Getting to know OWASP:
improving the security of software

By Yasser Aboukir
OWASP Luxembourg Chapter Leader

OWASP Luxembourg Chapter | June 17, 2021

What is OWASP?

- Open Web Application Security Project (OWASP) is a Global **nonprofit** foundation **improving the security of software**.

- The OWASP Foundation is the source for developers and technologists to secure the web:

  - **Over 200** local **chapters** worldwide
  - **~70 000 members**
  - Leading educational and training conferences

The OWASP Community and our mission

- OWASP is a worldwide **free** and **open community** focused on improving the security of application software.

- Our mission is to make application security **visible** so that people and organizations can make **informed decisions** about application security **risks**.

Session at Global AppSec Amsterdam

It’s all for free

- Everyone is **free** to participate in OWASP and **all** of our materials are available under a **free** and **open** software license.

- All OWASP events *(except conferences)* are free to attend by both members and non-members of OWASP - and can be attended by anyone who is interested in Application Security and Cyber Security in general.

Member Lounge at OWASP Conference

The OWASP Foundation

- We are a **Global not-for-profit charitable** organization
- Vendor-Neutral Community
- **Collective Wisdom** of the **Best Minds in Application Security Worldwide**
- Provide **free** tools, guidance, documentation
- Meetings are **free to attend** *(usually free drinks & food included)*
- Meetings are usually **1 to 2-hours seminars,** sometime with **hands on demos**

We are all VOLUNTEERS!

SUPPORTER

OWASP.ORG

2017

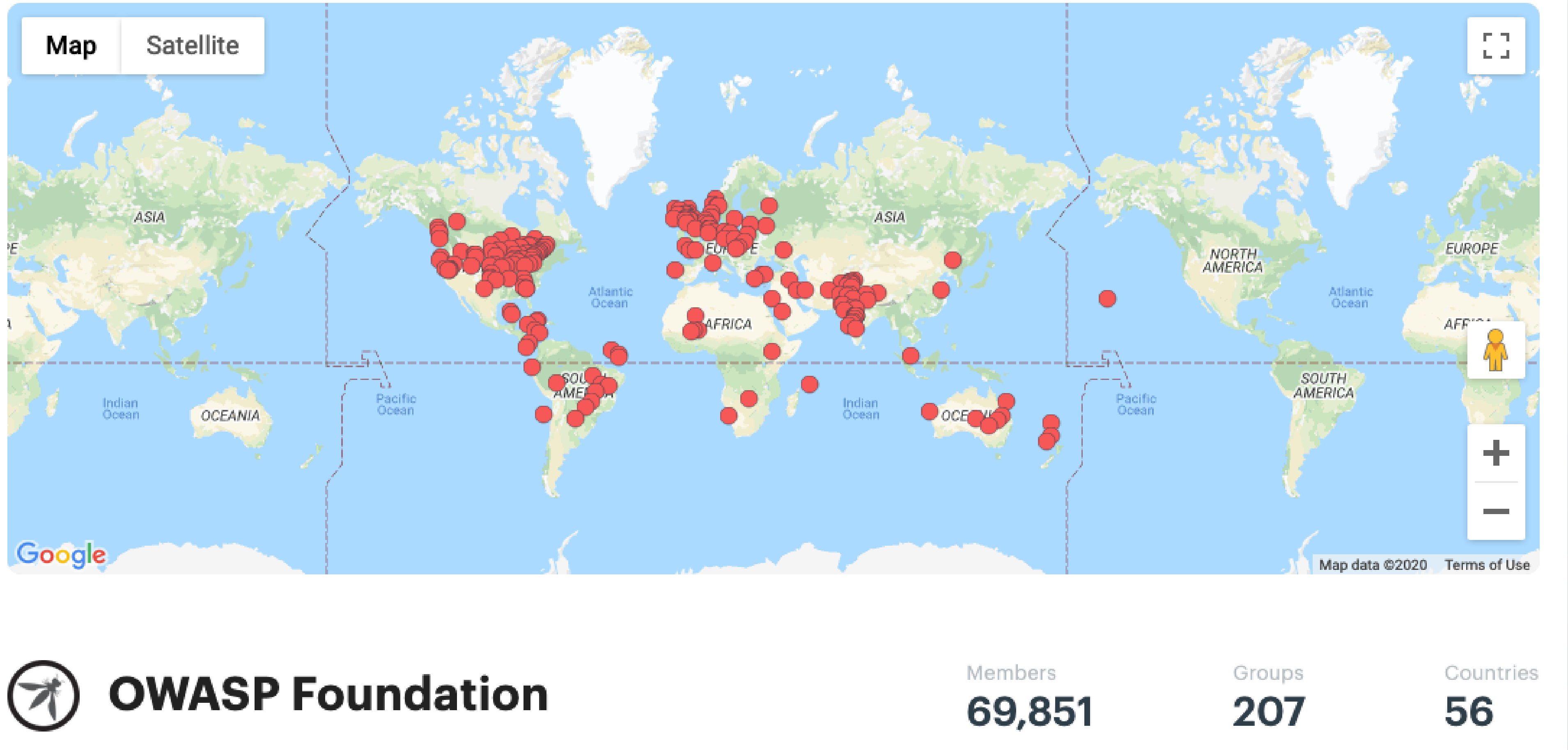
owasp.org

45,000+ OWASP volunteers worldwide

OWASP Video - We Are The Crazy Ones
https://www.youtube.com/watch?v=I8h563Q-GGA

World Wide

207 local Chapters in 56 countries… and counting!

