

The background of the slide is a dark, textured world map. In the top right corner, there are two circular logos. The one on the left is a faint watermark that says "OFFICIAL (ISC) CHAPTER". The one on the right is a white stamp with a scalloped edge that says "(ISC)² CHAPTER ITALY".

Project a Secure Web 2.0 (using Drupal)

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

May XX, 2016

Agenda



Web 2.0 & CMS

CMS Cyber Risk

Drupal Security

Agenda



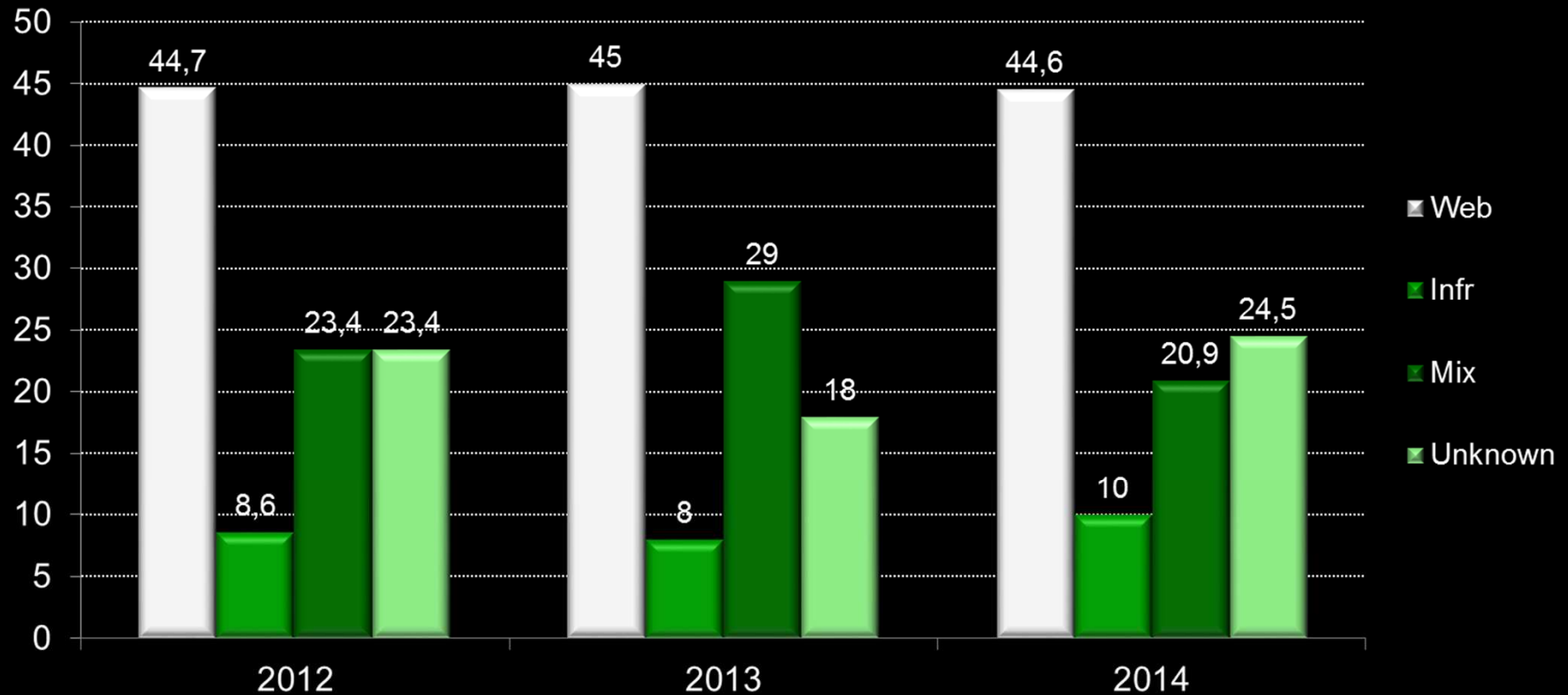
Web 2.0 & CMS

Needs, Functionalities, Selection

Web 2.0: Insecure by Design?



