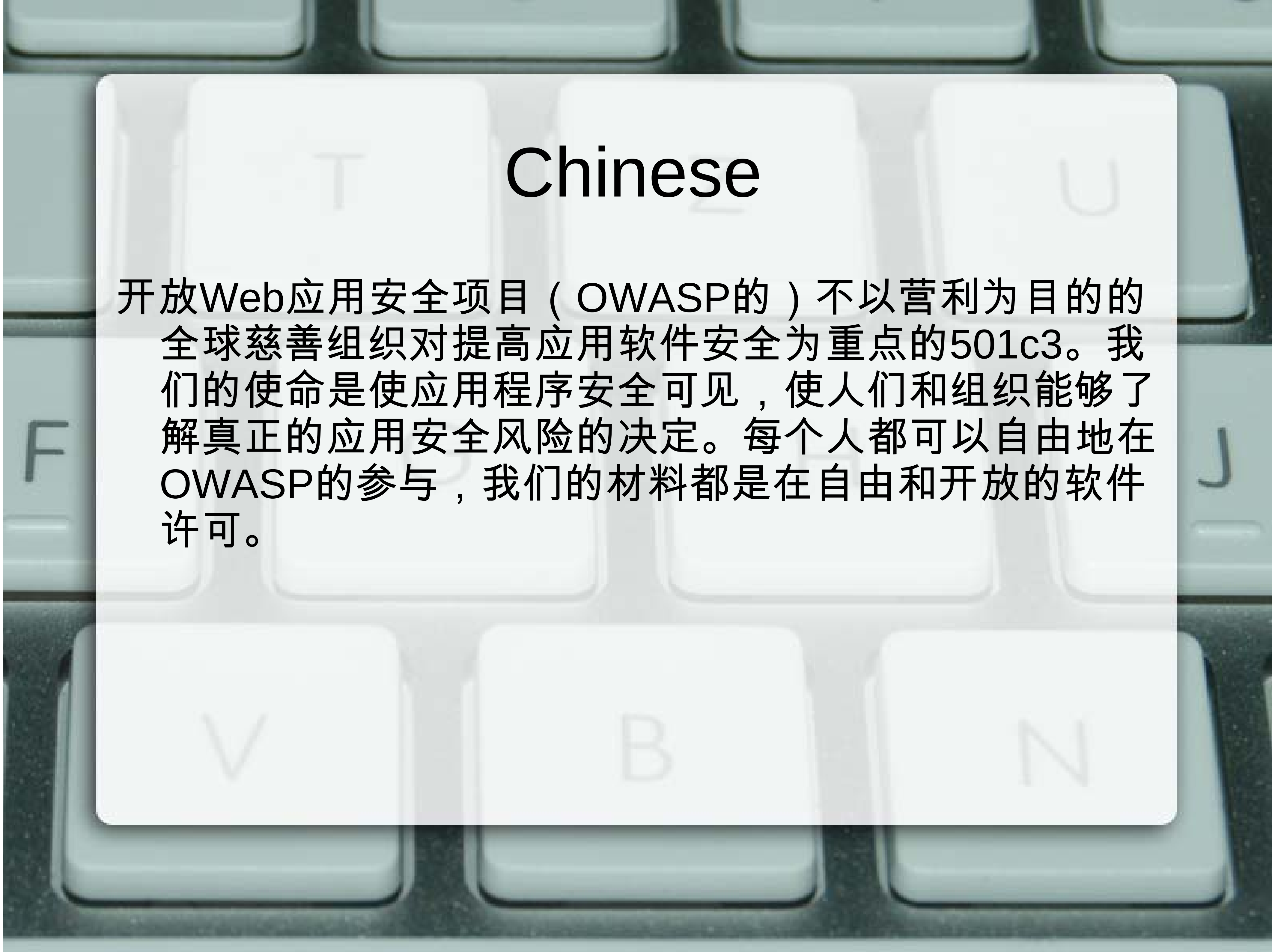
OWASP Foundation

OWASP Foundation **does not endorse or recommend commercial products or services** allowing our community to remain vendor agnostic with the collective wisdom of the best minds in application security worldwide.

OWASP AppSec Germany 2010, Keynote, Tom Brennan

German

Das Open Web Application Security Project (OWASP) ist eine 501c3 Non-Profit weltweit gemeinnützige Organisation zur Verbesserung der Sicherheit von Anwendungssoftware fokussiert. Unsere Mission ist, die Anwendungssicherheit sichtbar machen, so dass Menschen und Organisationen können Entscheidungen über die wahre Anwendung Sicherheitsrisiken informiert zu machen. Jeder ist frei in OWASP beteiligen und alle unsere Materialien sind unter einer freien und offenen Software-Lizenz verfügbar.



Chinese

开放Web应用安全项目（OWASP的）不以营利为目的的全球慈善组织对提高应用软件安全为重点的501c3。我们的使命是使应用程序安全可见，使人们和组织能够了解真正的应用安全风险的决定。每个人都可以自由地在OWASP的参与，我们的材料都是在自由和开放的软件许可。

English

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.

