RSACONFERENCE2013

Security: Looking Forward

Protecting Critical Applications with OWASP

Michael Coates
OWASP

Security in knowledge

Session ID: AST1-F42

Session Classification: General Interest

Reality Check

- “The global cost of cybercrime is greater than the combined effect on the global economy of trafficking in marijuana, heroin and cocaine”

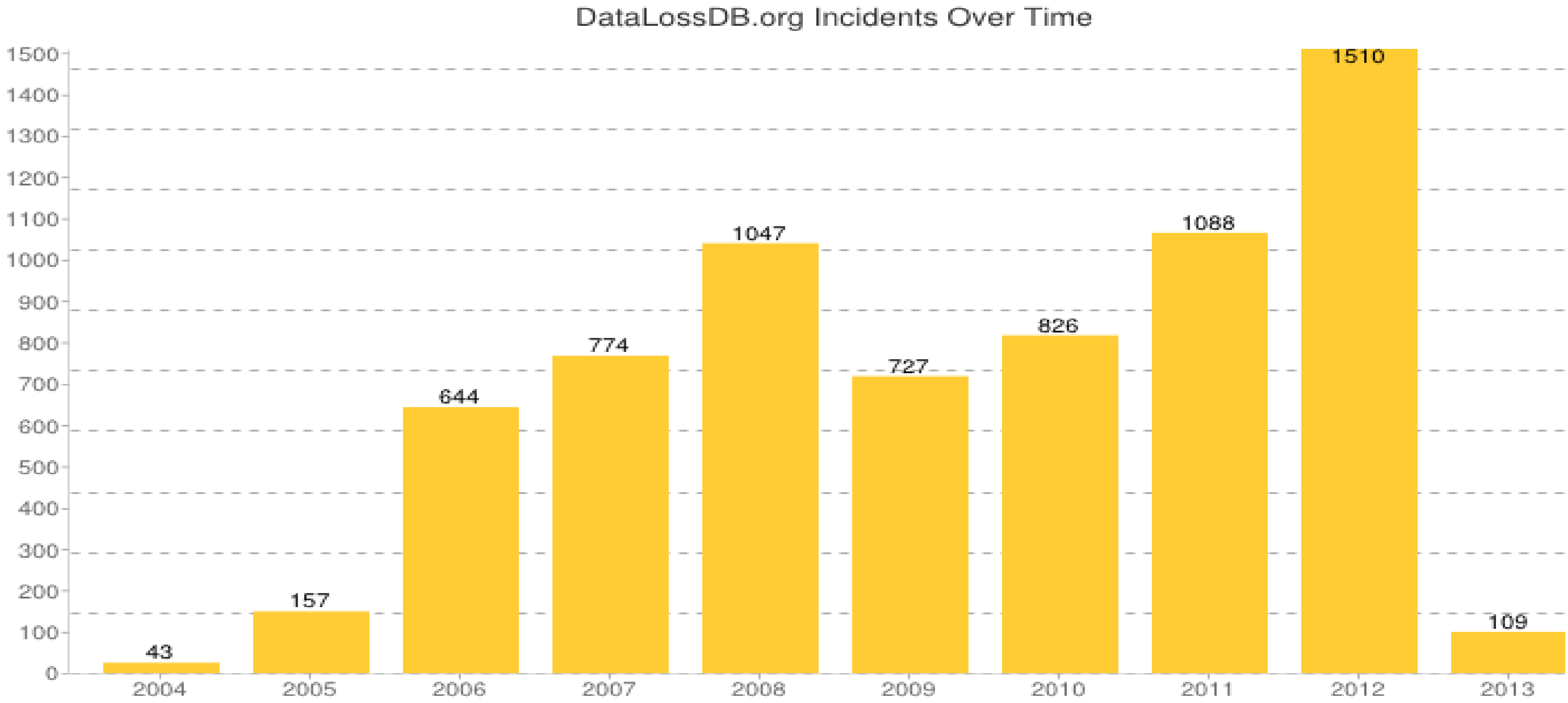
http://www.theregister.co.uk/2011/09/07/cost_is_more_than_some_drug_trafficking
http://uk.norton.com/content/en/uk/home_homeoffice/html/cybercrimereport/

Backed By Organized Crime

- most data thieves are professional criminals deliberately trying to steal information they can turn into cash
- organized criminal groups were behind 83% of breaches investigated by Verizon data breach report

