OWASP
Open Web Application
Security Project

The New OWASP Testing Guide v4

Matteo Meucci
OWASP Testing Guide Co-lead

17th March 2015 – Security Summit - 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

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

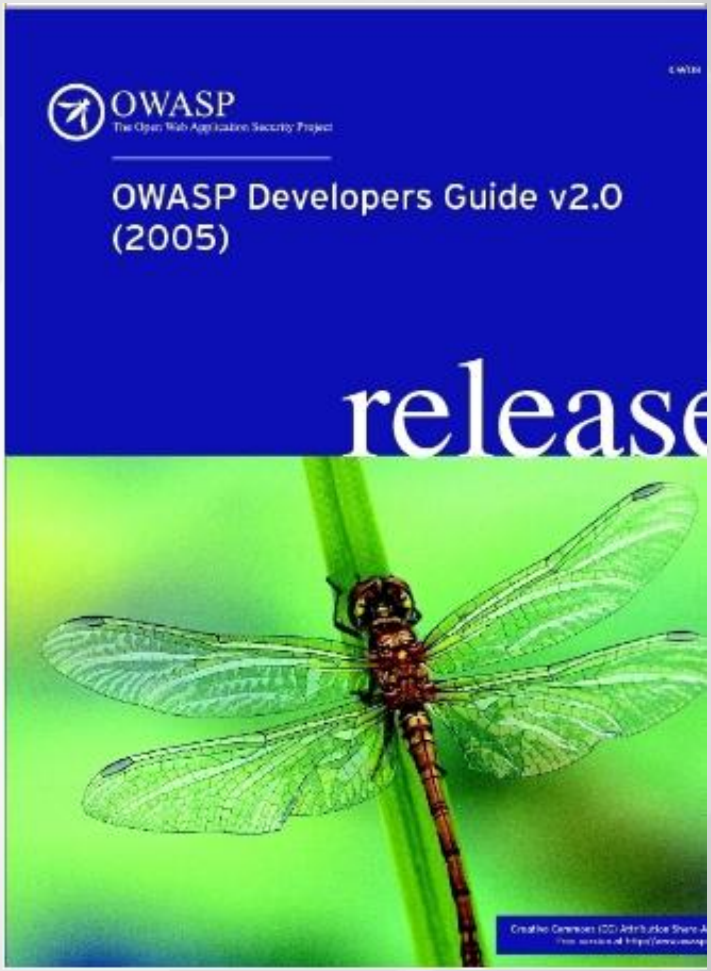
OWASP Guides today

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).

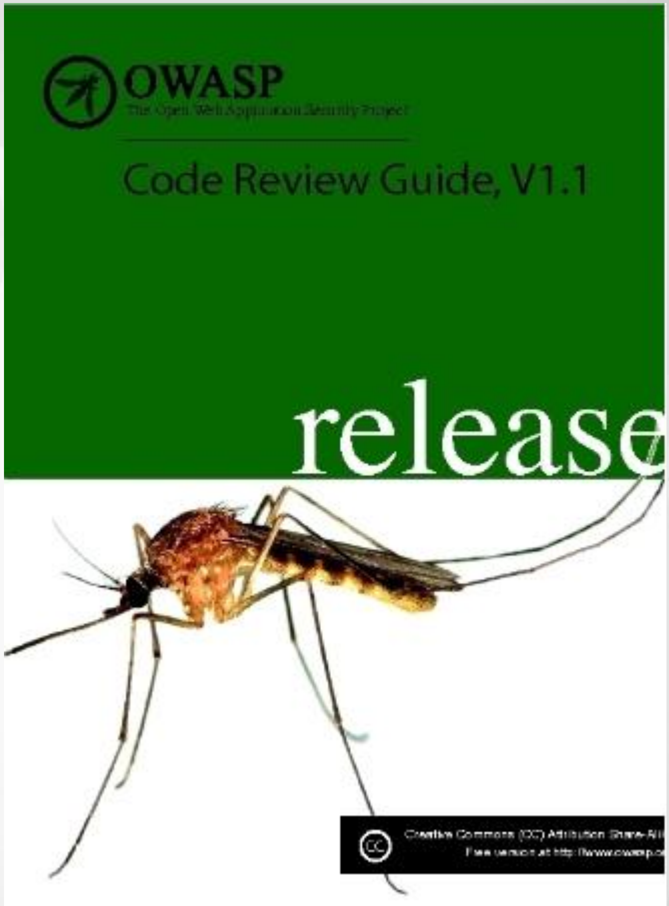
Developer Guide

- 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- Unfortunately Outdated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


OWASP
The Open Web Application Security Project
OWASP Developers Guide v2.0
(2005)
release

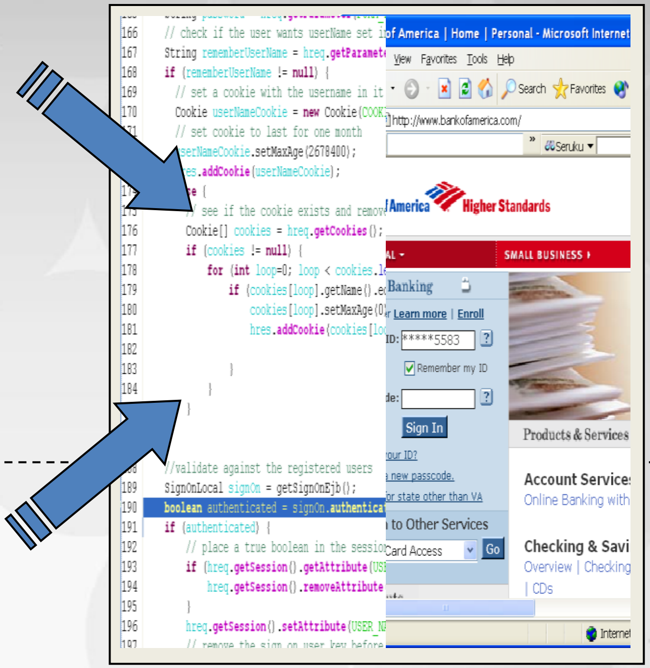
Code Review Guide

- 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


OWASP
The Open Web Application Security Project
Code Review Guide, V1.1
release
Creative Commons (CC) Attribution Share-Ali
Free version at http://www.owasp.o

