



OWASP Testing Guide v2

La nuova metodologia per l'audit di sicurezza degli applicativi web

(a cura di Matteo Meucci – CISA, CISSP - INS)

25 Jan 2007





Agenda:

- OWASP Projects
- The new Testing Guide: goals and deliverables
- The OWASP Testing Framework
- The Testing Methodology: how to test
- The reporting: how to value the risk and write a report
- Solution How the Guide will be useful to the web security industry
- ◎ Q&A







36,000+ successful client engagements 1,100+ certifications in 96+ categories 900 consulting and management employees 38 markets across North America, Europe & Asia 15 years in business-centric technology consulting partnerships with top technology leaders

Speaker:

- INS Consultant
- 6+ years on Information Security focusing on Application Security
- OWASP Italy founder and Chair
- OWASP Testing Guide AoC lead

INS:

- Focus on aligning technology and operations to business needs
- Multidisciplinary, IT infrastructure-to-application consulting expertise
- 900 employees worldwide, with more than 600 enterprise and service provider clients
- Dedicated quality program with world-class Customer Loyalty Index







- The Open Web Application Security Project (OWASP) is dedicated to finding and fighting the causes of insecure software. The OWASP Foundation is a 501c3 not-forprofit charitable organization that ensures the ongoing availability and support for our work.
- Participation in OWASP is free and open to all.
- S Everything here is free and open source.
- Main objective: produce tools, standards and documentation related on Web Application Security.
- Thousands active members, 82 local chapter in the world
- Millions of hits on <u>www.owasp.org</u>
- Defense Information Systems Agency (DISA), US Federal Trade Commisson (FTC), VISA, Mastercard, American Express has adopted OWASP in their standards and guidelines









25 Jan 2007





See and open...



25 Jan 2007

What Is the OWASP Testing Guide?



A project...

