



OWASP Backend Security Project

Carlo Pelliccioni

Senior Security Consultant
Spike Reply

c.pelliccioni@reply.it

OWASP-Day II
Università "La Sapienza", Roma
31st, March 2008

Copyright © 2008 - 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

- ❑ Qual'è la situazione attuale?
- ❑ Quali sono i principali rischi?
- ❑ Impatto sulle Web Application
- ❑ OWASP Backend Security Project



Carlo Pelliccioni

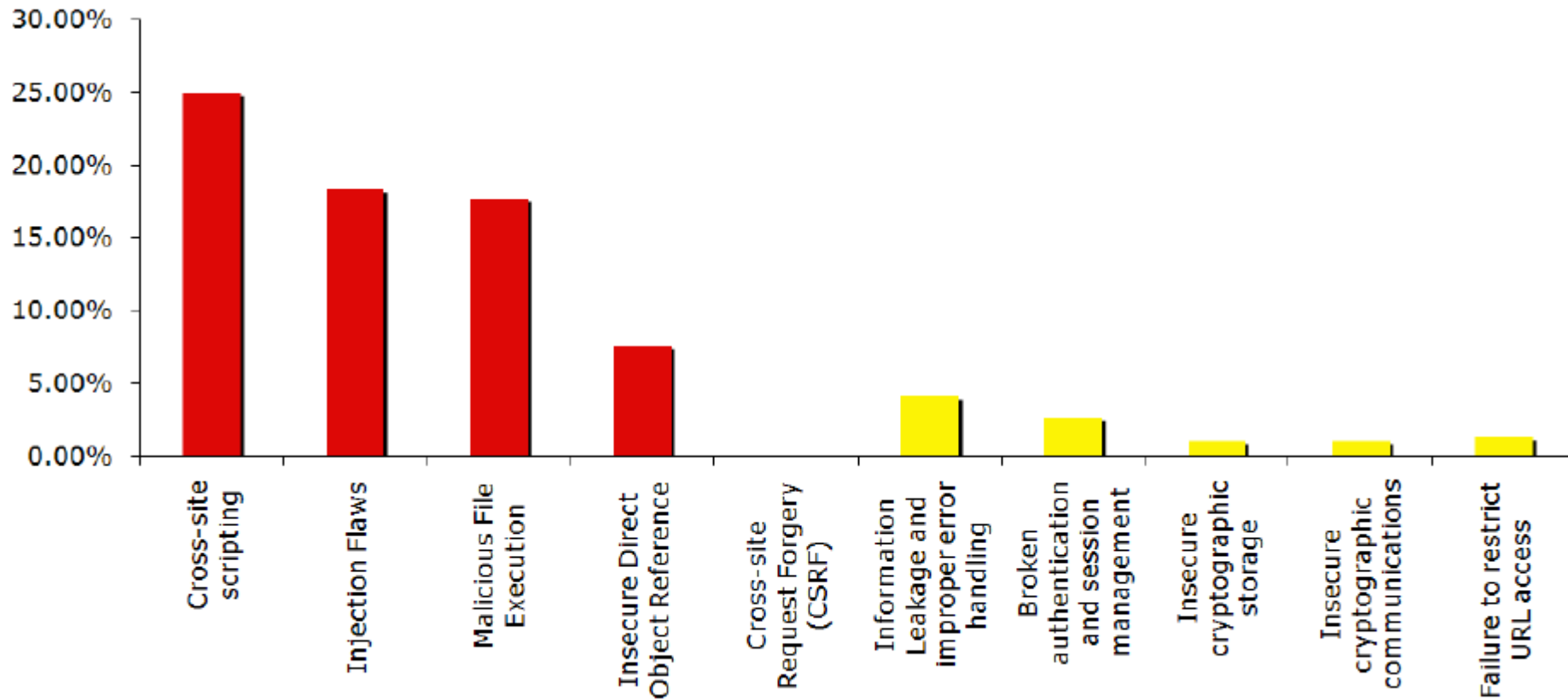
- ❑ Senior Security Consultant @ Spike Reply
- ❑ Penetration Tester
- ❑ Trainer su tematiche di Web Application Security
- ❑ OWASP Italy (contributor)
- ❑ OWASP Testing Guide v2.0 (contributor)
- ❑ OWASP Backend Security Project (leader)



Qual'è la situazione attuale?