www.owasp.org/index.php/Code_Review_Guide

Code Review Guide



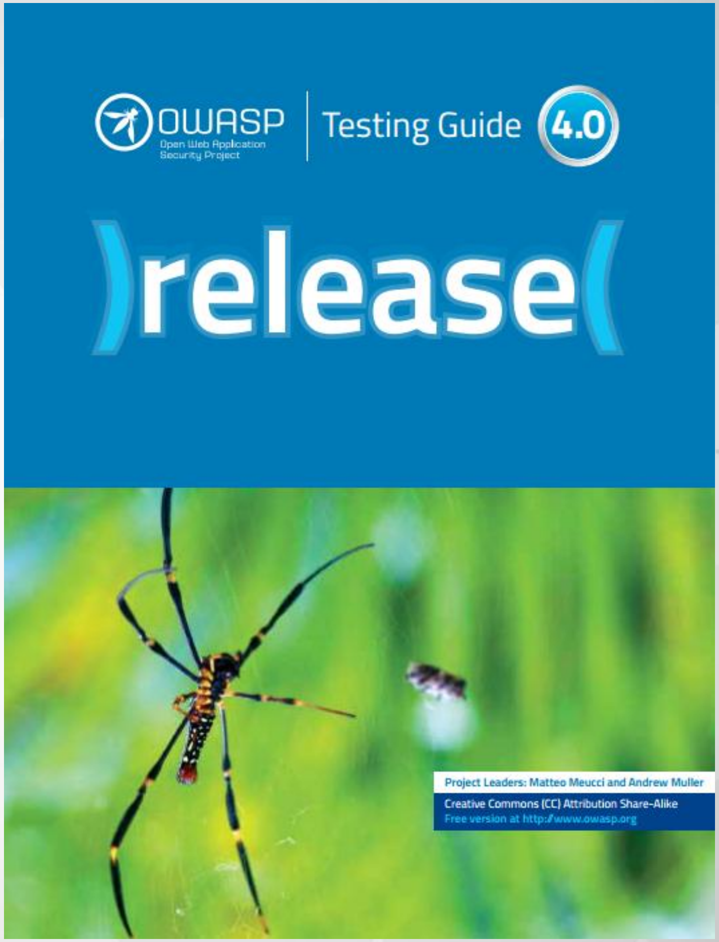
```
String password = hreq.getParameter(
// check if the user wants userName set i
String rememberUserName = hreq.getParamete
if (rememberUserName != null) {
  // set a cookie with the username in it
  Cookie userNameCookie = new Cookie(COOK
  // set cookie to last for one month
  serNameCookie.setMaxAge(2678400);
  es.addCookie(userNameCookie);
  e {
    / see if the cookie exists and remove
    Cookie[] cookies = hreq.getCookies();
    if (cookies != null) {
        for (int loop=0; loop < cookies.le
            if (cookies[loop].getName().eq
                cookies[loop].setMaxAge(0)
                hres.addCookie(cookies[loo

            }
        }
    }

//validate against the registered users
SignOnLocal signOn = getSignOnEjb();
boolean authenticated = signOn.authenticat
if (authenticated) {
    // place a true boolean in the session
    if (hreq.getSession().getAttribute(USE
        hreq.getSession().removeAttribute
    }
    hreq.getSession().setAttribute(USER_NA
    // remove the sign on user key before
```

```
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, andrew.muller@owasp.org

www.owasp.org/index.php/Testing_Guide



OWASP Open Web Application Security Project | Testing Guide 4.0

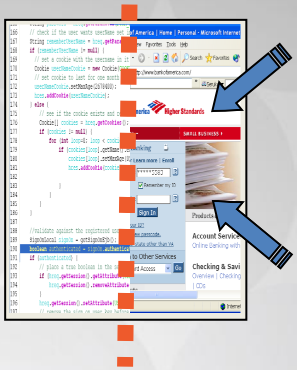
)release(

Project Leaders: Matteo Meucci and Andrew Muller

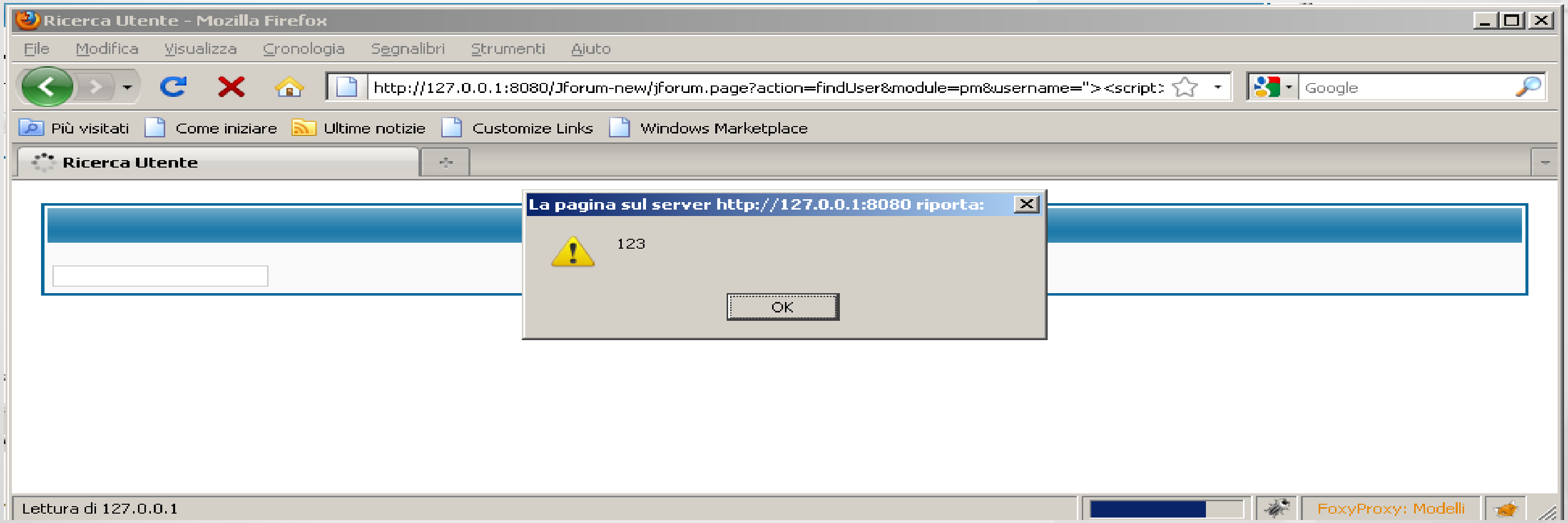
Creative Commons (CC) Attribution Share-Alike

Free version at http://www.owasp.org

Testing Guide



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



http://127.0.0.1:8080/Jforum-new/jforum.page?action=findUser&module=pm&username="><script>

La pagina sul server http://127.0.0.1:8080 riporta:

123

OK

Lettura di 127.0.0.1

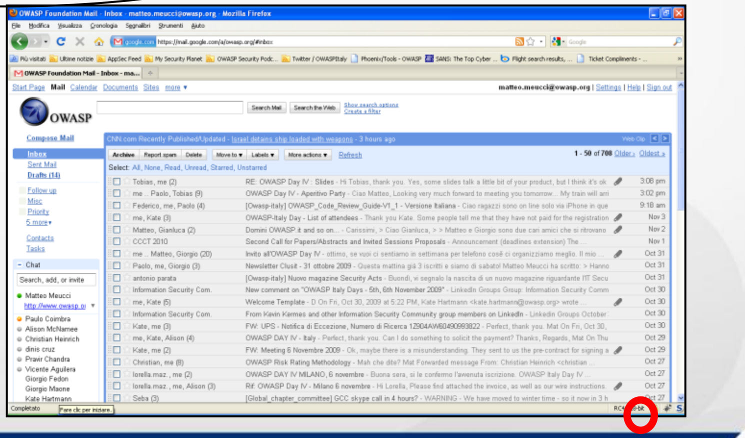
The new Testing Guide: why?

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!


File Modifica Visualizza Cronologia Segnalibri Strumenti Aiuto
google.com
Più visitati · Ultime notizie · AppSec Feed · My Security Planet · OWASP Security Podc... · Twitter / OWASPItaly · Phoenix/Tools - OWASP · SANS: The Top Cyber ... · Flight search results, ... · Ticket Compliments - ...