2012 Data Breach Investigations Report - Verizon

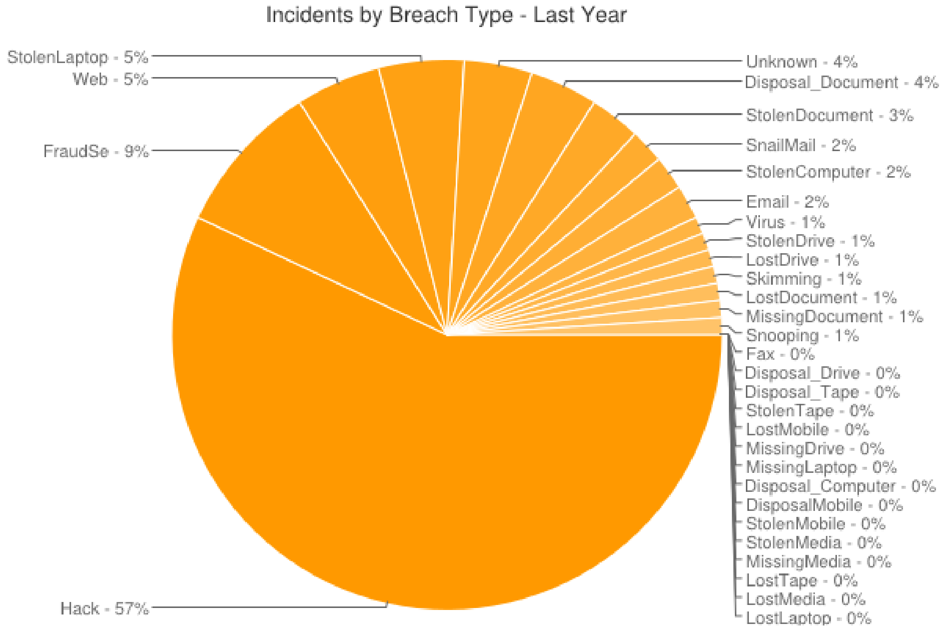
Data Loss: Growing Problem



http://datalossdb.org/statistics

Data Loss: Hacking Dominates

- 2012: Hacking accounts for 57% of intrusions with data loss

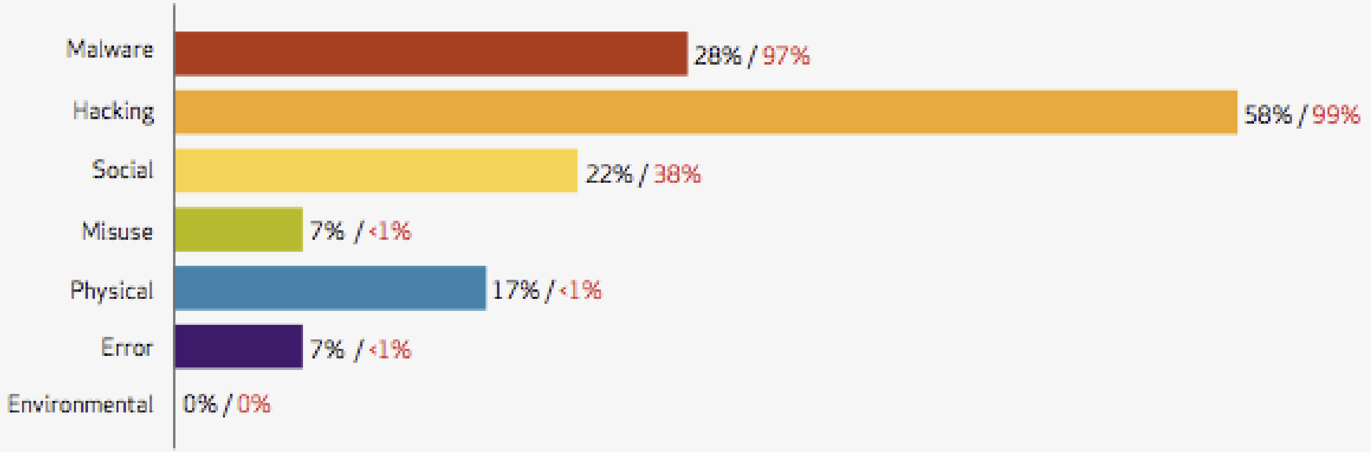


http://datalossdb.org/statistics

Data Loss: Hacking Dominates

- Hacking was involved 99% of incidents where data was lost

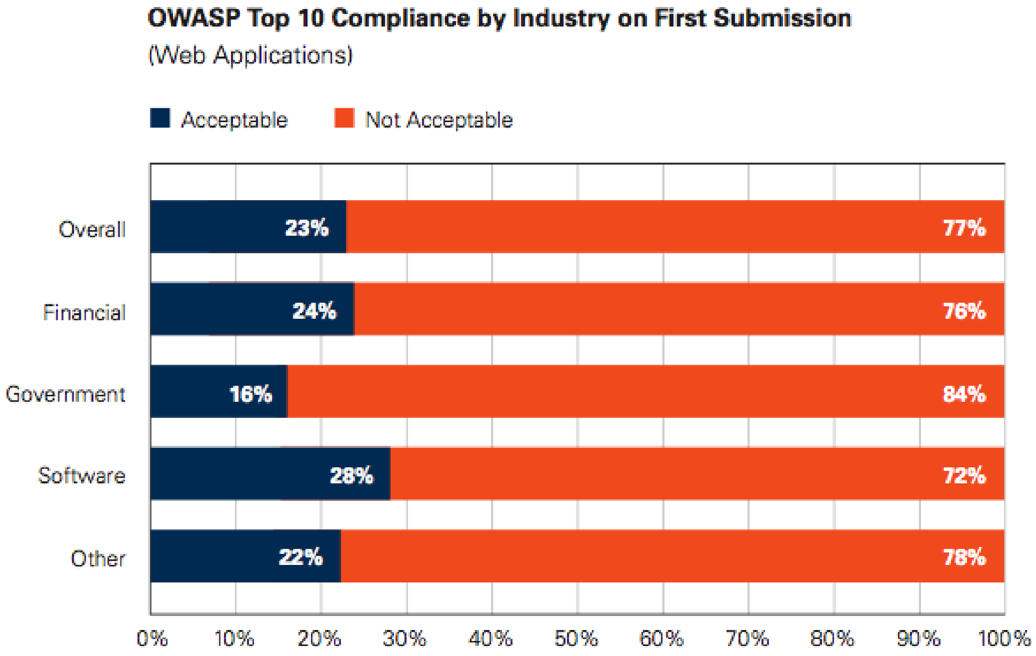
Figure 18. Threat action categories by percent of breaches and percent of records – LARGER ORGS



2012 Data Breach Investigations Report - Verizon

Motive & Opportunity

- Critical application vulnerabilities plague websites



OWASP Top 10 Compliance by Industry on First Submission
(Web Applications)

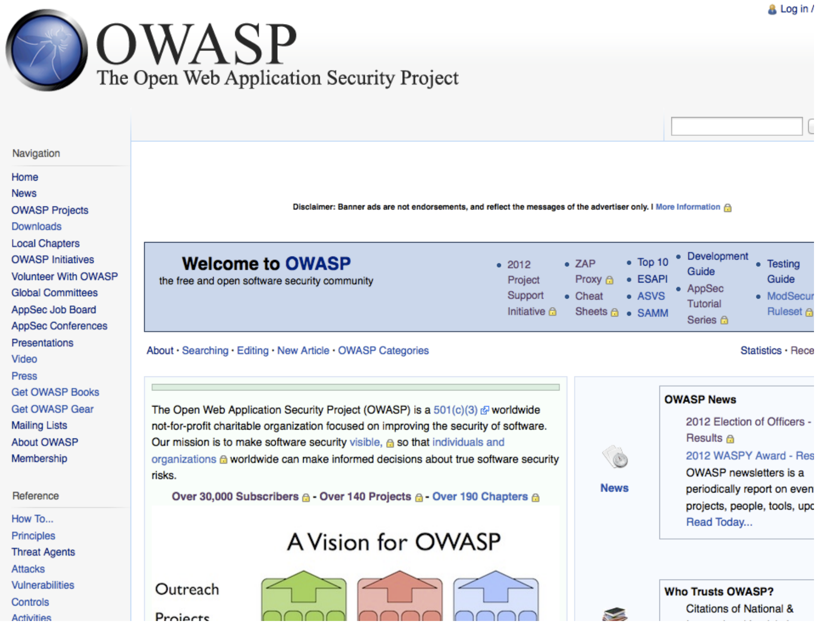
Figure 24: OWASP Top 10 Compliance by Industry on First Submission (Web Applications)

http://info.veracode.com/state-of-software-security-report-volume4.html

OWASP Can Help

Guidance, Knowledge, Power

- Open Web Application Security Project (OWASP)
  - Non Profit
  - Open Source
  - Vendor Neutral
- Core Values
  - Open
  - Innovation
  - Global
  - Integrity



Log in /

OWASP
The Open Web Application Security Project

Navigation

- Home
- News
- OWASP Projects
- Downloads
