OWASP
Open Web Application
Security Project

Welcome to OWASP Bristol Chapter

22nd June 2017

@OWASPBristol

Sponsor

Thanks very much to our sponsor

For hosting this event

About OWASP

Open **W**eb **A**pplication **S**ecurity **P**roject
(https://www.owasp.org)

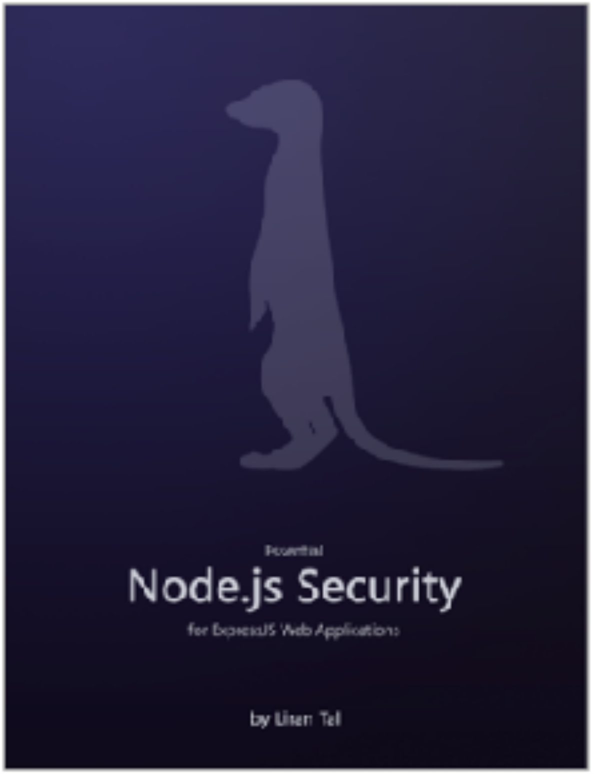
- Not-for-profit, open source, worldwide organization which promotes the improvement of web applications security.
- Everyone is free to participate
- All OWASP tools & materials are under open software license

OWASP
Open Web Application
Security Project

Free eBook

Node.js Security for ExpressJS Web application

Hands-on and a practical guide to Securing Node.js web applications.



Essential

Node.js Security

for ExpressJS Web Applications

by Liran Tal

https://bit.ly/freenodejsbook

OWASP

Open Web Application Security Project

Free eBook – Go

Go Secure Coding Practices

- helps developers avoid common mistakes
- Hands-on detail
- "how to do it securely”
- Donated by Checkmarx

The Go Language Guide

Web Application Secure Coding Practices

CHECKMARX

https://bit.ly/go-scp

OWASP
Open Web Application Security Project

SAMM – v1.5 release

Software Assurance Maturity Model

- an open framework to help organizations formulate and implement a strategy for software security that is tailored to the specific risks facing the organization.