OWASP Foundation Mail - Inbox - ma...
Start Page Mail Calendar Documents Sites more ▾
Settings | Help | Sign out
OWASP
Search Mail · Search the Web · Show search options · Create a filter
Compose Mail
Inbox
Sent Mail
Drafts (14)
Follow up
Misc
Priority
5 more▾
Contacts
Tasks
Chat
Search, add, or invite
Web Clip
Archive · Report spam · Delete · Move to ▾ · Labels ▾ · More actions ▾ · Refresh
Older › · Oldest »
Select: All, None, Read, Unread, Starred, Unstarred
Completato
Fare clic per iniziare.
RC4 -bit

OWASP Foundation Mail - Inbox - matteo.meucci@owasp.org - Mozilla Firefox

https://mail.google.com/a/owasp.org/#inbox

matteo.meucci@owasp.org

CNN.com Recently Published/Updated - Israel detains ship loaded with weapons - 3 hours ago

1 - 50 of 708

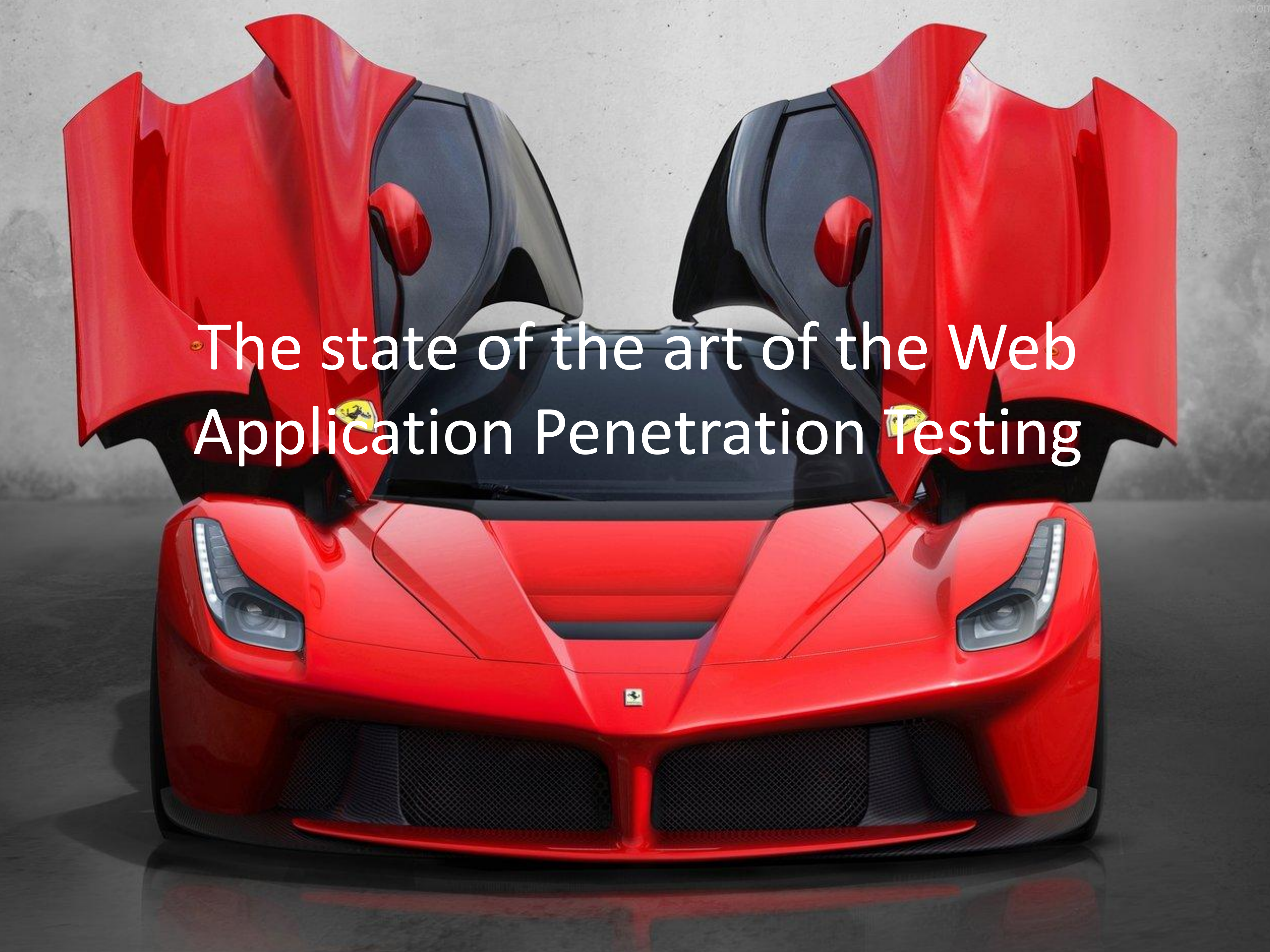
Matteo Meucci
http://www.owasp.o
Paulo Coimbra
Alison McNamee
Christian Heinrich
dinis cruz
Prawr Chandra
Vicente Aguilera
Giorgio Fedon
Giorgio Maone
Kate Hartmann

Tobias, me (2)	RE: OWASP Day IV : Slides - Hi Tobias, thank you. Yes, some slides talk a little bit of your product, but I think it's ok	3:08 pm
me .. Paolo, Tobias (9)	OWASP Day IV - Aperitivo Party - Ciao Matteo, Looking very much forward to meeting you tomorrow... My train will arri	3:02 pm
Federico, me, Paolo (4)	[Owasp-italy] OWASP_Code_Review_Guide-V1_1 - Versione Italiana - Ciao ragazzi sono on line solo via iPhone in que	9:18 am
me, Kate (3)	OWASP-Italy Day - List of attendees - Thank you Kate. Some people tell me that they have not paid for the registration	Nov 3
Matteo, Gianluca (2)	Domini OWASP.it and so on... - Carissimi, > Ciao Gianluca, > > Matteo e Giorgio sono due cari amici che si ritrovano	Nov 2
CCCT 2010	Second Call for Papers/Abstracts and Invited Sessions Proposals - Announcement (deadlines extension) The ...	Nov 1
me .. Matteo, Giorgio (20)	Invito all'OWASP Day IV - ottimo, se vuoi ci sentiamo in settimana per telefono cosě ci organizziamo meglio. Il mio ...	Oct 31
Paolo, me, Giorgio (3)	Newsletter Clusit - 31 ottobre 2009 - Questa mattina già 3 iscritti e siamo di sabato! Matteo Meucci ha scritto: > Hanno	Oct 31
antonio parata	[Owasp-italy] Nuovo magazine Security Acts - Buondì, vi segnalo la nascita di un nuovo magazine riguardante l'IT Secu	Oct 31
