Perchè chiedere la sicurezza del software?

Stefano Di Paola

OWASP-Italy R&D Director

OWASP Day per la PA
Roma
9, Novembre 2010

MEF
Ministero dell'Economia e delle Finanze

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

- Illustrazione di un tipico caso di studio per la realizzazione di un nuovo portale di una PA
- Analisi degli impatti di alcune vulnerabilità trascurate
- 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

Caso di studio:

Ministero dell'Informatica

Attori coivolti

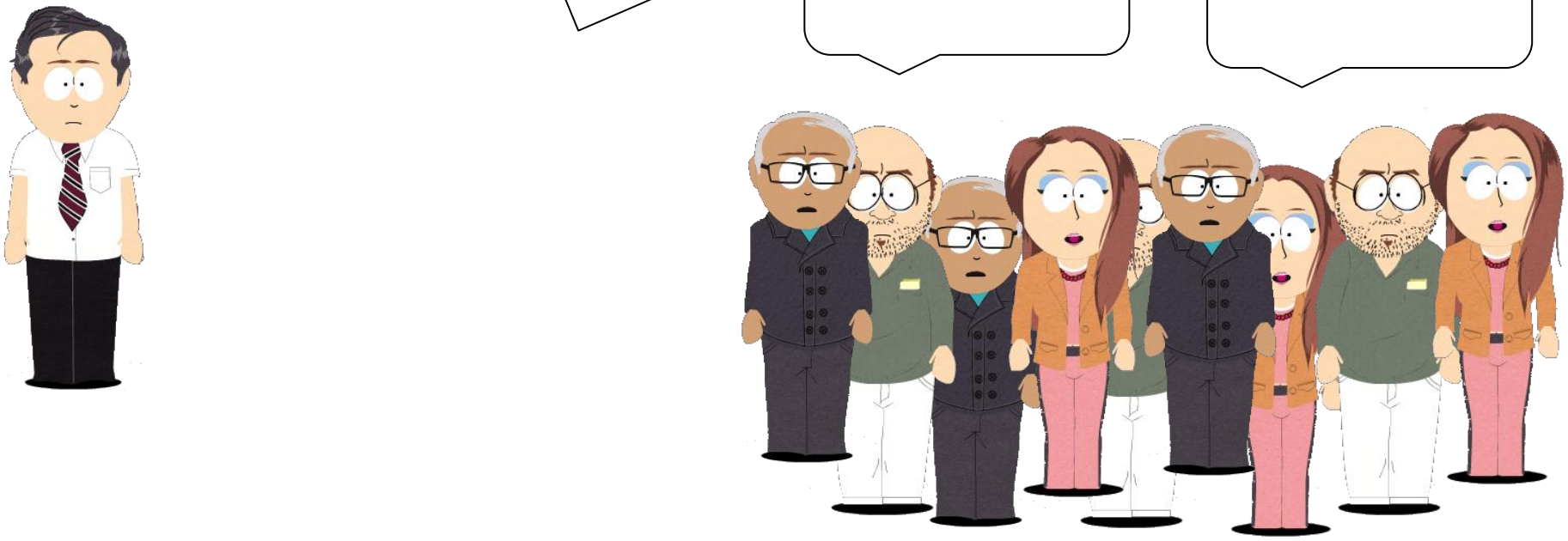
Ministero
Informatica

Amministratore
di sistema

Rompiscatole:
utente malizioso

Esperto di
sicurezza sw

Conferenza stampa per il lancio del portale



Il giorno dopo...

