OWASP
Open Web Application
Security Project

OWASP Summit 2017

Why, how, what, where

(v0.9, Jan 2017)

Close your eyes

Imagine a place where (some of) the best Application Security and OWASP minds come together to collaborate and work

… a meeting of minds focused on solving hard problems that we all have everyday

… a place where security experts, developers, users, government agencies and vendors work together on shared goals

… a place where you will find like minded individuals that care deeply about what you are passionate about

… an environment designed for maximum geek-time, synergies and collaboration

… basically it's AppSec from 8am till 2 am (next day)

This place is something that only OWASP can create

… because OWASP is at the epicentre of Application Security*

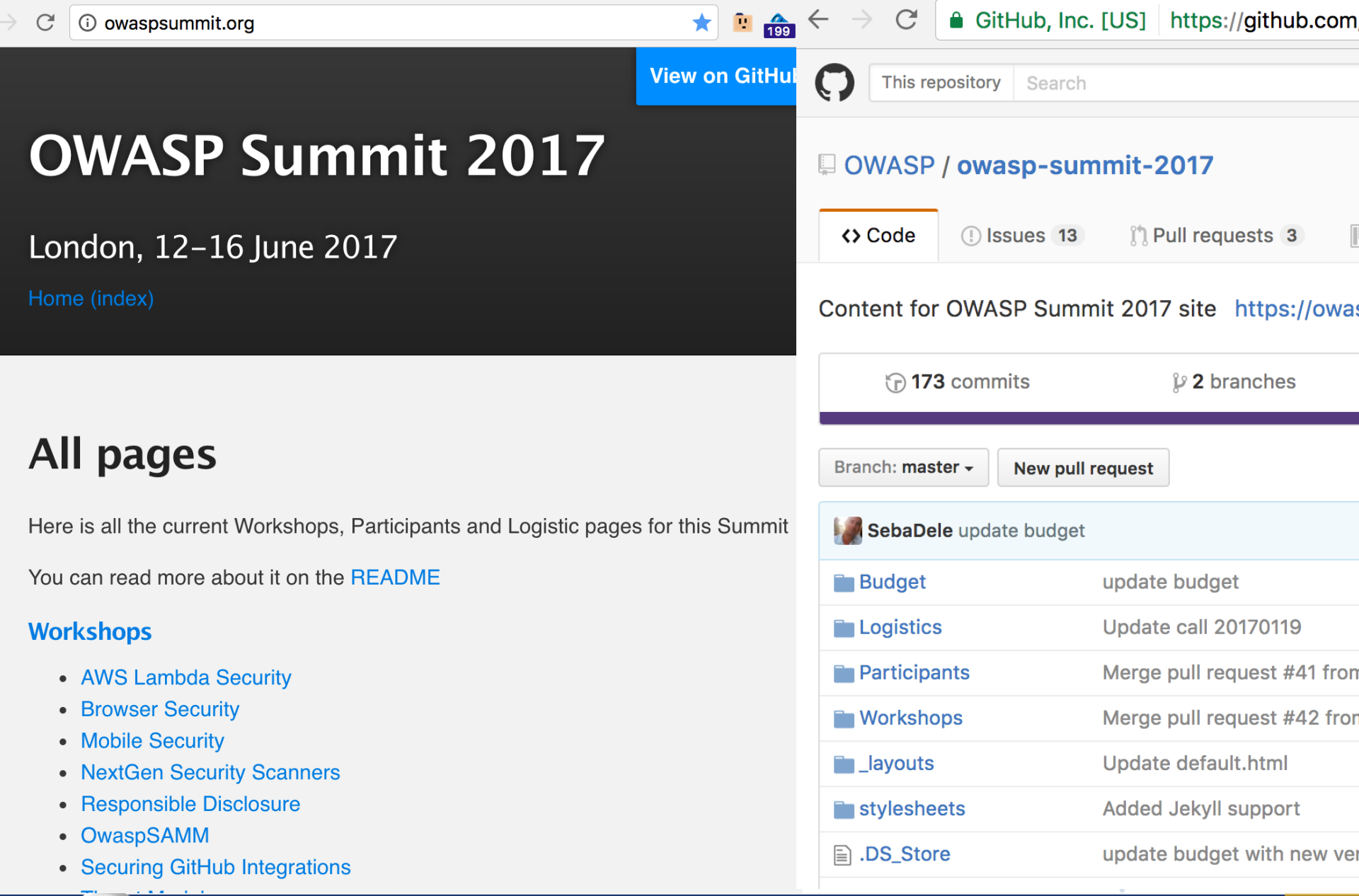
** OWASP is the collective wisdom of the best minds in software security worldwide. https://www.owasp.org/*