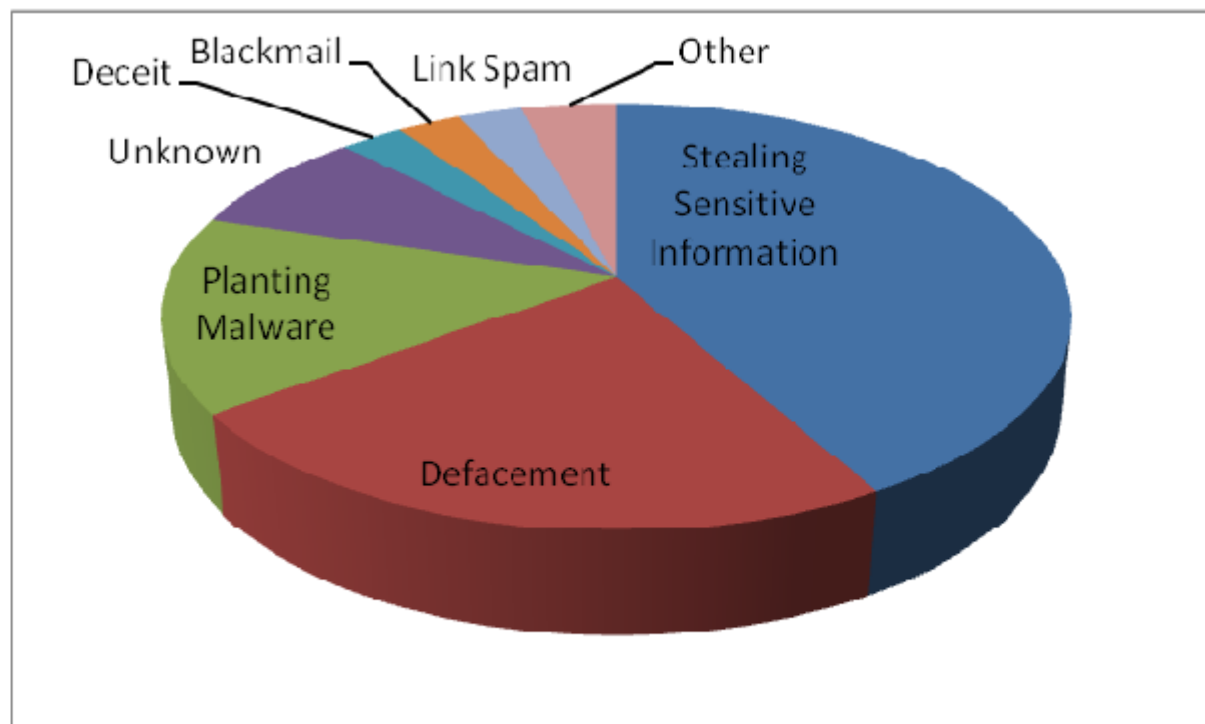


Statistiche da OWASP Top 10 2007



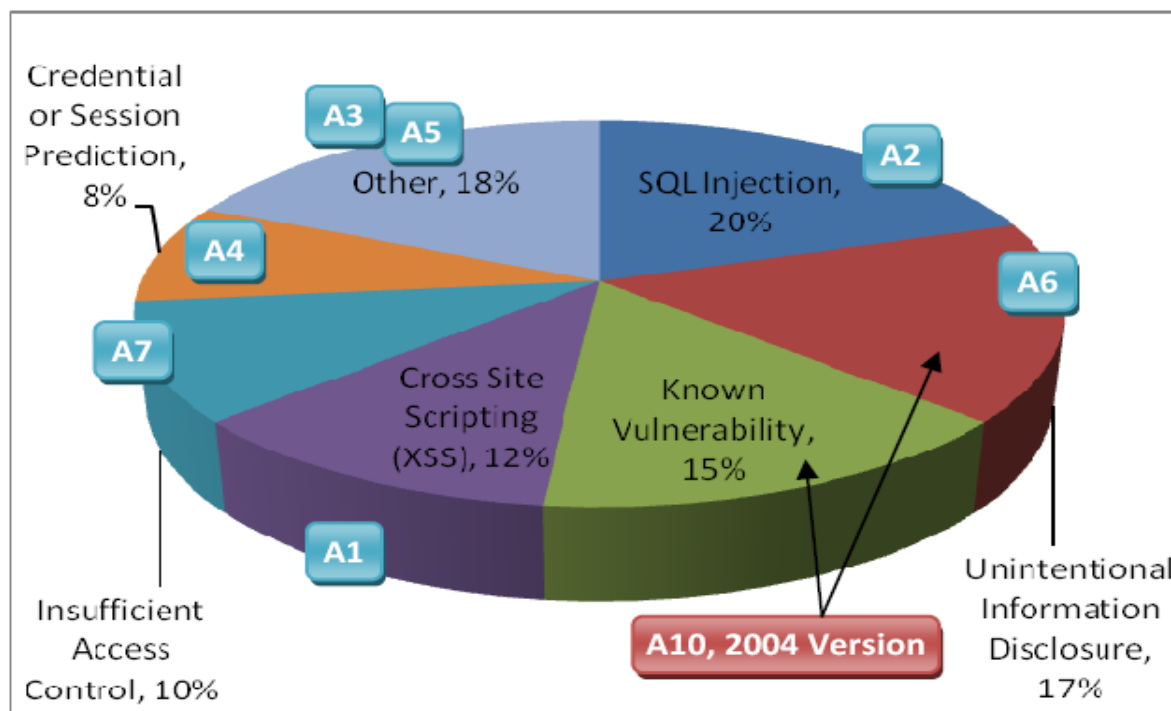
Statistiche Web Hacking Incident Database 2007 (WASC)