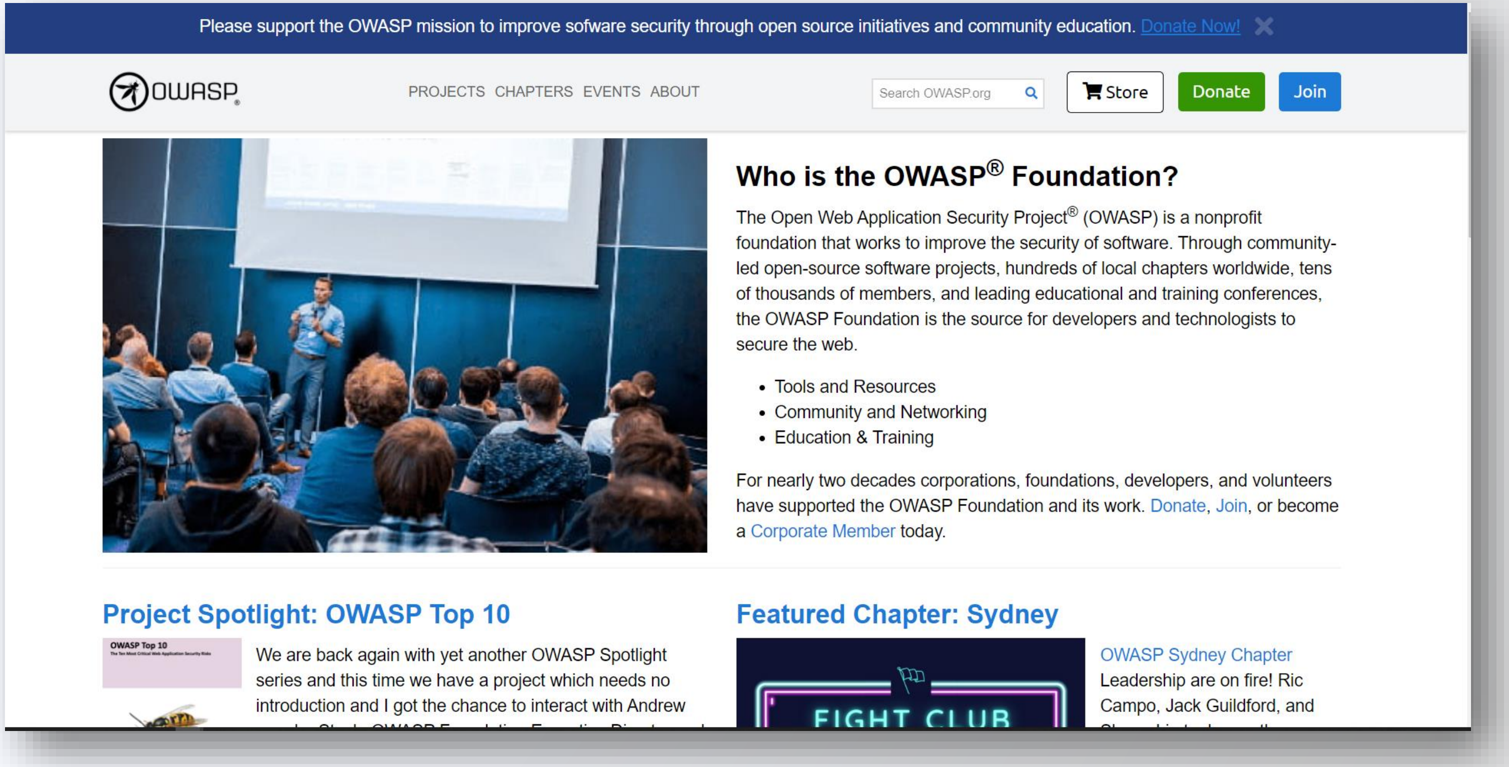


OWASP Foundation

Members	Groups	Countries
69,851	207	56

THE Website: https://owasp.org

Annually, **~7 million technologists & developers** unique-visitors use owasp.org



Please support the OWASP mission to improve sofware software security through open source initiatives and community education. Donate Now!

Who is the OWASP® Foundation?

The Open Web Application Security Project® (OWASP) is a nonprofit foundation that works to improve the security of software. Through community-led open-source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web.

- Tools and Resources
- Community and Networking
- Education & Training

For nearly two decades corporations, foundations, developers, and volunteers have supported the OWASP Foundation and its work. Donate, Join, or become a Corporate Member today.