Rome Chapter

<u>іслг</u>

		😻 Main Page - OW.	ASP - Mozilla Firefox				Editing How to value the real risk (section) - OWASP - Mozilla Firefox	X		
		File Edit View Go	Bookmarks Tools Help			0	je Edt Vew Go Bookmarks Tools Help				
		4.4.80	http://www.ewasp.org/jpdex.php/Main_Base		0.00		👍 • 📥 • 👰 🕥 🔗 🗈 hötmer/Annua	awara conjuder pho?ttle=How to unles the	mai nickartion-withortion-15 6 V 0 Go		
			Cu ca mapa/minimanaparginaca.php/hail_Page	20. a.		-0		The second second second second second			
		Google +	+ G Search * C C Check *	AutoLink 🔛 AutoFi	Log in / create accou	at a	8 leff 10 m	G search * @ Martin T Check * K Autol	Ink '53 Autora (5) Subscribe * M Optons 3		
			article discussion view source history		-		Jeff Williams	my talk my preferences	my watchlist my contributions log out		
			Main Page					article discussion	n edit history protect dele		
						_					
			BET A FREE SH	urity Assessment	EORTIFY	P		Editing How	to value the real		
					>>> Protect your code			riel (opetion			
		navigation	Sponsored advertisement.	OWASP does not endorse	commercial products or services		nevigation	risk (section	1)		
		= Home	Welcome to OWASP	= Guide	CLASP = Testing		navigation		,		
		 News Projects 	the free and open application security community	 Top Ten WebCost 	WebScarab Code Revie	w	 Home 	Stop 6. Cueto	miging Your Dick Dating		
		Downloads	About - Concrision - Edition - New Article - OWARD Cohenories	* Webboat	Statetor - Recent Changes		 News 	Madel	mizing four Kisk Racing		
		Conferences	About dearding comprise were were compared		constance - reaction continger		- Projects	MODET			
		Presentations	OWASP Overview	OWASP Communit	y (add)		Developede				
		* Papers	The Open Web Application Security Project (OWASP) is	15		No.	- Downloads	Having a risk r	anking framework that's		
		 Maling Lists About OWASP 	dedicated to finding and fighting the causes of insecure	144	Maline.	1	 Local Chapters 	customizable fo	r a business is critical		
		= Henbership	software. Everything here is free and open source. The OWASP Enundation is a 501c3 not-for-profit charitable	1.2.8.4	Stell C	3	. Conferences	for adoption.	A tailored model is much		
		reference	organization that ensures the ongoing availability and		ALL AND THE MAN		. Presentations	more likely to	produce results that match 🚪		
		 How To Drinciples 	support for our work. Participation in OWASP is free and				16dee	people's percep	tions about what is a		
		= Threat Agents				Autom 1	. video	serious risk. Y	ou can waste lots of time		
		 Atacks Vulnerabilities 	The OWASP mail list. Find out more.			•	 Papers 	arguing about t	he risk ratings if they're		
		= Countermeasures	Contact OWASP	(· .			 Mailing Lists 	not supported b	y a model like this. There		
		 Activities Technologies 	overp@overp.org Support our efforts	Click the map t	o find and join your local chapte	r	- About OWASP	are several way	s to tailor this model for		
		Glossery Code Sciences	Featured Story	Feb 13 (18:00h) - Irela	nd chapter meeting		Mambarahia	vour organizati	on.		
- رور الم		 Lode Shippets .NET Project 		Feb 6 (18:00h) - Melbo	surne chapter meeting		 inempersnip 	, sur orgunableet			
Owasp-	testing into Page - W	 Java Project 	and Adobe XSS	Jan 31 (15:00h) - Mum	hai chantar maoting		reference	===Adding facto	rs===		
0.	http://lists.owasp.or	search	OWASP contributors from Aspect Security # have	Jan 30 (11:30h) - Austi	W Recent changes	OWASP - Mozilla Fire	reierdlite	-nualing facto			
4	@ Owasputesting John Pro	Google Custom Search	developed two new Java EE filters to protect against	Jan 25 (14:30h) - Italy	File Edit View Go	Bookmarks Tools Help	 How To 	You gan abcore	difforent factors that		
	p	Dealch	web.xml file and enjoy the protection.	Jan 24 (17:30h) - 6th C	🦕 · 🍌 · 🔗 🙆	http://www.owa	 Principles 	hottor ropreser	t whatle important for		
_		s What loks here	CSRF and Reflected XSS Filter for Java EE	Jan 23 (18:00h) - Belg	Coorde		Threat Agents	better represen	c what S important for		
		 Related changes 	This filter adds a random token to forms and URLs	Jan 22 (18:00h) - Roch	Google .		Attestes	your organizati	on. For example, a		
		 Upload file Special pages 	and reflected XSS attacks.	Older events		special page	- ALLACKS	military applic	action might add impact		
		 Printable version 	Adobe XSS Filter for Java EE			Recent chang	 Vulnerabilities 	lactors related	to loss of human life or		
About	English (USA)	 remanent ink 	This filter protects against the recent XSS attacks	OWASP News (add			 Countermeasures 	classified info	rmation. You might also		
owasp		1	on MUF files. By using a redirect and an encrypted	Jan 16 - OWASP New		Track the most recent cha	Activitioe	add likelihood	factors, such as the		
- mag		Done				Below are the last 100 cha	(3		
lo see	the collection of pri	DOIR	· · · · ·		_	Show last 50 100 250 Hide bot	Done		🖄 🕲 2 Errors		
Using (Owasp-testing				navigation	Hide my edits					
					= News	Show new changes startin	ig from 21:47, 20 January 2007				
o post	a message to all the	e list members, send	i email to owasp-testing@lists.owasp.org.		Projects	Namespace: all	Go Invert selection				
(ou car	subscribe to the list	st, or change your ex	xisting subscription, in the sections below.		Local Chapters	20 January 2007					
					Conferences	= (diff) (hist) b Ottawa;	04:13 Koussa (Talk contribs)				
subscri	bing to Owasp-tes	ting			= Video	19 January 2007					
subscri	be to Owasp-testing	g by filling out the fo	ollowing form. You will be sent email		Papers	 (diff) (hist) b Phoenio (diff) (hist) b Phoenio 	c/Tools; Z2:18 Dre (Talk contribs) c/Tools; 22:16 Dre (Talk contribs)				
equesti	ng confirmation, to	prevent others from	a gratuitously subscribing you. This is a hidden		About OWASP	= (diff) (hist) b OWASP	P WebScarab NG Project; 15:43 Jeff	Williams (Talk contribs)			
ist, wh	ion means that the li	st of members is av	anable only to the list administrator.		Membership	= (diff) (hist) Nb Long I = (diff) (hist) h CMASS	ong ago; 11:32 EoinKeary (Talk o P Code Review Guide Table of Contents	contribs) : 11:22 FoinKeary (Talk I			
1	1.17				reference	contribs) (→Guide Hist	lory)	,			
	r our email address:				How To Discription	= (diff) (hist) b OWASP	P Code Review Guide Table of Contents	; 11:21 EoinKeary (Talk			
1	Your name (optional	1):			Threat Agents	= (diff) (hist) b Inner cla	asses; 11:17 Jmanico (Talk contrib:	3)			
	r'ou may enter a privace	y password below. This	provides only mild security,		= Attacks	= (diff) (hist) b Chapter	s Assigned; 10:10 EoinKeary (Talk	contribs) (→Examples by			
1	out should prevent othe	rs from messing with y	your subscription. Do not use		Countermeasures	= (diff) (hist) b XSS Att	tacks; 10:09 EoinKeary (Talk I contri	bs)	1		
1	cleartext.	is it will occasionally b	e emaneu oack to you m		Activities	= (diff) (hist) Nb Review	wing code for XSS issues; 10:06 Eoir	Keary (Talk contribs)			
					 Glossary 	 (aff) (hist) b OWASP contribs) (→Examples 	Code Keview Guide Table of Contents by Vulnerability)	; 10:05 EoinKeary (Talk			
If you choose not to enter a password, one will be automatically generated for you, and it will be sent to you once you've confirmed your subscription				Code Snippets	= (diff) (hist) b Belgium	; 08:31 Sdeleersnyder (Talk contrib	is)				
	You can always request	a mail-back of your pa	assword when you edit your		 NET Project Java Project 	 (diff) (hist) b Phoenix (diff) (hist) b Phoenix 	(Tools; 02:24 . Dre (Talk contribs)				
3	ersonal options. Once	a month, your passwor	rd will be emailed to you as a		easth	= (diff) (hist) b Phoenio	/Tools; 02:17 . Dre (Talk contribs)				
1	eminder.				Goosle Custom Search	= (diff) (hist) b Phoenio	v/Tools; 01:58 Dre (Talk contribs)				
1	Pick a password:				Search	 (diff) (hist) b Phoenix (diff) (hist) b Phoenix 	c/Tools; 01:57 . Dre (Talk contribs) c/Tools; 01:54 . Dre (Talk contribs)				
1	Reenter password to	0			te all ten	= (diff) (hist) b Phoenix	/Tools; 01:31 Dre (Talk contribs)				
4	confirm:				a ras abm	= (diff) (hist) b Categor	ry:OWASP Top Ten Project; 00:43 G	WASP (Talk contribs)			
						- fearly fursel n caredou	y or rep ren molect, d0:43 0	train Lean Leonnina)			
1	Which language do	you			 Uplead file 	= (diff) (hist) b Testing	for Session Management; 00:33 Mm	ieucci (Talk contribs) (→4.5			
1	Which language do y prefer to display you	you ur English (USA	A)	~	Upload file Special pages	 (diff) (hist) b Testing Session Management 	for Session Management; 00:33 Min Testing)	ieucci (Talk contribs) (-+4.5			







- Review all the documentation on testing:
 - July 14, 2004
 - "OWASP Web Application Penetration Checklist", Version 1.1
 - December 2004
 - "The OWASP Testing Guide", Version 1.0
- Create a complete new project focused on Web Application Penetration Testing
- Create a reference for application testing
- Describe the new OWASP Methodology
- Describe how to test each control



OWASP Testing Guide v2: **Action Plan**



Action Plan:

Oct 2006:

- Collect all old docs
- Brainstorming for the Index and template
- Involve major world experts on this field:
- * Vicente Aguilera
- * Mauro Bregolin
- * Tom Brennan
- * Gary Burns
- * Luca Carettoni
- * Dan Cornell
- * Mark Curphey
- * Daniel Cuthbert
- * Sebastien Deleersnyder
- * Stephen DeVries
- * Stefano Di Paola

- * David Endler
- * Giorgio Fedon
- * Javier Fernández-Sanguino * Laura Nunez
- * Glyn Geoghegan
- * Stan Guzik
- * Madhura Halasgikar
- * Eoin Keary
- * David Litchfield
- * Andrea Lombardini
- * Ralph M. Los
- * Claudio Merloni

