Project a Secure Web 2.0

perform a proper Risk Analysis
adopt a secure WCMS (like Drupal)

Paolo Ottolino CISSP-ISSAP CISA CISM OPST ITIL PMP
paolo.ottolino (at) isc2chapter-italy.it

September 27th, 2016

Agenda

1. Web 2.0 and Security

2. WCMS Cyber Risk

3. Drupal Security

Agenda

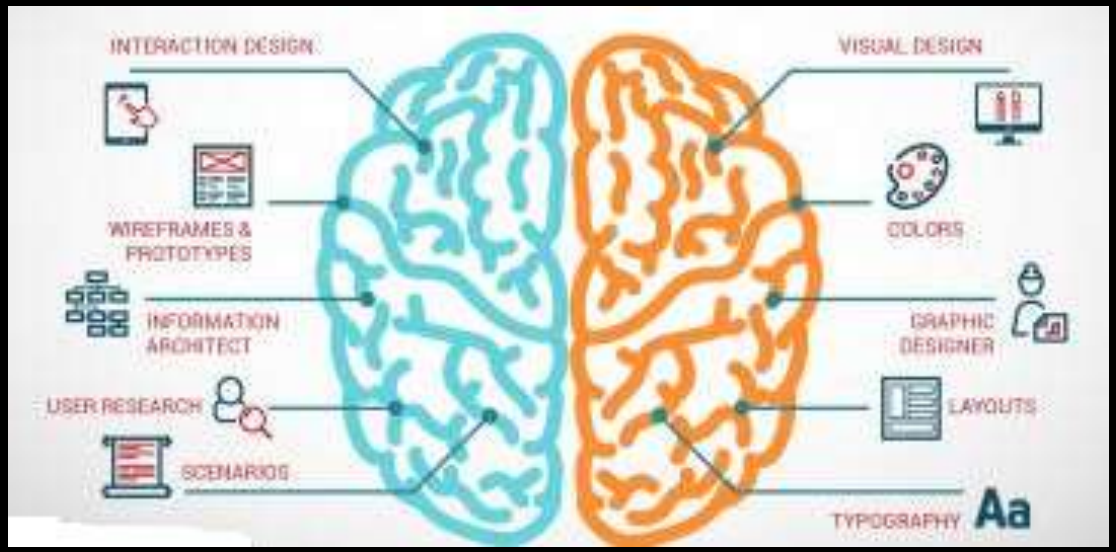
1. Web 2.0 and Security

