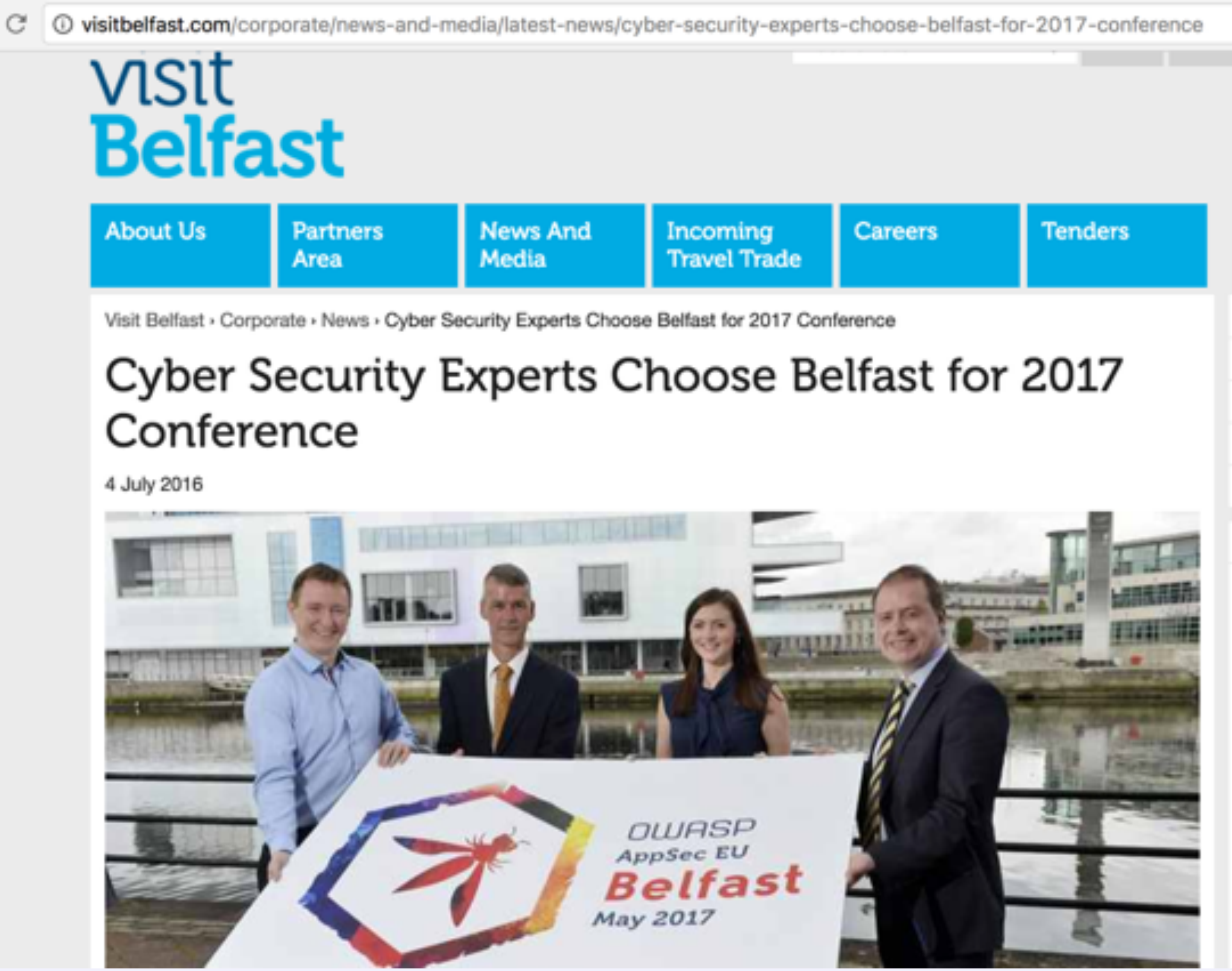
Discover the capital of Northern Ireland

KEY CONFERENCE

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

8-12 May 2017, Belfast
Northern Ireland

Belfast,Belfast!



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

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

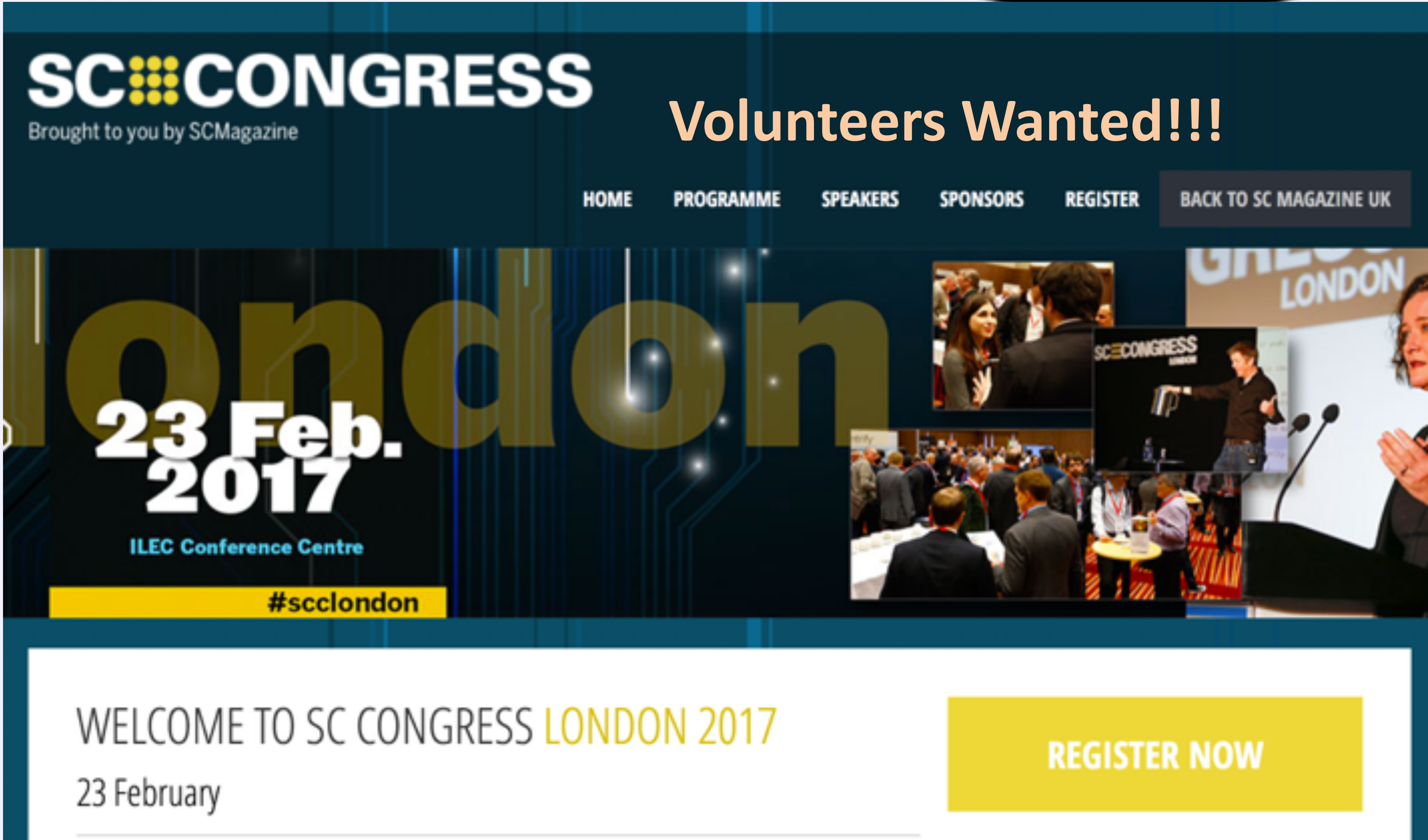
Cyber Security Experts Choose Belfast for 2017 Conference