This place is the :

OWASP Summit 2017

London, 12-16 June

http://owaspsummit.org


owaspsummit.org
199
GitHub, Inc. [US]
https://github.com
View on GitHub
OWASP Summit 2017
London, 12–16 June 2017
Home (index)
This repository
Search
OWASP / owasp-summit-2017
Code
Issues 13
Pull requests 3
Content for OWASP Summit 2017 site
173 commits
2 branches
Branch: master
New pull request
SebaDele update budget
Budget update budget
Logistics Update call 20170119
Participants Merge pull request #41 from
Workshops Merge pull request #42 from
_layouts Update default.html
stylesheets Added Jekyll support
.DS_Store update budget with new ver
All pages
Here is all the current Workshops, Participants and Logistic pages for this Summit
You can read more about it on the README
Workshops
AWS Lambda Security
Browser Security
Mobile Security
NextGen Security Scanners
Responsible Disclosure
OwaspSAMM
Securing GitHub Integrations

WHAT, WHERE AND WHO

Current Workshops ideas

Workshops

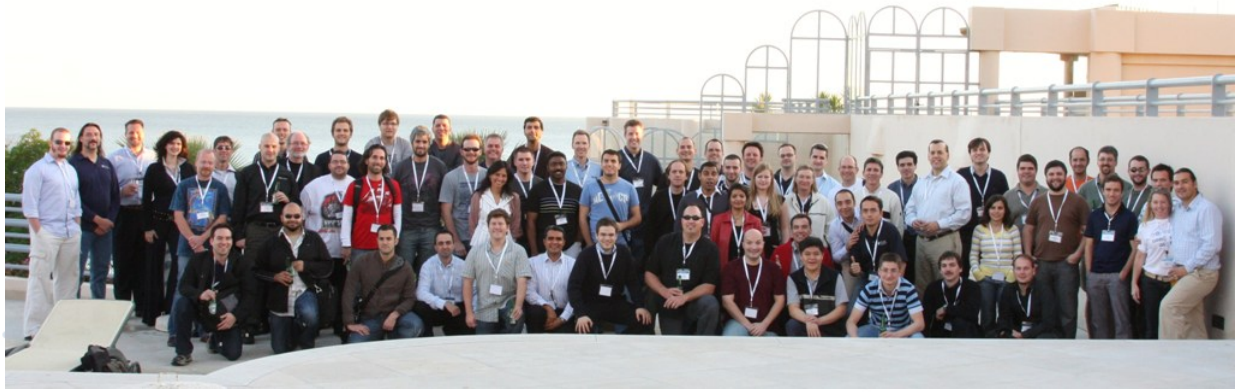
First pass at mapping Summit Workshops:

- AWS Lambda Security
- Browser Security
- Mobile Security
- NextGen Security Scanners
- Responsible Disclosure
- OwaspSAMM
- Securing GitHub Integrations
- Threat Model
- Webgoat
- ZAP

Using the same model as the previous 2 Summits

OWASP SUMMIT 2011
LISBON
PORTUGAL
FEB 8-11

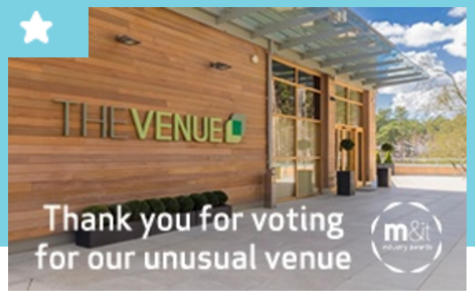
8 OWASP EU Summit Portugal



Hosted at Woburn Forest Centerparcs

Woburn Forest, Bedfordshire

Our new contemporary conference venue is now open for business. Woburn Forest boasts a prime location for networks, being in close proximity to the M1 and just 50 minutes away from London by rail.



We've been shortlisted

Find out more

Find out more about Jeep's 75th Anniversary event at Woburn Forest

Click here

Great conference facilities

Center Parcs offers distinctive expertise in conferences and events, presenting solutions for everything from intimate board meetings to large conferences and team building activity days. The combination of tranquil forest settings coupled with our dedicated onsite events teams at each location, provides an ideal environment, which will stimulate, motivate and inspire delegates.

Our purpose built conference and meeting facilities offer event space for up to 600 delegates and allow for privacy and freedom to create the perfect delegate experience. Whether looking for a flexible meeting space, an inspirational venue or a venue which provides the perfect balance of business and pleasure, Center Parcs can provide options that are seemingly endless.