Web 2.0: Continous Interaction

From Navigation to Inquiry

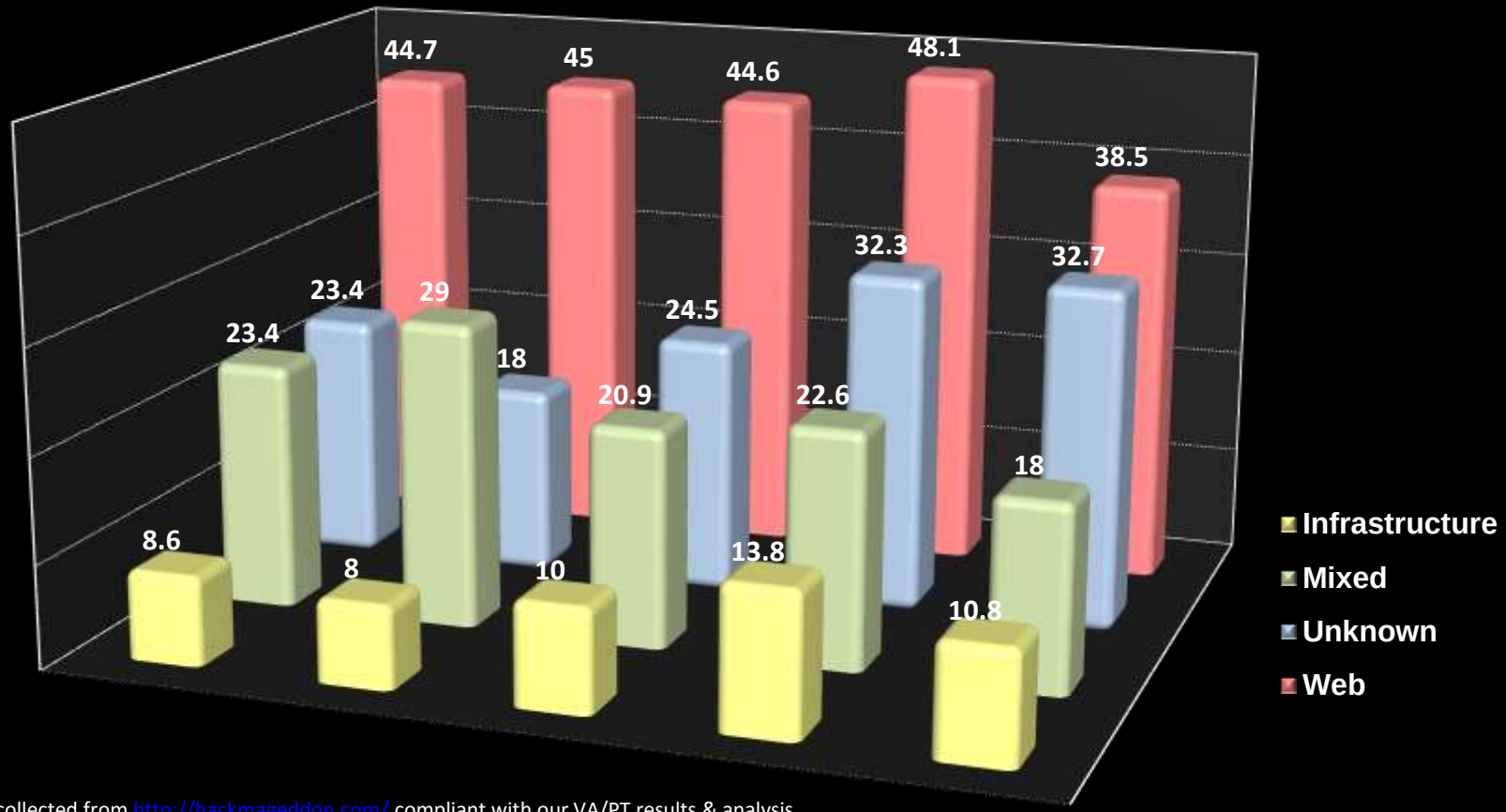
UX: User eXperience

UI: User Interface



UA: User Application

Web 2.0: Insecure by Design?



Data collected from http://hackmageddon.com/ compliant with our VA/PT results & analysis.

The most part of exploits come from Web 2.0 components. Infrastructural ones are residual.