- * Matteo Meucci
- * Marco Morana
- * Gunter Ollmann
- * Antonio Parata
- * Yiannis Pavlosoglou
- * Carlo Pelliccioni
- * Harinath Pudipeddi
- * Alberto Revelli
- * Mark Roxberry
- * Tom Ryan

- * Anush Shetty
- * Larry Shields
- * Dafydd Studdard
- * Andrew van der Stock
- * Ariel Waissbein
- * Jeff Williams





Action Plan:

Nov 2006:

- Write articles using our Wiki model
- Review articles

Dec 2006:

- Review all the Guide
- Write the Guide in doc format

Jan 2007:

- OWASP Testing Guide Release Candidate 1: 270 pages, 48 tests
- Feedback and review

Feb 2007:

• OWASP Testing Guide v2 will be officially released





- 1. Frontispiece
- **2. Introduction**
- 3. The OWASP Testing Framework
- 4. Web Application Penetration Testing
- **5. Writing Reports: value the real risk**
- **Appendix A: Testing Tools**
- **Appendix B: Suggested Reading**
- **Appendix C: Fuzz Vectors**





I. Introduction



- The problem of insecure software: companies next challenge
- Why OWASP?
 - "It's impossible to underestimate the importance of having this guide available in a completely free and open way" – Jeff Williams (OWASP Chair)
- Principles of Testing: comparing the state of something against a set of criteria defined and complete.
 - We want security testing not be a black art
- Testing Techniques:
 - Manual Inspections & Reviews
 - Threat Modeling
 - Code Review
 - Penetration Testing





Phase 1: Before Development Begins

Before application development has started:

- Test to ensure that there is an adequate SDLC where security is inherent.
- Test to ensure that the appropriate policy and standards are in place for the development team.
- Develop Measurement and Metrics Criteria (Ensure Traceability)







Phase 2: During Definition and Design

Before application development has started:

- Security Requirements Review:
 - User Management (password reset etc.), Authentication, Authorization, Data Confidentiality, Integrity, Accountability, Session Management, Transport Security, Privacy
- Design an Architecture Review
- Create and Review UML Models
 - How the application works
- Create and Review Threat Models
 - Develop realistic threat scenarios







Phase 3: During Development

- Code Walkthroughs:
 - high-level walkthrough of the code where the developers can explain the logic and flow.
- Code Reviews:
 - Static code reviews validate the code against a set of checklists:
 - CIA Triad
 - OWASP Top10, OWASP Code Review
 - Sox, ISO 17799, etc...







Phase 4: During Deployment

- Application Penetration Testing
 - Focus of this guide
- Configuration Management Testing
 - The application penetration test should include the checking of how the infrastructure was deployed and secured.







Phase 5: Maintenance and Operations

- Conduct operational management reviews
 - Process in place which details how the operational side, of the application and infrastructure, is managed.
- Conduct periodic health checks
 - Monthly or quarterly health checks should be performed
- Ensure change verification
 - The change is checked to ensure that the level of security hasn't been affected by the change.







- What is a Web Application Penetration Testing?
 - The process involves an active analysis of the application for any weaknesses, technical flaws or vulnerabilities
- What is a vulnerability?
 - A weakness on a asset that makes a threat possible
- Our approach in writing this guide
 - Open
 - Collaborative
- Defined testing methodology
 - Consistent
 - Repeatable
 - Under quality
- OWASP Testing Methodology
 - Penetration testing is only an appropriate technique for testing the security of web applications under certain circumstances.
 - Our goal is to collect all the possible testing techniques, explain them and keep the guide updated.



Testing model



- Black box approach:
 - Tester: Who performs the testing activities
 - Tools and methodology: The core of this Testing Guide project
 - Application: The black box to test
- The test is divided in 2 phases:
 - Passive mode: find all the access points (gates) of the application (e.g. Header HTTP, parameters, cookies).
 - https://www.example.com/login/Autentic_Form.html
 - http://www.example.com/Appx.jsp?a=1&b=1
 - Active mode: test using the methodology described.
- We have split the set of tests in 8 sub-categories (46 controls):
 - Information Gathering
 - Business logic testing
 - Authentication Testing
 - Session Management Testing

- Data Validation Testing
- Denial of Service Testing
- Web Services Testing
- AJAX Testing





Srief Summary

Describe in "natural language" what we want to test.

Description of the Issue

Short Description of the Issue: Topic and Explanation

- Black Box testing and example
 - Testing for Topic X vulnerabilities:

•••

. . .

- Result Expected:
- Gray Box testing and example
 - Testing for Topic X vulnerabilities:

... - De

- Result Expected:
- References
 - Whitepapers
 - Tools





- The first phase in security assessment is focused on collecting all the information about a target application.
- Using public tools (search engines), scanners, sending simple HTTP requests, or specially crafted requests, it is possible to force the application leak information by sending back error messages revealing the versions and technologies used by the application.

Application Fingerprint

First step: knowing the version and type of a running web server allows testers to determine known vulnerabilities and the appropriate exploits to use during testing.







Application Discovery

Is the process aimed at identifying web applications on given infrastructure: find out which particular applications are hosted on a web server.

nmap -P0	-sT -s'	V -p1-65535	192.168.1.100
PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 3.5p1 (protocol 1.99)
80/tcp	open	http	Apache httpd 2.0.40 ((Red Hat Linux))
443/tcp	open	ssl	OpenSSL
901/tcp	open	http	Samba SWAT administration server
1241/tcp	open	ssl	Nessus security scanner
3690/tcp	open	unknown	
8000/tcp	open	http-alt?	
8080/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1

- Spidering and googling
 - Our goal is to create a map of the application with all the points of access (gates) to the application (wget)
 - Using advanced tips of google, the goal is to find web-site information published on internet





Testing for error code

Error codes generated from applications or web servers reveal a lot of information about databases, bugs, and other technological components directly linked with web application(s).