OWASP Foundation

- Founded Dec 2nd 2001 - Current
- 160 Chapters around the world
- 20,000 people that care about AppSec
- 12,771 web pages
- 92,010 edits
- 45,115,334 page views

Principles

- Free & Open
- Governed by rough consensus & running code
- Abide by a code of ethics (see ethics)
- Not-for-profit
- Not driven by commercial interests
- Risk based approach

Code of Ethics

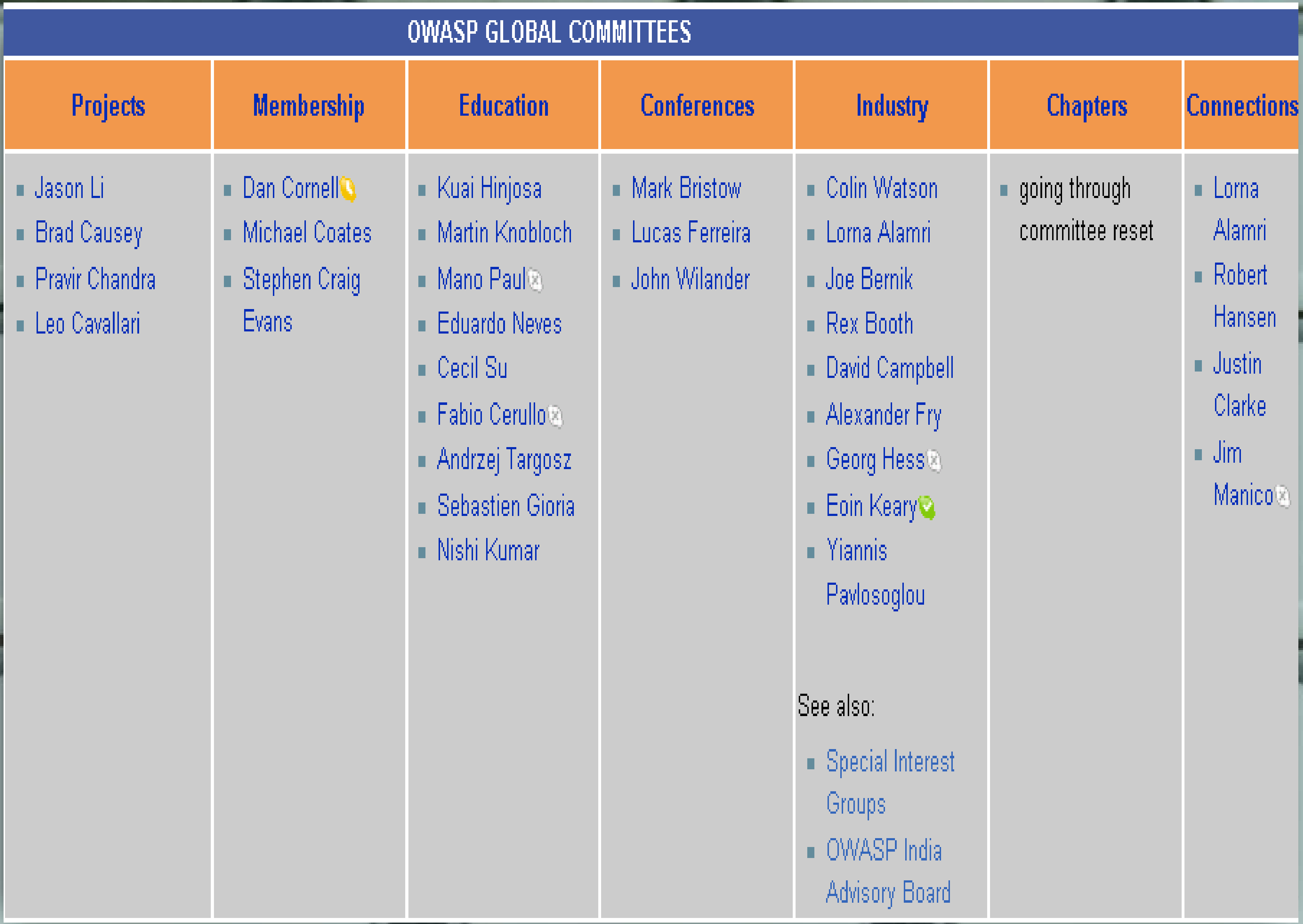
- **Perform all professional activities and duties in accordance with all applicable laws and the highest ethical principles;**
- **Promote the implementation of and promote compliance with standards, procedures, controls for application security;**
- **Maintain appropriate confidentiality of proprietary or otherwise sensitive information encountered in the course of professional activities;**
- **Discharge professional responsibilities with diligence and honesty;**
- **To communicate openly and honestly;**
- **Refrain from any activities which might constitute a conflict of interest or otherwise damage the reputation of employers, the information security profession, or the Association;**

.... continued

- To maintain and affirm our objectivity and independence;
- To reject inappropriate pressure from industry or others;
- Not intentionally injure or impugn the professional reputation of practice of colleagues, clients, or employers;
- Treat everyone with respect and dignity; and
- To avoid relationships that impair — or may appear to impair — OWASP's objectivity and independence.

Projects

- 118 Projects
  - Guidance
  - Books
  - Tools
- Project Leaders Wanted
  - Translate Everything



OWASP GLOBAL COMMITTEES

Projects	Membership	Education	Conferences	Industry	Chapters	Connections
- Jason Li - Brad Causey - Pravir Chandra - Leo Cavallari	- Dan Cornell - Michael Coates - Stephen Craig Evans	- Kuai Hinjosa - Martin Knobloch - Mano Paul - Eduardo Neves - Cecil Su - Fabio Cerullo - Andrzej Targosz - Sebastien Gioria - Nishi Kumar	- Mark Bristow - Lucas Ferreira - John Wilander	- Colin Watson - Lorna Alamri - Joe Bernik - Rex Booth - David Campbell - Alexander Fry - Georg Hess - Eoin Keary - Yiannis Pavlosoglou See also: - Special Interest Groups - OWASP India Advisory Board	- going through committee reset	- Lorna Alamri - Robert Hansen - Justin Clarke - Jim Manico