4 July 2016

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

SC London

Volunteers Wanted!!!



SC CONGRESS
Brought to you by SCMagazine

HOME PROGRAMME SPEAKERS SPONSORS REGISTER BACK TO SC MAGAZINE UK

london

23 Feb. 2017

ILEC Conference Centre

#scclondon

WELCOME TO SC CONGRESS LONDON 2017

23 February

REGISTER NOW

SC Congress

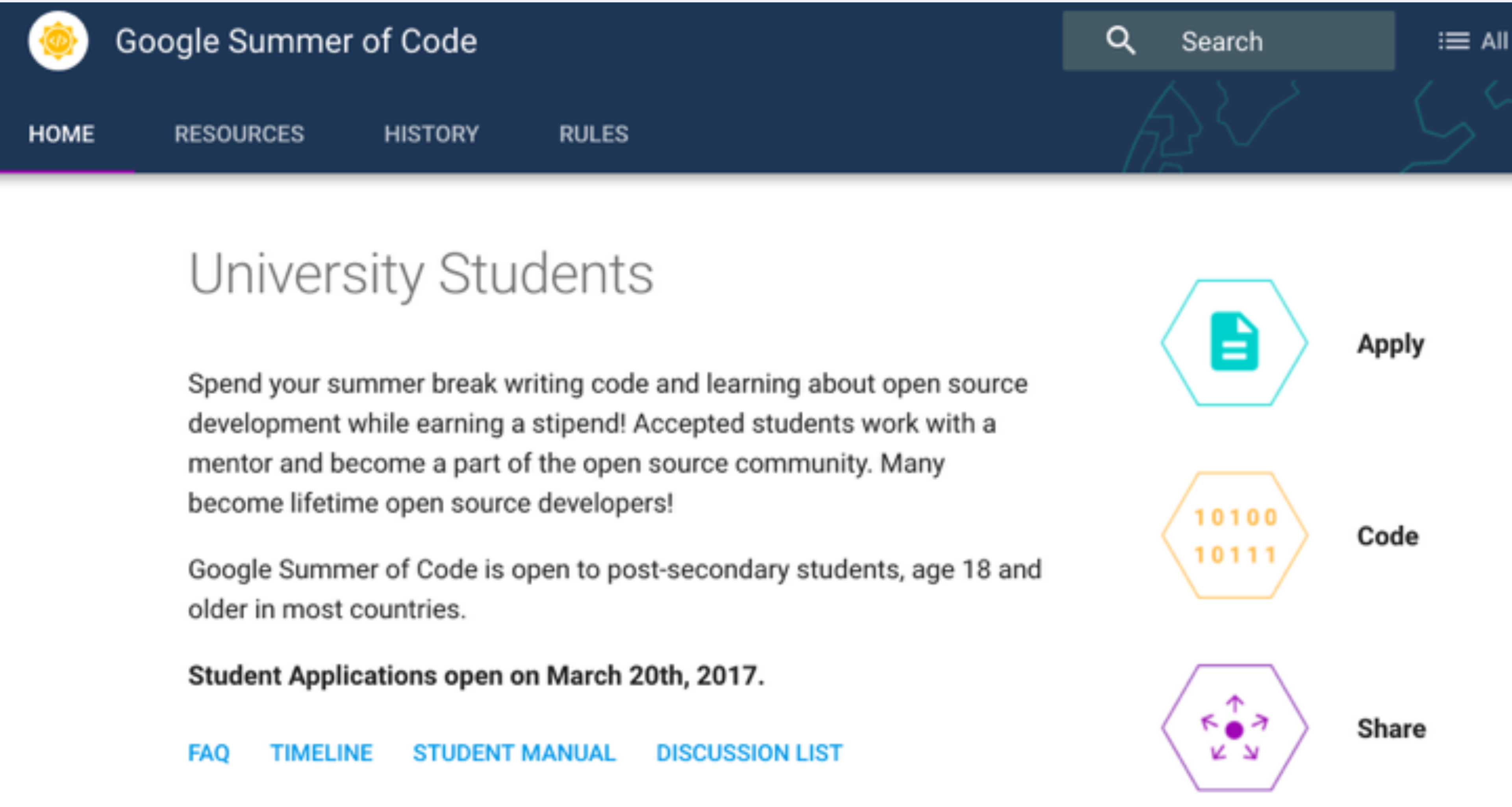
OWASP
The Open Web Application Security Project

- Volunteers wanted to staff the OWASP Booth on 23 February 2017

Please get in touch if you can volunteer

Google Summer of Code

Flip bits! Not burgers!