http://www.opensamm.org/

OWASP
Open Web Application Security Project

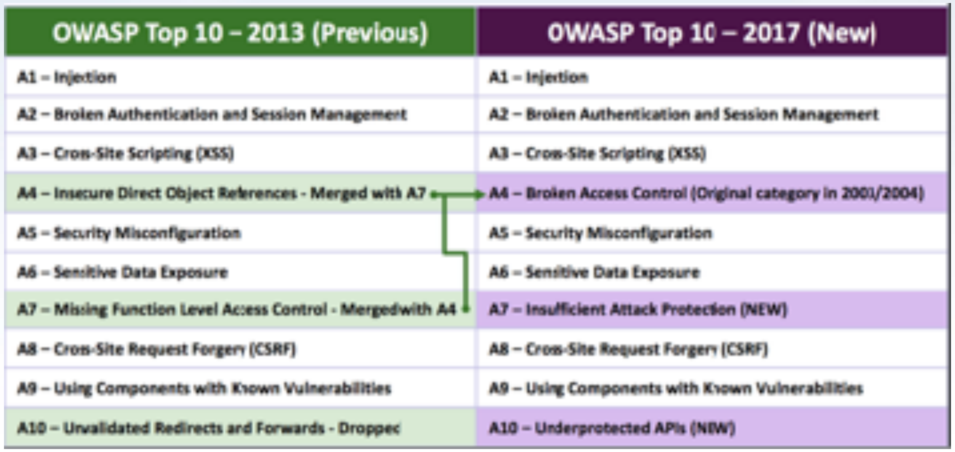
OWASP Summit London’17

OWASP
Open Web Application Security Project

OWASP Top 10 – 2017 RC1

New project leader - Andrew van der Stock

- New release process
- New data call – by Aug’17
- New release date – Nov’17



OWASP Top 10 – 2013 (Previous)	OWASP Top 10 – 2017 (New)
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References - Merged with A7	A4 – Broken Access Control (Original category in 2003/2004)
A5 – Security Misconfiguration	A5 – Security Misconfiguration
A6 – Sensitive Data Exposure	A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control - Mergedwith A4	A7 – Insufficient Attack Protection (NEW)
A8 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards - Dropped	A10 – Underprotected APIs (NEW)

https://github.com/OWASP/Top10/

OWASP
Open Web Application
Security Project

OWASP Juice Shop - v4.0 released

- Insecure webapp for security trainings
- Written entirely in JavaScript : Node.js, Express and AngularJS
- encompasses the OWASP Top Ten.

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

OWASP
Open Web Application Security Project

Pwning OWASP Juice Shop

- Official companion guide to the OWASP Juice Shop.
- 42+ intended security vulnerabilities

Björn Kimminich

Pwning OWASP Juice Shop

The official Companion Guide

Published with GitBook

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

OWASP
Open Web Application Security Project

OWASP Mobile Security Testing Guide

- a comprehensive manual for mobile app security testing
- reverse engineering.

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

2017 Global Board of Directors Election

4 open positions for the board.

https://www.owasp.org/index.php/2017_Global_Board_of_Directors_Election

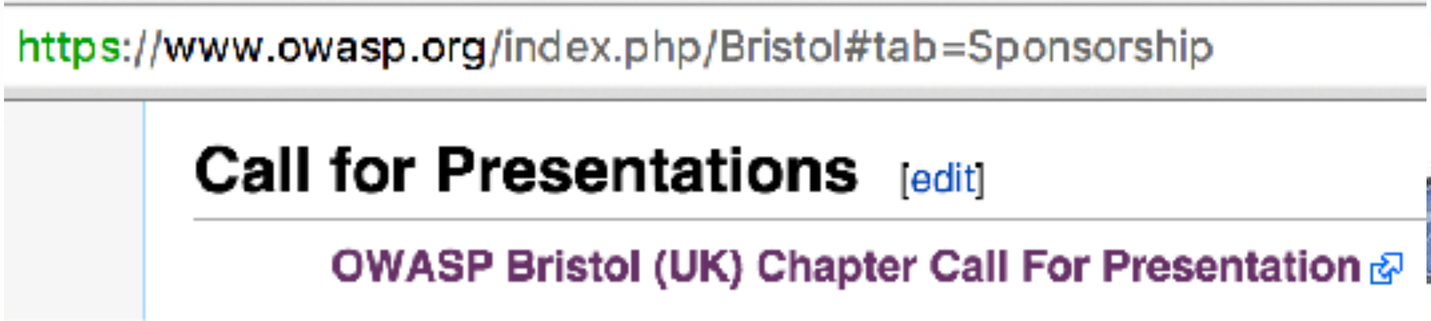
$50 / 40Euros - 12 Month Membership

Call for Speakers for future events

Topics:

- secure coding (JavaScript, PHP, .Net, Java, etc.)
- secure testing
- social engineering
- devops
- OWASP tools or projects
- any other topic related to security

Get in contact via - OWASP Bristol page, or contact katy.



https://www.owasp.org/index.php/Bristol#tab=Sponsorship

Call for Presentations [edit]

OWASP Bristol (UK) Chapter Call For Presentation

Keep in touch

Follow us on Twitter: @OWASPBristol

Find out about meetings:

http://www.meetup.com/OWASP-Bristol/

Find out more about OWASP Bristol:

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

Open Web Application Security Project

Thank you

@OWASPBristol