Planning the OWASP Testing Guide v4

Matteo Meucci, Giorgio Fedon, Pavol Luptak

AGENDA

- Few words about the TG history and adoption by the Companies
- Why we need the Common Numbering and Common Vulnerability list
- Update the set of test
- V4 Roadmap

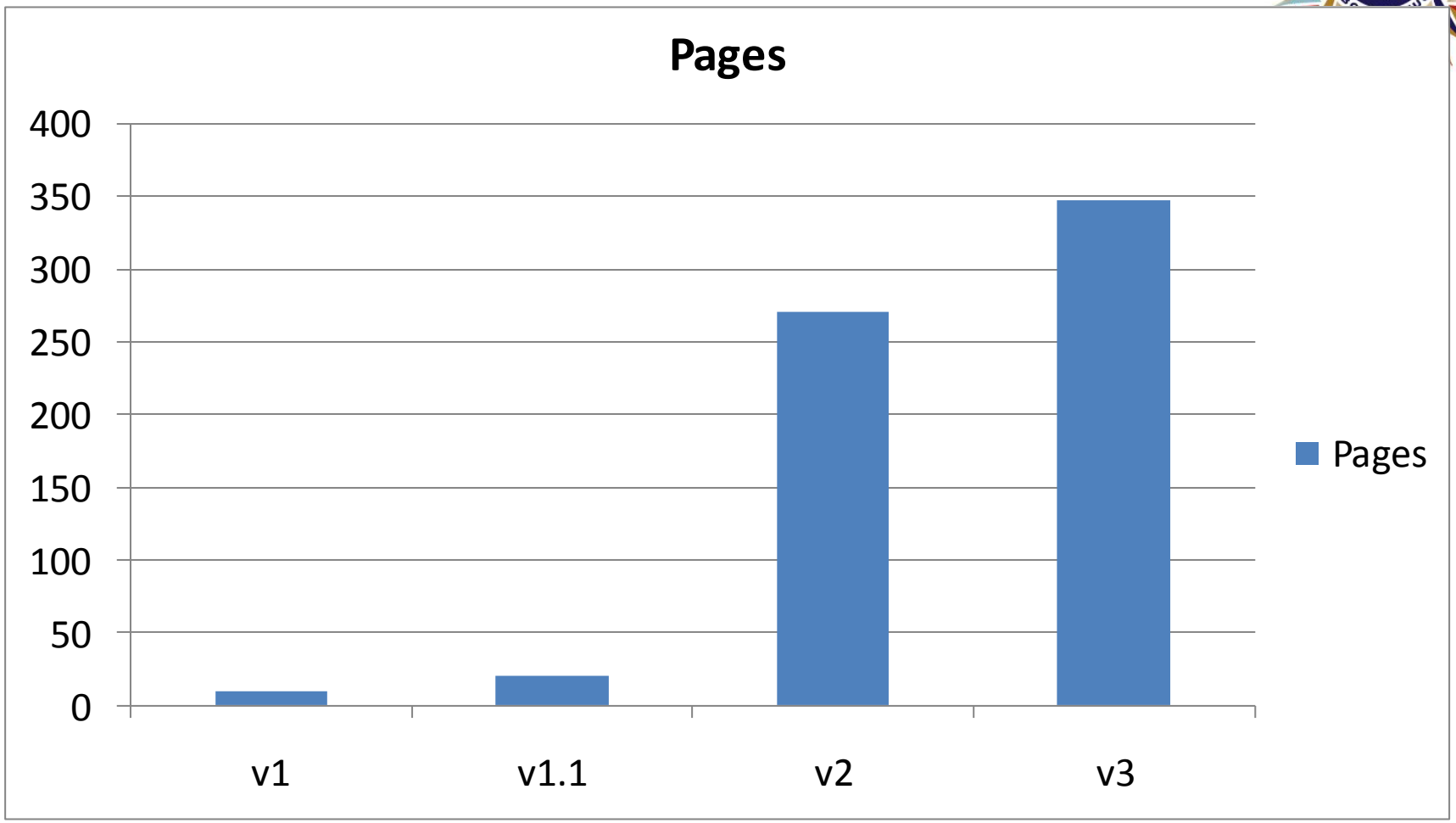
What is the OWASP Testing Guide?