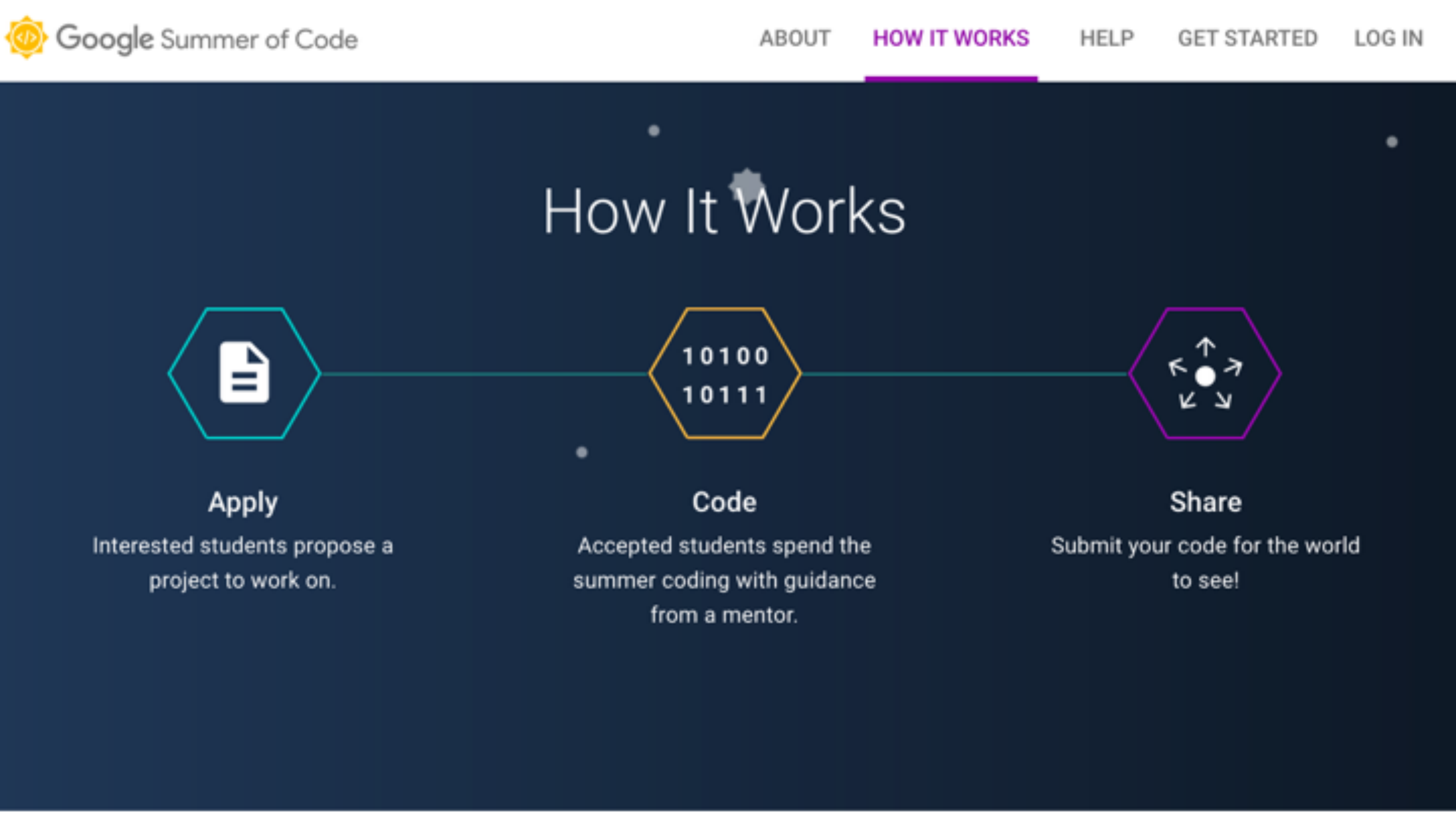
University Students

Spend your summer break writing code and learning about open source development while earning a stipend! Accepted students work with a mentor and become a part of the open source community. Many become lifetime open source developers!

Google Summer of Code is open to post-secondary students, age 18 and older in most countries.

Student Applications open on March 20th, 2017.

Google Summer Of Code



How It Works

Apply

Interested students propose a project to work on.

Code

Accepted students spend the summer coding with guidance from a mentor.

Share

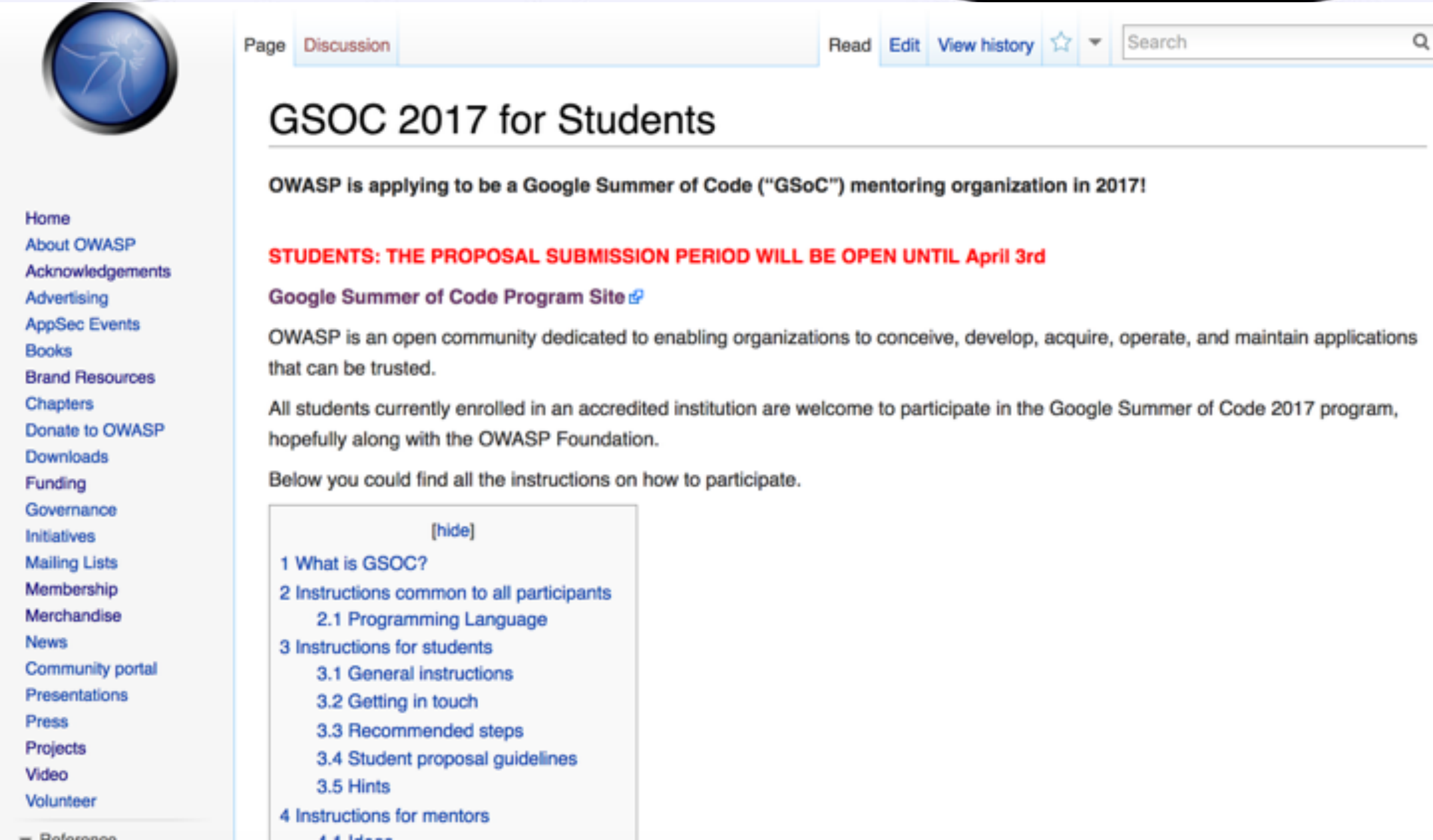
Submit your code for the world to see!