Project Spotlight: OWASP Top 10

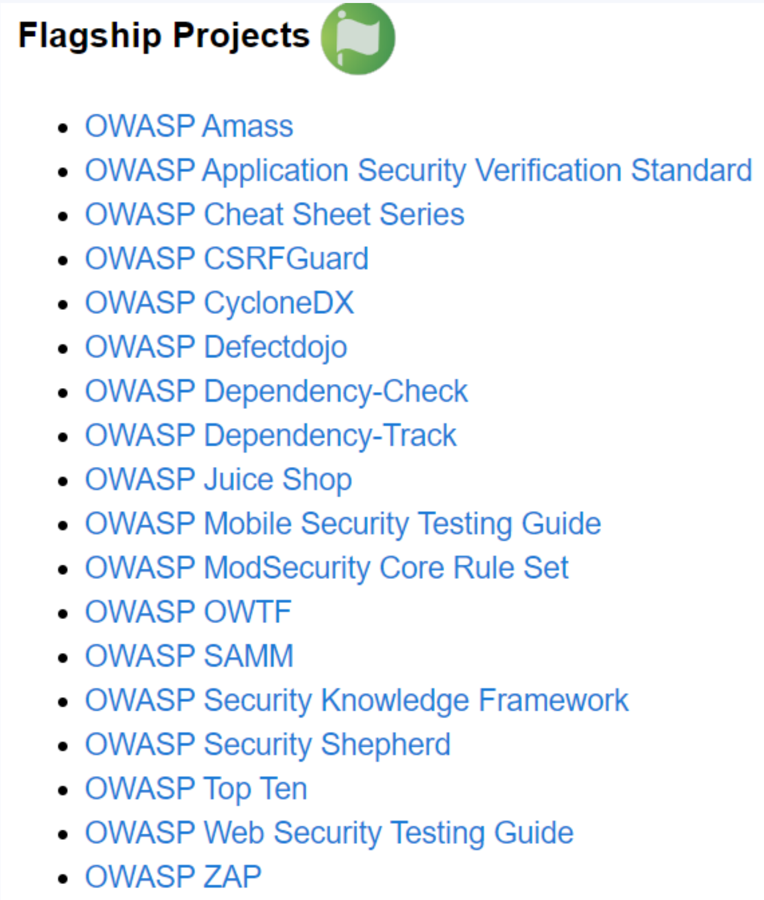
We are back again with yet another OWASP Spotlight series and this time we have a project which needs no introduction and I got the chance to interact with Andrew