Where are we now?

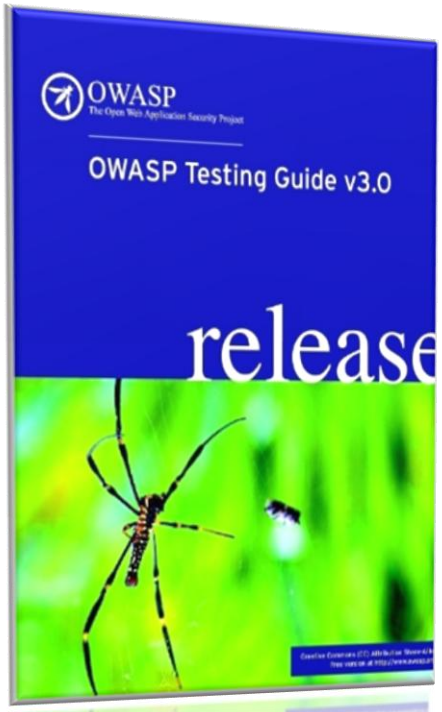
Testing Guide history

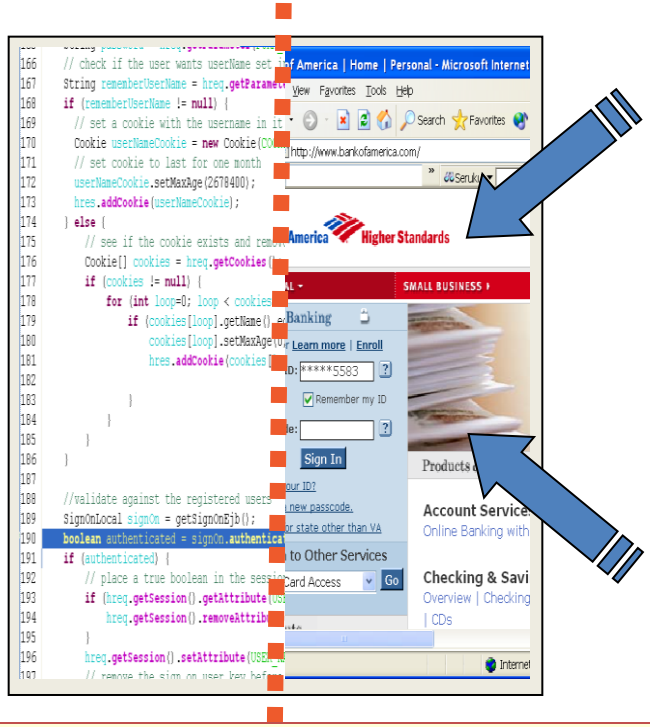
- January 2004
  - "The OWASP Testing Guide", Version 1.0
- July 14, 2004
  - "OWASP Web Application Penetration Checklist", Version 1.1
- December 25, 2006
  - "OWASP Testing Guide", Version 2.0
- December 16, 2008
  - "OWASP Testing Guide", Version 3.0 – Released at the OWASP Summit 08

Project Complexity



OWASP Testing Guide v3





- SANS Top 20 2007
- NIST "Technical Guide to Information Security Testing (Draft)"
- Gary McGraw (CTO Cigital) says: "In my opinion it is the strongest piece of Intellectual Property in the OWASP portfolio" – OWASP Podcast by Jim Manico

Testing Guide v3: Index

What are the difference between the OWASP Testing Guide and another book about WebApp PenTesting?