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



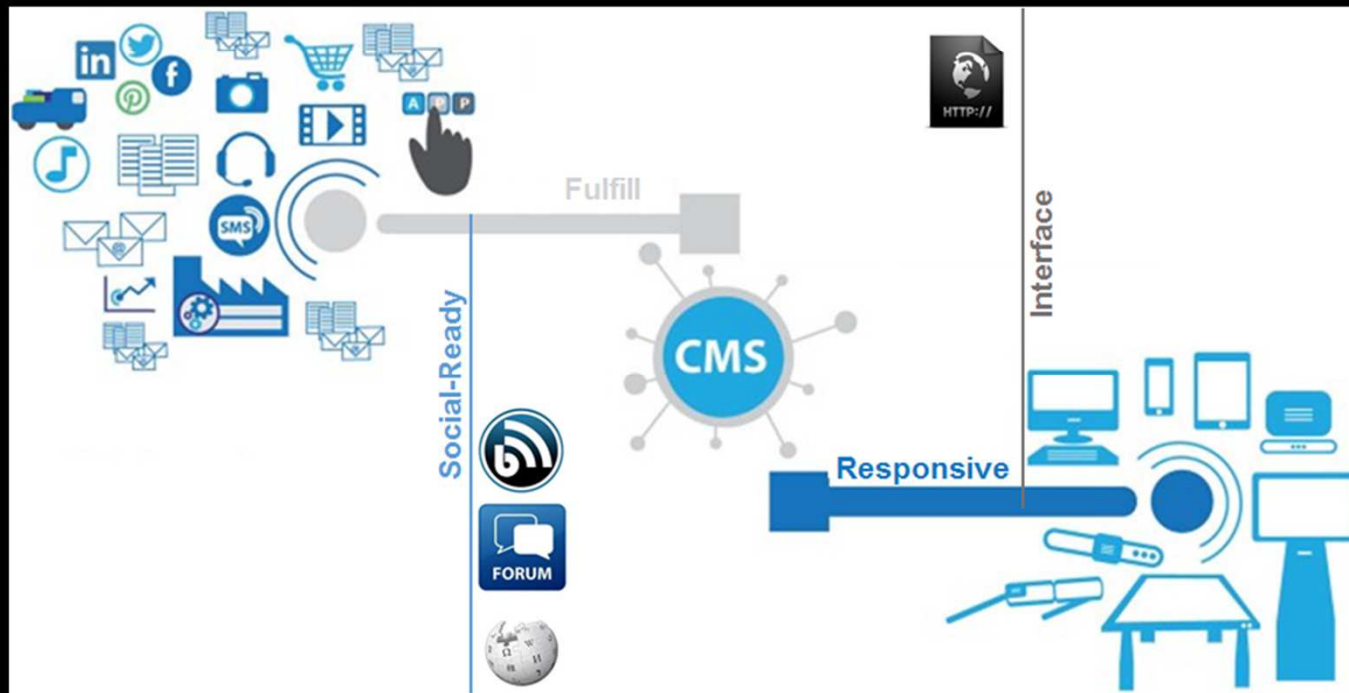
Data collected from <http://hackmageddon.com/> compliant with our VA/PT results & analysis.

Web 2.0 & CMS: Logical Architecture



The most part of vulnerable Web 2.0 sites are built around a **Content Management System**. The CMS offers a new web experience:

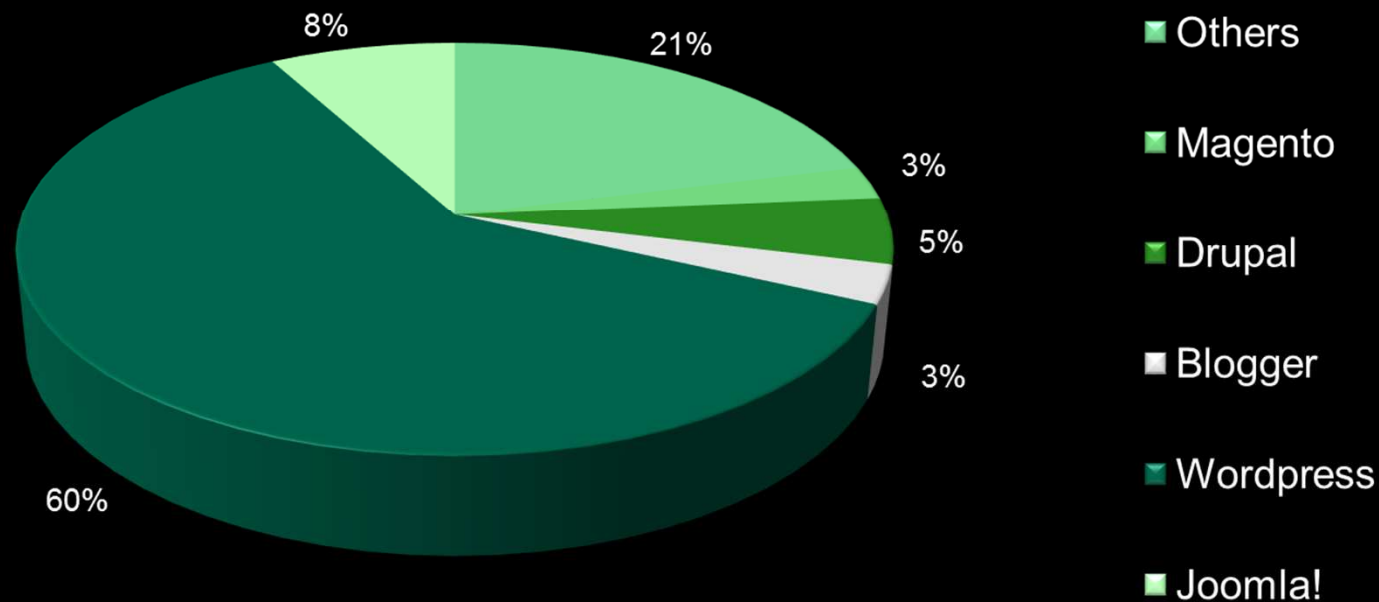
- **Same same**: unique interface for all the site-operations (reading, writing, configuring, etc)
- **But different**: separation between the content and how it is shown to the user



CMS Solution: Top 3 used products



CMS framework usage during 2014 (according to Webcom Websites). The Top 3 used products are: WordPress (60%), Joomla! (8%) and Drupal (5%)



Most wanted CMS Functionalities...



Function	WordPress	Joomla!	Drupal
Time to Market			
Usage Easiness			
Huge Community			
Themes and Layouts			
Plug-ins and Modules			
Social Network			

UK and EU Org & Biz use Drupal...



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

... but also US makes strong use of Drupal!



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
Harvard	University	http://www.harvard.edu/	US
Michigan	University	http://www.egr.msu.edu/	US
Arizona	University	https://www.asu.edu/	US
CyberLaw Stanford	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]

Full CMS 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			

Agenda



CMS Cyber Risk

Threats, Vulnerabilities, Countermeasures

CMS Threats: Security Hacking



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

CMS Vulnerabilities: 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

CMS 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

CMS Risks: Risk-Threat-Vulnerability Map



Risk	Threat	Final Goal	Attack Example	OWASP Vulnerability
Exploiting	Information Stoling	Harvest Data/Money	Pharming	A1 (Inj)
			Click-Jacking	A3 (XSS)
Profiteering	System Access	Gain Power	DDoS (3° p.ty)	A4 (Ins Obj Ref)
			DoS	A6 (Sens Data)
			Dox(x)ing	A8 (CSRF)
Wasting	DoS	Destroy Reputation		A10 (Unv Red/Fwd)
				A9 (Known Vulns)

CMS Risks: DevOps Security Strategy



Risk	Dev	Ops
Exploiting	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 Wasting		A9. Known Vulns: Patching
		A5. Sec Misconfiguration: Hardening
		A7. Function Access: ACL periodic check
		A2. Broken Auth: SSL