- Local Chapters
- OWASP Initiatives
- Volunteer With OWASP
- Global Committees
- AppSec Job Board
- AppSec Conferences
- Presentations
- Video
- Press
- Get OWASP Books
- Get OWASP Gear
- Mailing Lists
- About OWASP
- Membership

Reference

- How To...
- Principles
- Threat Agents
- Attacks
- Vulnerabilities
- Controls
- Activities

Disclaimer: Banner ads are not endorsements, and reflect the messages of the advertiser only. I More Information

Welcome to OWASP
the free and open software security community

- 2012 Project Support Initiative
- ZAP Proxy
- Cheat Sheets
- Top 10
- ESAPI
- ASVS
- SAMM
- Development Guide
- AppSec Tutorial Series
- Testing Guide
- ModSecur
  Ruleset

About · Searching · Editing · New Article · OWASP Categories

Statistics · Rece

The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software. Our mission is to make software security visible, so that individuals and organizations worldwide can make informed decisions about true software security risks.

Over 30,000 Subscribers - Over 140 Projects - Over 190 Chapters

A Vision for OWASP

Outreach

Projects

News

OWASP News

2012 Election of Officers - Results

2012 WASPY Award - Res

OWASP newsletters is a periodically report on even projects, people, tools, upc

Read Today...

