OWASP
Open Web Application
Security Project

OWASP Dorset

Welcome to our first Chapter Meeting

Housekeeping

- Fire Exits and Building Evacuation
- Help yourself to drinks (pizza halfway)
- Toilets
- Talks - 1900-2100

About Me

- Many years in Security - travelling around the globe - packets, laptop screens, forced and nasty air-con, interviews and reports.
- Loves an ethernet cable and carries one:
  - still uses wireless
- Enjoys infrastructure and architecture:
  - including efficient and appropriate security
- Used and Abused OWASP Projects (including to win £1500 'Hacking' competition)
- Multiple quals/certs – they're fun and a good test for retention (practice it or lose it though)

- Now paying it back through OWASP and who knows what next
- Why go to London for an event when we live in the *best place (no mountains)

Hacking = exploited vendor led marketing opportunity to bag 1st place – Thanks ZAP and lots of automation.

Agenda

- 1830 - Drinks and Networking
- 1900 - Intro to OWASP Dorset
- 1910 - 3 Sided Cube Overview and Shared Sec Model
- 1925 - OWASP Projects at their finest
- 1945 - Pizza
- 2000 - I know what you did last summer (mobile security)
- 2030 - Q&A – Discussion
- 2055 – Next meeting date – suggestions for location/sponsors
- 2100 - Close meeting

OWASP?

- What is OWASP
  - Global Not for Profit
  - Volunteer and Community Led (nobody asked me to do this)
  - Commercial Sponsors and Conferences generate most income
  - Everyone is equal – some more experienced than others
  - Projects are vital (some paid opportunities to collaborate)
  - Chapters are run by and for volunteers

OWASP Dorset?

- A meeting of curious minds interested in Application(Cyber) Security
- Share, listen and learn
- 5 times a year (inc 1 CTF)
- Enjoy making a difference
- Inspire confidence through collaboration
- Test yourself (CTF)

Questions

Over to 3 Sided Cube

BLANK

OWASP
Open Web Application
Security Project

OWASP Projects “at their finest”

A high level guide to some great resources proven to help you learn

OWASP

Open Web Application Security Project

- People fluctuate
- Funding appears and disappears
- Scales up and down
- Always collaborating to work towards a common goal (even though the goalposts move daily)
- Really a programme – multiple projects and working groups to support it

Some of the best are

OWASP Top Ten – who doesn't love a Top Ten (including vendors)

- In reality very hard to mitigate all 10
- Despite what you might get told by a Sales Rep
- E.g. Can a WAF block 10. Insufficient Logging and Monitoring… someone needs to check

OWASP ZED Attack Proxy – baseline vulnerability scanning for the masses (very configurable)

OWASP
Open Web Application Security Project

Welcome | Project Inventory | Former Project Task Force | Online Resources | Starting a New Project | Participating in a Project | Project Assessments | Brand Resources | Terminology | Sponsorships and Donations | Contact US | Current Project Review Guidelines

Welcome to the OWASP Global Projects Page

(The Projects pages are constantly being updated. Some pages may contain outdated information. You can help OWASP to keep these pages current by visiting FixME) Please contact the Projects team with questions using the Contact Us form

An OWASP project is a collection of related tasks that have a defined roadmap and team members. OWASP project leaders are responsible for defining the vision, roadmap, and tasks for the project. The project leader also promotes the project and builds the team. OWASP currently has '***over*** '93' ***active projects***', and new project applications are submitted every week.

This is one of the most popular divisions of OWASP as it gives members an opportunity to freely test theories and ideas with the professional advice and support of the OWASP community. Every project has an associated mail list. You can view all the lists, examine their archives, and subscribe to any project by visiting the OWASP Project Mailing Lists page. A summary of recent project announcements is available on the OWASP Updates page.

Download the **OWASP Project Handbook 2014**

Category:OWASP Top Ten Project

FLAGSHIP mature projects

OWASP Top 10 2017 Released

The OWASP Top 10 - 2017 is now available.

OWASP Top 10 Most Critical Web Application Security Risks

The OWASP Top 10 is a powerful awareness document for web application security. It represents a broad consensus about the most critical security risks to web applications. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

We urge all companies to adopt this awareness document within their organization and start the process of ensuring that their web applications minimize these risks. Adopting the OWASP Top 10 is perhaps the most effective first step towards changing the software development culture within your organization into one that produces secure code.