Featured Chapter: Sydney

OWASP Sydney Chapter Leadership are on fire! Ric Campo, Jack Guildford, and

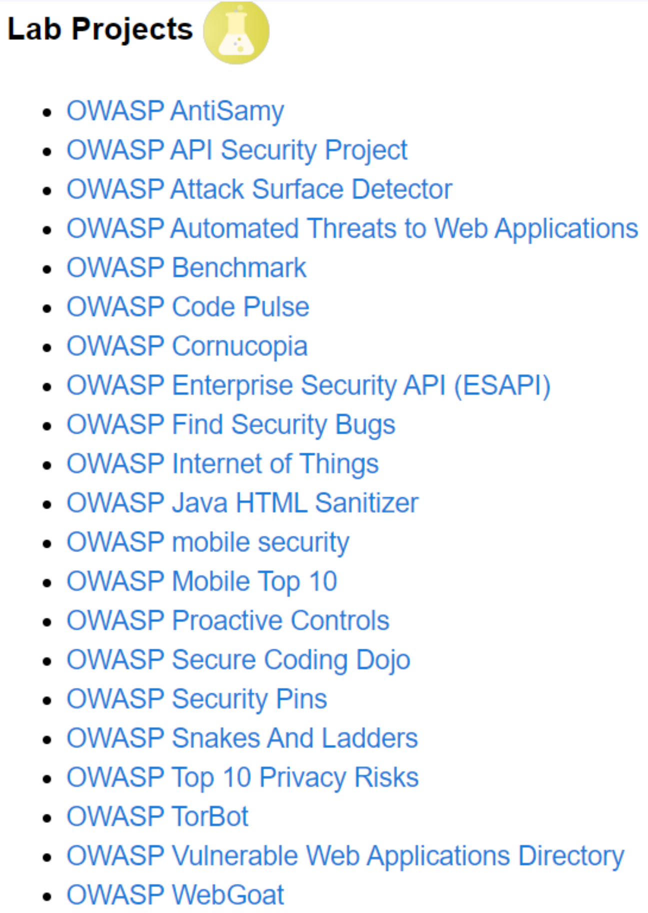
OWASP Projects

- **189 Projects** including **20 Flagship Projects**



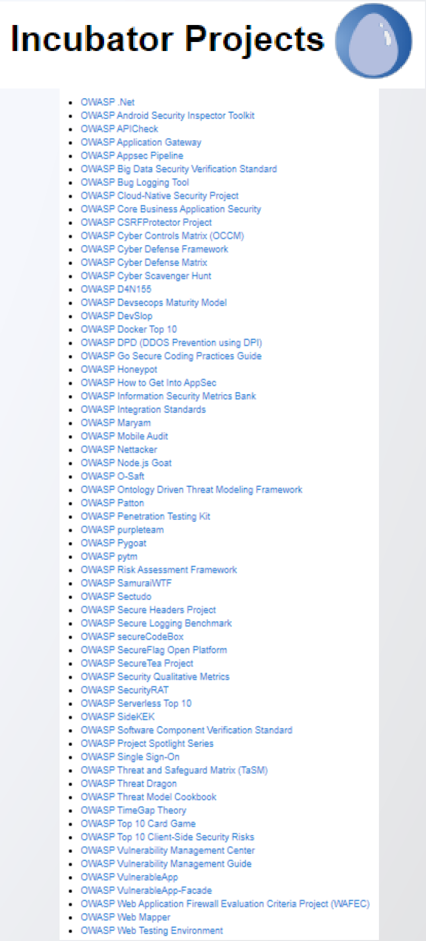
Flagship Projects

- OWASP Amass
- OWASP Application Security Verification Standard
- OWASP Cheat Sheet Series
- OWASP CSRFGuard
- OWASP CycloneDX
- OWASP Defectdojo
- OWASP Dependency-Check
- OWASP Dependency-Track
- OWASP Juice Shop
- OWASP Mobile Security Testing Guide
- OWASP ModSecurity Core Rule Set
- OWASP OWTF
- OWASP SAMM
- OWASP Security Knowledge Framework
- OWASP Security Shepherd
- OWASP Top Ten
- OWASP Web Security Testing Guide
- OWASP ZAP



Lab Projects

- OWASP AntiSamy
- OWASP API Security Project
- OWASP Attack Surface Detector
- OWASP Automated Threats to Web Applications
- OWASP Benchmark
- OWASP Code Pulse
- OWASP Cornucopia
- OWASP Enterprise Security API (ESAPI)
- OWASP Find Security Bugs
- OWASP Internet of Things
- OWASP Java HTML Sanitizer
- OWASP mobile security
- OWASP Mobile Top 10
- OWASP Proactive Controls
- OWASP Secure Coding Dojo
- OWASP Security Pins
- OWASP Snakes And Ladders
- OWASP Top 10 Privacy Risks
- OWASP TorBot
- OWASP Vulnerable Web Applications Directory
- OWASP WebGoat