Who Trusts OWASP?

Citations of National &

What is OWASP?

- **Mission Driven**
  - Nonprofit | World Wide | Unbiased

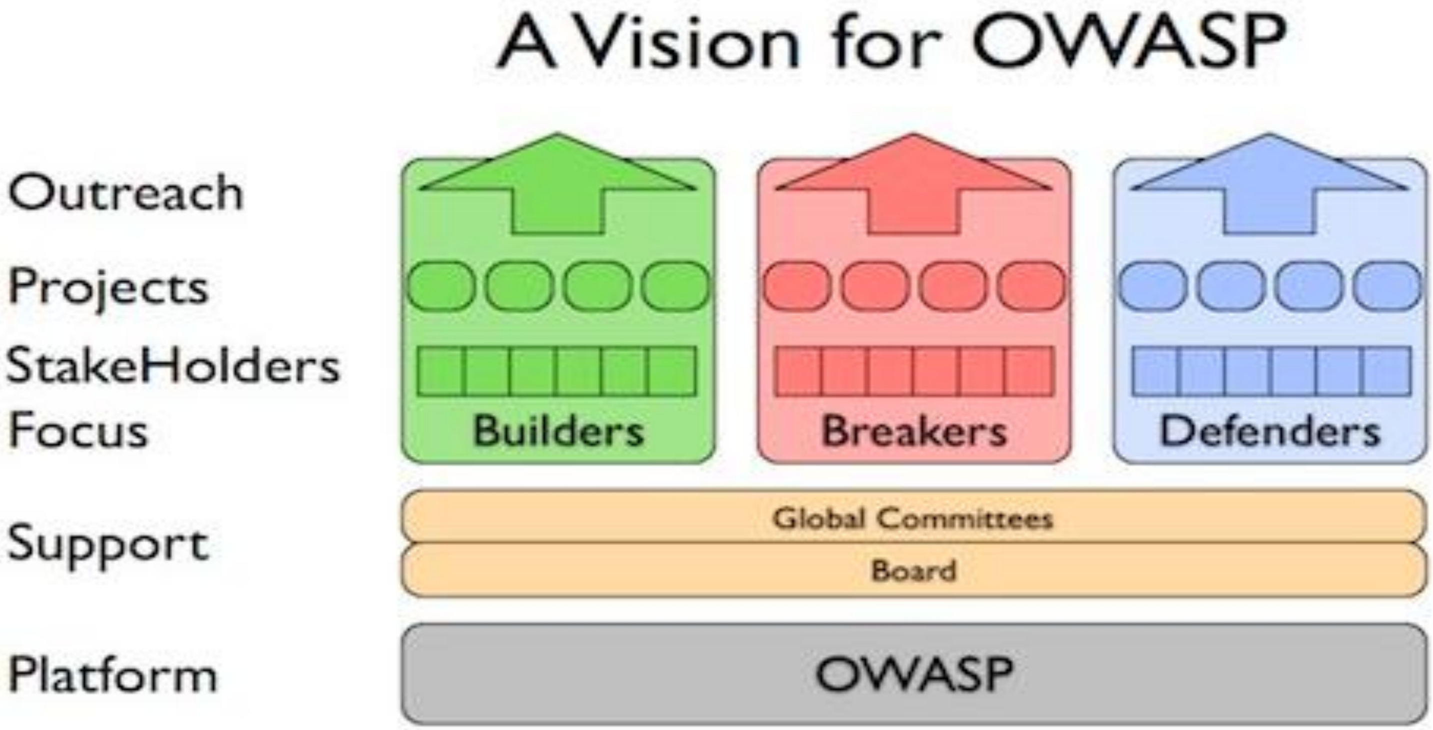
What is OWASP?

- Community Driven
  - 30,000 Mail List Participants | 190 Active Chapters in 76 countries
  - 2000+ Members | 57 Corporate Supporters | 56+ Academic Supporters