GSOC: How you can get involved

OWASP
The Open Web Application Security Project

- Become a **Mentor for a student**:
- Choose a **participating OWASP project** from the wiki page, preferably the one you are **most familiar** with.
- Touch base with the project leader and ask one of the OWASP Administrators to send you an invitation to get started today.
- Help OWASP Invite Students:
- Are you somehow affiliated with a university? Get in touch with students, inform them about the program and how they can participate with OWASP.
  Please direct students to the wiki page for details: https://www.owasp.org/index.php/GSOC_2017_for_Students

GSoC:April 3rd Deadline



GSOC 2017 for Students

OWASP is applying to be a Google Summer of Code ("GSoC") mentoring organization in 2017!

STUDENTS: THE PROPOSAL SUBMISSION PERIOD WILL BE OPEN UNTIL April 3rd

Google Summer of Code Program Site

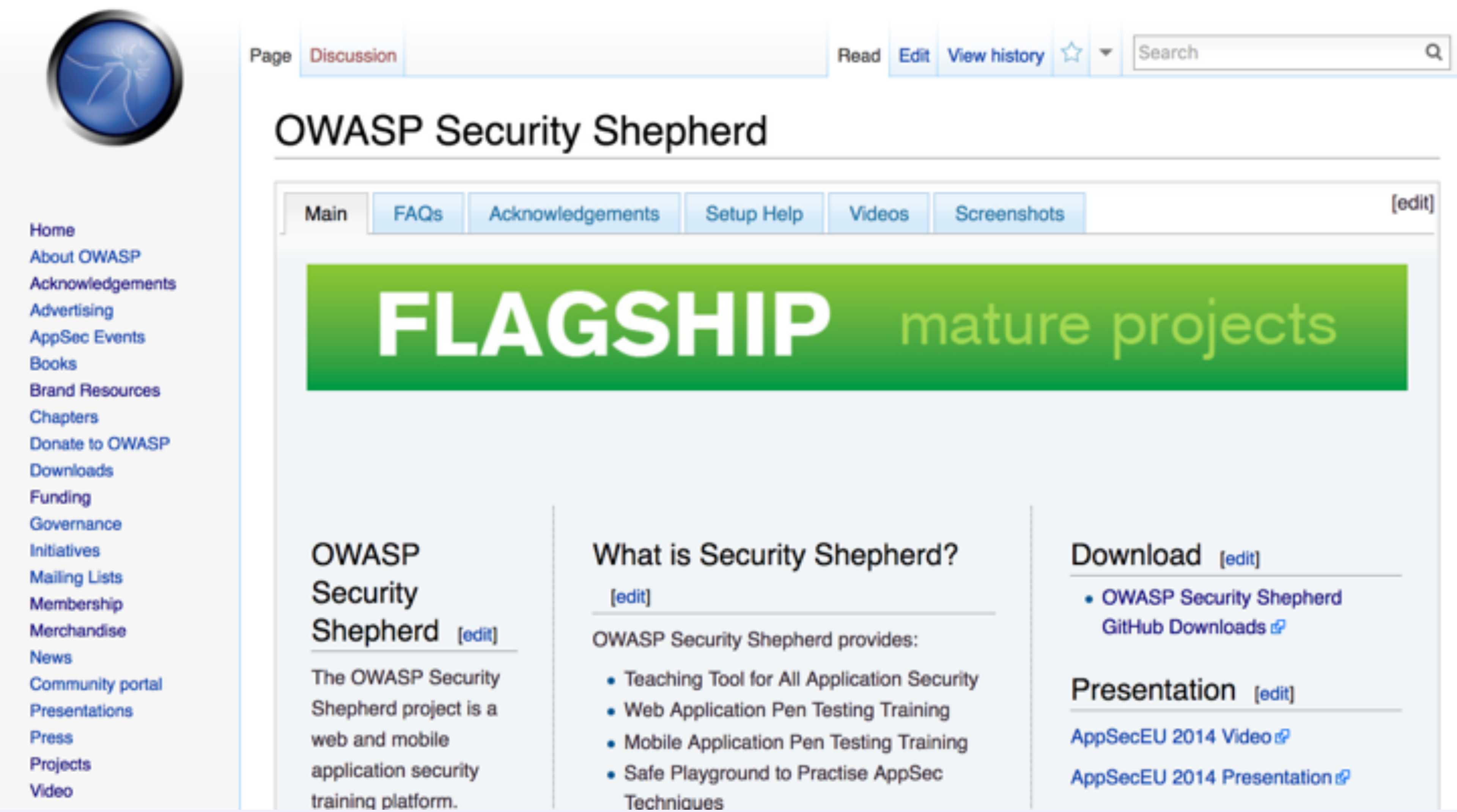
OWASP is an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted.

All students currently enrolled in an accredited institution are welcome to participate in the Google Summer of Code 2017 program, hopefully along with the OWASP Foundation.

Below you could find all the instructions on how to participate.

[hide]

New Flagship:Security Shepherd



OWASP Security Shepherd

- 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

FLAGSHIP mature projects

OWASP Security Shepherd [edit]

The OWASP Security Shepherd project is a web and mobile application security training platform.