CMS Risks: DevOps Security Strategy



Risk	Dev	Ops
Exploiting	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 Wasting		A9. Known Vulns: Patching
		A5. Sec Misconfiguration: Hardening
		A7. Function Access: ACL periodic check
		A2. Broken Auth: SSL

Agenda



Drupal Security

Security DevOps, Keeping Secure, Drupal 8

Drupal Security DevOps Strategy



Risk	Dev	Ops
Exploiting	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)
Profiteering Wasting		A9. Known Vulns: Patching
		A9. Known Vulns: Patching
		A5. Sec Misconfiguration: Hardening
		A7. Function Access: ACL periodic check
		A2. Broken Auth: SSL

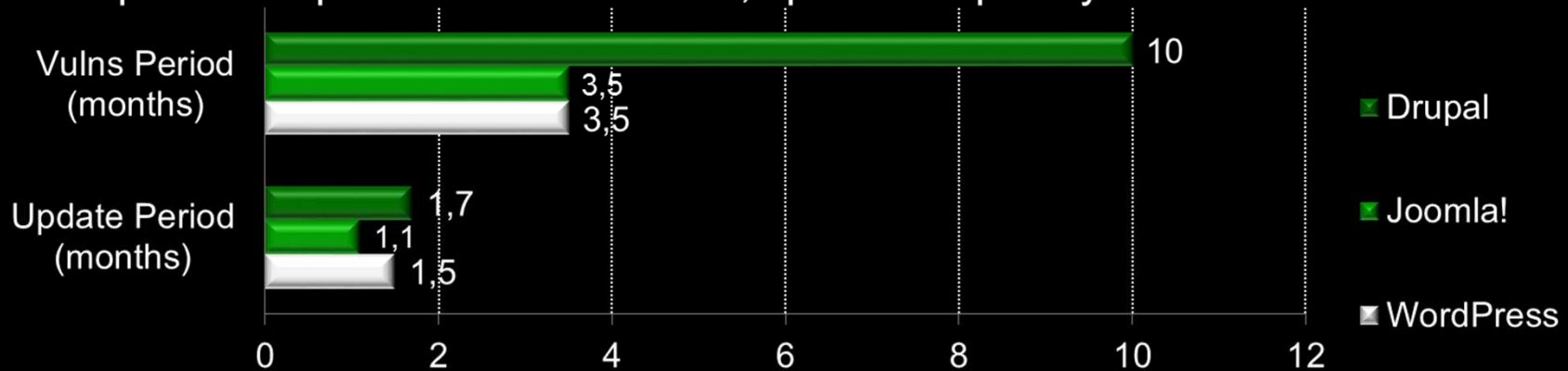
■ No more exploitable if Drupal is safely configured

■ Covered by proper Drupal API usage

Keeping Secure: CMS Patch Comparison



All the Top 3 used CMS products are OpenSource (GPLv2): a direct comparison is possible about #vulns, update frequency...



... and (most useful) update/vulns ratio: how many updates between 2 high vulns, in the average



Keeping Secure: Drupal actors (1/2)



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

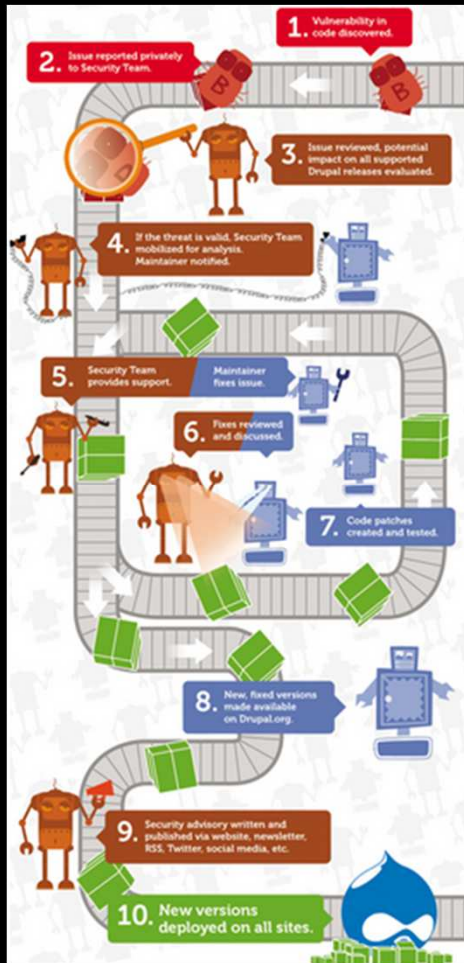
Active developer's community (15.000+), including strong experts in today web technology. Different mantainers are responsible for different plug-in modules and Drupal core