Board of Directors

- Eoin Keary – Ireland
- Dave Wichers – USA, Maryland
- Tom Brennan – USA, NYC
- Dinis Cruz – Europe – London
- Jeff Williams – USA, Maryland
- Sebastian Deleersnyder – Europe, Belgium
- Matt Tesauro – USA, Texas

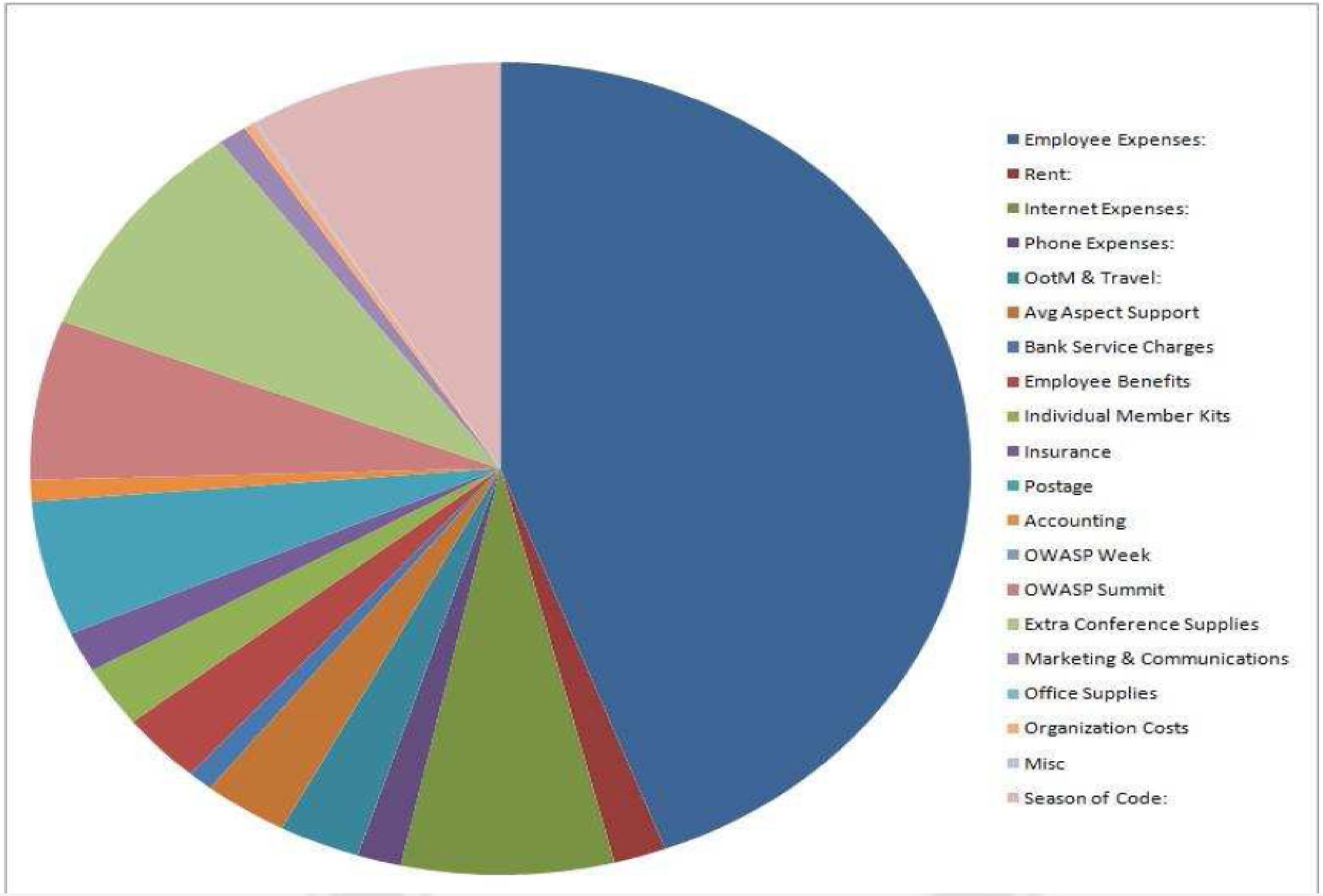
Governed by 100% volunteer members

Paid Employees

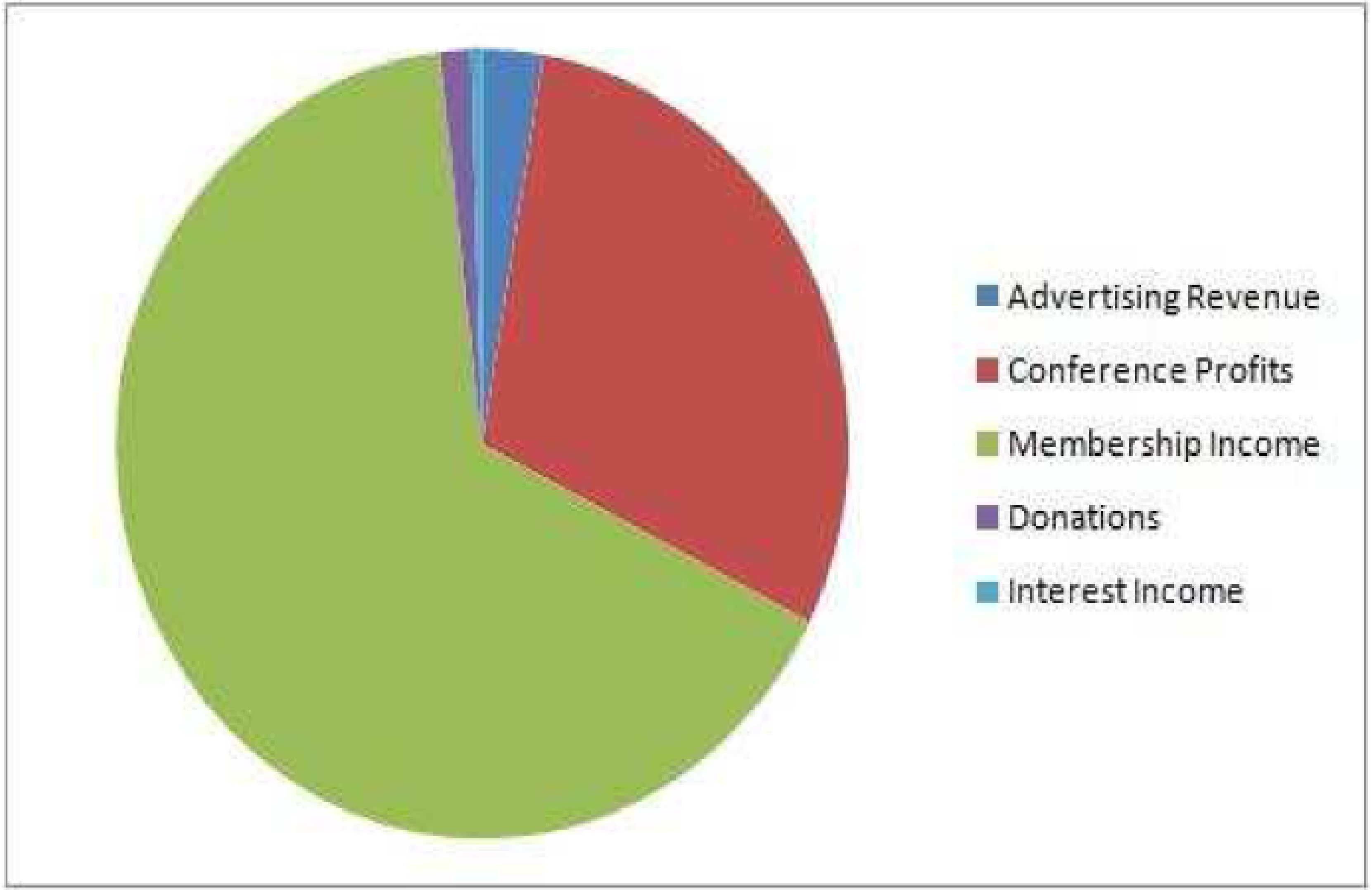
- OWASP Operations Director
  - Kate Hartman
- OWASP Project Manager
  - Paulo Coimbra
- OWASP Accounting
  - Alison Shrader