Information Security Com.	New comment on "OWASP Italy Days - 5th, 6th November 2009" - LinkedIn Groups Group: Information Security Comm	Oct 30
me, Kate (5)	Welcome Template - D On Fri, Oct 30, 2009 at 5:22 PM, Kate Hartmann <kate.hartmann@owasp.org> wrote ...	Oct 30
Information Security Com.	From Kevin Kermes and other Information Security Community group members on LinkedIn - LinkedIn Groups October	Oct 30
Kate, me (3)	FW: UPS - Notifica di Eccezione, Numero di Ricerca 1Z904AW60490993822 - Perfect, thank you. Mat On Fri, Oct 30,	Oct 30
me, Kate, Alison (4)	OWASP DAY IV - Italy - Perfect, thank you. Can I do something to solicit the payment? Thanks, Regards, Mat On Thu	Oct 29
Kate, me (2)	FW: Meeting 6 Novembre 2009 - Ok, maybe there is a misunderstanding. They sent to us the pre-contract for signing a	Oct 29
Christian, me (8)	OWASP Risk Rating Methodology - Mah che dite? Mat Forwarded message From: Christian Heinrich <christian ...	Oct 27
lorella.maz., me (2)	OWASP DAY IV MILANO, 6 novembre - Buona sera, si le confermo l'avvenuta iscrizione. OWASP Italy Day IV ...	Oct 27
lorella.maz., me, Alison (3)	Rif: OWASP Day IV - Milano 6 novembre - Hi Lorella, Please find attached the invoice, as well as our wire instructions.	Oct 27
Seba (3)	[Global_chapter_committee] GCC skype call in 4 hours? - WARNING - We have moved to winter time - so it now in 3 h	Oct 27

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



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 befor 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

OWASP
Open Web Application Security Project
Testing Guide 4.0
)release(
Project Leaders: Matteo Meucci and Andrew Muller
Creative Commons (CC) Attribution Share-Alike
Free version at http://www.owasp.org

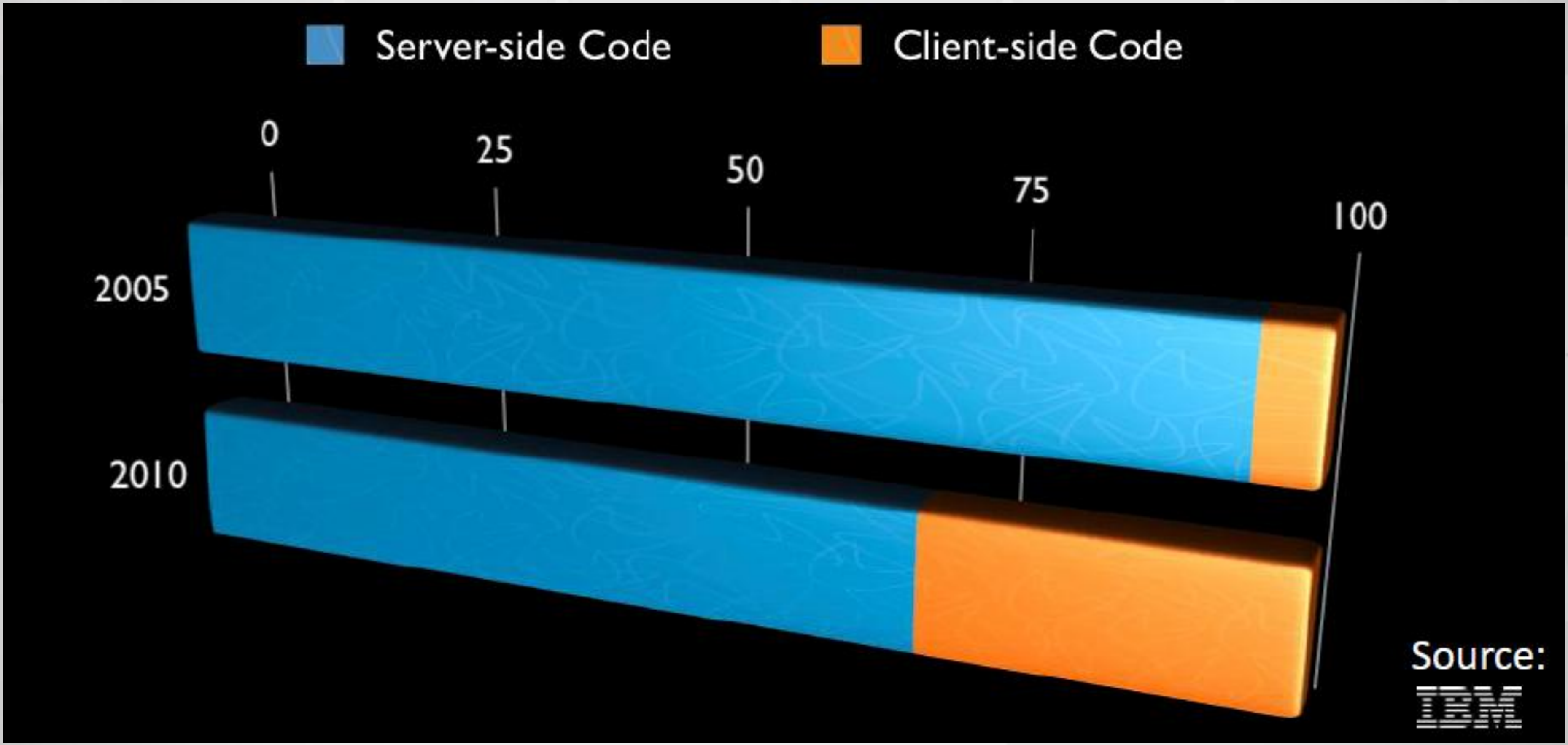
Contents

- 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



Source: IBM

Code Flow & Terminology

Sources:

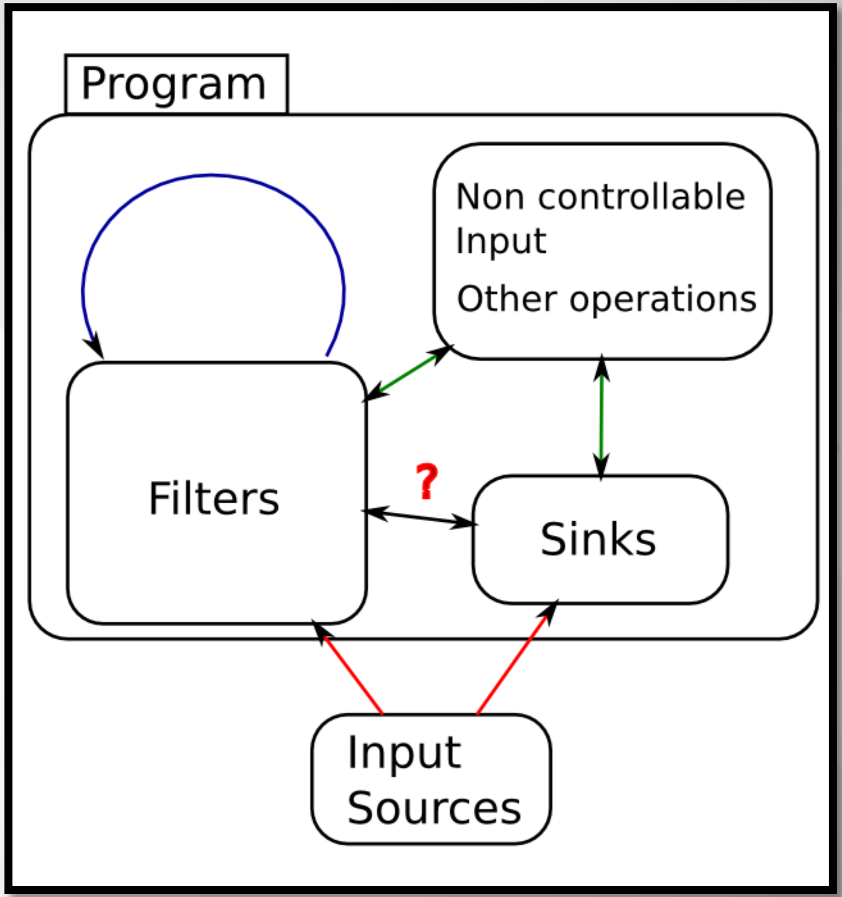
the input which can be directly or indirectly controlled by the attacker.

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”));          Tainted Source
   document.write(“Hello, ” + user);          Sink
</script>
```