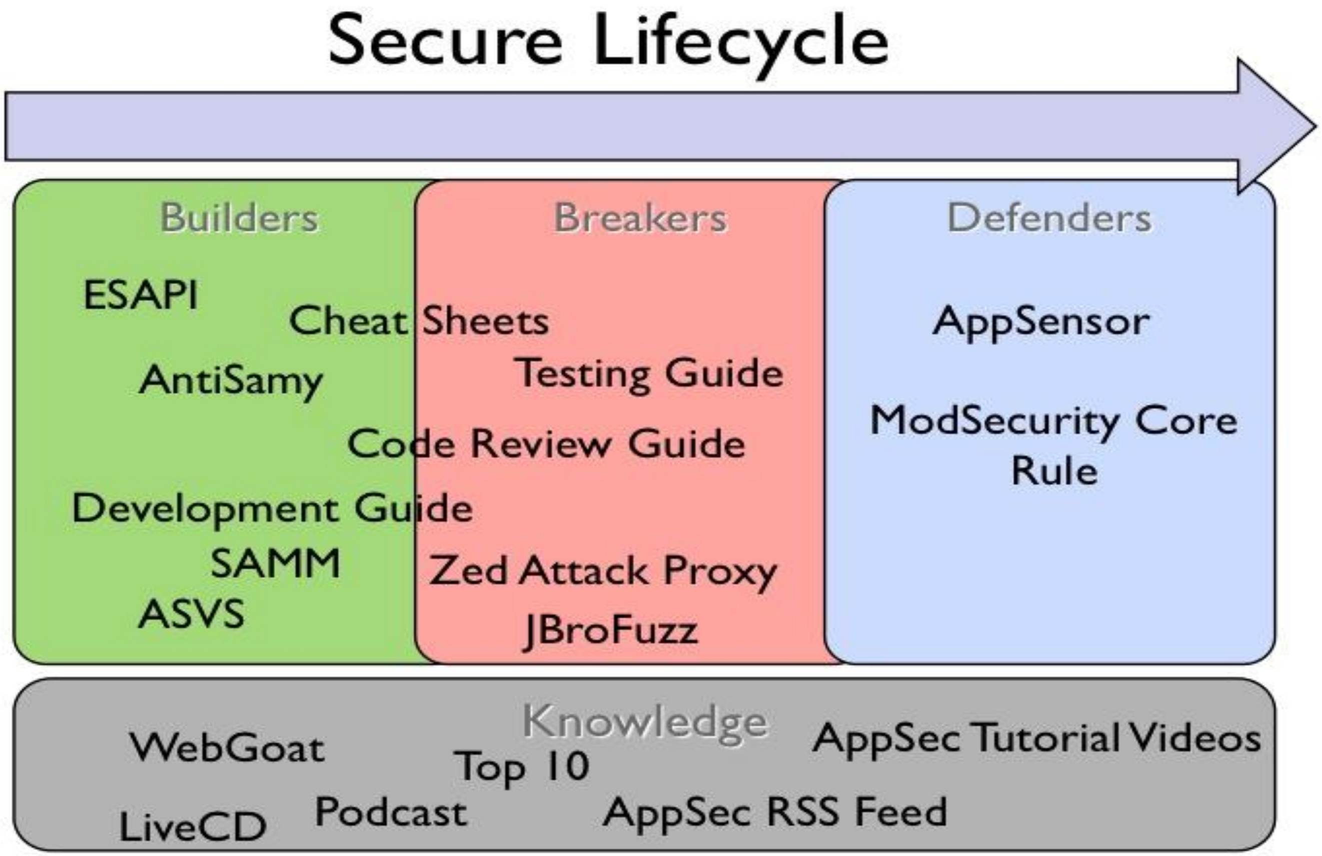
What is OWASP?

- Quality Resources
  - 15,000+ downloads of tools, documentation
  - 250,000+ unique visitors (monthly)
  - 800,000+ page views (monthly)

Security @ OWASP



Security Resources



Secure Lifecycle

Builders

ESAPI

Cheat Sheets

AntiSamy

Testing Guide

Code Review Guide

Development Guide

SAMM

ASVS

Breakers

Zed Attack Proxy

JBroFuzz

Defenders

AppSensor

ModSecurity Core Rule

Knowledge

WebGoat

Top 10

AppSec Tutorial Videos

LiveCD

Podcast

AppSec RSS Feed

OWASP Top 10

- Top 10 Application Security Risks
- Referenced by MITRE, PCI DSS, DISA, FTC, & more
- 2013 edition RC1

OWASP

The Open Web Application Security Project

OWASP Top 10 - 2013 rc1

The Ten Most Critical Web Application Security Risks

RELEASE CANDIDATE FOR COMMENT

owasp.org/index.php/Category:OWASP_Top_Ten_Project

ESAPI

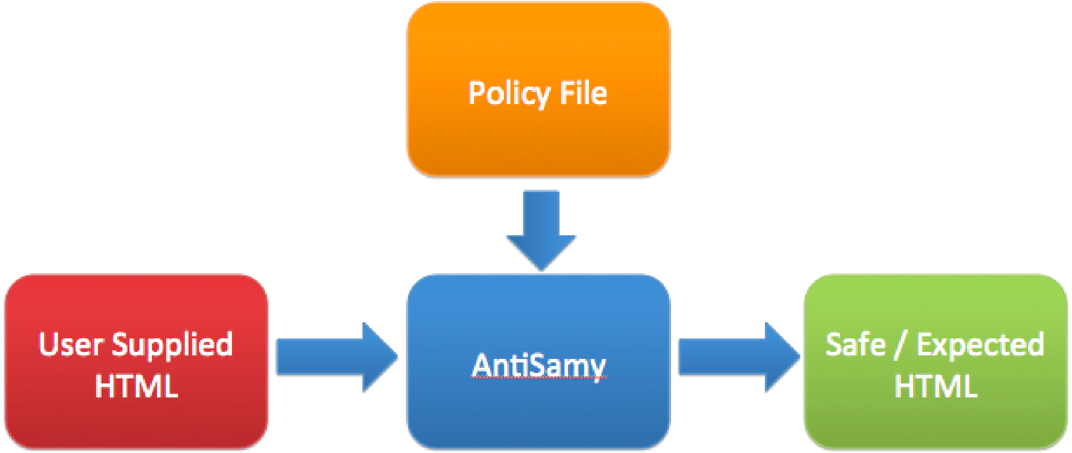
- a free, open source, web application security control library that makes it easier for programmers to write lower-risk applications
- Reuse security controls, don't reinvent!

