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?
Why do organisations need OWASP?
Why do organisations need OWASP?

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

This work by genavalunch.com is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported
Why do organisations need OWASP?

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 dropped 2.3 percent Friday in the first day of trading after a three-day break on the Tokyo stock exchange. It was the

weekend. We're working around the clock to get our games back online.

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/28w40e4K

39 minutes ago

SonyOnline Sony Online Ent.

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)

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.

Analyse now the company dealing from the impact on production...
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

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 most prominent recent example being the huge Sony hack that exposed personal data from 77 million PlayStation Network customers -- it’s hardening

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

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

12/05/2011 Swiss Cyber Storm III - May 2011 - Rapperswil
Why do organisations need OWASP?

• Inside organisations:
  – Developers dealing with dozens web technologies
  – Heterogeneous 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 use OWASP?
OWASP foundation

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

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

Core values

Open, Global, Innovation, Worldwide

Mission

Structure

Code of ethics

Independence from vendors, technology-agnostic

Mission
"strategy" (or so...)

Website
Board
Committees
Summit
Chapters
Projects
Conferences
Members

People
Methods
Tools

Web Application

Company assets

Threat

Swiss Cyber Storm III - May 2011 - Rapperswil
OWASP people
Project Leaders

• 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
Chapter Leaders

- 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

• 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

- Conference dedicated to research work on application security
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

• 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
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
OWASP Membership

• **Academic members:**
  - Annual fee: 0$/year
  - Donate: support
  - 40 members
  - Switzerland:
    • 1 officialised partnership (HEIG-VD)
    • 2 pending partnerships
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
  • XSS prevention cheat sheet
  • “sql injection”
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 projects
OWASP projects: Tools

Analyse
- AntiSAMMY
- ESAPI
- CSRFGuard
- Encoding
- Stinger

Design
- JBroFuzz
- LiveCD
- WebScarab
- O2
- Code Crawler

Implement

Verify
- ModSecurity
- CRS
- DirBuster
- WebScarab
- Orizon
- Zed Attack Proxy

Deploy

Academy portal, Broken Web applications, ESAPI Swingset, Webgoat

Respond

12/05/2011 Swiss Cyber Storm III - May 2011 - Rapperswil
OWASP projects: Documents

- Secure contract
- Threat risk modeling
- Development
- J2EE Security
- RoR Security
- .NET Security
- AJAX Security
- PHP Security
- Secure coding practices

- Application security requirements
- Code Review
- Backend Security
- Code Review
- Testing
- ASVS
- Testing

- 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`
Tools: ModSecurity core ruleset

• 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

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](https://www.owasp.org/index.php/ESAPI)
Documents: OWASP Top 10

Documents: code review guide

• Instructions and methodology manual for conducting code security reviews
• Guidance on detecting the major security flaws created during implementation
Documents: ASVS

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

- 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:
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](https://www.owasp.org)
Join the OWASP Switzerland mailing list: [http://www.owasp.ch](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