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

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, <img src="aaa" onerror=alert(1)></p>
```

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>
```

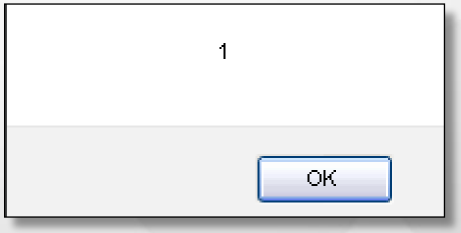
Source

Sink

+

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

=


1

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

Bank of America | Home | Personal - Microsoft Internet
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://www.bankofamerica.com/
Google
Seruku
Bank of America Higher Standards
PERSONAL
SMALL BUSINESS
Online Banking
New user Learn more | Enroll
Sign In
Forgot your ID?
Create a new passcode.
Sign in for state other than VA
Sign In to Other Services
Go
Products & Services
Account Service
Online Banking with
Checking & Savi
Overview | Checking
| CDs
Internet

Online ID: *****5583

☑ Remember my ID

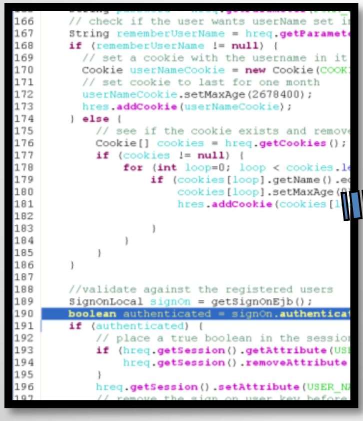
Passcode:

Credit Card Access

Web Application

Methodology

Report



```
    // check if the user wants userName set i
    String rememberUserName = hreq.getParamete
    if (rememberUserName != null) {
      // set a cookie with the username in it
      Cookie userNameCookie = new Cookie(COOK
      // set cookie to last for one month
      userNameCookie.setMaxAge(2678400);
      hres.addCookie(userNameCookie);
    } else {
        // see if the cookie exists and remove
        Cookie[] cookies = hreq.getCookies();
        if (cookies != null) {
            for (int loop=0; loop < cookies.le
                if (cookies[loop].getName().eq
                    cookies[loop].setMaxAge(0
                    hres.addCookie(cookies[l

                }
            }
        }
    }

    //validate against the registered users
    SignOnLocal signOn = getSignOnEjb();
    boolean authenticated = signOn.authenticat
    if (authenticated) {
        // place a true boolean in the sessior
        if (hreq.getSession().getAttribute(USE
            hreq.getSession().removeAttribute
        }
        hreq.getSession().setAttribute(USER_NA
```

Source Code

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

this.context.put("showResult",
showResult);