The extensive selection of leisure activities, including the award winning Aqua Sana spa ensures that delegates will feel relaxed and invigorated. We also have a diverse selection of team building activities, designed to motivate and challenge a team's ability to work together.

A wide variety of onsite dining choices from high-street restaurants, private barbecue's to cooking challenges coupled with an abundance of accommodation preferences, that include executive lodges equipped with saunas and games rooms, offer an entertaining end to a day's conference or a chance to recoup

Even better collaboration environment

The villas/lodges are key to it an 'Summit'

- This is where synergy and serendipity is created
- AppSec threads start at breakfast
  - …continue during workshops
  - … and keep going though dinner
  - …. late night sessions (at villas)

Current Participants

owaspsummit.org/participants.html

Participants

List of Summit attendees

- Alexander Antukh
- Bjoern Kimminich
- Colin Domoney
- David Rook
- Dinis Cruz
- Francois Raynaud
- Geoff Hill
- Lucas Ferreira
- Mike Milner
- Nanne-Baars
- Ofer Maor
- Sam Stepanyan
- Sebastien Deleersnyder
- Stefan Streichsbier
- Steven van der Baan
- Sven Schleier
- Viktorija Almazova

WORKSHOPS IDEAS

Mobile Security Workshop

Mobile Security

Questions to answer:

- How can requirements from MASVS be integrated into Agile environments?
- What are pain points at the moment in Mobile Security development, when considering/implementing s
- What are pain points at the testing mobile Apps?
- How can testing be automa
  - BDD
  - MobSF
- How can mobile developers
- How can (Penetration/QA) t implemented mobile Apps?

Mobile Application (MASVS)

- Working on MASVS - https:
- Review MASVS in order to

Mobile Security Testing Guide (MSTG)

- Working on MSTG - https://github.com/OWASP/owasp-mstg
- Review MSTG in order to agree on a beta version and get acceptance from the community

Hacking-Playground

- Working on Mobile Hacking Playground, https://github.com/OWASP/OMTG-Hacking-Playground
- Working on curriculum/study material for mobile education purpose in trainings and workshops.
  - Offensive: For penetration testers / security researchers to identify bad practices, dangerous methods and classes they should look at when assessing a Mobile App. Goal is to gain more knowledge through the information provided in the MSTG.
  - Defensive: For developers to identify vulnerable code in the provided App's so they can see the implications and risks if such patterns are used and can look for the best practices in the MSTG to mitigate the vulnerabilities.

NextGen Security Scanners (Workshops)

NextGen Security Scanners

Problem statement

Today's security scanners were built for yesterday's web applications, based on server-side rendering concepts. They often fail or at least lack functionality when it comes to modern web applications using rich Javascript clients.

Questions

- What makes scanning Javascript-heavy applications so different?
- What funcionality is missing in today's scanner tools?
- How to improve the automation parts of existing tools?
- How to further assist users during proxied manual pentests?
- How can vulnerable applications like OWASP Juice Shop be used by scanner vendors as a sample victim?

Participant candidates

- OWASP ZAP, Arachni and otl
- Burp, Acunetix and other com
- Javascript frontend developer
- Web application developers

Potential outcomes

- OWASP ZAP extensions for Javascript client-side code analysis
- Improvements of OWASP ZAP Ajax Spider
- Additional vulnerabilities for OWASP Juice Shop that showcase vulnerabilities found in the wild

Securing GitHub Integrations (Workshop)

Securing GitHub Integrations

As more and more services are integrated with GitHub, companies public and private repos are being exposed to a much wider set of attackers and threats.

At the moment the GitHub Security model does not allow the granularity required to control this access (for example read-access to only one repo), which means that the only choices tend to be either:

a) provide no access and not use the 3rd party service (which ironically might be providing a security service)

b) give that 3rd party service full access to public and private repos (i.e full control to modify the code)

To Invite:

- GitHub Security Team and developers
- 3rd party service providers: Travis, SNYK, Codiscope, Node Security, ….
- GitHub corporate users which large (hundreds) numbers of GitHub repos

Threat Model (Workshops)

Threat Modeling Workshop ideas

- pain of manual processes and how to optimise them
- linking threat models and sub-threat models together
- creating threat model templates for security patterns
- better threat model diffing
- integration into DevOps
- use of output by downstream systems… development, test, deployment, etc
- making the infrastructure and system (as opposed to just software) threat modeling more mature
- integration of common taxonomies that are useful across multiple sSDL tiers (not just threat modeling)
- are threat trees actually useful in live business environments
- unified input and output in a sSDL
- simplifying threat modeling for business environments
- Scaling threat models throughout an organization (central storage, versioning control, etc)
- Automating threat models
- Splitting up threat models integration into domain-agnostic and domain-specific
- Enabling Security champions to perform domain agnostic threat models