Microsoft OLE DB Provider for ODBC Drivers (0x80004005) [DBNETLIB][ConnectionOpen(Connect())] - SQL server does not exist or access denied

SSL/TLS Testing

SSL Test Results		
OpenSSL Cipher Name	Cipher Description	Cipher Strength
NULL-MD5	Key Exchange: None; Authentication: None; Encryption: None; MAC: MD5	No Security
NULL-SHA	Key Exchange: None; Authentication: None; Encryption: None); MAC: SHA1	No Security
EXP-DES-CBC-SHA	Key Exchange: RSA(512); Authentication: RSA; Encryption: DES(40); MAC: SHA1	Weak Security
EXP-RC2-CBC-MD5	Key Exchange: RSA(512); Authentication: RSA; Encryption: RC2(40); MAC: MD5	Weak Security
EXP-RC4-MD5	Key Exchange: RSA(512); Authentication: RSA; Encryption: RC4(40); MAC: MD5	Weak Security
EXP1024-DHE-DSS-DES-CBC-SHA	Key Exchange: EDH (EXPORT - 1024); Authentication: DSS; Encryption: DES(56); MAC: SHA1	Weak Security
EXP1024-DHE-DSS-RC4-SHA	Key Exchange: EDH (EXPORT - 1024); Authentication: DSS; Encryption: RC4(56); MAC: SHA1	Weak Security
EXP1024-DES-CBC-SHA	Key Exchange: RSA (EXPORT - 1024); Authentication: RSA; Encryption: DES(56); MAC: SHA1	Weak Security
EXP1024-RC4-SHA	Key Exchange: RSA (EXPORT - 1024); Authentication: RSA; Encryption: RC4(56); MAC: MD5	Weak Security
DES-CBC-SHA	Key Exchange: RSA; Authentication: RSA; Encryption: DES(56); MAC: SHA1	Weak Security
ADH-AES128-SHA	Key Exchange: ADH ; Authentication: RSA ; Encryption: AES(128); MAC: SHA1	Weak Security
ADH-AES256-SHA	Key Exchange: ADH; Authentication: RSA; Encryption: DES(256); MAC: SHA1	Weak Security
DH-DSS-AES128-SHA	Key Exchange: DH; Authentication: DSS; Encryption: AES(128); MAC: SHA1	Strong Security
DH-RSA-AES128-SHA	Key Exchange: DH; Authentication: RSA; Encryption: AES(128); MAC: SHA1	Strong Security





DB Listener Testing

The DB listener is the entry point for remote connections to an Oracle database: obtain detailed information on the Listener, database, and application configuration.

File extensions handling

Determining how web servers handle requests corresponding to files having different extensions may help to understand web server behaviour depending on the kind of files we try to access.

Old, backup and unreferenced files

Leaving in the web tree old files or unreferenced files may reveal sensitive data





Testing for business logic comprises:

- Business rules that express business policy (such as channels, location, logistics, prices, and products); and
- Workflows that are the ordered tasks of passing documents or data from one participant (a person or a software system) to another.
- Test the logic: perhaps you are supposed to do operations in a particular order, but an attacker could invoke them in a different order.

Receiver	Sender	[1] Sender compose a MMS – insert MSISDN Receiver– begin authc. process	ļ	Web App	TELCO Network
	•	[2] Server send a form asking for [MSISDN Sender]			
		[3] POST MSISDN Sender	_		
	-	[4] Network send Short Message Service (SMS) with			
	-	[4] Server send a form asking [OTP]			
		[5] POST OTP received on mobile phone		Two facto	r authenticatior
		[6] Server set cookie OTP, MSISDN on browser		(OTP) OK	
		[7] Call the servlet to charge the user	_	Charge Se	nder
		[8] Send MMS to Receiver via GPRS	- 22	Send MMS	to Receiver
		[8] Sent MMS ok!			





Testing the authentication schema means understanding how the authentication process works and using that information to circumvent the authentication mechanism.

Default or guessable account

We test for leave backdoors to easily access and test the application and later forgetting to remove them, non-removable default accounts with a preset username and password and blank passwords.

Srute Force

Systematically enumerating all possible candidates for the solution and checking whether each candidate satisfies the problem's statement.

Brute force on username given a set of password, or bruteforce on password given a set of username.

Sypassing authentication schema

Test if it's possible to bypass authentication measures by tampering with requests and tricking the application into thinking that we're already authenticated



Authentication testing (2)

File Modifica Visualizza Vai

Ultime notizie



O Vai G

-

- 🗆 X

- Bypassing authenticatic Owasp Testing Guide Browser
 - Direct page request
 - Parameter Modifica
 - Session ID Predictic You Are Auhtenticated
 - Sql Injection
- Directory traversal/file ir
 - Input Vectors Enum vector)
 - http://exam
 - http://example.com/getUserProfile.jsp?item=../../../etc/passwd

Strumenti 2

http://www.site.com/page asp?authenticated=yes

Segnalibri

- http://example.com/index.php?file=content
- http://example.com/main.cgi?home=index.htm





- Vulnerable remember password and pwd reset
 We test the password reset schema ("security question") and "cache password" function
- Logout and Browser Cache Management Testing
 - Check that the application provides a logout function
 - Check the session token at logout, and "back button"
 - Re-set the original authc token to test tha application answer
 - Test the time-out logout
 - Cached pages: check for "Pragma: no-cache" directive



Session Management Testing



Session Management Schema

Mario Rossi	/management	Authentication process	Web Application	
		[1] https://www.mia-banca.it		
	•	[2] Sent authentication form over HTTPS		
		🖲 Mia-Banca - Mozilla Firefox		
		File Modifica Visualizza Vaj Segnalibri Strumenti ?		
		Username Login		
		Hai dimenticato la password? Login		
		Palmare?		
25 Jan 2007			Pa	g. 30