        }
```

Fixing

Methodology

Retest Report

Common misunderstanding

I DON'T WANT A DIVORCE...
I DIDN'T KNOW WE WERE MARRIED...
GL

Example of unstructured approach:

Ministry of Informatics

Actors

Ministry of Informatics: who buys the software

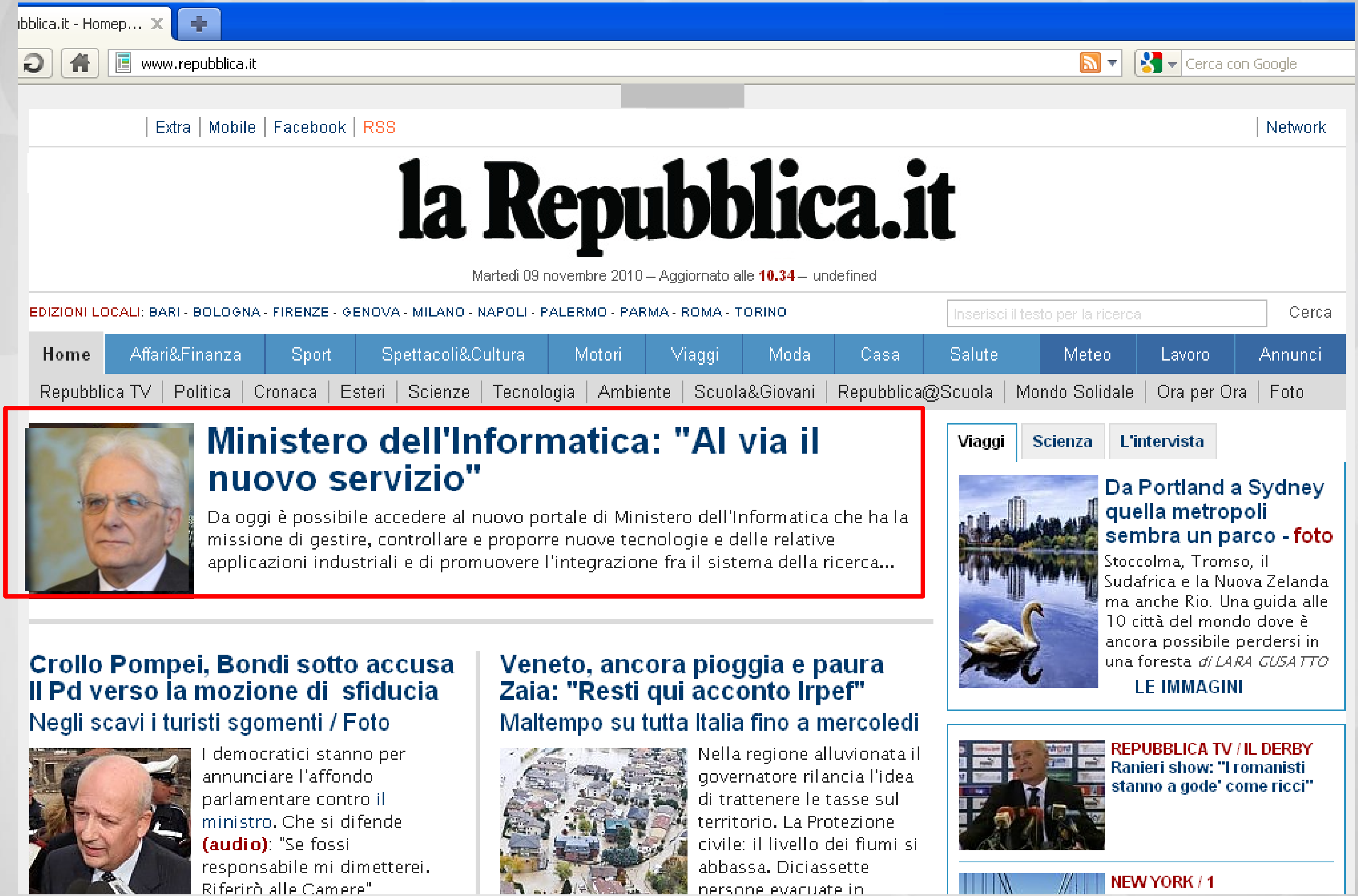
Development teams (internal/external): who develops the software

User: who uses the software

Press conference for the launch of the service

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

The day after…



ıbblica.it - Homep…

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

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

Viaggi | Scienza | L'intervista

Da Portland a Sydney quella metropoli sembra un parco - foto

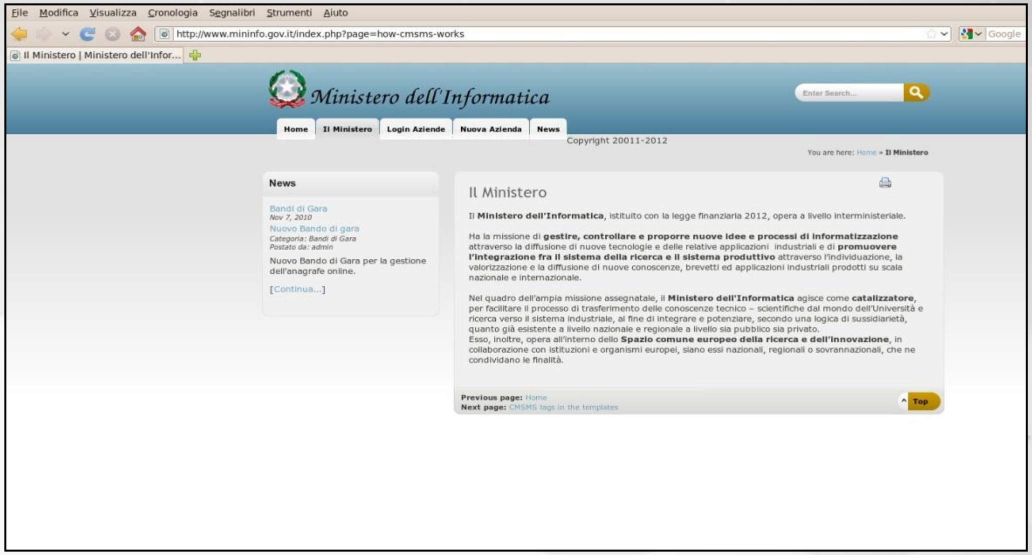
Stoccolma, Tromso, il Sudafrica e la Nuova Zelanda ma anche Rio. Una guida alle 10 città del mondo dove è ancora possibile perdersi in una foresta *di LARA GUSATTO*

LE IMMAGINI

REPUBBLICA TV / IL DERBY Ranieri show: "I romanisti stanno a gode' come ricci"

NEW YORK / 1

Users access to the portal…


File Modifica Visualizza Cronologia Segnalibri Strumenti Aiuto
http://www.mininfo.gov.it/index.php?page=how-cmsms-works
Google
Il Ministero | Ministero dell'Infor...
Ministero dell'Informatica
Enter Search...
Home
Il Ministero
Login Aziende
Nuova Azienda
News

Copyright 20011-2012

You are here: Home » Il Ministero

News

Bandi di Gara
Nov 7, 2010
Nuovo Bando di gara
Categoria: Bandi di Gara
Postato da: admin

Nuovo Bando di Gara per la gestione dell'anagrafe online.

[Continua...]

Il Ministero

Il **Ministero dell'Informatica**, istituito con la legge finanziaria 2012, opera a livello interministeriale.

Ha la missione di **gestire, controllare e proporre nuove idee e processi di informatizzazione** attraverso la diffusione di nuove tecnologie e delle relative applicazioni industriali e di **promuovere l'integrazione fra il sistema della ricerca e il sistema produttivo** attraverso l'individuazione, la valorizzazione e la diffusione di nuove conoscenze, brevetti ed applicazioni industriali prodotti su scala nazionale e internazionale.

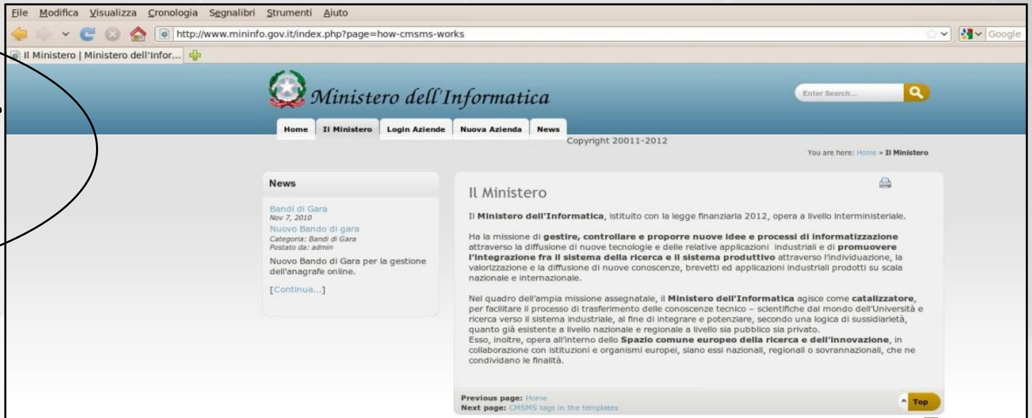
Nel quadro dell'ampia missione assegnatale, il **Ministero dell'Informatica** agisce come **catalizzatore**, per facilitare il processo di trasferimento delle conoscenze tecnico – scientifiche dal mondo dell'Università e ricerca verso il sistema industriale, al fine di integrare e potenziare, secondo una logica di sussidiarietà, quanto già esistente a livello nazionale e regionale a livello sia pubblico sia privato.