Web 2.0: Cyber Threats

Principal Goals

- **Crime**: immediate economic advantage

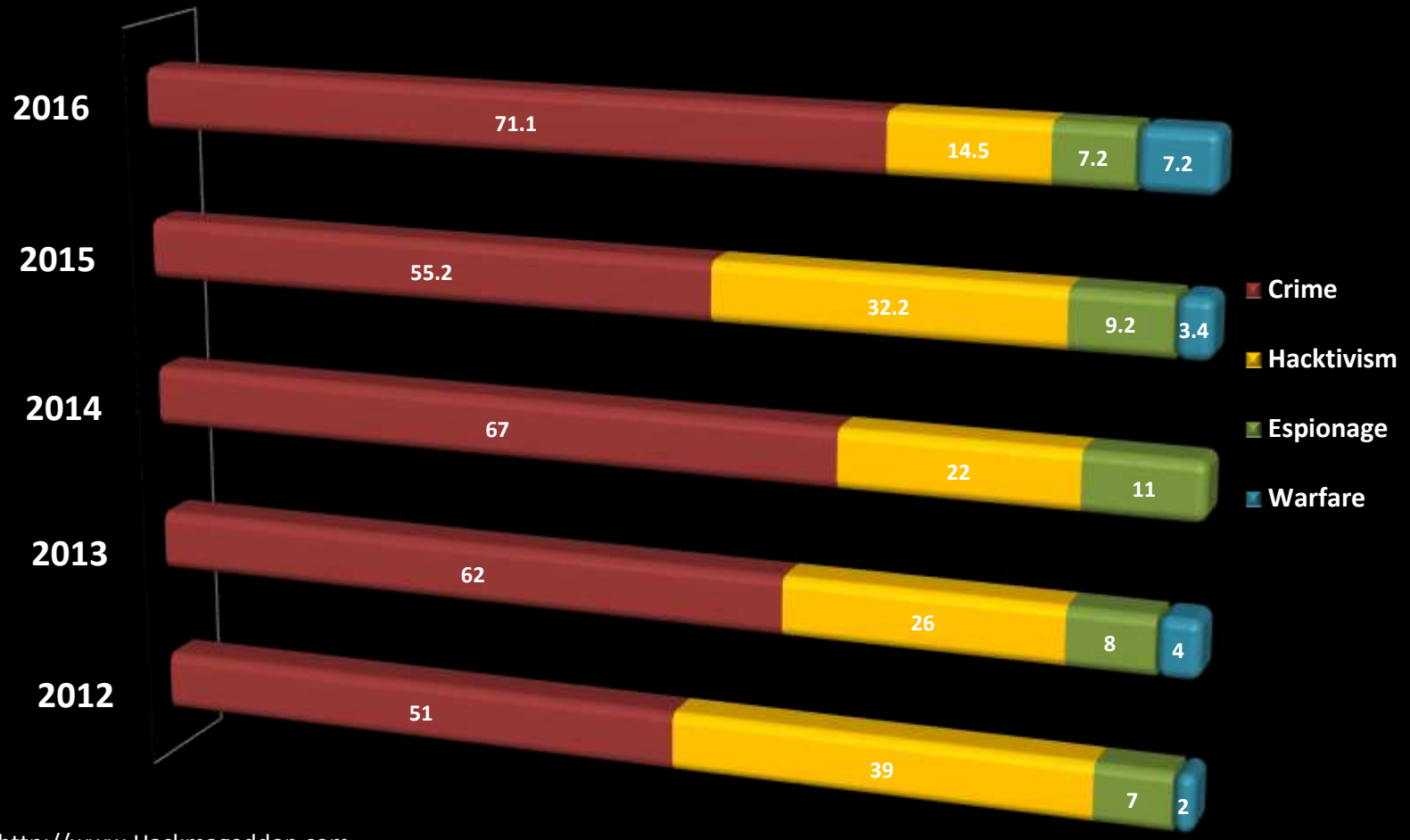
- **Hacktivism**: social and political objectives

- **Espionage**: industrial information stoling

- **Warfare**: war battles among states

Web 2.0: Cyber Threats

Percentage Composition



source: http://www.Hackmageddon.com

Web 2.0: Cyber Risks

Exploiting, Profiteering, Wasting

- **Intruding**: access system in order to harvest information

- **Damaging**: make the system unaccessible from anyone

- **Profiteering**: access to system, in order to take advantage from elaboration and network capacities (to 3° parties)

Web 2.0: Risks-Threats

Mapping Agents (examplification)

	 **Crime**	 **Hacktivism**	 **Warfare**	 **Espionage**
 **Intruding**	Stole Money Read User-Info	Stoling Info	Stole Info	Stole Info
 **Damaging**	DDoS (competitors)	Defacement	Break System	
 **Profiteering**	Spam DDoS (3° party)			

Web 2.0: Risks-Threats

Mapping Agents (exemplification)

	Average	Web Service	Risks
 **Crime**	61%	Web-Banking e-Commerce Social Collaboration Communication (email, instant message system, etc)	Intruding Damaging Profiteering
 **Hacktivism**	27%	Government (Central, Local) Information System (news, TV)	Intruding Damaging
 **Espionage**	8%	Collaboration	Intruding

