



# Perchè chiedere la sicurezza del software?

**Stefano Di Paola**

**OWASP-Italy R&D Director**



**MEF**

Ministero dell'Economia e delle Finanze

**OWASP Day per la PA**

Roma

9, Novembre 2010

Copyright © 2009 - The OWASP Foundation  
Permission is granted to copy, distribute and/or modify this document  
under the terms of the GNU Free Documentation License.

**The OWASP Foundation**  
<http://www.owasp.org>

# Agenda

- ➊ Illustrazione di un tipico caso di studio per la realizzazione di un nuovo portale di una PA
- ➋ Analisi degli impatti di alcune vulnerabilità trascurate
- ➌ Analisi delle criticità da affrontare per una PA



# Who am I?

## Research

- ▶ OWASP-Italy R&D Director
- ▶ OWASP Flash Security lead
- ▶ Dom-XSS wiki lead
- ▶ Hundreds security advisories released



## Work

- ▶ CTO @ Minded Security Application Security Consulting
- ▶ 15+ years experience on Application Security



**Minded**  
security



# **Caso di studio: Ministero dell'Informatica**



# Attori coinvolti



Ministero  
Informatica



Amministratore  
di sistema



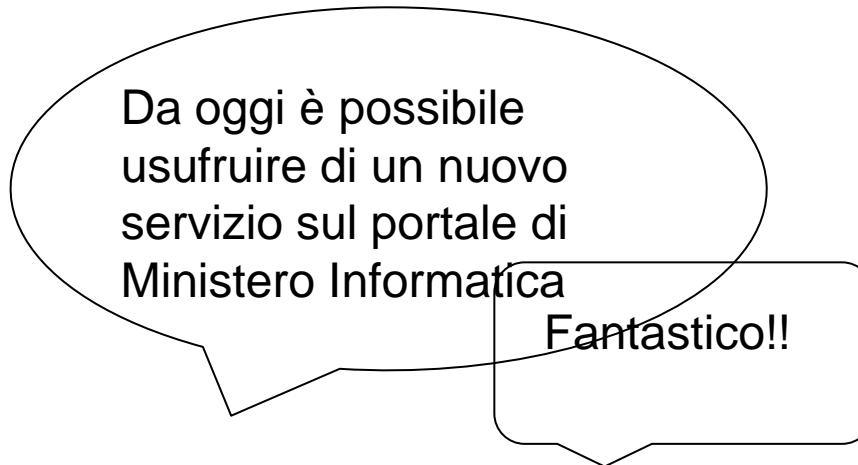
Rompiscatole:  
utente malizioso



Esperto di  
sicurezza sw



# Conferenza stampa per il lancio del portale



Fantastico!!

Complimenti!!



# Il giorno dopo...

iblica.it - Home... X +

www.repubblica.it

Rss 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 Zai: "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, 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



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

NEW YORK / 1

OWASP Day per la PA – 9 Novembre 10

OWASP-Italy

# Accesso al portale...



The screenshot shows a web browser displaying the official website of the Italian Ministry of Information (<http://www.mininfo.gov.it/index.php?page=how-cmsms-works>). The page title is "Ministero dell'Informatica". The main content area features a news item titled "Bandi di Gara" with a link to "Nuovo Bando di gara". Below the news item, there is a detailed description of the ministry's mission and its role in promoting innovation and integration between research and production systems. The footer includes copyright information (Copyright 2001-2012) and navigation links.



**Mario Verdi – 12/12/1970**  
**Mario Rossi- 10/09/1982**  
**Paolo Rossi – 09/02/1960**



# Accesso al portale...

Oh oh...ho trovato un  
problemino...



The screenshot shows a web browser window displaying the official website of the Italian Ministry of Information (Ministero dell'Informatica). The URL in the address bar is <http://www.mininfo.gov.it/index.php?page=how-cmsms-works>. The page content indicates a 404 error, stating "Sorry, the page you were looking for does not exist". Below this, there is a message about the ministry's mission to manage, control, and propose new ideas and processes of informatization through the diffusion of new technologies and their related applications, industrial and promotional, between the research system and the productive system. It also mentions the integration of the research system and the productive system through individualization, valorization, and diffusion of new knowledge, patents, and industrial products at national and international levels. The page includes a sidebar with news items and a footer with copyright information and links.



# Qualche giorno dopo...

ubblica.it - Home... 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



## 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 ...

Viaggi | Scienza | L'intervista

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

**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**

**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*



# Le reazioni...



Ohh..ma come è stato  
possibile?

Non saprei...ma è  
impossibile!?



# Perchè è potuto succedere?

Avete fatto un'analisi  
delle criticità prima di  
rilasciare il sito in  
esercizio?



# Analisi delle criticità

- ⌚ Non abbiamo richiesto requisiti di sicurezza al software acquistato
- ⌚ Non ci sono state verifiche di sicurezza per il sw
- ⌚ Non ci sono state verifiche di sicurezza per l'infrastruttura su cui gira la applicazione



# **Video dimostrativi relativi all'applicazione di esempio**



# Grazie!

## Domande?

<http://www.owasp.org/index.php/Italy>

stefano.dipaola@owasp.org