OWASP Foundation 2009 Financials

2009 Expenses $299,445.04



2009 Income $204,089.21

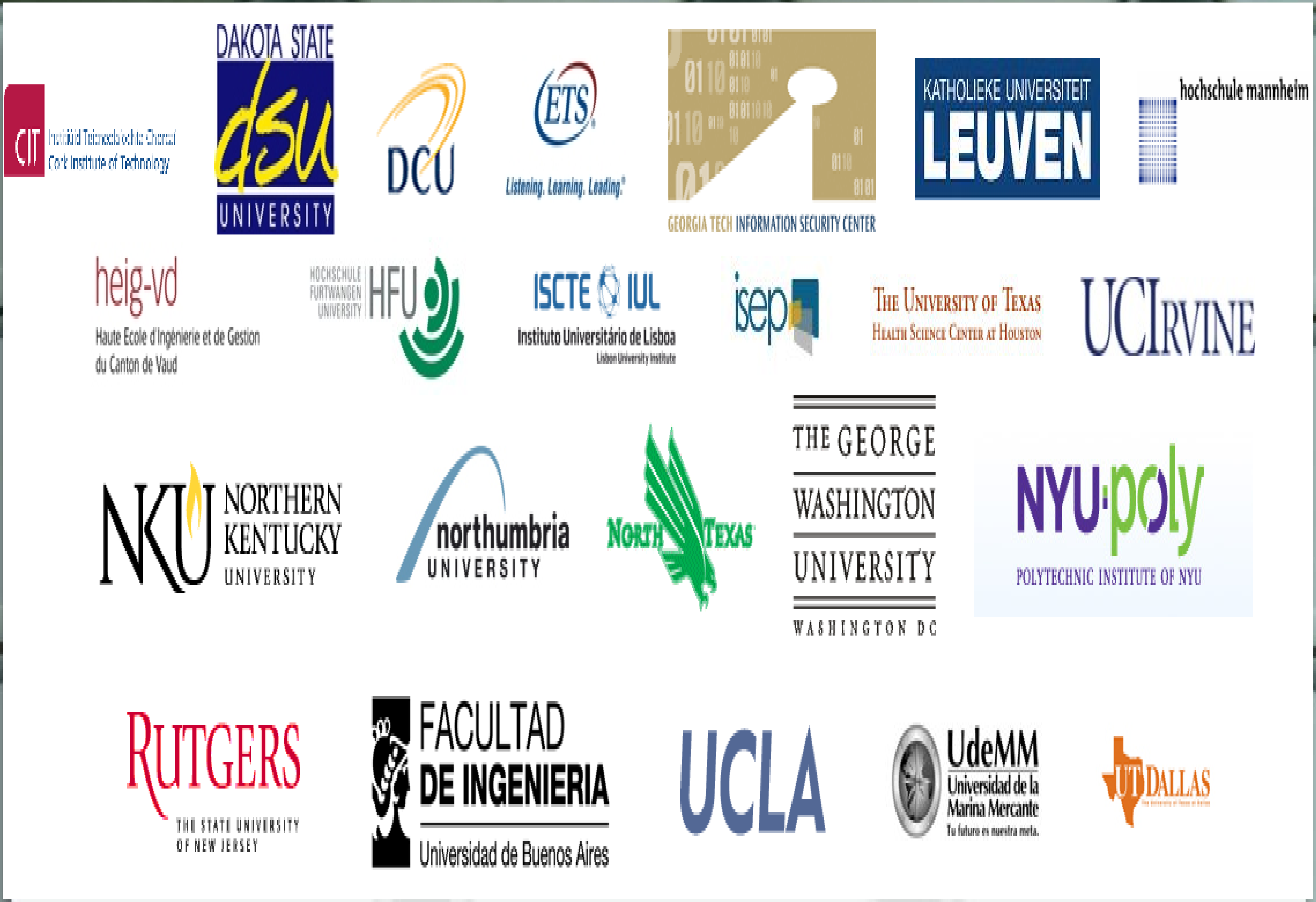


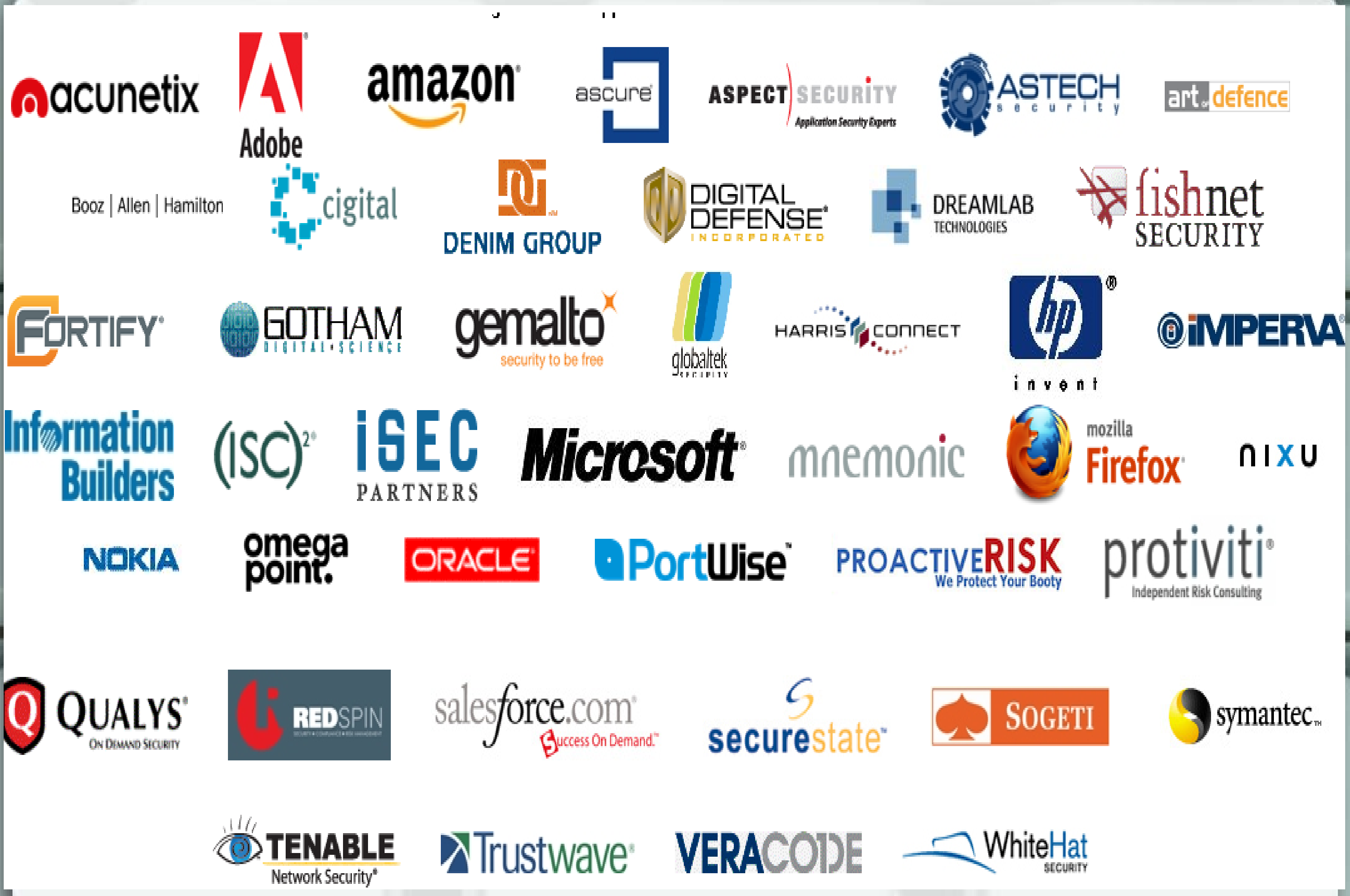
F
J

OWASP SUMMIT

Join OWASP

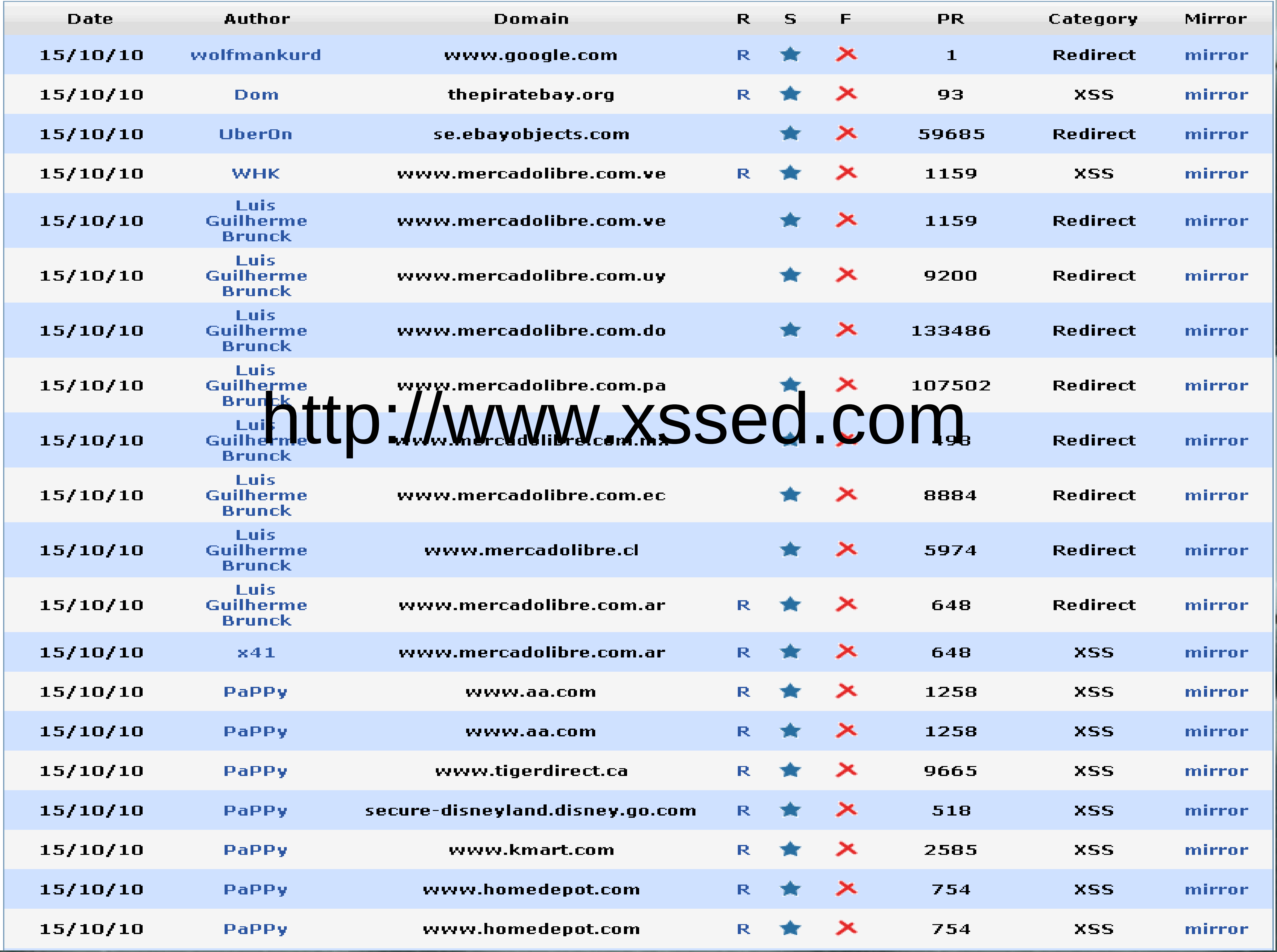
- Become a member
- Request a @owasp.org email address
- Join mailing lists for projects/efforts
- Contribute
- Support local chapter efforts


CIT
Instititiúid Teicneolaíochta Chorcaí
Cork Institute of Technology
DAKOTA STATE
dsu
UNIVERSITY
DCU
ETS
Listening. Learning. Leading.
GEORGIA TECH INFORMATION SECURITY CENTER
KATHOLIEKE UNIVERSITEIT
LEUVEN
hochschule mannheim
heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud
HOCHSCHULE FURTWANGEN UNIVERSITY
HFU
ISCTE IUL
Instituto Universitário de Lisboa
Lisbon University Institute
isep
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
FACULTAD DE INGENIERIA
Universidad de Buenos Aires
UCLA
UdeMM
Universidad de la Marina Mercante
Tu futuro es nuestra meta.
UT DALLAS


acunetix
Adobe
amazon
ascure
ASPECT SECURITY
Application Security Experts
ASTECH security
art of defence
Booz | Allen | Hamilton
cigital
DENIM GROUP
DIGITAL DEFENSE INCORPORATED
DREAMLAB TECHNOLOGIES
fishnet SECURITY
FORTIFY
GOTHAM DIGITAL SCIENCE
gemalto
security to be free
globaltek SECURITY
HARRIS CONNECT
hp
invent
IMPERVA
Information Builders
(ISC)²
iSEC PARTNERS
Microsoft
mnemonic
mozilla Firefox
NIXU
NOKIA
omega point.
ORACLE
PortWise
PROACTIVERISK
We Protect Your Booty
protiviti
Independent Risk Consulting
QUALYS
ON DEMAND SECURITY
REDSPIN
salesforce.com
Success On Demand.
securestate
SOGETI
symantec.
TENABLE
Network Security
Trustwave
VERACODE
WhiteHat SECURITY