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

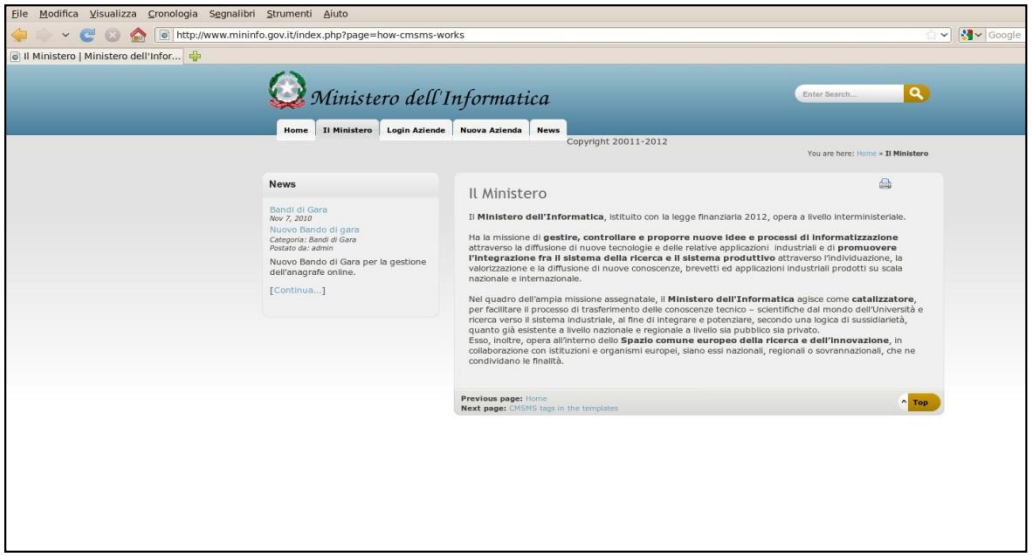
Stoccolma, Tromso, il Sudafrica e la Nuova Zelanda ma anche Rio. Una guida alle 10 città del mondo dove è ancora possibile perdersi in una foresta *di LARA GUSATTO*

LE IMMAGINI

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

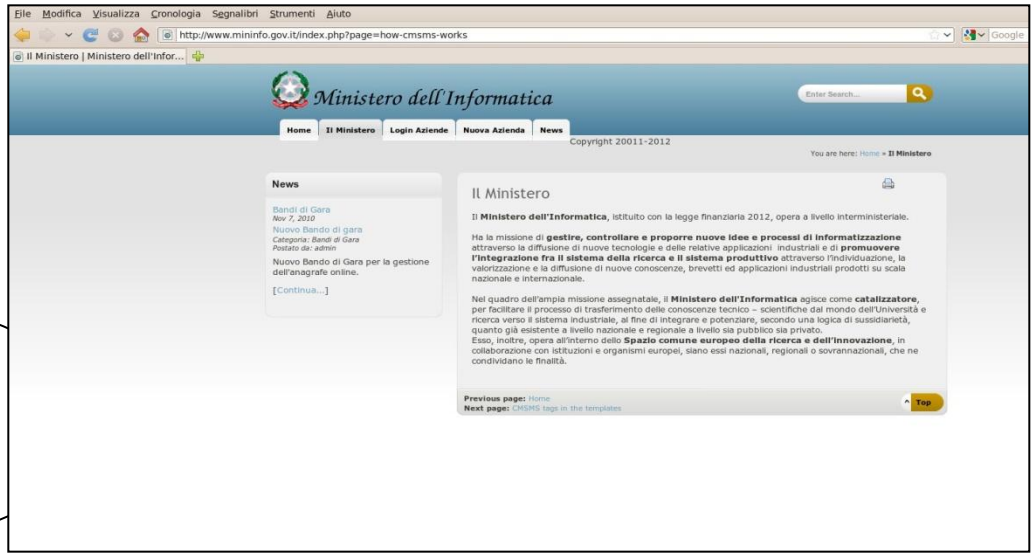
NEW YORK / 1

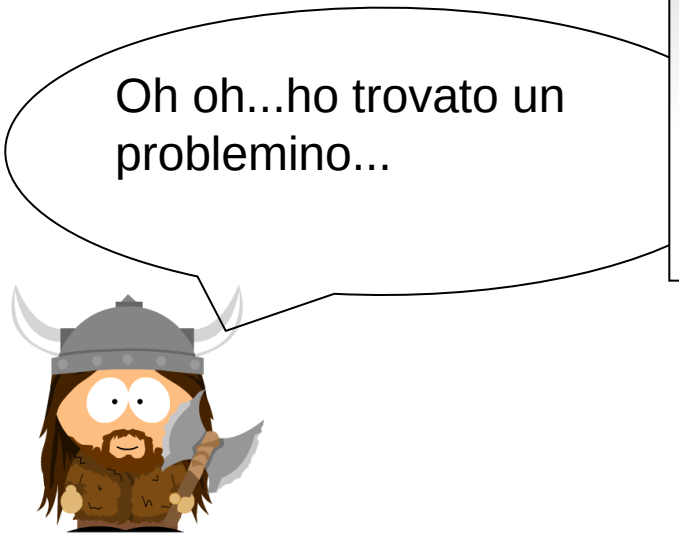
Accesso al portale...