Esso, inoltre, opera all'interno dello **Spazio comune europeo della ricerca e dell'innovazione**, in collaborazione con istituzioni e organismi europei, siano essi nazionali, regionali o sovrannazionali, che ne condividano le finalità.

Previous page: Home
Next page: CMSMS tags in the templates

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…



http://www.mininfo.gov.it/index.php?page=how-cmsms-works

Il Ministero | Ministero dell'Infor...

Ministero dell'Informatica

Copyright 20011-2012

You are here: Home » **Il Ministero**

News

Bandi di Gara
Nov 7, 2010
Nuovo Bando di gara
Categoria: Bandi di Gara
Postato da: admin

Nuovo Bando di Gara per la gestione dell'anagrafe online.

[Continua...]

Il Ministero

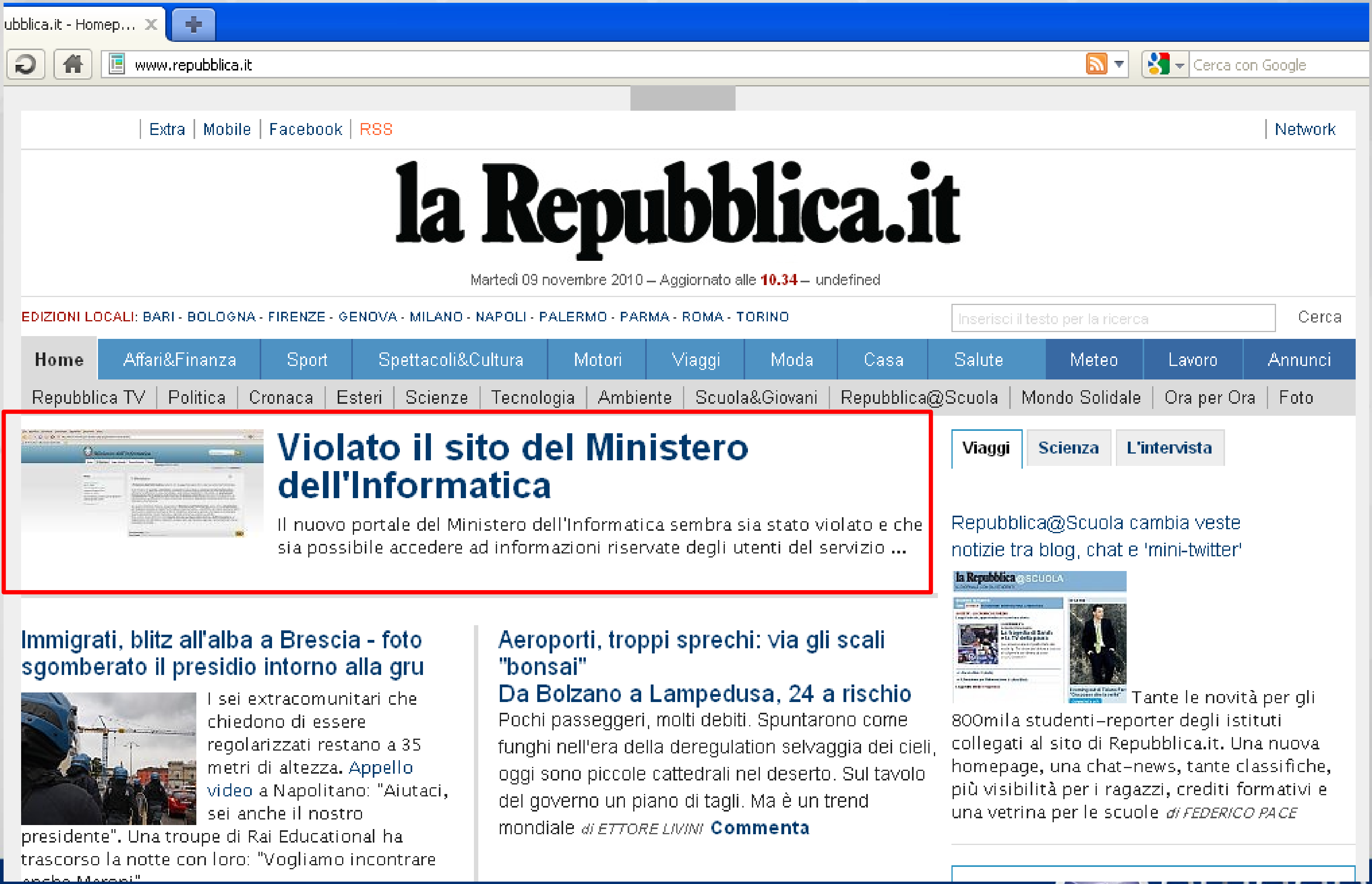
Il **Ministero dell'Informatica**, istituito con la legge finanziaria 2012, opera a livello interministeriale.

Ha la missione di **gestire, controllare e proporre nuove idee e processi di informatizzazione** attraverso la diffusione di nuove tecnologie e delle relative applicazioni industriali e di **promuovere l'integrazione fra il sistema della ricerca e il sistema produttivo** attraverso l'individuazione, la valorizzazione e la diffusione di nuove conoscenze, brevetti ed applicazioni industriali prodotti su scala nazionale e internazionale.

Nel quadro dell'ampia missione assegnatale, il **Ministero dell'Informatica** agisce come **catalizzatore**, per facilitare il processo di trasferimento delle conoscenze tecnico – scientifiche dal mondo dell'Università e ricerca verso il sistema industriale, al fine di integrare e potenziare, secondo una logica di sussidiarietà, quanto già esistente a livello nazionale e regionale a livello sia pubblico sia privato.
Esso, inoltre, opera all'interno dello **Spazio comune europeo della ricerca e dell'innovazione**, in collaborazione con istituzioni e organismi europei, siano essi nazionali, regionali o sovrannazionali, che ne condividano le finalità.

Previous page: Home
Next page: CMSMS tags in the templates

Some days after…



ubblica.it - Homep… ✕

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

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

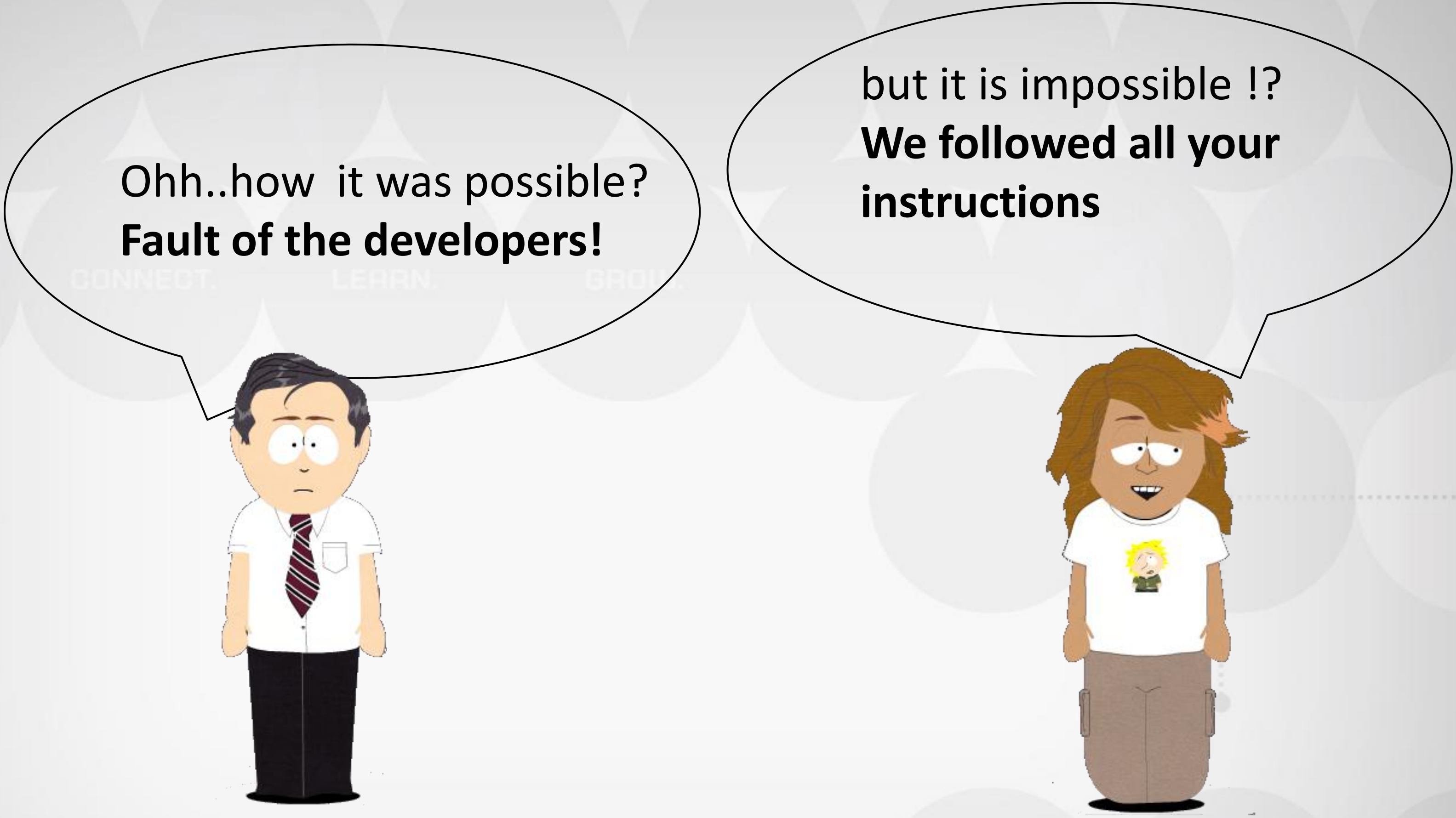