Session Management testing







Session management testing



Cookie=TWFyaW8123 Authentication token [5] Request "movimenti" Cookie=TWFyaW8123 [6] Response with user data Image: Data of the second o	Mario Rossi 🥭		Follow	ing r	equest	Web Application
Authentication token	Cookie=TWFyaW8123	[5] Peque	st "movimenti"			Cookie verifing:
token Cookie=TWFyaW8123 Send data to us [6] Response with user data Image: Send data to us Image: Send data to us Image: Send data to us Image: Send data to us Image: Send data to us Image: Send data to us Image: Send data to us Image: Send data to us Image: Send data to us Image: Send data to us Image: Send data to us Image: Send data to us Image: Send data to us Image: Send data to us Image: Send data to us Image: Send data to us Image: Send data to us Image: Send data to us Image: Send data to us Image: Send data to us Image: Send data to us Image: Send data to us Image: Send data to us Image: Send data to us Image: Send data to us Image: Send data to us Image: Send data to us Image: Send data to us Image: Send data to us Image: Send data to us Image: Send data to us Image: Send data to us Image: Send data to us Image: Send data to us Image: Send data to us Image: Send data to us Image: Send data to us Image: Send data to us Image: Send data to us Image:	Authentication					\rightarrow Identify user
[6] Response with user data Imid-bance - Mozillo Firefox: Imid-bance - Mozillo Firefox: <td>token</td> <td></td> <td>Cooki</td> <td>e=TWFy</td> <td>vaW8123</td> <td>Send data to user</td>	token		Cooki	e=TWFy	vaW8123	Send data to user
▼mia-bance - Mozilia Elefox File Bodica You Segnable Strunerki Z		[6] Respo	nse with user da	ata		
Ele Bodita yuakza Va Segailari grunenti 2			II. Electron			
Image: Second and the second and th		File Modifica Visualizza	Vai Segnalibri Strumenti ?			
Movimenti: Mario Rossi MIBTEL +5,03% SPMIB +0,06% DOW JONES +0,08% NASDAQ +0,43 Conto Corrente: 123456 Divisa: EUR Saldo disponibile: 20.303,83 Conto Saldo disponibile: 20.303,83 Conto Saldo disponibile: 21.002004 11/10/2004 Disposizioni 11/10/2004 11/10/2004 140,40 Disposizioni 12/10/2004 140,40 prelevamento da distributora automatico numero 274 carta 12 Conto 12/10/2004 140,40 prelevamento da distributora automatico numero 274 carta 12 Disposizioni 11/10/2004 140,40 prelevamento pos pagobancomat 12346 del 18/10 carrer Disposizioni 11/10/2004 140,40 prelevamento pos pagobancomat 12346 del 18/10 gas pagamento pos pagobancomat 12346 del 22/10 acrosot pagamento pos pagobancomat						
Mia-Banca Movimenti: Mario Rossi [MIBTEL +5,05% SPMIB ++0,06% DOW JONES ++0,08% NASDAQ ++0,43 Conto Corrente: 123456 Divisa: EUR Saldo disponibile: 20.303,83 Conto Saldo disponibile: Disposizioni Dia operazione Data valuta Impoto Conto Saldo disponibile: 20.303,83 Conto 11/10/2003 9/10/2004 Disposizioni 11/10/2004 1-440,00 Disposizioni 11/10/2004 1-460,00 Conto 12/20/2004 9/16/00/204 Accreditio 11/10/2004 1-460,00 Pagamento pos pagobancomat 12345 del 5/19 carred 12/16/2004 Conto 12/20/2004 1-560,00 Accreditio 11/10/2004 1-460,00 Accreditio 12/20/2004 1-560,00 Altiva 2/20/2004 1-56,00 Accreditio 12/20/2004 1-66,07 Altiva 2/20/2004 1-76,00 pagamento pos pagobancomat 12346 del 12/10 gas pagobancomat 12346 del 22/10 gas pagobancomat 12346 del 2			The second secon	imov/movimenti.	sp	
Movimenti: Mario Rossi MIBTEL _ +5,03% SPMIB _ +0,06% DOW JONES _ +0,08% NASDAQ +0,43 Conto Corrente: 123456 Divisa: EUR Saldo disponibile: 20.303,83 Conto Saldo Pete operazine Data valuta Importo Causale Movimenti 10/10/2004 \$7/0/2004 -31,05 pagamento pos pagobancomat 12346 del 9/10 carret Disposizioni 10/10/2004 \$7/0/2004 -149,00 prelevamento da distributore automatico numero 274 carta 12 Conto 12/1/0/2004 11/10/2004 -149,00 prelevamento pos pagobancomat 12346 del 9/10 carret Disposizioni 10/10/2004 11/10/2004 -149,00 prelevamento pos pagobancomat 12346 del 9/10 carret Disposizioni 12/10/2004 11/10/2004 -149,00 prelevamento pos pagobancomat 12346 del 9/10 carret Conto 12/11/10/2004 11/10/2004 -149,00 prelevamento pos pagobancomat 12346 del 9/10 carret Conto 12/10/2004 11/10/2004 -149,00 pagamento pos pagobancomat 12346 del 9/10 carret Conto 12/10/2004 13/10/2004 -149,00 pagamento pos pagobancomat 12346 del 1					Mia-Banca	
Image:			Movimenti: Mario Ross	i		
Conto Corrente: 123456 Divisa: EUR Saldo disponibile: 20.303,83 Conto Saldo Data operazione Data valuta Importo Causale Movimenti 10/10/2004 9/10/2004 -31,05 pagamento pos pagobancomat 12345 del 9/10 carret Disposizioni 10/10/2004 9/10/2004 -4140,00 prelevamento da distributore automatico numero 274 carta 12 Conto 12/10/2004 11/10/2004 11/10/2004 160,000 vostri emolumenti bonifico da rossi pago automat 12345 del 18/10 gas pago automat 12345 del 22/10 esso giove pet Bonifici 19/10/2004 11/10/2004 -1160,00 sottoscrizione titoi 12345 Accredito 12/10/2004 21/10/2004 -160,00 sottoscrizione titoi 12345 Bonifici 19/10/2004 21/10/2004 -77,00 pagamento pos pagobancomat 12345 del 22/10 esso giove pet Lista 31/10/2004 28/10/2004 -76,00 pagamento pos pagobancomat 12345 del 22/10 esso giove pet Lista 31/10/2004 28/10/2004 -76,00 pagamento pos pagobancomat 12345 del 22/10 esso giov			MIBTEL ▲ +5,03%	SPMIB 🔺	+0,06% DOW JONES ▲ +0,08% NASDAQ ▲ +0,4	3
Saldo disponibile: 20.303,83 Conto Saldo Data operazione Data valuta Importo Causale Movimenti Disposizioni 10/10/2004 9/10/2004 -31,05 pagamento pos pagobancomat 12345 del 9/10 carret Disposizioni 11/10/2004 11/10/2004 -1440,00 prelevamento da distributore automatico numero 274 carta 12 Conto 12/10/2004 9/10/2004 -1400,00 vostri emolumenti bonifico da rossi s Accredito 12/10/2004 16/10/2004 -74,000 pagamento pos pagobancomat 12345 del 16/10 scarpe e scarpe Bonifici 19/10/2004 18/10/2004 -15,17 pagamento pos pagobancomat 12345 del 18/10 gs spi Informazioni 12/10/2004 21/10/2004 -15,000 sottoscrizione titoli 12348 Attiva 24/10/2004 21/10/2004 -76,00 pagamento pos pagobancomat 12345 del 24/10 esso giove pet Lista 31/10/2004 24/10/2004 -76,00 pagamento pos pagobancomat 12345 del 24/10 distribuerg matter Assegni 31/10/2004 28/10/2004 -76,00 pagamento pos pagobancomat 12346 del 24/10 distribuerg matter			Conto Corrente:	123456	Divisa: EUR	