Attack Goal	%
Stealing Sensitive Information	42%
Defacement	23%
Planting Malware	15%
Unknown	8%
Deceit	3%
Blackmail	3%
Link Spam	3%
Worm	1%
Phishing	1%
Information Warfare	1%



Statistiche Web Hacking Incident Database 2007 (WASC)

Attack/Vulnerability Used	%
SQL Injection	20%
Unintentional Information Disclosure	17%
Known Vulnerability	15%
Cross Site Scripting (XSS)	12%
Insufficient Access Control	10%
Credential/Session Prediction	8%
OS Commanding	3%
Misconfiguration	3%
Insufficient Anti-automation	3%
Denial of Service	3%
Redirection	2%
Insufficient Session Expiration	2%
Cross Site Request Forgery (CSRF)	2%



Quali sono i principali rischi?



Scenario post-attacco

- Furto d'informazioni personali/sensibili
- Furto di carte di credito
- Trasferimento fondi autorizzati
- Impersonificazione di soggetti
- Denial of Service
- Sistema ponte per successivi attacchi
- Repository per materiale protetto da copyright



Impatto sulle Web Application



Firefox

Modifica Visualizza Cronologia Segnalibri Strumenti ?

Navigation and search area of the browser interface, including icons for back, forward, and search, and a search bar containing the text "Google".




Camtasia Studio Tip
Press F9 to pause/resume recording.
Press F10 to stop recording.

OWASP Backend Security Project



OWASP Backend Security Project



Log in / create account

category discussion view source history

Category:OWASP Backend Security Project

Contents [hide]

- 1 Welcome to the OWASP Backend Security Project
- 2 Objectives
- 3 Join the project
- 4 Mailing List
- 5 News
- 6 Contacts

Welcome to the OWASP Backend Security Project

OWASP Backend Security Project is the first OWASP project entirely dedicated to the core of the Web Applications.

[OWASP Backend Security Project wiki v0.1](#)

Objectives

The aim of this OWASP project is to create a new guide that could allow developers, administrators and testers to comprehend any parts of the security process about back-end components that directly communicate with the web applications as well as databases, Idaps, payment gateway, and much more.

Join the project

To reach this purpose our community needs more Information Technology security professionals as possible to create a new point of reference for the entire OWASP community. Although these information are briefly discussed in the others OWASP projects the community would like to collect those already existing information and creating new sections related to the not mentioned back-end components.

OWASP Backend Security Project is composed of three sections: security development, security hardening, security testing.

Below are described the main professional skills requested:

- Web Developers

http://www.owasp.org/index.php/Category:OWASP_Backend_Security_Project



OWASP Backend Security Project

Il progetto è composto da tre sezioni orientate a definire linee guida per aziende e professionisti dell'IT per una corretta organizzazione in sicurezza dei processi di sviluppo, gestione sistemistica e gestione delle componenti del back-end tecnologico in ambienti enterprise.

- Security Development
- Security Hardening
- Security Testing

http://www.owasp.org/index.php/Category:OWASP_Backend_Security_Project



OWASP Backend Security Project

(Per molti...
...ma non per tutti 😊)

- Sviluppatori Web
- Amministratori di sistema
- DBA
- Penetration Tester



OWASP Backend Security Project (Development)

- Java Back-end security programming
- PHP Back-end security programming
- ASP Back-end security programming

OWASP Backend Security Project (Hardening)

- Oracle
- SQL Server
- DB2
- MySQL
- PostgreSQL
- iPlanet Ldap
- OpenLdap
- Active Directory
- ... ?!



OWASP Backend Security Project (Testing)

- DBMS Security Testing
- LDAP Security Testing
- Tools



Join the OWASP Backend Security Project!



Q?

A!