Agenda

2. WCMS Risk Evaluation

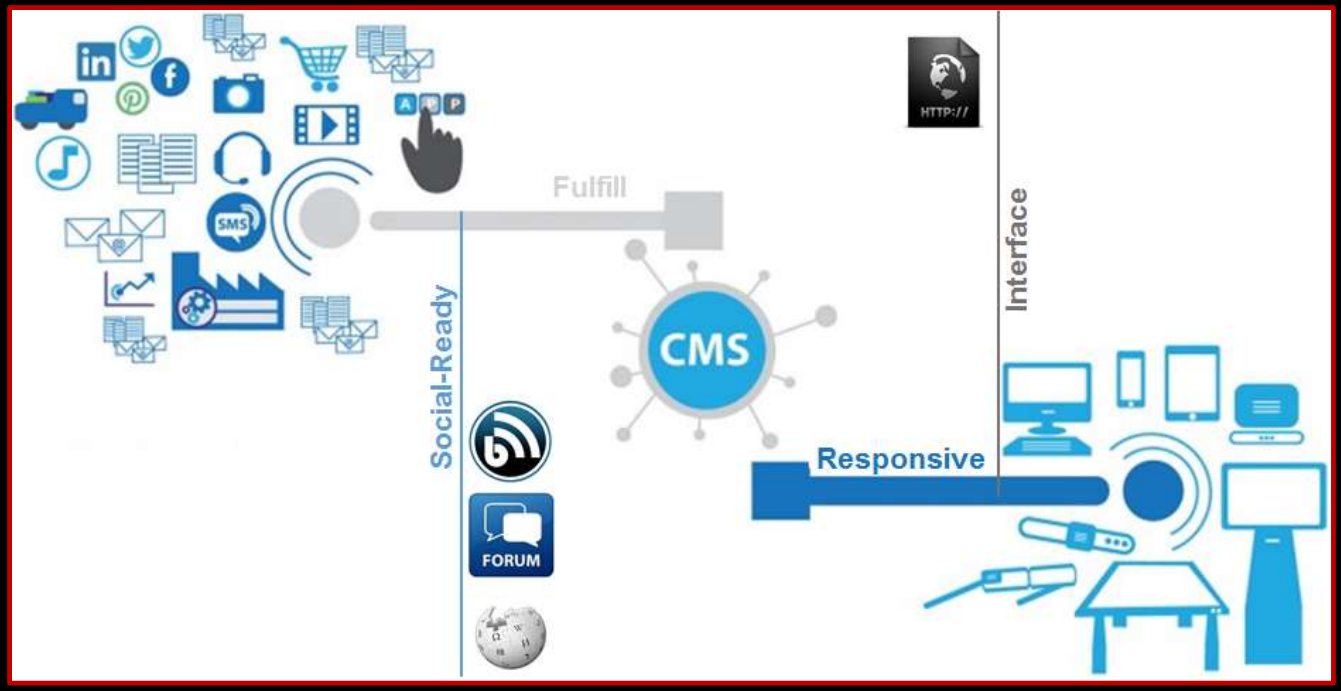
WCMS: Logical Architecture

The most part of vulnerable

Web 2.0 sites are built around a

Content Management System.

(WCMS)