Pochi passeggeri, molti debiti. Spuntarono come funghi nell'era della deregulation selvaggia dei cieli, oggi sono piccole cattedrali nel deserto. Sul tavolo del governo un piano di tagli. Ma è un trend mondiale *di ETTORE LIVINI* **Commenta**

Viaggi | Scienza | L'intervista

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

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*

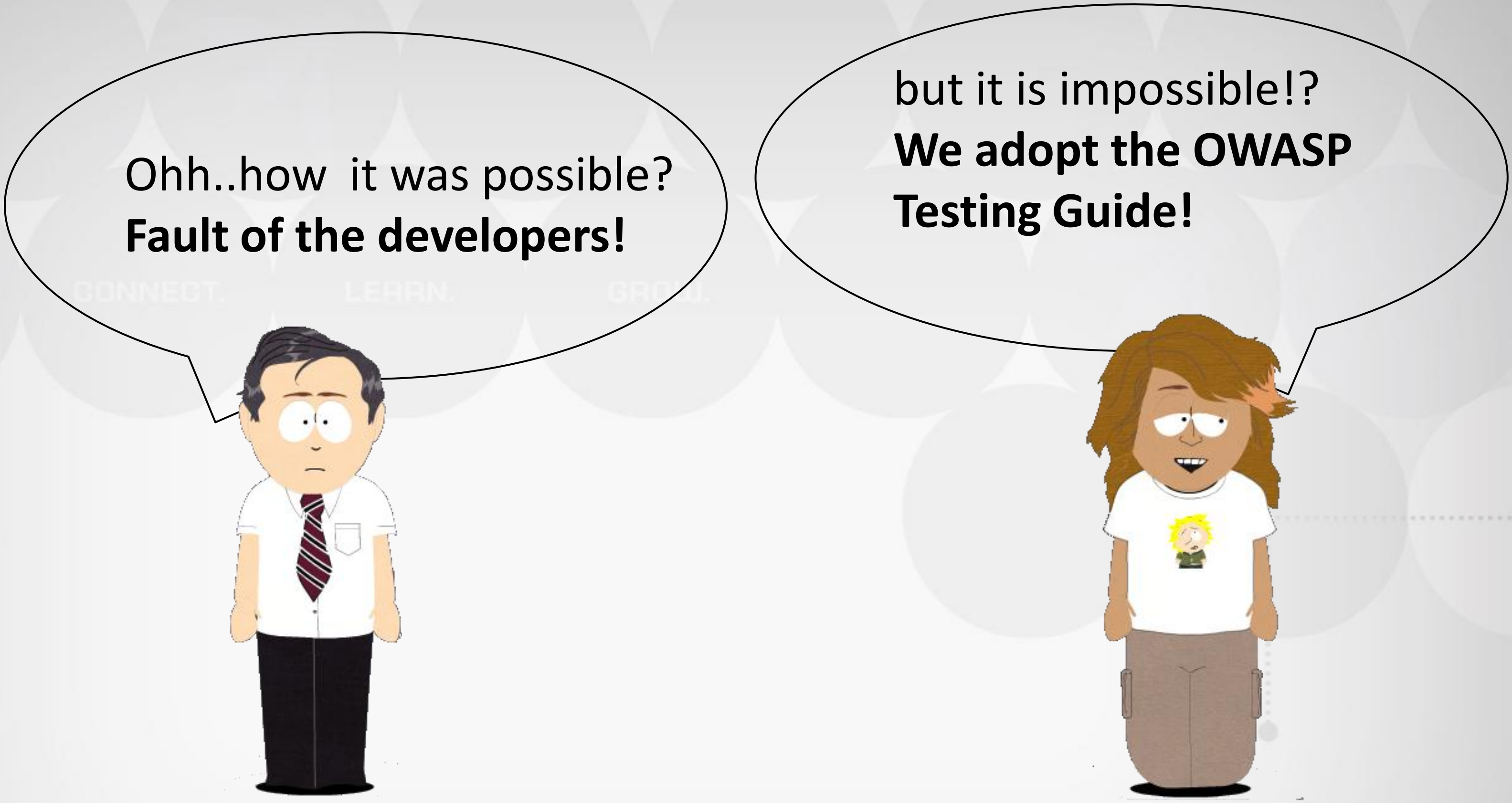
The reactions…


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

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

CONNECT. LEARN. GROW.

A structured approach:

OWASP Guidelines and tools

The Importance to use all the OWASP resources into your SDLC

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

OWASP

SECURE SOFTWARE DEVELOPMENT CONTRACT ANNEX

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

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

OWASP

OWASP Top 10 - 2013

release

OWASP

Application Security Guide For CISOs

Version 1.0 (November 2013)

- Use the OWASP Top 10 for General Awareness
- Use the CISO Guide for Management's Awareness

Vulnerabilities in the software development process are expected

Enterprise Security API

OWASP

OWASP Deve (2005)

OWASP

Code Review

re

OWASP Testing Guide 4.0

release

- 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

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 Guidelines in the SAMM model

Governance

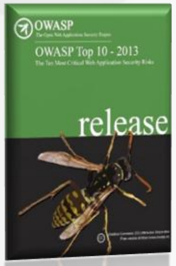
Construction

Verification

Deployment

OWASP

SECURE SOFTWARE DEVELOPMENT CONTRACT ANNEX


OWASP

The Open Web Application Security Project

OWASP Top 10 - 2013

The Ten Most Critical Web Application Security Risks

release

Custom Enterprise Web Application

Enterprise Security API

Authenticator | User | AccessController | AccessReferenceMap | Validator | Encoder | HTTPUtilities | Encryptor | EncryptedProperties | Randomizer | Exception Handling | Logger | IntrusionDetector | SecurityConfiguration

Existing Enterprise Security Services/Libraries

OWASP

Application Security Verification Standard (2014)

Web Application Standard

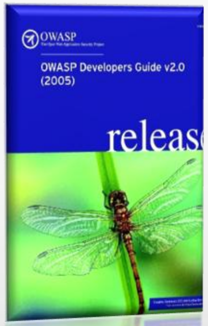
OWASP ZAP

Software Assurance Maturity Model

OWASP

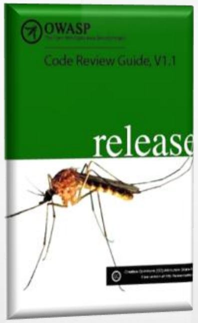
Application Security Guide For CISOs

Version 1.0 (November 2013)


OWASP

OWASP Developers Guide v2.0 (2005)

release


OWASP

Code Review Guide, V1.1

release

OWASP

Testing Guide 4.0

)release(

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

matteo.meucci@owasp.org