What is Security Shepherd? [edit]

OWASP Security Shepherd provides:

- Teaching Tool for All Application Security
- Web Application Pen Testing Training
- Mobile Application Pen Testing Training
- Safe Playground to Practise AppSec Techniques

Download [edit]

- OWASP Security Shepherd GitHub Downloads

Presentation [edit]

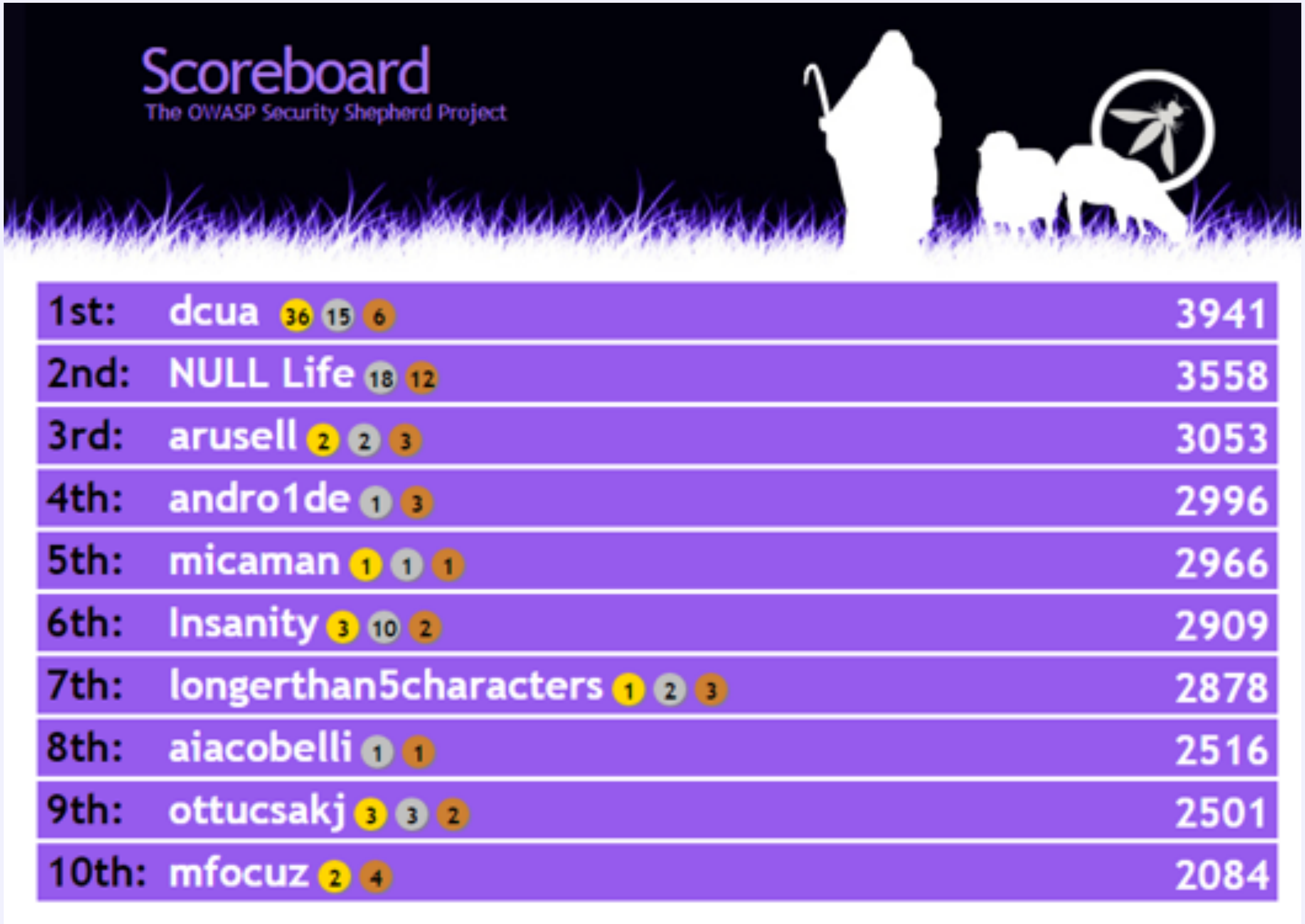
AppSecEU 2014 Video

AppSecEU 2014 Presentation

Security Shepherd CTF

OWASP
The Open Web Application Security Project

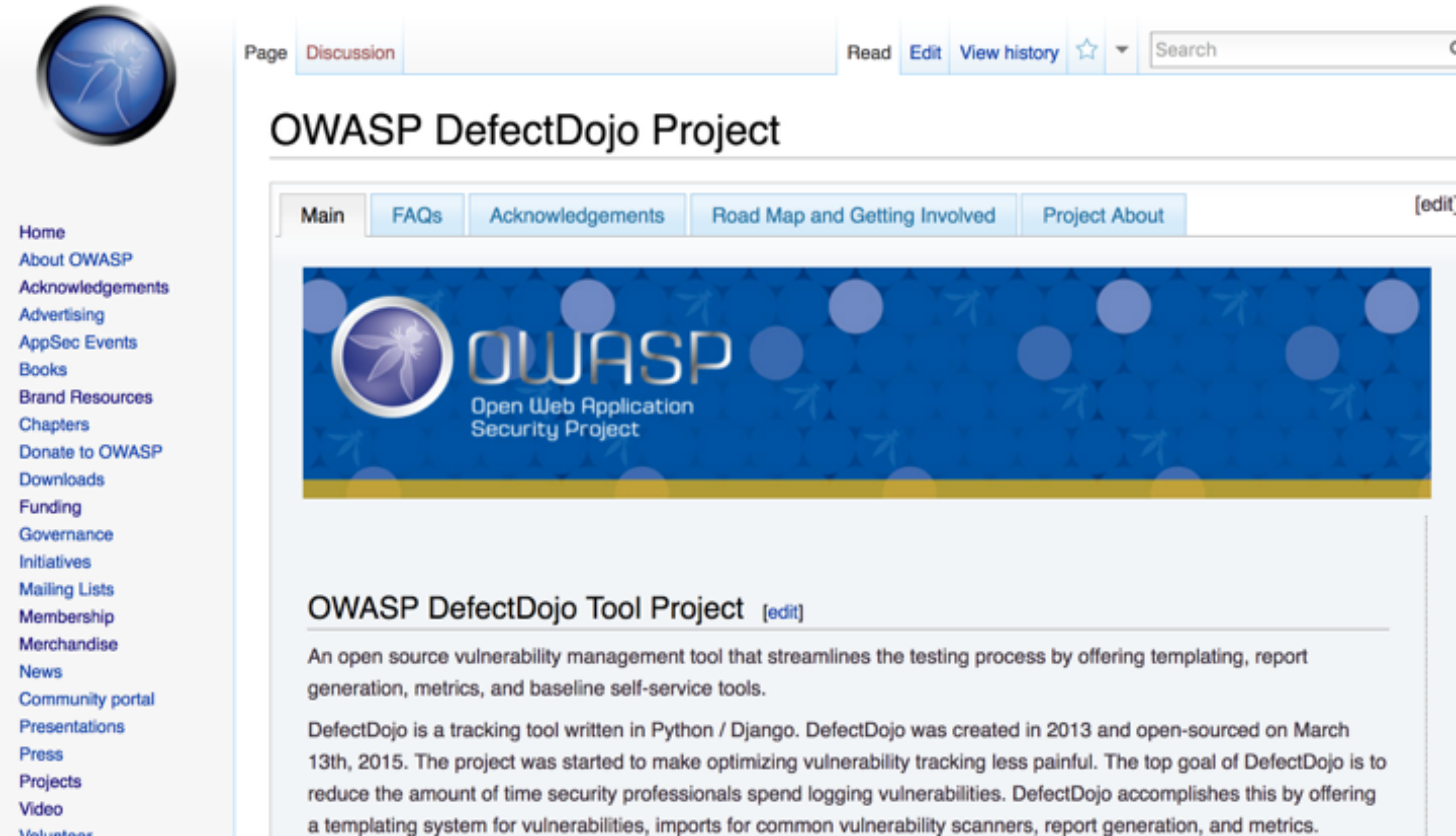
Competitive Learning Environment - learn about vulnerabilities!