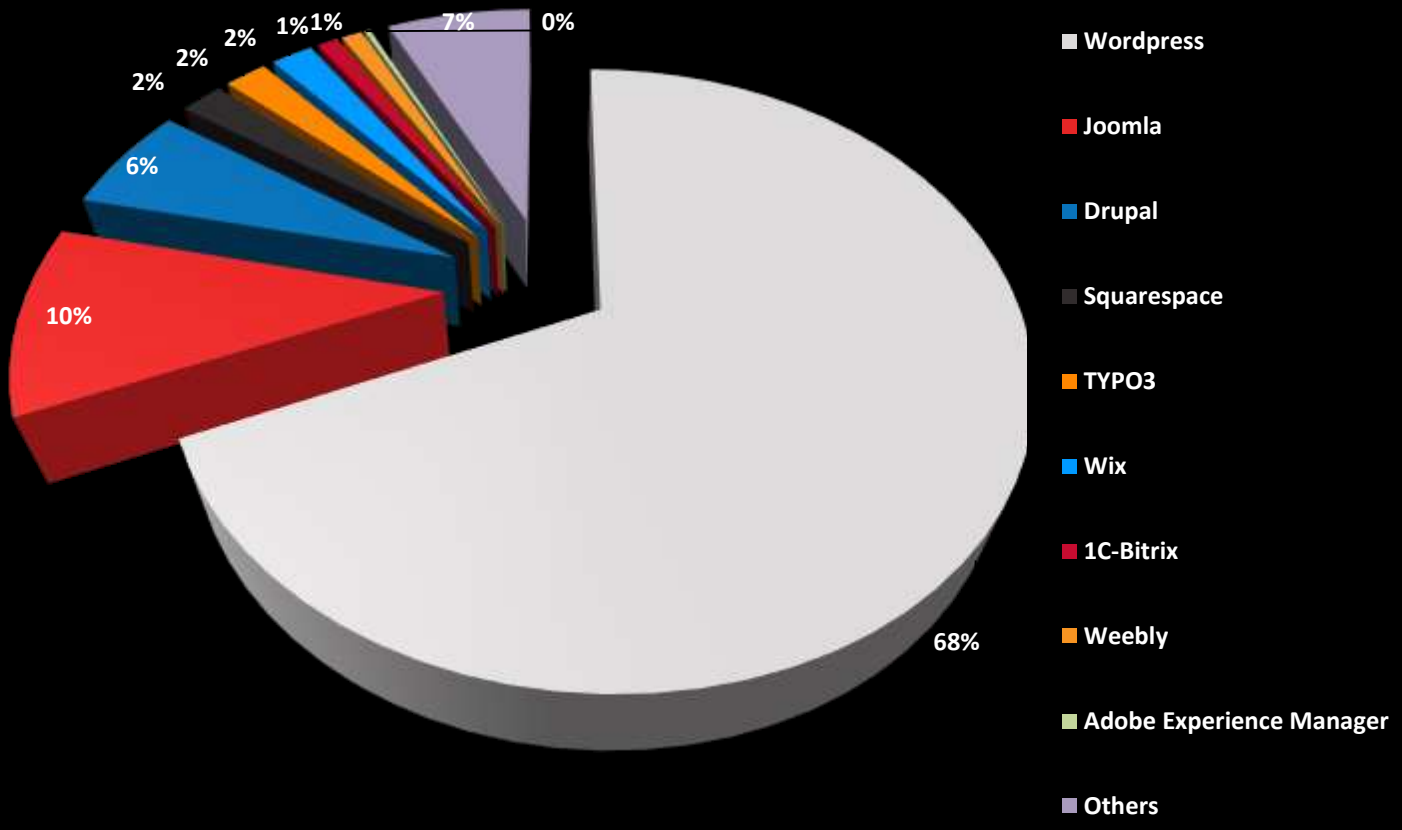


The CMS offers a new web experience:

- **Same same**: unique interface for all the site-operations (read/write, conf, etc)
- **But different**: separation between the content and how it is shown to the user

WCMS: the Top 3 used products

Global Market Share: The current market leader is WordPress (according to wappalizer.com)

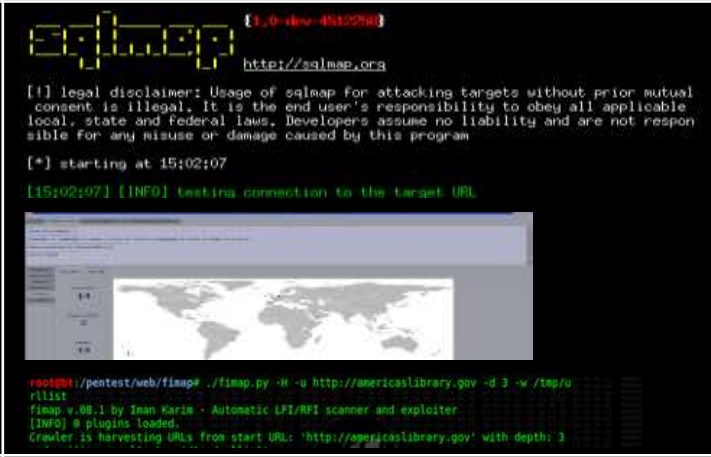


(*) SaaS managed: Squarespace, Wix, 1C-Bitrix, Weebly

WCMS: Functionalities

Function	WordPress	Joomla!	Drupal
Time to Market			
Usage Easiness			
Huge Community			
Themes and Layouts			
Plug-ins and Modules			
Social Network			
SEO Oriented			
Content Strategy/Org.			
Completeness, Powerness			
Workflow			
Security			

WCMS: Security Hacking

	Classic IT Attack	Web Attack	Web Tool	
Information Gathering "pre" phase: harvesting information	Footprinting: identify target domain and info Scanning: detect the actual infrastructure Enumerating: individuate running version	Harvest information, matching with vulns DB	Wappalizer http://www.BuiltWith.com	 built with
Attack Exploitation "go" phase: the action	Gaining Access: entering the CMS, executing cmd Escalating Privilege: gaining more powerness Pilfering: harvesting information	Starting Attack	SQLmap Nmap XSSer FImap	
Hide & Return	Post Fase	Post Fase		

WCMS: OWASP

Open Web Application Security Project

Started on September 9, 2001 by Mark Curphey, it is an online community dedicated to Web Application Security. OWASP works for creating freely-available materials. The most useful ones are:

- **OWASP Top Ten** (article): awareness about application security by identifying most critical vulnerabilities, on a 3 years basis