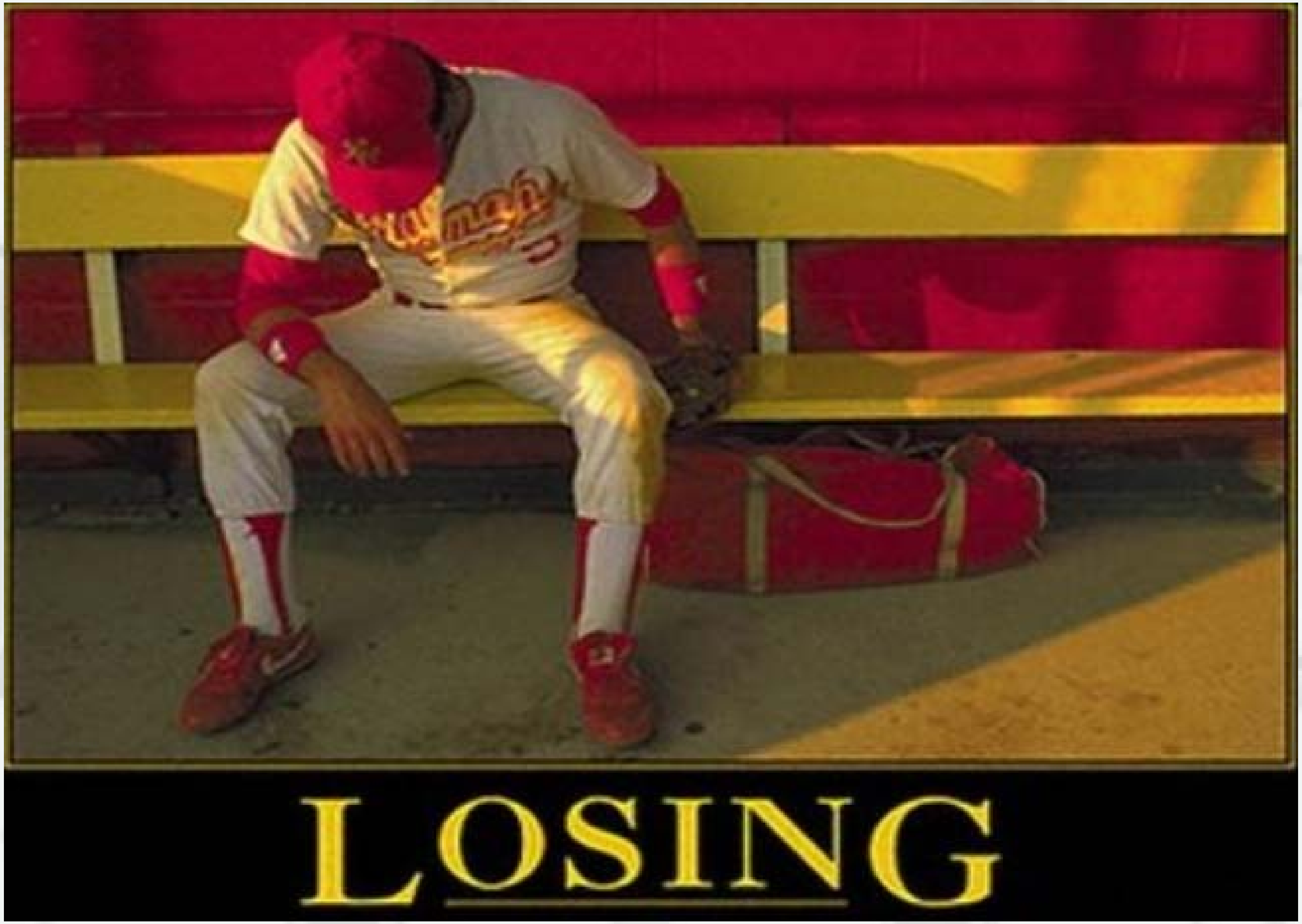
http://www.google.com/search?btnI&q=allinurl:http://www.proactiverisk.com/

