OWASP London
28th April 2016

OWASP
The Open Web Application Security Project
• Networking, food and beer
• Welcome and OWASP Update
  Sam Stepanyan
• Threat Intelligence (remote talk)
  Sherif Mansour
• Drones and their Flaws
  Aatif Khan
• How (NOT) to Code Your Ransomware
  Liviu Itoafa
• OWASP Roundup
  Sam Stepanyan
• Networking in the pub, more beer
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!
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:

GOTHAM DIGITAL SCIENCE  Quotium  netsparker

VERACODE  ThoughtWorks  intelligent environments

Meeting Sponsors

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

skype  Hotels.com
Contributing Members

These corporate members support OWASP at the $6,000 USD level annually.
Premier Members

These corporate members support OWASP at the $20,000 USD level annually.
OWASP Releases Software Assurance Maturity Model (SAMM) Version 1.1 for Improving Software Security

Successor of OpenSAMM as OWASP SAMM v1.1 released to enable organizations to measure and improve their software security

Software Assurance Maturity Model v1.1

Maturity Levels
Each of the twelve Security Practices has three defined Maturity Levels and an implicit starting point at zero. The details for each level differs between the Practices, but they generally represent:

0: Implicit starting point representing the activities in the Practice being unfulfilled
1: Initial understanding and ad hoc provision of Security Practice
2: Increase efficiency and/or effectiveness of the Security Practice
3: Comprehensive mastery of the Security Practice at scale
Version 4

The OWASP Top Ten Proactive Controls 2016 is a list of security concepts that should be included in every software development project. They are ordered by order of importance, with control number 1 being the most important.

1. Verify for Security Early and Often
2. Parameterize Queries
3. Encode Data
4. Validate All Inputs
5. Implement Identity and Authentication Controls
6. Implement Appropriate Access Controls
7. Protect Data
8. Implement Logging and Intrusion Detection
9. Leverage Security Frameworks and Libraries
10. Error and Exception Handling
WebGoat Version 7.0.1
1st February 2016

https://github.com/

WebGoat is a deliberately insecure application that allows interested developers just like you to test vulnerabilities commonly found in Java-based applications that use common and popular open source components.
Remote “lightning” talk
OWASP Internet of Things (IoT) Project

Oxford defines the Internet of Things as: “A proposed development of the Internet in which everyday objects have network connectivity, allowing them to send and receive data.”

The OWASP Internet of Things Project is designed to help manufacturers, developers, and consumers better understand the security issues associated with the Internet of

What is the OWASP Internet of Things Project?

The OWASP Internet of Things Project provides:

- IoT Attack Surface Areas
The OWASP Anti-Ransomware Guide

Open up any newspaper or news site and an increasingly common headline is becoming “hospital held for ransom”. While hospitals and other organizations often have downtime procedures that let them revert back to paper for dealing with power outages and other disasters, it is still a nightmare scenario to find your entire organization’s IT infrastructure screeching to a halt all because someone clicked on a malicious link or opened a questionable email attachment. Moreover, many organizations have a significant number of legacy systems that make security a challenge and beyond very basic security provisions often do not have a corporate culture that is heavily focused on information security. This has left many

Project Leaders
- Christopher M Frenz
- Christian Diaz

Download
- Version 1.0
OWASP AppSec Europe '16

27/06/2016 - 01/07/2016

Welcome to Rome

27 June – 1 July 2016
Rome
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:

- Gotham
- Quotium
- Netsparker
- Veracode
- Thoughtworks
- Intelligent Environments

Meeting Sponsors

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

- Skype
- Hotels.com
Thank You

Speakers
• Aatif Khan
• Liviu Itoafa

Your Chapter Leaders
• Sam Stepnyan
• Sherif Mansour

Hosts for this event
• Skype (Microsoft)
• Christian Martorella

Attendees
### Corporate Sponsors

**Premier Members**
These corporate members support OWASP at the $20,000 USD level annually.

- Adobe
- HP
- Qualys

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

- Accuvant
- Acunetix
- ADP
- Akamai
- Amazon
- ARXAN

- Aspect Security
- ASTECH
- Best Buy
- Black Hat
- BOSS Lab
- Denim

- Checkmarx
- CloudPassage
- Cloudscape
- COVERT
- Gemalto
- Gotham

- Digital Defense
- Dropbox
- FICO
- Fortinet
- GoTenna
- Group

- Imperva
- Information Builders
- Intel
- Moki
- Mstar

- Netsparker
- netsuite
- Nokia
- One Consult
- OpaQ
- Protiviti

- PwC
- RackSpace
- Rakuten
- Ranorex
- Riverbed
- rubber

- SecurYourSite
- SmartRAC
- Sonatype
- Solutions II
- SWAMP

- Trend Micro
- Trustwave
- Trivago
- TSF
- UDI

**Academic Supporters**

- Wadsworth Institute of Technology
- Illinois Institute of Technology
- University of Arizona
"OWASP 24/7" is a series of recorded broadcasts, highlighting OWASP projects and people from around the world. They are available on demand, at any time, anywhere on the planet. You are welcome to embed the broadcasts on your page, listening or keep up to date by subscribing to the iTunes channel.

As of March 21, 2016, we had over 133,500+ plays of the broadcast.
As of February 25, 2016, we had over 127,000+ plays of the broadcast.
As of January 22, 2016, we had over 120,000+ plays of the broadcast.
As of November 24, 2015, we had over 114,100+ plays of the broadcast.
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
http://twitter.com/owasplondon

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

Visit OWASP London Chapter webpage
https://www.owasp.org/index.php/London
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 (at) owasp.org
Drinks and Networking
“The Inn Of Court Pub”

18 Holborn
(across the road)