Translation Efforts

The OWASP Top 10 has been translated to many different languages by numerous volunteers. These translations are available as follows:

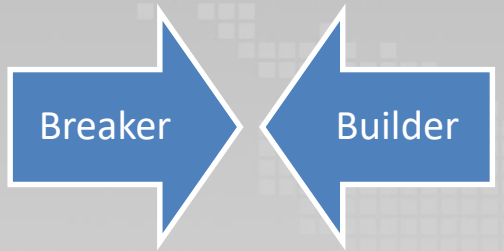
Quick Download

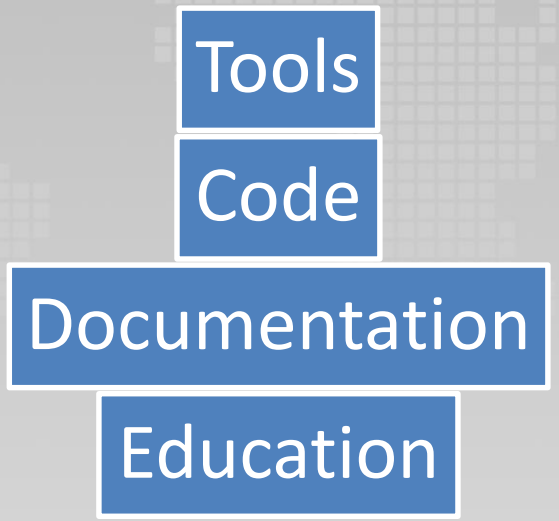
- OWASP Top 10 - 2017 - PDF
- OWASP Top 10 - 2017 - wiki
- Historic:
  - OWASP Top 10 2013 - PDF
  - OWASP Top 10 2013 - wiki
  - OWASP Top 10 2013 Presentation (PPTX).

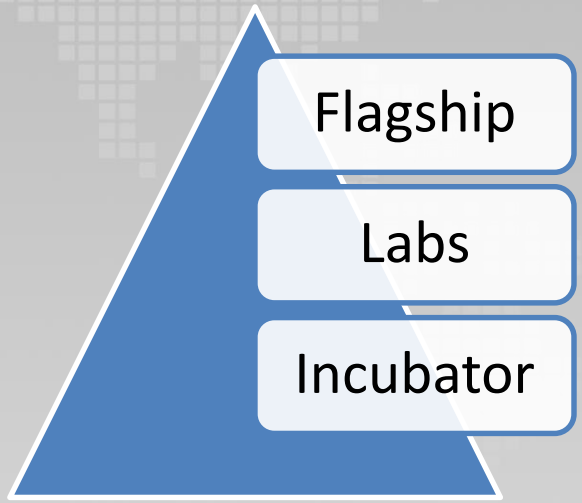
Donate to OWASP

Donate

Project Concepts to understand







Flagship Overview

- Strategic in nature
- Deliver known value
- Generally well funded
- A thousand pairs of eyes are better than ten (as a concept)

Flagship Examples

1. OWSAP Top Ten (closely linked to ModSecurity Rule Set)
2. OWASP Zed Attack Proxy
3. OWASP SAMM – Software Assurance Maturity Model

Labs Overview and Examples

Delivered some value, may not be well sponsored or resourced (you can join)

1. OWASP WebGoat
2. OWASP ES API (Enterprise Security API) – don't write your own controls use verified ones
3. OWASP Cheat Sheets – what it says on the tin (sheet)

Incubators Overview and Examples

Very small or early stages, looking to secure resource/sponsorship to demonstrate value

1. OWASP Mutillidae 2 – deliberately vulnerable LAMP stack (install and learn)
2. OWASP Anti Ransomware Guide – who wants ransomware (apart from Sec Researchers)
3. OWASP Vulnerable Web Apps Directory – a valuable collation of learning Tools and Platforms to hone your skills and expand your knowledge

Chapter Challenge

How will you use an OWASP Project to enhance security?

- Come back and tell us one evening

Pay it forward – tells others about OWASP

Join OWASP

- Member
- Chapter
- Sponsor
- Project

Search the OWASP wiki for more info

Go to Conference

- AppSec USA
  - 2018 San Jose, California
  - 2019 California (TBC)
- AppSec EU
  - 2018 London
  - 2019 Tel Aviv

Lead from the front

- We’re all volunteers
- People make the difference

Become a:

- Chapter Leader (any help is welcome)
- Project Leader (find your passion and prove it)
- Contributor (delivering value)

Questions

Pizza

Next Talk at 2010