Drupal Users

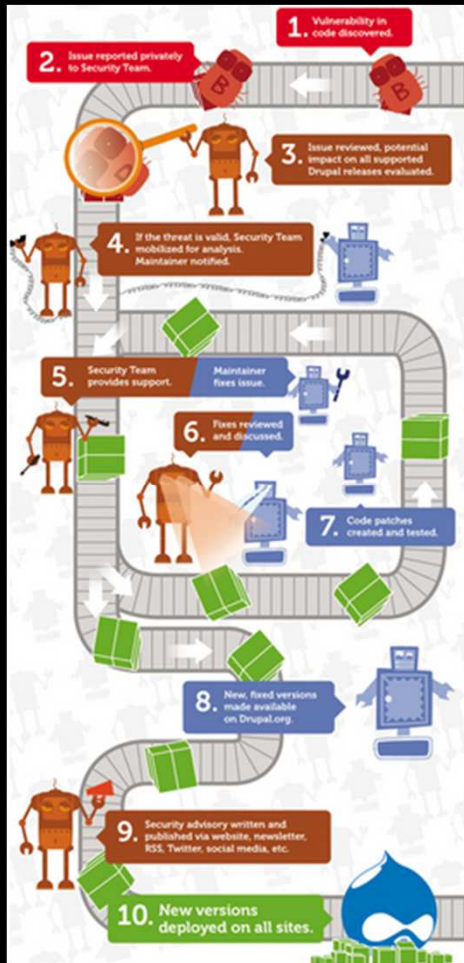
70.000+ people running 1M+ websites. They run, test and improve Drupal day-to-day. New vulnerabilities are quickly identified and confidentially reported to Security Team

Keeping Secure: Drupal process (2/2)



1. Discover **Vulnerability**
2. Reported **Issue**
3. Evaluated **Impact**
4. Mobilized **Security Team / Mantainer**
5. Issued **Fix**
6. Performed **Review**
7. Created **Patch**
8. Fixed **Version**
9. Written **Advisory**
10. Deployed **Version**




















Keeping Secure: Drupal process (2/2)



1. Discover **Vulnerability**
2. Reported **Issue**
3. Evaluated **Impact**
4. Mobilized **Security Team / Mantainer**
5. Issued **Fix**
6. Performed **Review**
7. Created **Patch**
8. Fixed **Version**
9. Written **Advisory**
10. Deployed **Version**

Drupal8: Cover the Lacking 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			

Drupal 8: Welcome Easiness!



Mobile in its DNA

Deploy content once and watch it display the way you want on any device



New Configuration Management

Transport configuration changes and manage versions with ease



Better User Experience

Leverage jQuery UI's autocomplete and modal dialogs



Effortless Authoring

Use the WYSIWYG editor and in-place editing



Better Markup with HTML5

Output elements and classes with native input tools for mobile



Accessibility Integration

support for standard accessibility technologies: WAI-ARIA and semantic HTML5

... and more.

Drupal is available since November 19th, 2015

The background features a dark, textured globe with a grid of latitude and longitude lines. In the upper right corner, there is a circular seal that reads "OFFICIAL (ISC)² CHAPTER" and a rectangular stamp that reads "(ISC)² CHAPTER ITALY".

Grazie

Paolo Ottolino

PMP CISSP-ISSAP CISA CISM OPST ITIL

paolo.ottolino (at) isc2chapter-italy.it