ContoSaldoData operazioneData valutaImportoCausaleMovimenti10/10/20049/10/2004-31,05pagamento pos pagobancomat 12345 del 9/10 carretDisposizioni11/10/20041/1/10/2004-140,00prelevamento da distributore automatico numero 274 carta 12Disp. sul11/10/20049/10/20041.500,00vostri emolumenti bonifico da rossi sConto12/10/20049/10/2004-74,00pagamento pos pagobancomat 12345 del 16/10 scarpe e scarptBonifici19/10/200416/10/2004-74,00pagamento pos pagobancomat 12345 del 18/10 gs spGiroconti19/10/200418/10/2004-151,71pagamento pos pagobancomat 12345 del 18/10 gs spInformazioni20/10/200421/10/2004-77,00pagamento pos pagobancomat 12345 del 22/10 esso giove petLista25/10/200428/10/2004-76,00pagamento pos pagobancomat 12345 del 24/10 distrib.erg matterAssegni21/10/200428/10/2004-1.240,00disposizione di addebito generica bolifico a gigi rossi per di			Saldo disponibile:	20.303	,83	
Movimenti Disposizioni10/10/20049/10/2004-31,05pagamento pos pagobancomat 12345 del 9/10 carret DisposizioniDisposizioni Disp.sul Conto11/10/200411/10/2004-140,00prelevamento da distributore automatico numero 274 carta 12 vostri emolumenti bonifico da rossi e AccreditoAccredito12/10/20049/10/20041.500,00vostri emolumenti bonifico da rossi e accreditoBonifici Giroconti17/10/200416/10/2004-74,00pagamento pos pagobancomat 12345 del 16/10 scarpe e scarpe BonificiBonifici Giroconti19/10/200418/10/2004-15,17pagamento pos pagobancomat 12345 del 18/10 gs pa sottoscrizione titoli 12345Attiva24/10/200421/10/2004-150,00sottoscrizione titoli 12345Attiva24/10/200422/10/2004-77,00pagamento pos pagobancomat 12345 del 22/10 esso giove pet 25/10/2004Lista 		Saldo	Data operazione Data valuta	Importo	Causale	-
Disp. sul Disp. sul Conto11/10/200411/10/2004-140,00prelevamento da distributore automatico numero 274 carta 12 vostri emolumenti bonifico da rossi e AccreditoAccredito12/10/20049/10/20041.500,00vostri emolumenti bonifico da rossi e AccreditoBonifici17/10/200416/10/2004-74,00pagamento pos pagobancomat 12345 del 16/10 scarpe e scarpe BonificiGiroconti19/10/200418/10/2004-15,17pagamento pos pagobancomat 12345 del 18/10 gs spInformazioni20/10/200421/10/2004-165,000sottoscrizione titoli 12345Attiva24/10/2004-77,00pagamento pos pagobancomat 12345 del 2/10 esso giove pet 25/10/2004-77,00Lista Assegni28/10/2004-76,00pagamento pos pagobancomat 12345 del 24/10 distrib.erg matter disposizione di addebito generica bonifico a girossi per qi 21/10/2004-76,00		Movimenti Disposizioni	10/10/2004 9/10/2004	-31,05	pagamento pos pagobancomat 12345 del 9/10 carro	ef
Conto12/10/20049//0/20041.500,00vostri emolumenti bonifico da rossi sAccredition17/10/200415//0/2004-74,00pagamento pos pagobancomat 12345 del 16/10 scarpe e scarpeBonifici19/10/200418//0/2004-16,17pagamento pos pagobancomat 12345 del 18/10 gs spGiroconti19/10/200418//0/2004-165,00sottoscrizione titoli 12345Informazioni20/10/200421//0/2004-77,00pagamento pos pagobancomat 12345 del 22/10 esso giove petAttiva24/10/200422//0/2004-77,00pagamento pos pagobancomat 12345 del 24/10 esso giove petLista Assegni28//0/2004-76,00pagamento pos pagobancomat 12345 del 24/10 esso giove pet		Disp. sul	11/10/2004 11/10/2004	-140,00	prelevamento da distributore automatico numero 274 carta 1	12
Activation17/10/200415/10/2004-/*4,00pagamento pos pagobancomat 12345 del 16/10 scape e scapeBonifici Giroconti19/10/200418/10/2004-/15,17pagamento pos pagobancomat 12345 del 18/10 gs spInformazioni Attiva20/10/200421/10/2004-/150,00sottoscrizione titoli 12345Lista Assegni21/10/200424/10/2004-/75,00pagamento pos pagobancomat 12345 del 22/10 esso giove pet25/10/200424/10/2004-/75,00pagamento pos pagobancomat 12345 del 24/10 distrib.org matter		Conto	12/10/2004 9/10/2004	1.500,00	vostri emolumenti bonifico da rossi	
Giroconti Text02004 Text02004 -16,17 pagamento pos pagobancontal 12345 del 12/16 ge spi Informazioni 20/10/2004 21/10/2004 -160,00 sottoscrizione titoli 12345 Attiva 24/10/2004 22/10/2004 -77,00 pagamento pos pagobancomat 12345 del 22/10 esso giove pet Lista 25/10/2004 24/10/2004 -76,00 pagamento pos pagobancomat 12345 del 24/10 distrib.erg antes Assegni 31/10/2004 28/10/2004 -1.240,00 disposizione di addebito generica bonifico a gi gi rossi per af		Bonifici	17/10/2004 16/10/2004	-74,00	pagamento pos pagobancomat 12346 del 16/10 scarpe e scarj	De la companya de la
Informazioni 20/02/201 21/02/201 11/02/201 <td></td> <td>Giroconti</td> <td>20/10/2004 18/10/2004</td> <td>-10,11</td> <td>pagamento pos pagobancomat 1234o del 16/10 ys sj sottoscrizione titoli 1234</td> <td>16</td>		Giroconti	20/10/2004 18/10/2004	-10,11	pagamento pos pagobancomat 1234o del 16/10 ys sj sottoscrizione titoli 1234	16
Lista Assegni 21/10/2004 24/10/2004 -76,00 pagamento pos pagobancomat 12345 del 24/10 distrib.erg matter Assegni 31/10/2004 28/10/2004 -1.240,00 disposizione di addebito generica bonifico a gigi orosi per afi		Attiva	24/10/2004 22/10/2004	-77.00	pagamento pos pagobancomat 12345 del 22/10 esso niove ne	st
Lista 31/10/2004 28/10/2004 -1.240,00 disposizione di addebito generica bonifico a gigi rossi per afi Assegni 21/10/2004 20/10/2004 -0.000 persemente non persemente 13246 del 20/10 price di imposi i di			25/10/2004 24/10/2004	-75,00	pagamento pos pagobancomat 12345 del 24/10 distrib.erg matte	Es l
Assegui		Lista	31/10/2004 28/10/2004	-1.240,00	disposizione di addebito generica bonifico a gigi rossi per a	
Carta		Carta	31/10/2004 30/10/2004	-60,00	pagamento pos pagobancomat 12345 del 30/10 agip f.lli morsill	<u>i</u>