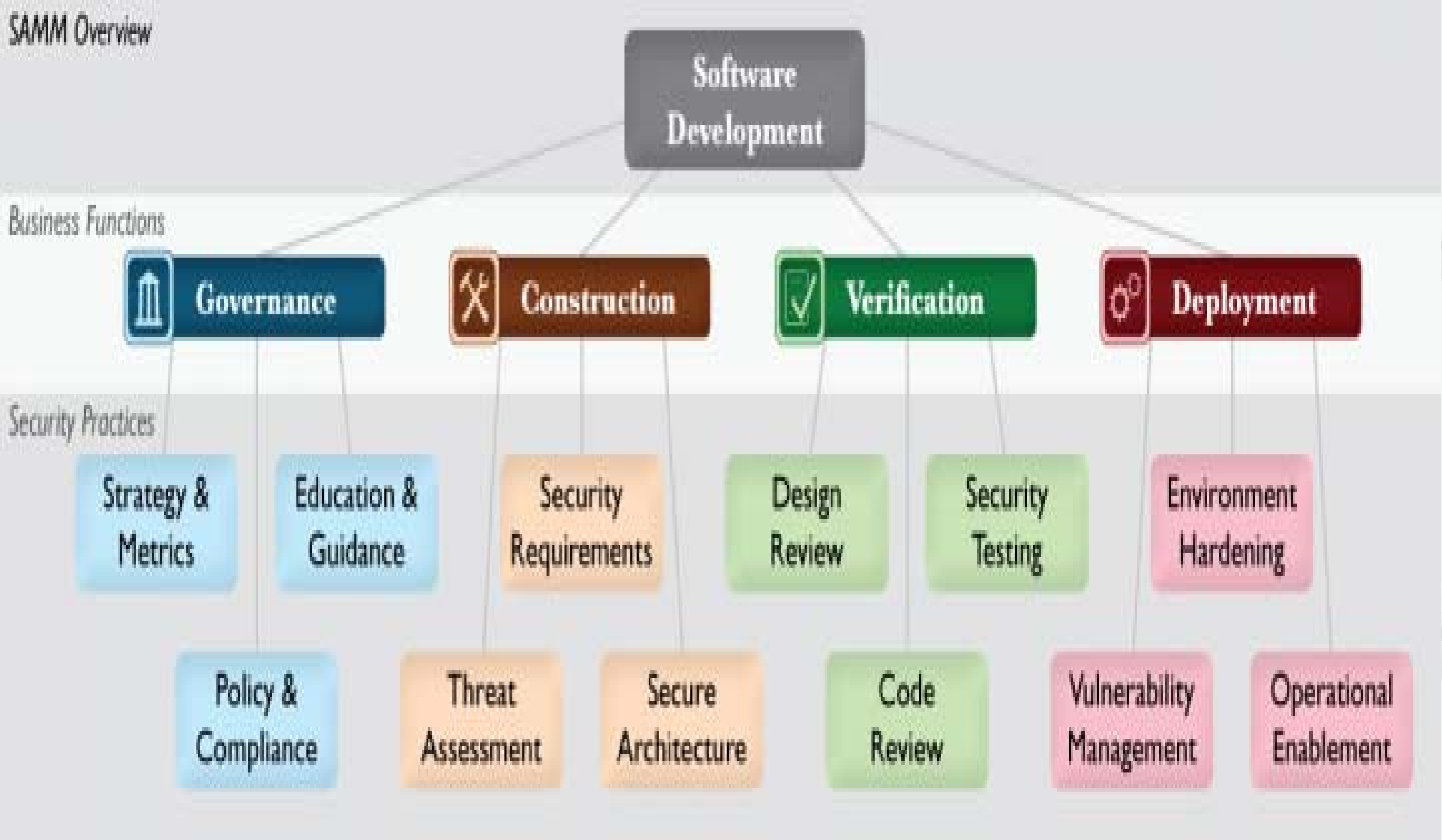
http://www.kmart.com/shc/s/s_10151_10104_Bed+%26+Bath_Bedding_Pillows--%3E%3Cimg%20src=x%20onerror=%22alert(1);%22%3E#viewItems=21&pageNum=1&sortOption=SALE_HIGH_TO_LOW&&filter=Brand|Cannon|Essential+Home|Joe+Boxer%22%3E%3C/a%3Etest|Abbey+Hill&lastFilter=Brand?adCell=A2



Date	Author	Domain	R	S	F	PR	Category	Mirror
15/10/10	wolfmankurd	www.google.com	R	★	✗	1	Redirect	mirror
15/10/10	Dom	thepiratebay.org	R	★	✗	93	XSS	mirror
15/10/10	Uber0n	se.ebayobjects.com		★	✗	59685	Redirect	mirror
15/10/10	WHK	www.mercadolibre.com.ve	R	★	✗	1159	XSS	mirror
15/10/10	Luis Guilherme Brunck	www.mercadolibre.com.ve		★	✗	1159	Redirect	mirror
15/10/10	Luis Guilherme Brunck	www.mercadolibre.com.uy		★	✗	9200	Redirect	mirror
15/10/10	Luis Guilherme Brunck	www.mercadolibre.com.do		★	✗	133486	Redirect	mirror
15/10/10	Luis Guilherme Brunck	www.mercadolibre.com.pa		★	✗	107502	Redirect	mirror
15/10/10	Luis Guilherme Brunck	www.mercadolibre.com.mx		★	✗	498	Redirect	mirror
15/10/10	Luis Guilherme Brunck	www.mercadolibre.com.ec		★	✗	8884	Redirect	mirror
15/10/10	Luis Guilherme Brunck	www.mercadolibre.cl		★	✗	5974	Redirect	mirror
15/10/10	Luis Guilherme Brunck	www.mercadolibre.com.ar	R	★	✗	648	Redirect	mirror
15/10/10	x41	www.mercadolibre.com.ar	R	★	✗	648	XSS	mirror
15/10/10	PaPPy	www.aa.com	R	★	✗	1258	XSS	mirror
15/10/10	PaPPy	www.aa.com	R	★	✗	1258	XSS	mirror
15/10/10	PaPPy	www.tigerdirect.ca	R	★	✗	9665	XSS	mirror
15/10/10	PaPPy	secure-disneyland.disney.go.com	R	★	✗	518	XSS	mirror
15/10/10	PaPPy	www.kmart.com	R	★	✗	2585	XSS	mirror
15/10/10	PaPPy	www.homedepot.com	R	★	✗	754	XSS	mirror
15/10/10	PaPPy	www.homedepot.com	R	★	✗	754	XSS	mirror

http://www.xssed.com


LOSING



SAMM Overview

Software Development

Business Functions

Governance

Construction

Verification

Deployment

Security Practices

Strategy & Metrics

Education & Guidance

Policy & Compliance

Security Requirements

Threat Assessment

Secure Architecture

Design Review

Security Testing

Code Review

Environment Hardening

Vulnerability Management

Operational Enablement

Final Thoughts

- Software is simultaneously getting radically more critical, complex, and interconnected. This creates a perfect storm for attackers, who are having a field day with our systems.
- We will never hack our way secure. Instead, we need to change the way we think about software, build software, and buy software.
- OWASP's audacious goal is to reach all developers everywhere and help them build rugged code - because our future depends on it – how will you help us?

Danke

谢谢您

Thank You

tomb@owasp.org