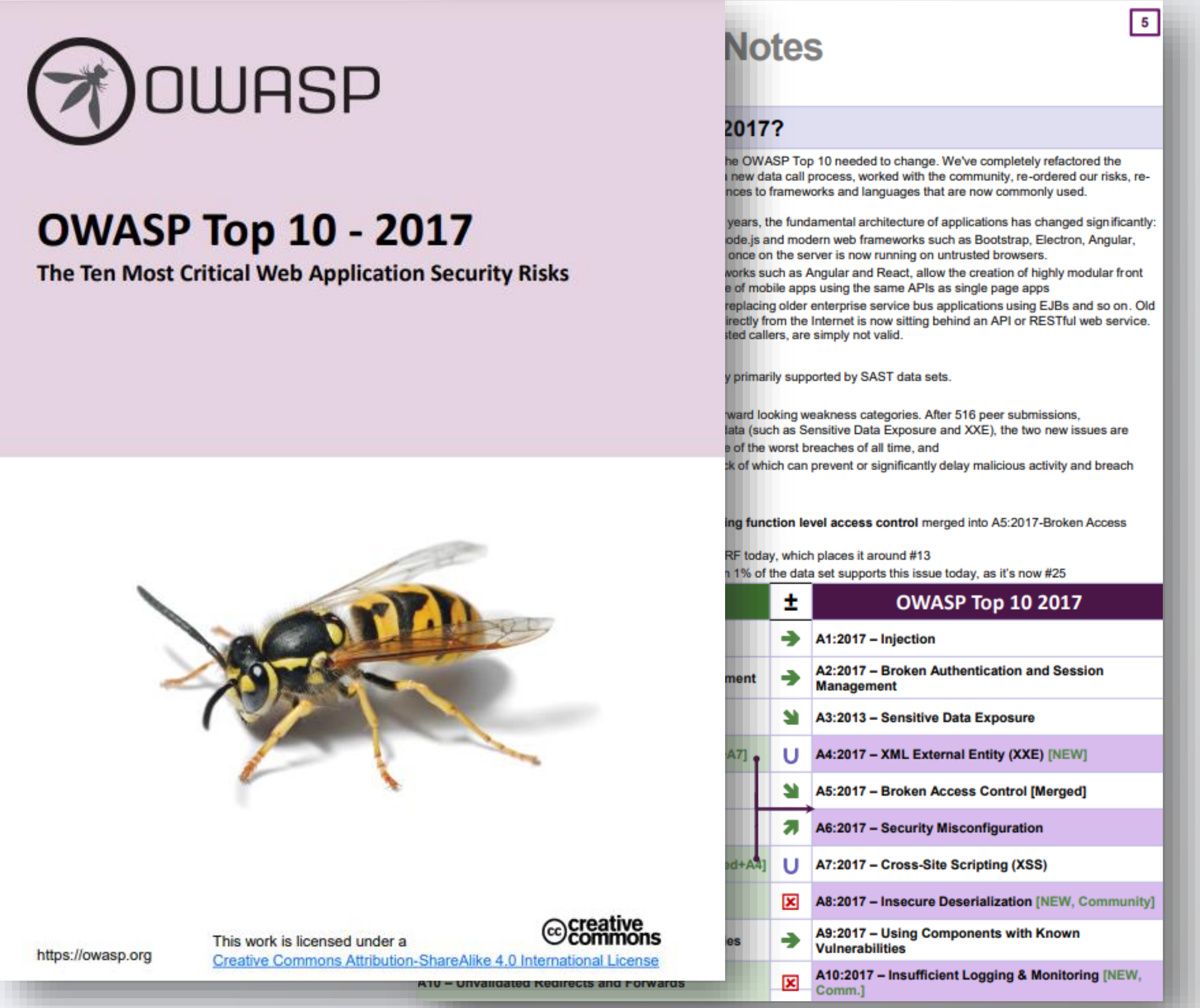


Incubator Projects

- OWASP .Net
- OWASP Android Security Inspector Toolkit
- OWASP APICheck
- OWASP Application Gateway
- OWASP Appsec Pipeline
- OWASP Big Data Security Verification Standard
- OWASP Bug Logging Tool
- OWASP Cloud-Native Security Project
- OWASP Core Business Application Security
- OWASP CSRFProtector Project
- OWASP Cyber Controls Matrix (OCCM)
- OWASP Cyber Defense Framework
- OWASP Cyber Defense Matrix
- OWASP Cyber Scavenger Hunt
- OWASP D4N155
- OWASP Devsecops Maturity Model
- OWASP DevSlop
- OWASP Docker Top 10
- OWASP DPD (DDOS Prevention using DPI)
- OWASP Go Secure Coding Practices Guide
- OWASP Honeypot
- OWASP How to Get Into AppSec
- OWASP Information Security Metrics Bank
- OWASP Integration Standards
- OWASP Maryam
- OWASP Mobile Audit
- OWASP Nettacker
- OWASP Node.js Goat
- OWASP O-Saft
- OWASP Ontology Driven Threat Modeling Framework
- OWASP Patton
- OWASP Penetration Testing Kit
- OWASP purpleteam
- OWASP Pygoat
- OWASP pytm
- OWASP Risk Assessment Framework
- OWASP SamuraiWTF
- OWASP Sectudo
- OWASP Secure Headers Project
- OWASP Secure Logging Benchmark
- OWASP secureCodeBox
- OWASP SecureFlag Open Platform
- OWASP SecureTea Project
- OWASP Security Qualitative Metrics
- OWASP SecurityRAT
- OWASP Serverless Top 10
- OWASP SideKEK
- OWASP Software Component Verification Standard
- OWASP Project Spotlight Series
- OWASP Single Sign-On
- OWASP Threat and Safeguard Matrix (TaSM)
- OWASP Threat Dragon
- OWASP Threat Model Cookbook
- OWASP TimeGap Theory
- OWASP Top 10 Card Game
- OWASP Top 10 Client-Side Security Risks
- OWASP Vulnerability Management Center
- OWASP Vulnerability Management Guide
- OWASP VulnerableApp
- OWASP VulnerableApp-Facade
- OWASP Web Application Firewall Evaluation Criteria Project (WAFEC)
- OWASP Web Mapper
- OWASP Web Testing Environment

E.g. #1: OWASP Top 10

- Flagship Project
- The most critical security risks to web applications.
- Although the original goal was simply to **raise awareness** amongst developers, it has become the **de facto application security standard**.
- Updated every 2-3 years from 2003 to 2017.



OWASP

OWASP Top 10 - 2017

The Ten Most Critical Web Application Security Risks

https://owasp.org

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

creative commons

5

Notes

2017?

he OWASP Top 10 needed to change. We've completely refactored the
new data call process, worked with the community, re-ordered our risks, re-
nces to frameworks and languages that are now commonly used.

years, the fundamental architecture of applications has changed significantly:
ode.js and modern web frameworks such as Bootstrap, Electron, Angular,
once on the server is now running on untrusted browsers.
works such as Angular and React, allow the creation of highly modular front
e of mobile apps using the same APIs as single page apps
replacing older enterprise service bus applications using EJBs and so on. Old
irectly from the Internet is now sitting behind an API or RESTful web service.
sted callers, are simply not valid.

y primarily supported by SAST data sets.