owasp.org/index.php/Category:OWASP_Enterprise_Security_API

AntiSamy

- an HTML validation tool and API

to safely and gracefully handle rich html input



owasp.org/index.php/Category:OWASP_AntiSamy_Project

Cheat Sheets

- Just what you're looking for,
  - nothing more,
  - nothing less
- Cheat sheets for CSRF, TLS, DOM Based XSS & more

OWASP Top Ten, Authentication, Cross-Site Request Forgery (CSRF) Prevention, Transport Layer Protection, Cryptographic Storage, Input Validation, XSS Prevention, DOM based XSS Prevention, Forgot Password, Query Parameterization, SQL Injection Prevention, Session Management, HTML5 Security, Web Service Security, Application Security Architecture, Logging

owasp.org/index.php/Cheat_Sheets

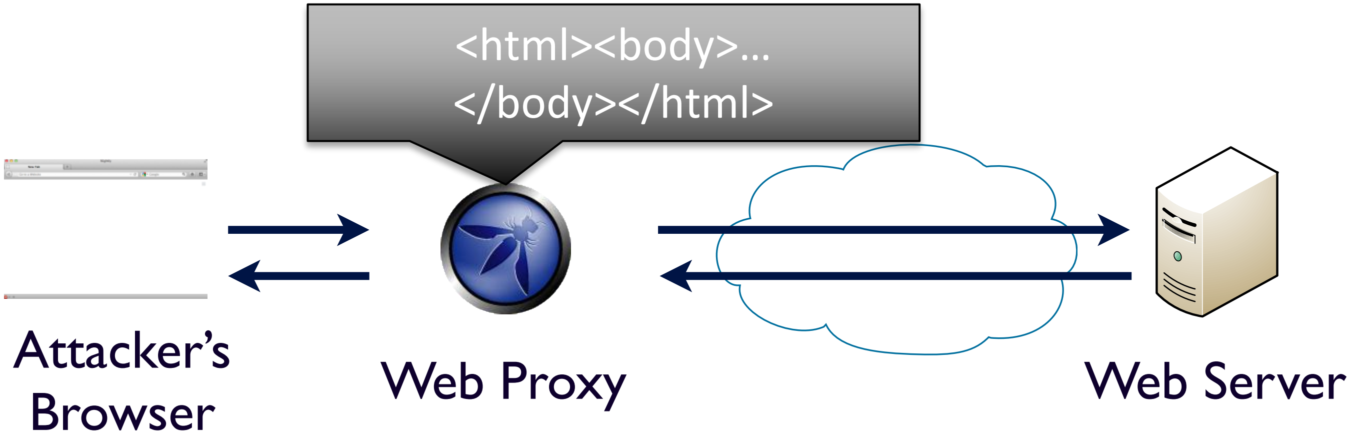
Security Guides

- Development Guide
  - comprehensive manual for designing, developing and deploying secure Web Applications and Web Services
- Code Review Guide
  - mechanics of reviewing code for certain vulnerabilities & validation of proper security controls
- Testing Guide
  - understand the what, why, when, where, and how of testing web applications

owasp.org/index.php/Category:OWASP_Guide_Project
owasp.org/index.php Category:OWASP_Code_Review_Project
owasp.org/index.php/Category:OWASP_Testing_Project

Zed Attack Proxy

- an easy to use integrated penetration testing tool for finding vulnerabilities in web applications