- **OWASP Development Guide** (doc): practical guidance with coding examples. It covers an extensive array of application-level security issues (not only Top10)
- **OWASP Testing Guide** (methodology): "best practice" penetration testing framework + "low level" penetration testing guide
- **OWASP Code Review Guide** (methodology): a key enabler for the OWASP fight against software insecurity
- **WebScarab** (tools) web security application testing tool (acting as a proxy)
- **Enterprise Security API** (technology): free, open source, web application security control library for writing lower-risk applications

WCMS: Vulnerabilities

OWASP Top10

Published every on a 3-years interval (2007, 2010, 2013, …), it resumes the most important web application security concerns

A1 – Injection (e.g. SQL)

A2 – Broken Authentication and Session Management

A3 – Cross-Site Scripting (XSS)

A4 – Insecure Data Object Reference

A5 – Security Misconfiguration

A6 – Sensitive Data Exposure

A7 – Missing Function Level Access Control

A8 – Cross-Site Request Forgery (CSRF)

A9 – Using Component with Known Vulnerabilities

A10 – Unvalidated Redirects and Forwards

WCMS: Vulnerabilities

OWASP Top10

Risk	Threat	Final Goal	Attack Example	OWASP Vulnerability
Intruding	Crime Hacktivism Espionage	Harvest Data/Money	Pharming Click-Jacking	A1 (Inj) A3 (XSS) A4 (Ins Obj Ref) A6 (Sens Data) A8 (CSRF) A10 (Unv Red/Fwd) A9 (Known Vulns)
Damaging	Crime Hacktivism	Destroy Reputation	DoS DDoS (3° p.ty)	A9 (Known Vulns) A2 (Brk Auth/Session)
Profiteering	Crime	Gain Access	DoS Dox(x)ing	A5 (Sec Misconf) A7 (Func ACL)