Scoreboard
The OWASP Security Shepherd Project

1st:	dcua	36 15 6	3941
2nd:	NULL Life	18 12	3558
3rd:	arusell	2 2 3	3053
4th:	andro1de	1 3	2996
5th:	micaman	1 1 1	2966
6th:	Insanity	3 10 2	2909
7th:	longerthan5characters	1 2 3	2878
8th:	aiacobelli	1 1	2516
9th:	ottucsakj	3 3 2	2501
10th:	mfocuz	2 4	2084

Defect Dojo



OWASP DefectDojo Project

OWASP DefectDojo Tool Project [edit]

An open source vulnerability management tool that streamlines the testing process by offering templating, report generation, metrics, and baseline self-service tools.

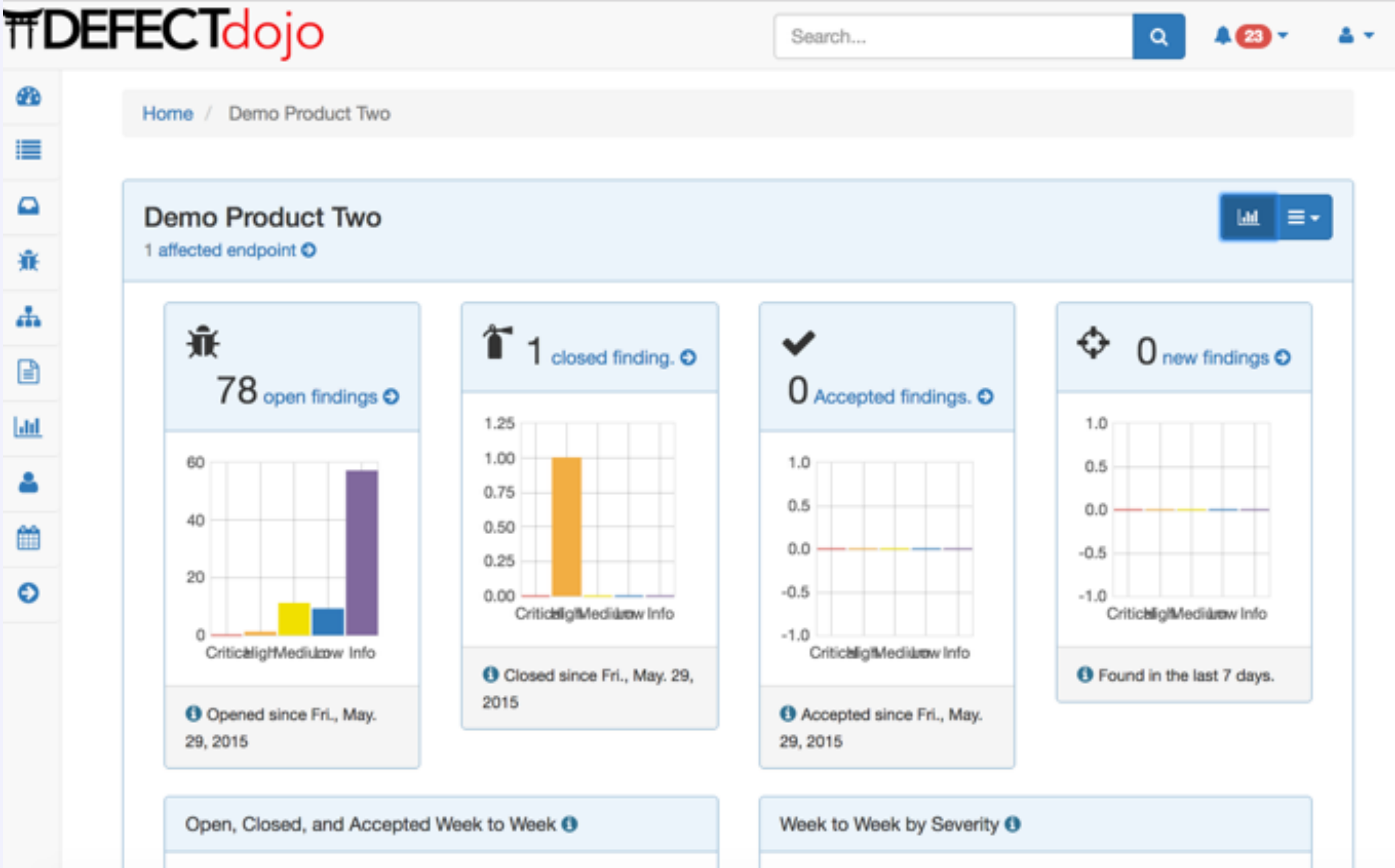
DefectDojo is a tracking tool written in Python / Django. DefectDojo was created in 2013 and open-sourced on March 13th, 2015. The project was started to make optimizing vulnerability tracking less painful. The top goal of DefectDojo is to reduce the amount of time security professionals spend logging vulnerabilities. DefectDojo accomplishes this by offering a templating system for vulnerabilities, imports for common vulnerability scanners, report generation, and metrics.

Defect Dojo

OWASP
The Open Web Application Security Project

- OWASP DefectDojo is a security program and vulnerability management tool.
- DefectDojo allows you to manage your application security program, maintain product and application information, schedule scans, triage vulnerabilities and push findings into defect trackers

Defect Dojo



DEFECTdojo

Home / Demo Product Two

Demo Product Two

1 affected endpoint

78 open findings

Opened since Fri., May. 29, 2015

1 closed finding.