ward looking weakness categories. After 516 peer submissions,
data (such as Sensitive Data Exposure and XXE), the two new issues are
e of the worst breaches of all time, and
k of which can prevent or significantly delay malicious activity and breach

ing **function level access control** merged into A5:2017-Broken Access

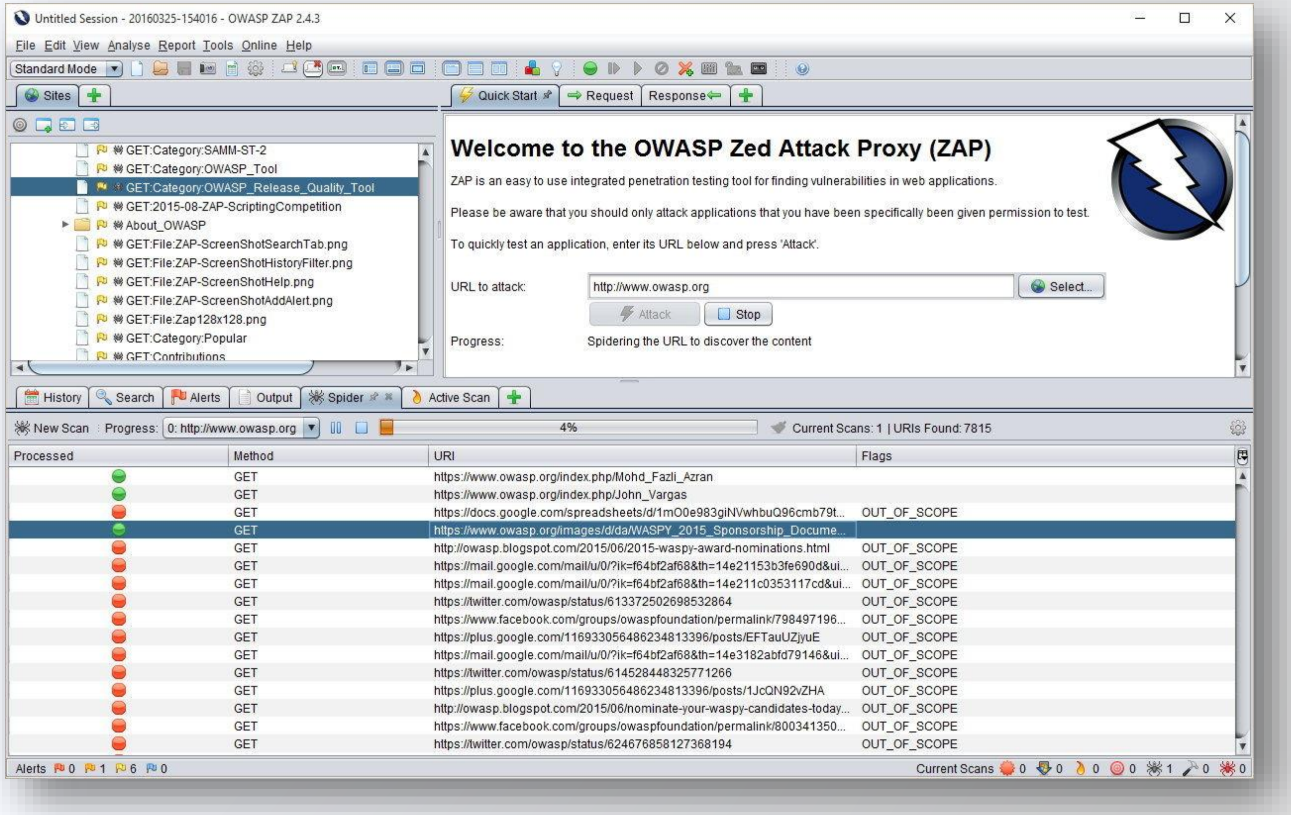
RF today, which places it around #13
1% of the data set supports this issue today, as it's now #25

	±	OWASP Top 10 2017
	→	A1:2017 – Injection
ment	→	A2:2017 – Broken Authentication and Session Management
	↘	A3:2013 – Sensitive Data Exposure
A7]	∪	A4:2017 – XML External Entity (XXE) [NEW]
	↘	A5:2017 – Broken Access Control [Merged]
	↗	A6:2017 – Security Misconfiguration
d+A4]	∪	A7:2017 – Cross-Site Scripting (XSS)
	☒	A8:2017 – Insecure Deserialization [NEW, Community]
es	→	A9:2017 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017 – Insufficient Logging & Monitoring [NEW, Comm.]

E.g. #2: OWASP ZAP

OWASP
Zed Attack Proxy

- Flagship Project
- Web App DAST tool
- Integrates into CI/CD Pipeline
- GitHub Actions and GitLab Modules exist
- 140+ Contributors
- https://www.zaproxy.org/



Untitled Session - 20160325-154016 - OWASP ZAP 2.4.3
File Edit View Analyse Report Tools Online Help
Standard Mode
Sites
Quick Start
Request
Response
History
Search
Alerts
Output
Spider
Active Scan

GET:Category:SAMM-ST-2
GET:Category:OWASP_Tool
GET:Category:OWASP_Release_Quality_Tool
GET:2015-08-ZAP-ScriptingCompetition
About_OWASP
GET:File:ZAP-ScreenShotSearchTab.png
GET:File:ZAP-ScreenShotHistoryFilter.png
GET:File:ZAP-ScreenShotHelp.png
GET:File:ZAP-ScreenShotAddAlert.png
GET:File:Zap128x128.png
GET:Category:Popular
GET:Contributions

Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

To quickly test an application, enter its URL below and press 'Attack'.

URL to attack: http://www.owasp.org Select...