WCMS: Risk Strategy

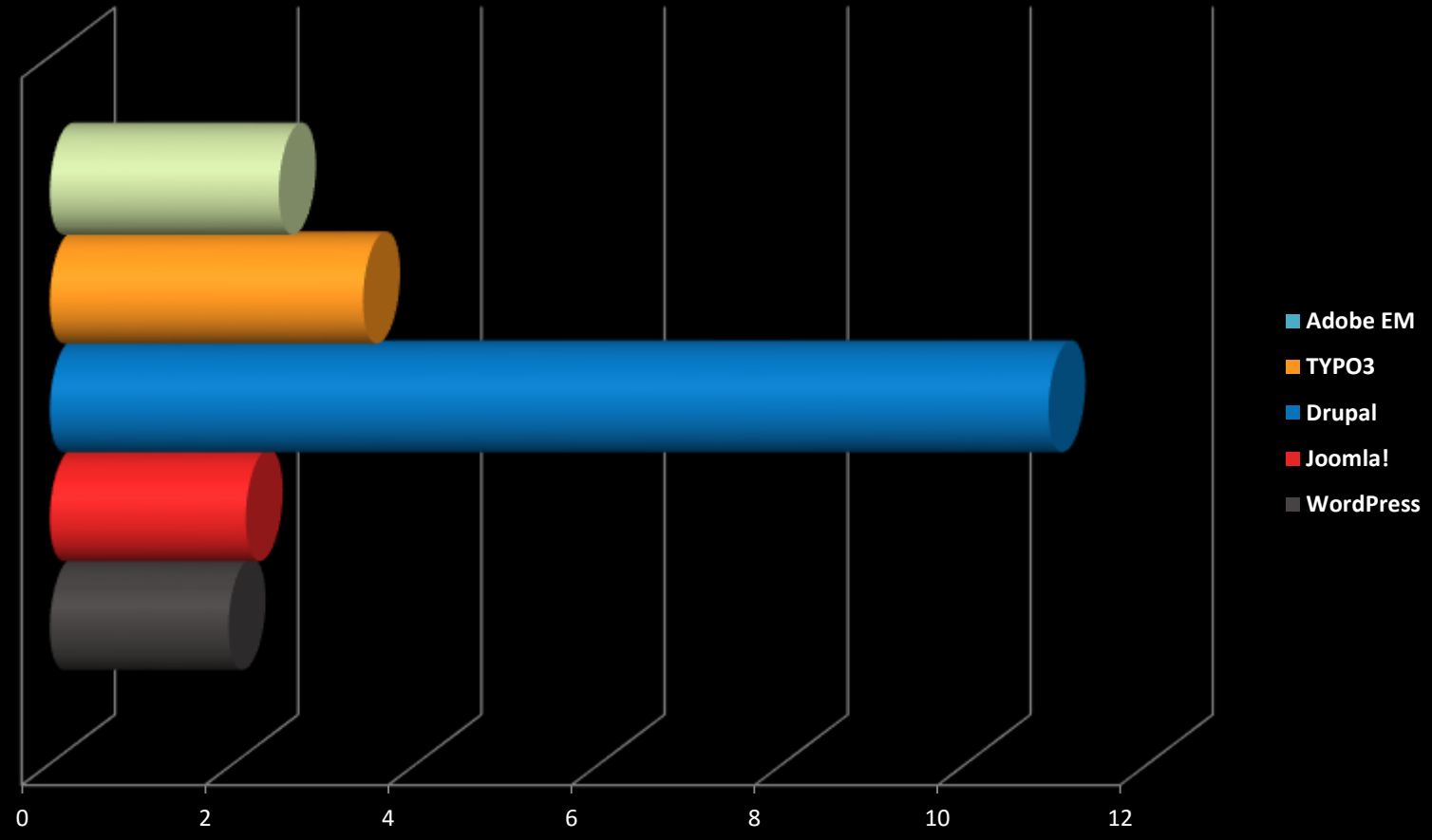
DevOps Security Approach

Risk	Dev	Ops
Intruding	A2. Injection: Filter	
	A3. XSS: Filter	
	A4. Object Reference: File Access	
	A6. Data Exposure: File Access	A6. Data Exposure: File Permission Check
	A8. CSRF: Filter	
	A10. Unv Ref/Fwd: Filter	A10. Unv Ref/Fwd (no HTML permissions)
		A9. Known Vulns: Patching
Profiteering Damaging		**A9. Known Vulns: Patching**
		A5. Sec Misconfiguration: Hardening
		A7. Function Access: ACL periodic check
		A2. Broken Auth: SSL

WCMS: Known Vulns (A9)

Patching Rate

Amount of upgrades between 2 high rate vulnerabilities, in the average



Source: http://www.vulnerabilitycenter.com

Agenda

3. Drupal Security

Drupal: Risk Strategy

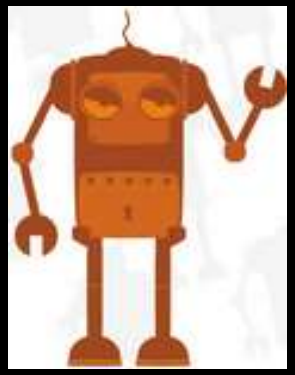
DevOps Security Approach

Risk	Dev	Ops
Intruding	A1. Injection: Filter	
	A3. XSS: Filter	
	A4. Object Reference: File Access	
	A6. Data Exposure: File Access	A6. Data Exposure: File Permission Check
	A8. CSRF: Filter	
	A10. Unv Ref/Fwd: Filter	A10. Unv Ref/Fwd (no HTML permissions)
		A9. Known Vulns: Patching
Profiteering Damaging		A9. Known Vulns: Patching
		A5. Sec Misconfiguration: Hardening
		A7. Function Access: ACL periodic check
		A2. Broken Auth: SSL

- Covered by safe configuration of Drupal
- Covered by frequent update of Drupal
- Covered by proper Drupal API usage
- Covered by periodic maintenance of Drupal

Drupal: Keeping Secure

Drupal Actors



Security Team

global group of the world's leading web security expert, always on-call to assess, evaluate and address issues affecting security in Drupal components.