Session Token Manipulation

Shup prosy v1.1	number of cookie	samples;
intercept options history alerts Request to http://	e cookie generatio	on
forward drop	🖲 text 🔿 hex	
GET http://u) Sport proxy v1.1	_ 🗆 ×
url=Q2Fzbz03JkFkdj0wJkRic3Q9IDM5MzI4MzAxOTU1O6ZTaXpIPT	TEOM2 intercept options history alerts	
application/ind.ms.excel, application/msword, application/k-shock	clowave Request to http://	
Accept-Language; it	forward drop	⊛ text ⊖ hex
soo11700211052016762428; IOLADVACT=ACP0-00-0-00; IOLADVPRF=WCP0000; IOLADVLCT= JSESSIONID=A2A5VpbNim79V10u2gwwChq1 aXuffq6JC941TRFs(800117002 User-Agent Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 4.0) Host Prost-Connection: Keep-Alive Prost-Connection: Keep-Alive Prost-Connection: Keep-Alive Prost-Connection: Keep-Alive Prost-Connection: Keep-Alive Prost-Connection: Keep-Alive Prost-Connection: Keep-Alive	Accept image/gif, image/x-xbitmap, image/jpeg, image/jpeg, application/vnd application/vnd.ms-excel, application/msword, application/x-shockwave-flash Accept-Language: it Cookie: codeOneShot=51566; msisdnOneShot=3 sessionID=A2ASVpbNirh79Vt0u2gwwChq1aXuffq0JC941TRFsQoqCLmF1Dt 8001!7002!1082015782428; IOLADVACT=ACP0-00-0:0; IOLADVPRF=WCP0000; IOLADVLCT=CLP0000; JSESSIONID=A2ASVpbNirh79Vt0u2gwwChq1aXuffq0JC941TRFsQoqCLmF1 8001!7002 User-Agent Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 4.0)	.ms-powerpoint, ,*/* VI-855668859I-1062677649I OLADVID=B155250362; DfVI-855668859I-1062677649I
Message Body (e.g. PC	Proxy-Connection: Keep-Alive	
Message body (e.g. 1 O	oon bage ballent	
Cookies		





Cross Site Request Forgery

Test if it is possible to force a user to submit an undesirable command to the logged application:

<html><body>

</body></html>



- HTTP Exploit
 - HTTP splitting
 - HTTP smuggling





When an HTTP request arrives from a client:

- the application must <u>validate</u> it before interact with all other application's components:
- File System, output, HTTP methods, DB, LDAP, XML doc, IMAP/SMTP command, OS command, code





Cross site scripting

Cross Site Scripting (XSS) testing when we try to manipulate the parameters that the application receive in input. A XSS breaks the following pattern:

Input -> Output == cross-site scripting

HTTP Methods and XST

Check that the web server is not configured to allow potentially dangerous HTTP methods and that XST is not possible. A XST breaks the following pattern:

Input -> HTTP Methods == XST

SQL Injection

The goal is to simulate a manipulation of data in the database that represents the core of every company. An SQL Injection breaks the following pattern:

Input -> Query SQL == SQL injection

The Guide analyze Oracle, MySql, Ms SQL Servers testing





LDAP Injection

Similar to SQL Injection Testing: the differences are that we use LDAP protocol instead of SQL and the target is an LDAP Server instead of an SQL Server. An LDAP Injection breaks the following pattern:

Input -> Query LDAP == LDAP injection

SML Injection

try to inject a particular XML doc to the application: if the XML parser fails to make an appropriate data validation the test will results positive. An XML Injection breaks the following pattern:

Input -> XML doc == XML injection

SSI Injection

If the web server's SSI support is enabled, the server will parse the directives received by the HTML. It can enable an attacker to inject code into html pages, or even perform remote code execution.





- IMAP/SMTP Injection
- Code Injection
- OS Commanding
- Buffer overflow
- Incubated vulnerability





- Usually not performed in "live" environment because you can cause service not available.
- DoS are types of vulnerabilities within applications that can allow a malicious user to make certain functionality or sometimes the entire website unavailable. These problems are caused by bugs in the application, often resulting from malicious or unexpected user input.
- Locking Customer Accounts
- User Specified Object Allocation
- User Input as a Loop Counter
- Writing User Provided Data to Disk
- Failure to Release Resources
- Storing too Much Data in Session





- SOA (Service Oriented Architecture)/Web services applications are up-andcoming systems which are enabling businesses to interoperate and are growing at an unprecedented rate.
- The vulnerabilities are similar to other "classical" vulnerabilities such as SQL injection, information disclosure ad leakage etc but web services also have unique XML/parser related vulnerabilities
- SML Structural Testin

```
<Envelope>
<Header>
<wsse:Security>
<Hehehe>I am a Large String (1MB)</Hehehe>
<Hehehe>I am a Large String (1MB)</Hehehe>
<Hehehe>I am a Large String (1MB)</Hehehe>...
<Signature>...</Signature>
</wsse:Security>
</Header>
<Body>
<BuyCopy><ISBN>0098666891726</ISBN></BuyCopy>
</Body></Envelope>
```



WS Testing



XML content-level Testing

An attacker can craft an XML document (SOAP message) that contains malicious elements in order to compromise the target system. We test for proper content validation.



master..xp_cmdshell 'net user Vxr pass /Add &userId=asi9485jfuhe92



WS Testing



Naughty SOAP attachments

```
POST /Service/Service.asmx HTTP/1.1
Host: somehost
Content-Type: text/xml; charset=utf-8
Content-Length: length
SOAPAction: http://somehost/service/UploadFile
<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"</pre>
 xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
<soap:Body>
<UploadFile xmlns="http://somehost/service">
<filename>eicar.pdf</filename>
<type>pdf</type>
<chunk>X50!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*</chunk>
<first>true</first>
</UploadFile>
</soap:Body>
</soap:Envelope>
```





AJAX (Asynchronous JavaScript and XML) is a web development technique used to create more responsive web applications.