Web Application Penetration Testing

- OWASP Testing Guide is driven by our Community
- It's related to the other OWASP guides

- Our approach in writing this guide
  - Open
  - Collaborative

- Defined testing methodology
  - Consistent
  - Repeatable
  - Under quality

Testing Guide Categories & vulnerability list

Category	Ref. Number	Test Name	Vulnerability
Information Gathering	OWASP-IG-001	Spiders, Robots and Crawlers	N.A.
	OWASP-IG-002	Search Engine Discovery/Reconnaissance	N.A.
	OWASP-IG-003	Identify application entry points	N.A.
	OWASP-IG-004	Testing for Web Application Fingerprint	N.A.
	OWASP-IG-005	Application Discovery	N.A.
	OWASP-IG-006	Analysis of Error Codes	Information Disclosure
Configuration Management Testing	OWASP-CM-001	SSL/TLS Testing (SSL Version, Algorithms, Key length, Digital Cert. Validity)	SSL Weakness
	OWASP-CM-002	DB Listener Testing	DB Listener weak
	OWASP-CM-003	Infrastructure Configuration Management Testing	Infrastructure Configuration management weakness
	OWASP-CM-004	Application Configuration Management Testing	Application Configuration management weakness
	OWASP-CM-005	Testing for File Extensions Handling	File extensions handling
	OWASP-CM-006	Old, backup and unreferenced files	Old, backup and unreferenced files
	OWASP-CM-007	Infrastructure and Application Admin Interfaces	Access to Admin interfaces
	OWASP-CM-008	Testing for HTTP Methods and XST	HTTP Methods enabled, XST permitted, HTTP Verb
Authentication Testing	OWASP-AT-001	Credentials transport over an encrypted channel	Credentials transport over an encrypted channel
	OWASP-AT-002	Testing for user enumeration	User enumeration
	OWASP-AT-003	Testing for Guessable (Dictionary) User Account	Guessable user account
	OWASP-AT-004	Brute Force Testing	Credentials Brute forcing

What we need now to improve the v3 and plan the v4?

OWASP Common Vulnerability List

We need a common vulnerability list

Looking at the Testing Guide Categories & vulnerability list

Category	Ref. Number	Test Name	Vulnerability
Information Gathering	OWASP-IG-001	Spiders, Robots and Crawlers	N.A.
	OWASP-IG-002	Search Engine Discovery/Reconnaissance	N.A.
	OWASP-IG-003	Identify application entry points	N.A.
	OWASP-IG-004	Testing for Web Application Fingerprint	N.A.
	OWASP-IG-005	Application Discovery	N.A.
	OWASP-IG-006	Analysis of Error Codes	Information Disclosure
Configuration Management Testing	OWASP-CM-001	SSL/TLS Testing (SSL Version, Algorithms, Key length, Digital Cert. Validity)	SSL Weakness
	OWASP-CM-002	DB Listener Testing	DB Listener weak
	OWASP-CM-003	Infrastructure Configuration Management Testing	Infrastructure Configuration management weakness
	OWASP-CM-004	Application Configuration Management Testing	Application Configuration management weakness
	OWASP-CM-005	Testing for File Extensions Handling	File extensions handling
	OWASP-CM-006	Old, backup and unreferenced files	Old, backup and unreferenced files
	OWASP-CM-007	Infrastructure and Application Admin Interfaces	Access to Admin interfaces
	OWASP-CM-008	Testing for HTTP Methods and XST	HTTP Methods enabled, XST permitted, HTTP Verb
Authentication Testing	OWASP-AT-001	Credentials transport over an encrypted channel	Credentials transport over an encrypted channel
	OWASP-AT-002	Testing for user enumeration	User enumeration
	OWASP-AT-003	Testing for Guessable (Dictionary) User Account	Guessable user account
	OWASP-AT-004	Brute Force Testing	Credentials Brute forcing

The new team

Andrew Muller
Aung KhAnt
Cecil Su
Colin Watson
Daniel Cuthbert
Giorgio Fedon
Jason Flood
Javier Marcos de Prado
Juan Galiana Lara
Kenan Gursoy
Kevin Horvat
Lode Vanstechelman
Marco Morana
Matt Churchy
Matteo Meucci
Michael Boman
Mike Hryekewicz
Nick Freeman
Norbert Szetei
Paolo Perego
Pavol Luptak
Psiinon
Ray Schippers
Robert Smith
Robert Winkel
Roberto Suggi Liverani
Sebastien Gioria
Stefano Di Paola
Sumit Siddharth
Thomas Ryan
Tim Bertels
Tripurari Rai
Wagner Elias