<html><body>…
</body></html>

Attacker's Browser

Web Proxy

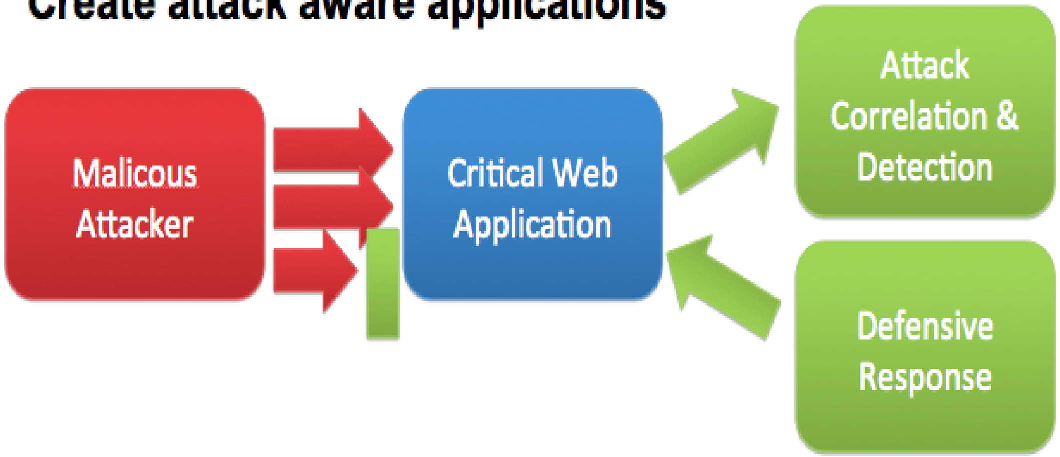
Web Server

owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

AppSensor

- guidance to implement intrusion detection and automated response inside an application

Create attack aware applications



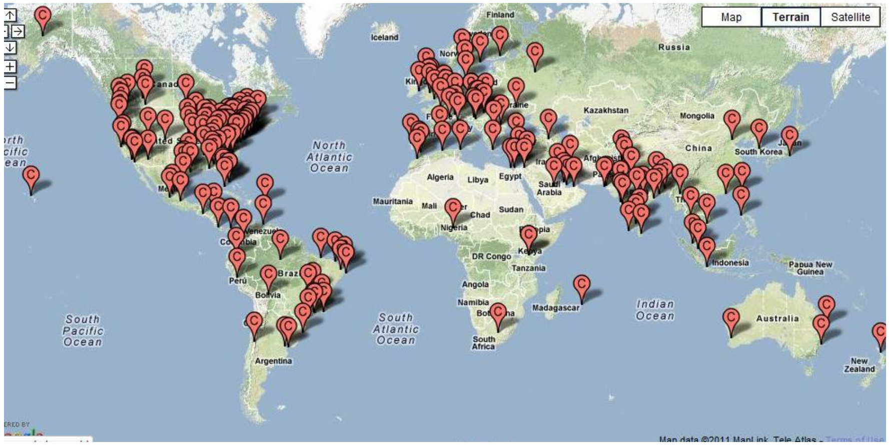
owasp.org/index.php/OWASP_AppSensor_Project