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

Accesso al portale...





Qualche giorno dopo...

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 ...

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*

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

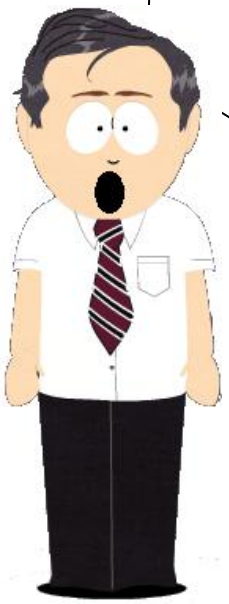
I sei extracomunitari che chiedono di essere regolarizzati restano a 35 metri di altezza. Appello video a Napolitano: "Aiutaci, sei anche il nostro presidente". Una troupe di Rai Educational ha trascorso la notte con loro: "Vogliamo incontrare

Aeroporti, troppi sprechi: via gli scali "bonsai"

Da Bolzano a Lampedusa, 24 a rischio

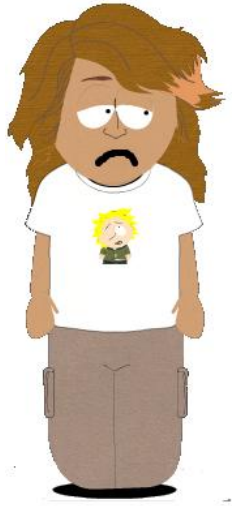
Pochi passeggeri, molti debiti. Spuntarono come funghi nell'era della deregulation selvaggia dei cieli, oggi sono piccole cattedrali nel deserto. Sul tavolo del governo un piano di tagli. Ma è un trend mondiale *di ETTORE LIVINI* **Commenta**

Le reazioni...

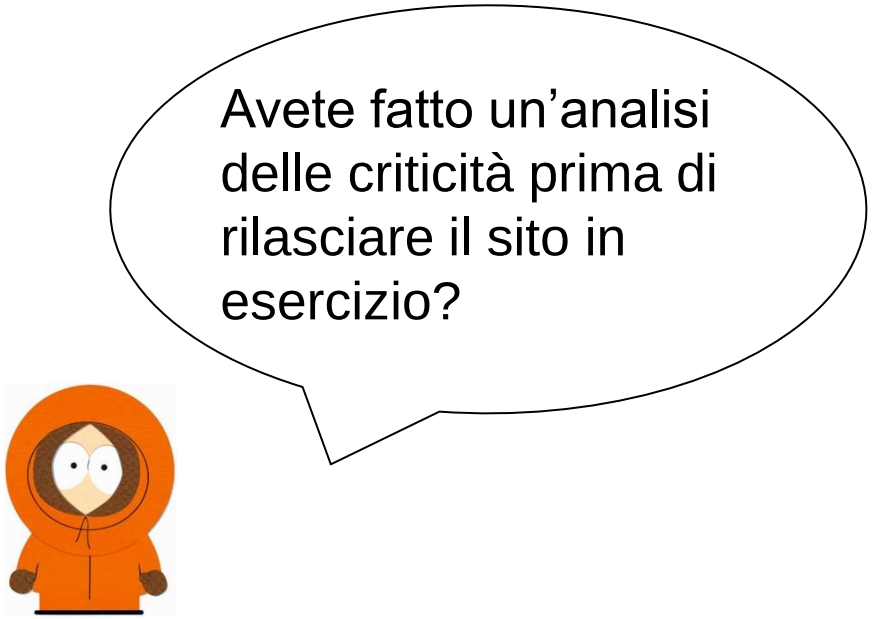


Ohh..ma come è stato possibile?

Non saprei...ma è impossibile!?



Perchè è potuto succedere?



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