- The OWASP Risk Rating Methodology
 - Estimate the severity of all of these risks to your business
 - This is not universal risk rating system: vulnerability that is critical to one organization may not be very important to another
- Simple approach to be tailored for every case
 - standard risk model: Risk = Likelihood * Impact
- Step 1: identifying a risk

You'll need to gather information about:

- the threat agent involved
- the attack they're using
- the vulnerability involved
- the impact of a successful exploit on your business.





Step 2: factors for estimating likelihood

Generally, identifying whether the likelihood is low, medium, or high is sufficient. Rate 0-9.

Threat Agent Factors:

- Skill level
- Motive
- Opportunity
- Size

Vulnerability Factors:

- Ease of discovery
- Ease of exploit
- Awareness
- Intrusion detection





Step 3: factors for estimating impact

Technical impact:

- Loss of confidentiality
- Loss of integrity
- Loss of availability
- Loss of accountability

Business impact:

- Financial damage
- Reputation damage
- Non-compliance
- Privacy violation





Step 4: determining the severity of the risk

	Threat age	ent factors			Vulnerability factors			
Skill level Motive Opportunity Size Ec		Ease of discovery	Ease of exploit	Awareness	Intrusion detection			
5	2	7	1	3	6	9	2	
		Ov	erall likelihood:	=4.375 (MEDIU	M)			
	Technie	cal Impact			Business Impact			
Loss of confidentialit	Loss of integrity	Loss of availability	Loss of accountabilit	Financial y damage	Reputation damage	Non- compliance	Privacy violation	
9	7	5	8	1	2	1	5	
O	verall technica	l impact=7.25 i	(HIGH)	С	verall business	impact=2.25 (LOW)	

In the example above, the likelihood is MEDIUM, and the technical impact is HIGH, so from technical the overall severity is HIGH. <u>But business impact</u> is actually LOW, so the overall severity is best described as <u>LOW</u> as well.





Step 5: Deciding What To Fix

As a general rule, you should fix the most severe risks first. Some fix seems to be not justifiable based upon the cost of fixing the issue but may be reputation damage from the fraud that could cost the organization much more than implement a security control

- Step 6: Customizing Your Risk Rating Model
 - Adding factors
 - Customizing options
 - Weighting factors



Writing Report



Category	Ref. Number	Name	Affected Item	Finding	Comment/Solution	Risk
Information Gathering	OWASP-IG- 001	Application Fingerprint				
	OWASP-IG- 002	Application Discovery				
	OWASP-IG- 003	Spidering and googling				
	OWASP-IG- 004	Analysis of error code				
	OWASP-IG- 005	SSL/TLS Testing				
	OWASP-IG- 006	DB Listener Testing				
	OWASP-IG- 007	File extensions handling				
	OWASP-IG- 008	Old, backup and unreferenced files				
Business logic testing	OWASP-BL- 001	Testing for business logic				
	OWASP-AT- 001	Default or guessable account				
	OWASP-AT- 002	Brute Force				

25 Jan 2007



What's next



You should adopt this guide in your organization

			Suggested Penetration Test and Vulnerability Analysis Procedures	\checkmark
0	Continuously	Wireless continued	WL110, Enterasys Roamabout Elsa Airlancer MC-11), freeware software, and an antenna and GPS. One technique used for finding a wireless network is War Driving. This is done by detecting the beacon and broadcast. War Driving is used to capture and map wireless band signal. Crack the WEP (Wired Equivalent Privacy) keys by using automated tools such as WEPCrack and	
\bigcirc	What's next:		AirSnort. The techniques used include IV Collisions and Weak key packet capture.	
	 Continuous 		a variety of automated tools, such as PrismDump, Iris, AiroPeek and Sniffer Wireless.	
			issues noted for management review. Before this test, it is best to consult legal representatives	
	 OWASP ar 		provide reasonable assurance that performing this test will not violate any laws or regulations due to picking up information packets from other unintended targets.	
	(P8) Security	Web Application	Analyse the web application and environment by first crawling through the web pages to gather the information including mapping of all pages and general understanding of all functionality to	
	Analysis Pr		ebsleuth) to find hidden data and locate form weaknesses. In conjunction with this survey, complete the following:	
			 Review inventory SSL/TLS ciphers to determine accordance with policies or standard industry practices. 	
			 Analyse session tracking including mechanism and session ID. 	
			 Identify authentication methods employed, including client certificates, auditing and revoking certificates, use of encryption or HTTP basic authentication and deployment of SSL. 	
			 Identify sign-on and sign-off (use of anticaching techniques and session inactivity cause automatic sign-off) mechanisms. 	
			 Identify all points of user input by recording every form element, specifically: 	
			 Lest SQL injection Attempt buffer overflow to gain control 	
			 Cross-site scripting (XSS) 	
			 Special characters (pipes, returns, etc.) 	
			 For numeric input try 0, a negative value, a really large value 	





Thank you!



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

matteo.meucci@owasp.org

25 Jan 2007





<u>References :</u>

- OWASP Foundation "OWASP Building Guide v3" 2006 <u>http://www.owasp.org/index.php/OWASP_Guide_Project</u>
- OWASP Foundation "OWASP Testing Guide v2 RC1" 2007 <u>http://www.owasp.org/index.php/OWASP_Testing_Project</u>
- OWASP Foundation "OWASP Top10" <u>http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project</u>
- OWASP Foundation Software:

WebGoat – <u>http://www.owasp.org/index.php/OWASP_WebGoat_Project</u>

WebScarab – <u>http://www.owasp.org/index.php/OWASP_WebScarab_Project</u>