OPEN SOURCE SECURITY -

Building Community & Resources

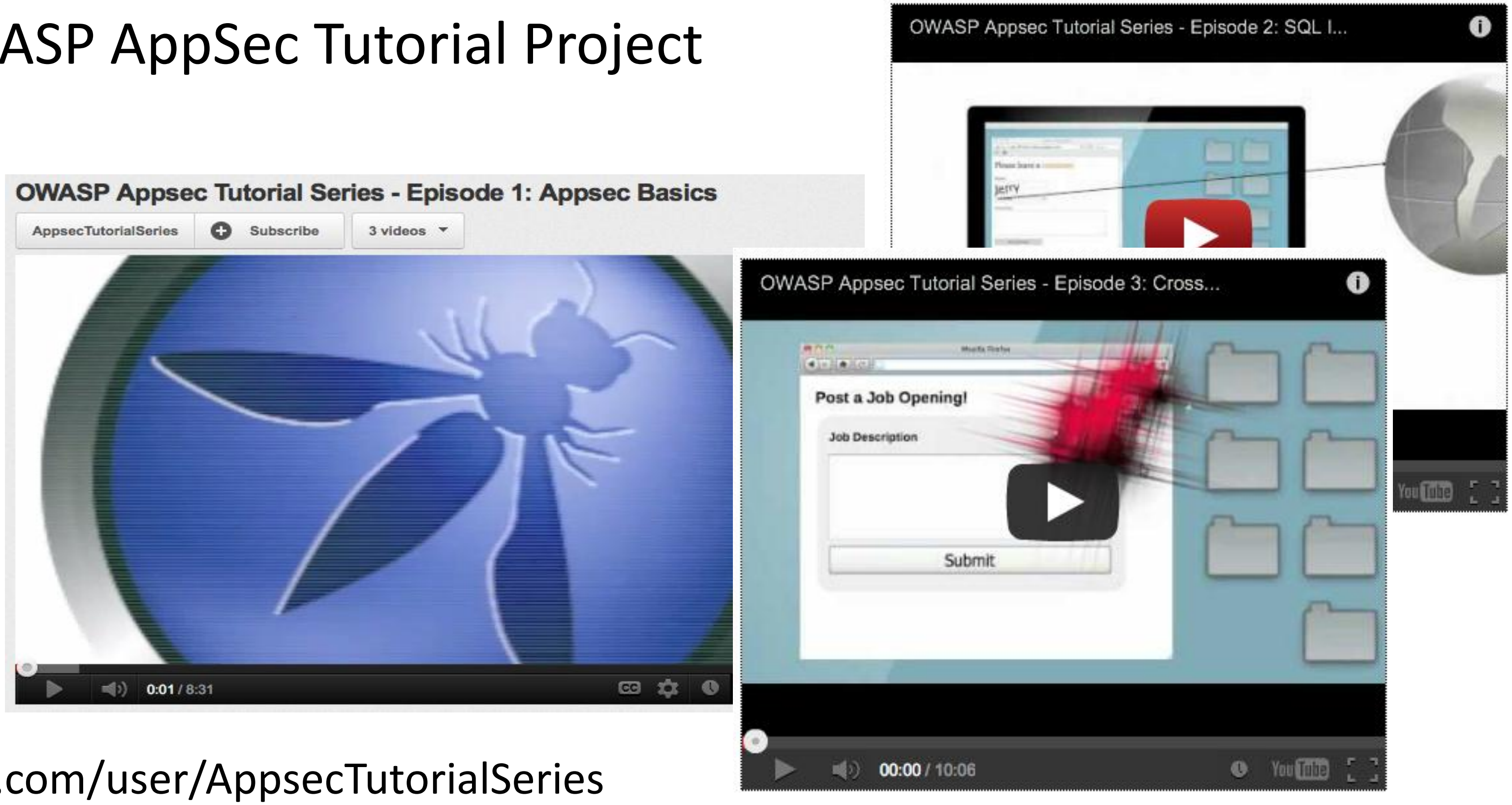
Community

- **Grass Roots** - Support your local chapter
  - Speak, host, attend
  - 180 Chapters in 70 Countries
- **Grow an Idea**
  - Projects & research can be started by anyone
- **Support the Foundation**
  - Individual, corporate & educational



Learning

- OWASP AppSec Tutorial Project

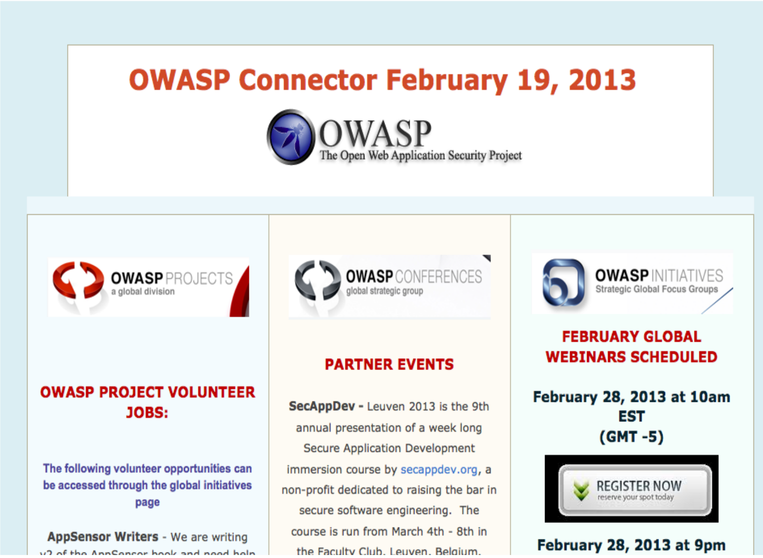

OWASP Appsec Tutorial Series - Episode 1: Appsec Basics
AppsecTutorialSeries
Subscribe
3 videos
0:01 / 8:31
OWASP Appsec Tutorial Series - Episode 2: SQL I...
OWASP Appsec Tutorial Series - Episode 3: Cross...
Post a Job Opening!
Job Description
Submit
00:00 / 10:06

youtube.com/user/AppsecTutorialSeries
owasp.org/index.php/OWASP_Appsec_Tutorial_Series

Sharing & Connecting

- Security101@lists.owasp.org : Enabling growth in security space
  - Intro to security questions
  - Participate with questions or as expert
  - lists.owasp.org/mailman/listinfo/security101
- OWASP Connector
  - Monthly report with call to action, updates

OWASP Connector February 19, 2013



OWASP Connector February 19, 2013

OWASP PROJECT VOLUNTEER JOBS:

The following volunteer opportunities can be accessed through the global initiatives page

AppSensor Writers - We are writing v2 of the AppSensor book and need help

PARTNER EVENTS

SecAppDev - Leuven 2013 is the 9th annual presentation of a week long Secure Application Development immersion course by secappdev.org, a non-profit dedicated to raising the bar in secure software engineering. The course is run from March 4th - 8th in the Faculty Club, Leuven, Belgium.

FEBRUARY GLOBAL WEBINARS SCHEDULED

February 28, 2013 at 10am EST (GMT -5)

February 28, 2013 at 9pm

Global AppSec Events

- Global events focused on application security
  - South Korea – Feb, 2013
  - Germany – Aug, 2013
  - USA – Nov, 2013

owasp.org/index.php/Category:OWASP_AppSec_Conference

Wrap Up

- Our applications are under attack
- Leverage OWASP's free resources to bolster your application security program
- Contribute back to the OWASP global community & help grow application security awareness and resources

OWASP

The Open Web Application Security Project