Project Mantainers

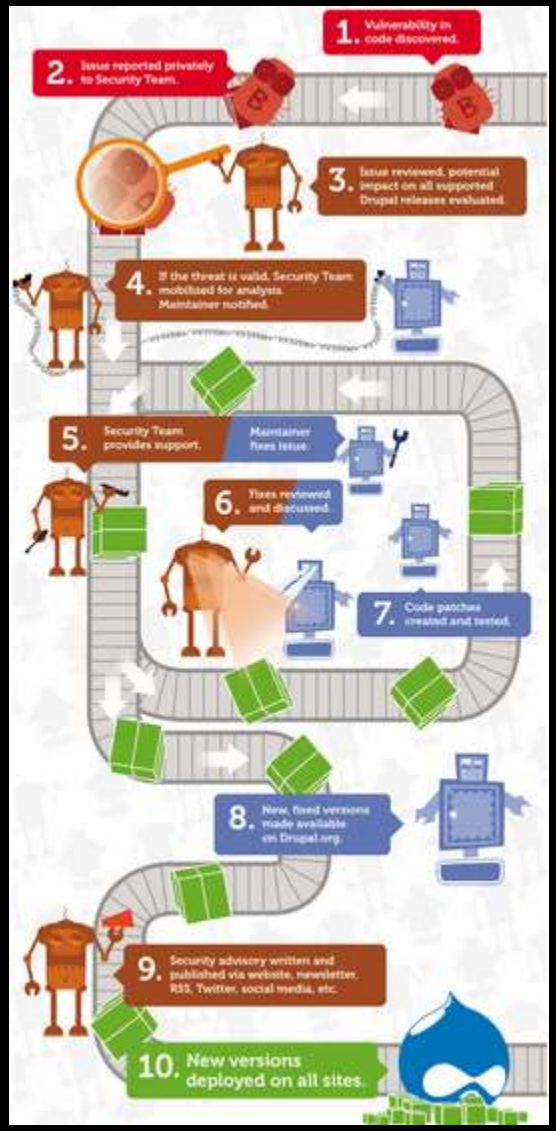
Active developer's community (15.000+), including strong experts in today web technology. Different mantainers are responsible for different plug-in modules and Drupal core

Drupal Users

70.000+ people running 1M+ websites. They run, test and improve Drupal day-to-day. New vulnerabilities are quickly identified and confidentially reported to Security Team

Drupal: Keeping Secure

Drupal Process



1. Discover **Vulnerability**
2. Report **Issue**
3. Evaluate **Impact**
4. Mobilized **Security Team** / **Mantainer**
5. Issue **Fix**
6. Performe **Review**
7. Create **Patch**
8. Fix **Version**
9. Write **Advisory**
10. Deploy **Version**

Drupal: UK and EU Org & Biz using

Company	Sector	URL	Country
CERN	Research	http://home.web.cern.ch/	CH
World Food Programme	Government	http://www.wfp.org/	ONU
Prince of Wales	Government	http://www.princeofwales.gov.uk/	UK
UK PS Data	Government	http://data.gov.uk	UK
British Council	Government	http://www.britishcouncil.org/	UK
Cambridge	University	http://www.cam.ac.uk/	UK
Oxford	University	http://www.ox.ac.uk/	UK
Virgin	Private	http://www.virgin.com/	UK
Agenzia Spaziale Italiana	Government	http://www.asi.it/	IT
Ministero degli Interno	Government	http://www.interno.gov.it/	IT
Agenzia per l'Italia Digitale	Government	http://www.agid.gov.it/	IT
Avvocatura dello Stato	Government	http://www.avvocaturastato.gov.it/	IT
Dati della PA	Government	http://www.dati.gov.it/	IT
Sapienza	University	http://uniroma1.it/	IT
CIS	University	http://www.cis.uniroma1.it/	IT
LUISS	University	http://www.luiss.it/	IT
LUMSA	University	http://www.lumsa.it/	IT

Drupal: also US is using

Company	Sector	URL	Country
NASA	Government	http://www.nasa.gov/	US
US-CERT	Government	https://www.us-cert.gov	US
WhiteHouse	Government	http://www.whitehouse.gov/	US
Department of Homeland Security	Government	http://www.dhs.gov/	US
Task Force on Childhood Obesity	Government	http://www.letsmove.gov/	US
US Department of Education	Government	http://www.ed.gov/	US
Harward	University	http://www.harvard.edu/	US
Michigan	University	http://www.egr.msu.edu/	US
Arizona	University	https://www.asu.edu/	US
CyberLaw Standford	University	http://cyberlaw.stanford.edu/	US
Cornell Library	University	https://www.library.cornell.edu/	US
Symantec Connect	Software	http://www.symantec.com/connect/	US
SkyBox	Software	https://www.vulnerabilitycenter.com	US
The Economist	NewsPaper	http://www.economist.com/	US
The Hill	NewsPaper	http://thehill.com/	US

"*Drupal powers twice as many federal government websites as every other CMS combined. That's more than six Drupal sites for every one WordPress*."

[Benjamin Balter, US E-Government and Federal IT Team, Executive Office of the President]

Thank You

Paolo Ottolino

PMP CISSP-ISSAP CISA CISM OPST ITIL

paolo.ottolino (at) isc2chapter-italy.it