Attack Stop

Progress: Spidering the URL to discover the content

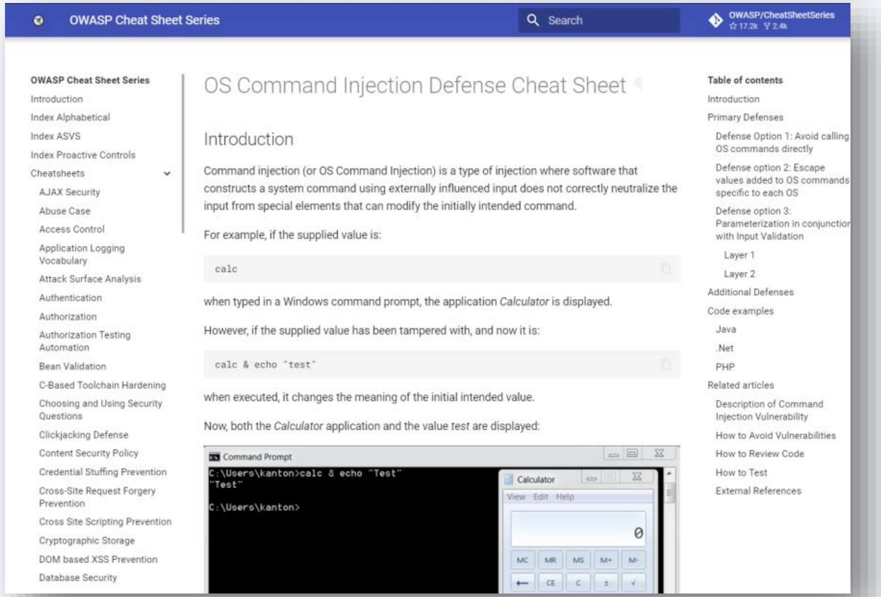
New Scan Progress: 0: http://www.owasp.org 4% Current Scans: 1 | URIs Found: 7815

Processed	Method	URI	Flags
●	GET	https://www.owasp.org/index.php/Mohd_Fazli_Azran	
●	GET	https://www.owasp.org/index.php/John_Vargas	
●	GET	https://docs.google.com/spreadsheets/d/1mO0e983giNVwhbuQ96cmb79t...	OUT_OF_SCOPE
●	GET	https://www.owasp.org/images/d/da/WASPY_2015_Sponsorship_Docume...	
●	GET	http://owasp.blogspot.com/2015/06/2015-waspy-award-nominations.html	OUT_OF_SCOPE
●	GET	https://mail.google.com/mail/u/0/?ik=f64bf2af68&th=14e21153b3fe690d&ui...	OUT_OF_SCOPE
●	GET	https://mail.google.com/mail/u/0/?ik=f64bf2af68&th=14e211c0353117cd&ui...	OUT_OF_SCOPE
●	GET	https://twitter.com/owasp/status/613372502698532864	OUT_OF_SCOPE
●	GET	https://www.facebook.com/groups/owaspfoundation/permalink/798497196...	OUT_OF_SCOPE
●	GET	https://plus.google.com/116933056486234813396/posts/EFTauUZjyuE	OUT_OF_SCOPE
●	GET	https://mail.google.com/mail/u/0/?ik=f64bf2af68&th=14e3182abfd79146&ui...	OUT_OF_SCOPE
●	GET	https://twitter.com/owasp/status/614528448325771266	OUT_OF_SCOPE
●	GET	https://plus.google.com/116933056486234813396/posts/1JcQN92vZHA	OUT_OF_SCOPE
●	GET	http://owasp.blogspot.com/2015/06/nominate-your-waspy-candidates-today...	OUT_OF_SCOPE
●	GET	https://www.facebook.com/groups/owaspfoundation/permalink/800341350...	OUT_OF_SCOPE
●	GET	https://twitter.com/owasp/status/624676858127368194	OUT_OF_SCOPE

Alerts 0 1 6 0 Current Scans 0 0 0 0 1 0 0

E.g. #3: OWASP Cheat Sheet

- Flagship Project
- Helps Devs with AppSec issues
- Project is led by industry veterans
- 130+ Contributors
- https://cheatsheetseries.owasp.org



OS Command Injection Defense Cheat Sheet

Introduction

Command injection (or OS Command Injection) is a type of injection where software that constructs a system command using externally influenced input does not correctly neutralize the input from special elements that can modify the initially intended command.

For example, if the supplied value is:

```
calc
```

when typed in a Windows command prompt, the application *Calculator* is displayed.

However, if the supplied value has been tampered with, and now it is:

```
calc & echo "test"
```

when executed, it changes the meaning of the initial intended value.