Closed since Fri., May. 29, 2015

0 Accepted findings.

Accepted since Fri., May. 29, 2015

0 new findings

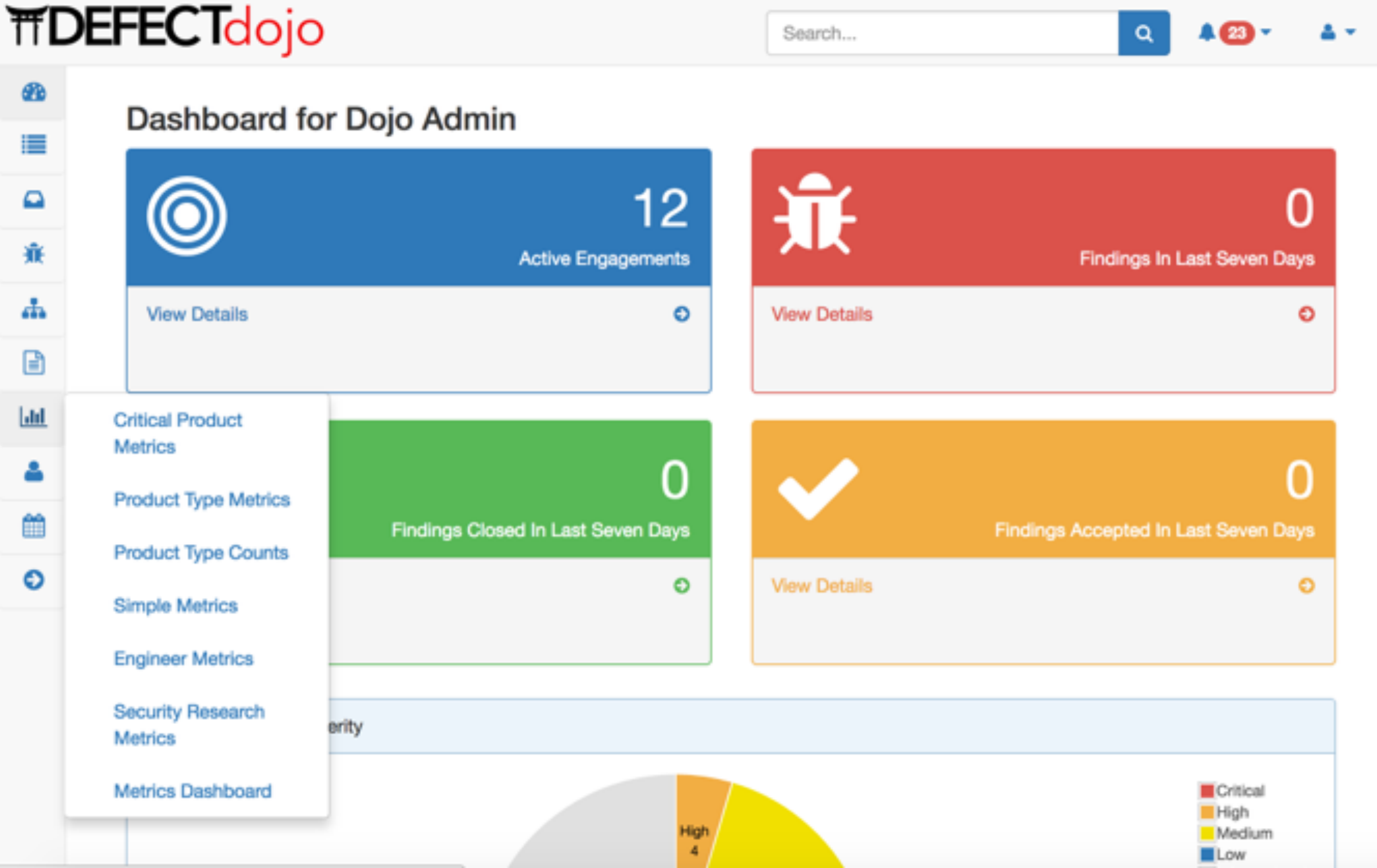
Found in the last 7 days.

Open, Closed, and Accepted Week to Week

Week to Week by Severity

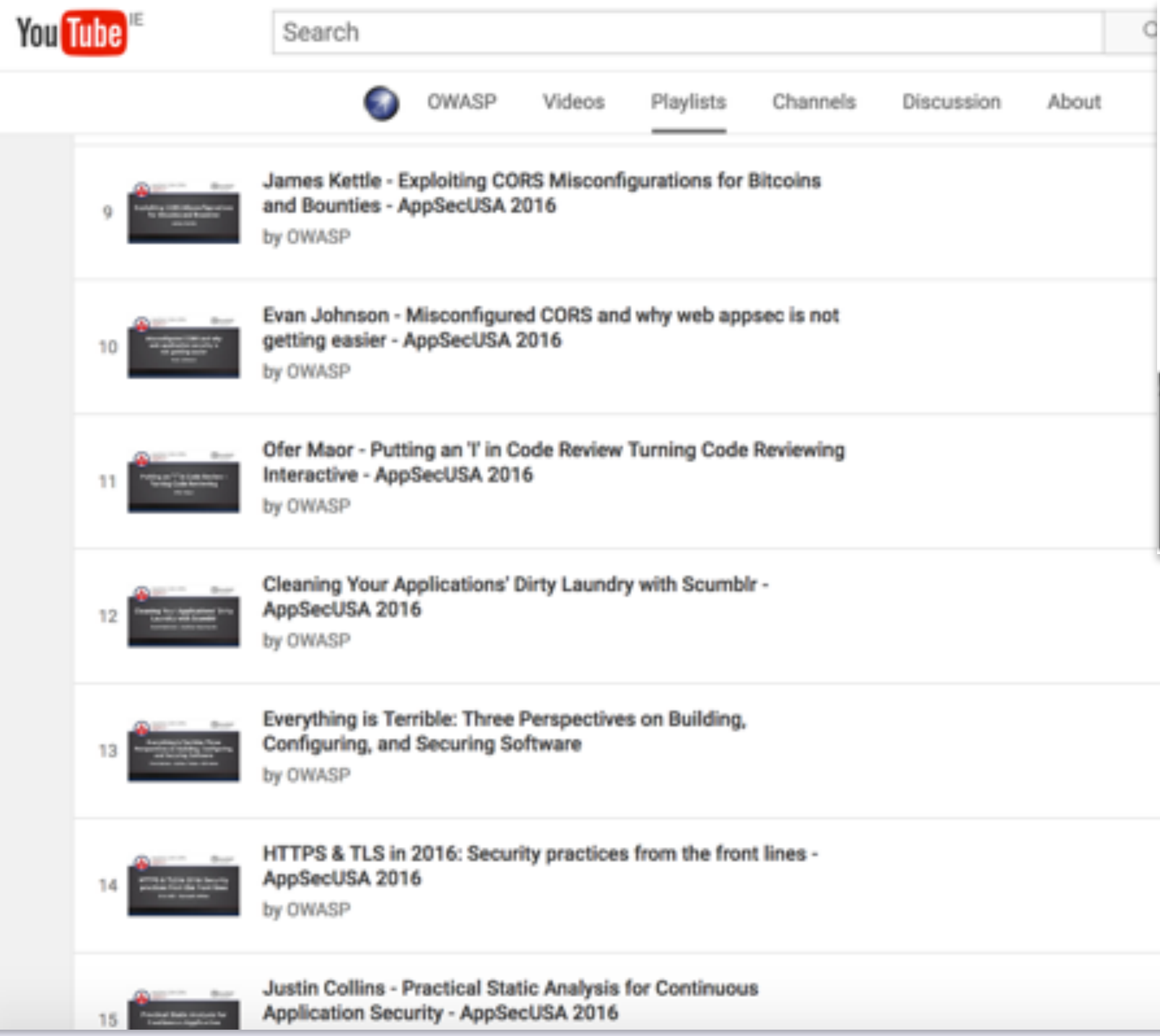
Search...
23
60
40
20
0
Critical High Medium Low Info
1.25
1.00
0.75
0.50
0.25
0.00
Critical High Medium Low Info
1.0
0.5
0.0
-0.5
-1.0
Critical High Medium Low Info
1.0
0.5
0.0
-0.5
-1.0
Critical High Medium Low Info