Proposed v4 list: let's discuss it

Category	Vulnerability name	Where implemented	Source
Information Gathering	Information Disclosure	TG, ecc, --> link	TG
Configuration and Deploy Management	Infrastructure Configuration management weakness		TG
	Application Configuration management weakness		TG
	File extensions handling		TG
	Old, backup and unreferenced files		TG
	Access to Admin interfaces		TG
	Bad HTTP Methods enabled, (XST permitted: to eliminate or		TG
	Informative Error Messages		
	Database credentials/connection strings available		
Business logic	Business Logic		TG
Authentication	Credentials transport over an unencrypted channel		TG
	User enumeration (also Guessable user account)		TG
	Default passwords		TG
	Weak lock out mechanism		new TG
	Account lockout DoS		
	Bypassing authentication schema		TG
	Directory traversal/file include		TG
	vulnerable remember password		TG
	Logout function not properly implemented, browser cache weakness		TG
	Weak Password policy		New TG
	Weak username policy		New Anurag
	weak security question answer		New
	Failure to Restrict access to authenticated resource		New Top10
	Weak password change function		New Vishal

Proposed v4 list: let's discuss it (2)

Authorization	Path Traversal	TG
	Bypassing authorization schema	TG
	Privilege Escalation	TG
	Insecure Direct Object References	Top10 2010
	Failure to Restrict access to authorized resource	TG
Session Managment	Bypassing Session Management Schema	TG
	Weak Session Token	TG
	Cookies are set not 'HTTP Only', 'Secure', and no time validity	TG
	Exposed sensitive session variables	TG
	CSRF	
	Session passed over http	Vishal
	Session token within URL	Vishal
	Session Fixation	Vishal
	Session token not removed on server after logout	Vishal
	Persistent session token	Vishal
	Session token not restrcited properly (such as domain or path not set properly)	Vishal
Data Validation	Reflected XSS	TG
	Stored XSS	TG - Vishal
	HTTP Verb Tampering	new TG
	HTTP Parameter pollution	new TG
	Unvalidated Redirects and Forwards	T10 2010: new TG
	SQL Injection	TG
	SQL Fingerprinting	
	LDAP Injection	TG
	ORM Injection	TG
	XML Injection	TG
	SSI Injection	TG
	XPath Injection	TG
	SOAP Injection	
	IMAP/SMTP Injection	TG
	Code Injection	TG
	OS Commanding	TG
	Buffer overflow	
	Incubated vulnerability	
	HTTP Splitting/Smuggling	

Proposed v4 list: let's discuss it (3)

Data Encryption?	Application did not use encryption Weak SSL/TSL Ciphers, Insufficient Transport Layer Protection Cacheable HTTPS Response Cache directives insecure Insecure Cryptographic Storage Sensitive information sent via unencrypted channels	only SCR guide	T10 2010: new TG
XML interpreter?	Weak XML Structure XML content-level WS HTTP GET parameters/REST WS Naughty SOAP attachments WS Replay Testing		
Client side?	DOM XSS Cross Site Flashing ClickHijacking		TG TG new TG

Proposed v4 news from Pavol

- add new opensource testing tools that appeared during last 3 years (and are missing in the OWASP Testing Guide v3)

- add few useful and life-scenarios of possible vulnerabilities in Bussiness Logic Testing (many testers have no idea what vulnerabilities in Business Logic exactly mean)

- "Brute force testing" of "session ID" is missing in "Session Management Testing", describe other tools for Session ID entropy analysis (e.g. Stompy)

- in "Data Validation Testing" describe some basic obfuscation methods for malicious code injection including the statements how it is possible to detect it (web application obfuscation is quite succesfull in bypassing many data validation controls)

- split the phase Logout and Browser Cache Management" into two sections

Roadmap

- Review all the control numbers to adhere to the OWASP Common numbering,
- Review all the sections in v3,
- Create a more readable guide, eliminating some sections that are not really useful,
- Insert new testing techniques: HTTP Verb tampering, HTTP Parameter Pollutions, etc.,
- Rationalize some sections as Session Management Testing,
- Create a new section: Client side security and Firefox extensions testing?

Questions?

http://www.owasp.org/index.php/OWASP_Testing_Project

matteo.meucci@owasp.org

Thanks!!