Now, both the *Calculator* application and the value *test* are displayed:

```
C:\Users\kanton>calc & echo "Test"
"Test"

C:\Users\kanton>
```

Luxembourg Chapter – Our aim

- Building an **active AppSec** community in **Luxembourg** and Greater Luxembourg (***Grande Région***).
- Ambitiously aiming to organize at **least 4 meetings** annually.
- Carrying on the synergy with OWASP in **BeNeLux:**

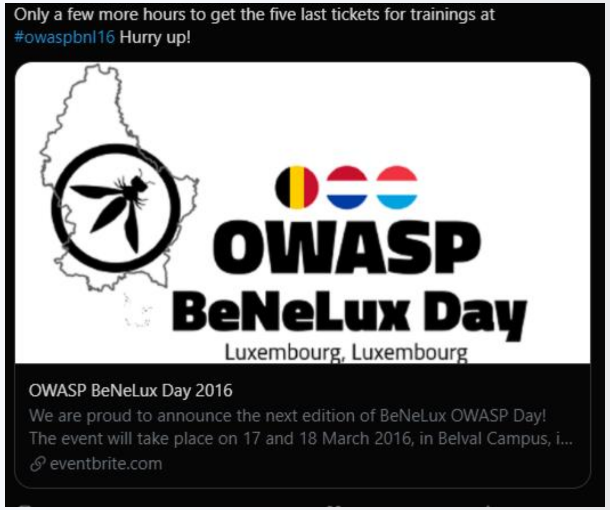
  co-organizing and contributing to https://www.owaspbenelux.eu

OWASP BeNeLux Days Conferences
by OWASP Foundation

- Involving **communities outside the infosec** industry (e.g. Devs/Ops, architects, technologists, IT generalists, managers, executives, etc.)
- Active actor in the Luxembourgish cyber security ecosystem

CYBERSECURITY LUXEMBOURG
A trusted cybersecurity ecosystem for a flourishing economy

Luxembourg Chapter – Since 2009

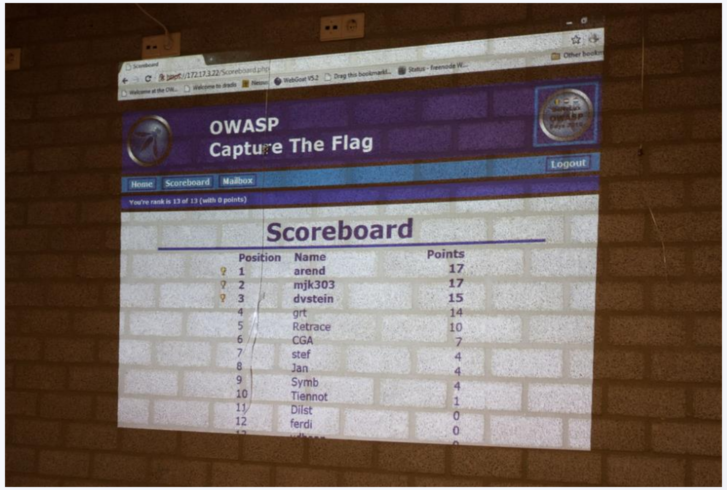


Only a few more hours to get the five last tickets for trainings at #owaspbnl16 Hurry up!

OWASP BeNeLux Day 2016

We are proud to announce the next edition of BeNeLux OWASP Day! The event will take place on 17 and 18 March 2016, in Belval Campus, i...

eventbrite.com



OWASP
Capture The Flag

You're rank is 13 of 13 (with 0 points)

Scoreboard

Position	Name	Points
1	arend	17
2	mjk303	17
3	dvstein	15
4	grt	14
5	Retrace	10
6	CGA	7
7	stef	4
8	Jan	4
9	Symb	4
10	Tiennot	1
11	Dilst	0
12	ferdi	0

Luxembourg Chapter - Call for action
We need you!

- Get involved now! we need you as
  - OWASP ambassador / enthusiast
  - OWASP **member** / contributor / board member
  - Our meetings host

- Volunteer to be a **Speaker**

- **Follow us** on social media, mailing list, channels (share them with your network – and not only with cyber / infosec folks ☺)

Upcoming meeting topics

- We will start with **Foundational-level** talks, presentation, hands-on labs:
  - OWASP Top 10 Risks in Applications
  - Security requirements in AppSeC
  - Etc.
- Focus on **flagship** projects (ASVS, OWASP SAMM, Dependency Track, etc.)
- Focus on **technologies** (Mobile, Thick Client, IoT, etc.)
- Focus on **culture** (DevSecOps, Agile, Automation, Cloud native, etc.)
- **Gamification - Capture de flag** challenges

Call for action – We need you!

Visit our **Chapter website**:
https://owasp.org/www-chapter-luxembourg/

Follow our **Linkedin page**:
https://www.linkedin.com/company/71683313

Join us on **LinkedIn Group**:
https://www.linkedin.com/groups/9026319

Join an **OWASP Mailing List**:
https://groups.google.com/u/0/a/owasp.org/g/luxembourg-chapter/

Chapter leaders contacts:
Yasser Aboukir: yasser.aboukir a_t owasp.org
Raffaele Perrone: raffaele.perrone a_t owasp.org

SCAN ME

Follow us on **Twitter**
@LuxembourgOwasp Hashtag: ***#OWASPLux***

Join our **MeetUp group:**
https://www.meetup.com/en-AU/owasp-luxembourg-group/

Watch us on **YouTube**: Coming soon