Defect Dojo


DEFECTdojo
Search...
23
Dashboard for Dojo Admin
12
Active Engagements
View Details
0
Findings In Last Seven Days
View Details
0
Findings Closed In Last Seven Days
0
Findings Accepted In Last Seven Days
View Details
Critical Product Metrics
Product Type Metrics
Product Type Counts
Simple Metrics
Engineer Metrics
Security Research Metrics
Metrics Dashboard
erity
High
4
Critical
High
Medium
Low

AppSec USA 2016 Videos

OWASP
The Open Web Application Security Project



9 James Kettle - Exploiting CORS Misconfigurations for Bitcoins and Bounties - AppSecUSA 2016
by OWASP

10 Evan Johnson - Misconfigured CORS and why web appsec is not getting easier - AppSecUSA 2016
by OWASP

11 Ofer Maor - Putting an 'I' in Code Review Turning Code Reviewing Interactive - AppSecUSA 2016
by OWASP

12 Cleaning Your Applications' Dirty Laundry with Scumblr - AppSecUSA 2016 53:07
by OWASP

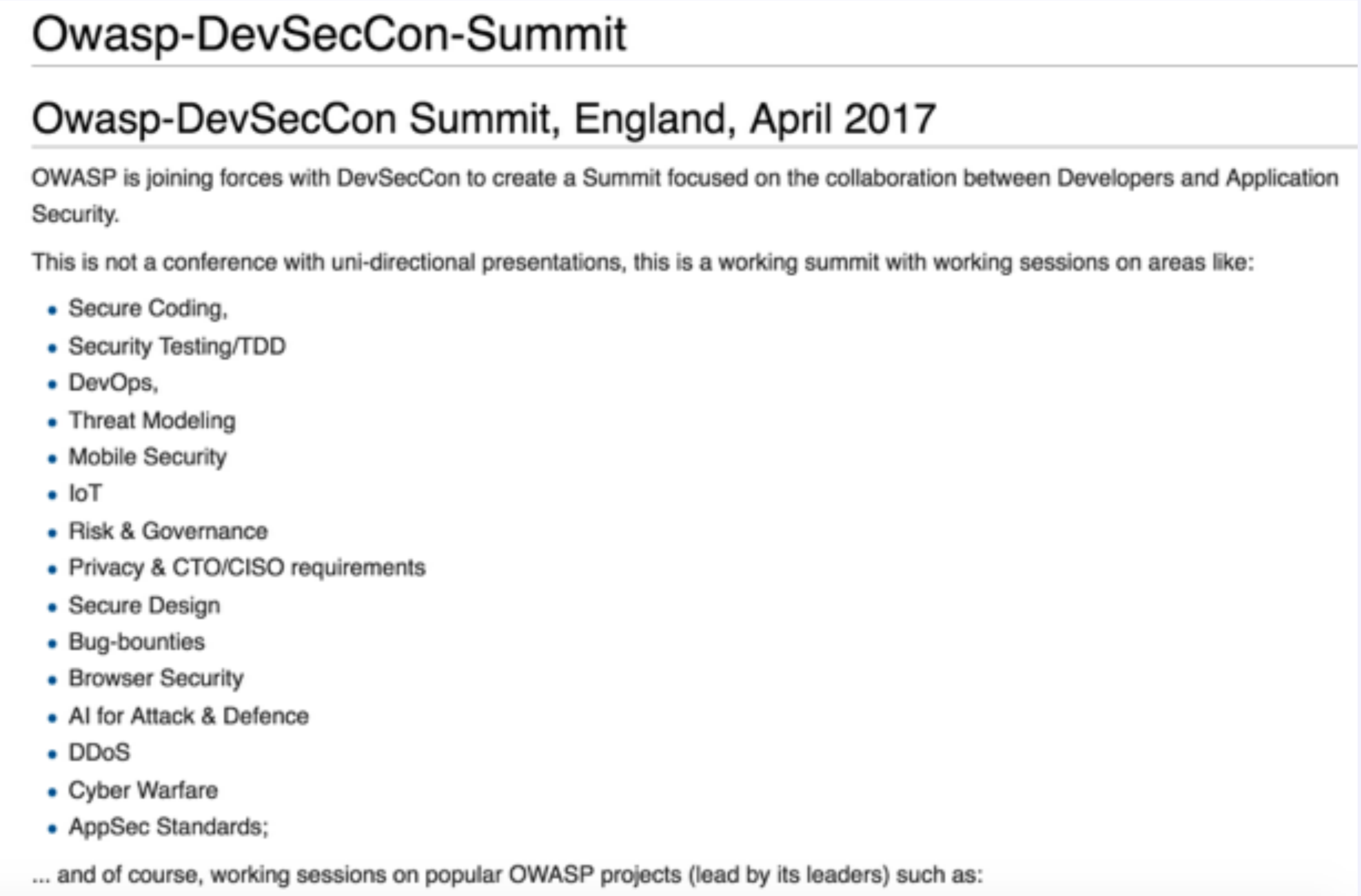
13 Everything is Terrible: Three Perspectives on Building, Configuring, and Securing Software 49:10
by OWASP

14 HTTPS & TLS in 2016: Security practices from the front lines - AppSecUSA 2016 1:01:12
by OWASP

15 Justin Collins - Practical Static Analysis for Continuous Application Security - AppSecUSA 2016 38:44

DevSecCon Summit Planned

OWASP
The Open Web Application Security Project



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:

Talk time

Main Talks:

- David Johansson
- Dinis Cruz

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

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
Save The Dates of Future meetings:

30 March 2017

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:

- David Johansson
- Dinis Cruz
- Francois Raynaud

Hosts for this event

- J.P. Morgan Chase

- Attendees (you!)

Pub Time!

- Networking and Drinks in the local pub