WebGoat

WebGoat

Introduction

WebGoat is a deliberately insecure web application maintained by OWASP designed to teach web application security lessons. You can install and practice with WebGoat. There are other 'goats' such as WebGoat for .Net. In each lesson, users must demonstrate their understanding of a security issue by exploiting a real vulnerability in the WebGoat application. For example, in one of the lessons the user must use SQL injection to steal fake credit card numbers. The application aims to provide a realistic teaching environment, providing users with hints and code to further explain the lesson.

The main focus of WebGoat 8.0 is on the training aspect which will teach developers not only on how to exploit a vulnerability but also how t

Questions / Ideas

1. Add the ability to fix a vulnerability within a lesso
   want to add the ability for users to try to fix the is
   challenging to implement this without restarting t
2. For 1 we need to 'automatically' verify an implem
   which will try to trigger the issue at hand. It woul
   knowledge base in which you can submit your s
   proposed solutions.
3. Can we share come up with a shared knowlegde base for different Goat implementations? Only the language implementation details are different the explanation about a specific vulnerability and mitigation can be shared.
4. Develop more lesson content, for example lessons specifically about crypto.

To invite

- Webapplication developers
- Teachers in the area of webapplication security

Organizer

For more details, more ideas etc you can contact https://github.com/OWASP/owasp-summit-2017/blob/master/Participants/Nanne-Baars.md

TICKETS AND SPONSORSHIPS

2 types of ticket

- There are two types of tickets for this Summit both covering participation in the summit for the full 5 days.
  - 5 days x 24h participant
    (venue, lunch, dinner, accommodation):
    £1,200 GBP (about $1,500 USD)
  - 5 days x 8h participant
    (venue, lunch) -
    £400 GBP (about $500 USD)

- Individual daily tickets will be available at a later date

Sponsorship

Platinum sponsor:

villa – 10.000$
- 4 full ticket including accomodation
- name associated with villa
- sponsor of project
- swag/promotional material in people accomodations
- logo on website
- logo on summit guide
- social media announcement

gold sponsor: 7000$

project specific:
- 4 full ticket including accomodation
- ability to sponsor the project
- name right in project work
- logo on website
- logo on summit guide
- social media announcement

silver sponsor: 3500$
- 2 full ticket including accomodation
- swag/promotional material in people accomodations
- logo on website
- logo on summit guide
- social media announcement

other sponsoring opportunities:

drinks (display of company logo somehow) – 500$
- daily
- end of summit party

entertainment (display of company logo somehow) – 1000$
- clay piegon shooting
- tennis
- bowling
- ...

Meals (display of company logo somehow) – 500$
- breakfast
- lunch
- dinner

WE NEED YOUR HELP NOW

At the moment we have

- Secured the use of 10 lodges
  - have meeting rooms for about 20 participants on each lodges/villa
  - This means that we already have a Summit for 200 people :)
- Have a hold on the main conference venue
  - will scale from 200 to 500 people
  - better meeting place for larger sessions
  - we need to confirm it by the 5th of Feb (there are two other interested parties for the venue)

If you are planning to attend

- PLEASE book your ticket or sponsorship package ASAP
  - Payment can be dealt with OWASP central
- If your chapter or project have funds, PLEASE allocated them ASAP
- We need to get at least £25k (Ideally £40k) by the 5th of February so that we get a lock on the venue

We need Workshop leaders and ideas

- If you don't see something that you are passionate about in the current list of Workshops, please add your idea to it
- If you want to lead that workshop, please take a leadership role
- The Summit is about the workshops and the participants, all that we are doing is setting the stage and creating the environment for maximum AppSec collaboration and work :)

We need Developers, Security Champions, CISOs, etc…

- Key objective of the summit is to focus on the collaboration between: OWASP Projects, Developers, Application Security, DevOps and C-Level execs.
- The Summit is the perfect place to bring together security focused developers and members of AppSec teams
- We want to work on real-world problems faced by companies and organisations that are trying to write secure code and protect their applications/networks
- Please reach out to these communities and invite them to participate in the Summit

… in conclusion

…the place to be for AppSec in 2017 is going to be the

OWASP Summit 2017

… the question is

Are you going?

QUESTIONS?