

# Quaderni Clusit

4  
00

La verifica della  
sicurezza di applicazioni  
Web-based ed  
il progetto OWASP

R. Chiesa, L. De Santis,  
M. Graziani, L. Legato,  
M. Meucci, A. Revelli

# La verifica della sicurezza di applicazioni Web-based ed il progetto OWASP

*OWASP-Italy*

*Comitato Tecnico Scientifico*



---

Quaderni CLUSIT – Giugno 2006

# CLUSIT

Il CLUSIT - Associazione Italiana per la Sicurezza Informatica, è una associazione "no profit" con sede presso l'Università degli studi di Milano, Dipartimento di Informatica e Comunicazione, fondata nel luglio 2000.

Le principali attività del CLUSIT sono:

- la diffusione di una cultura della sicurezza informatica rivolta alle Aziende, alla Pubblica Amministrazione ed ai cittadini;
- l'elaborazione sia a livello comunitario che italiano di leggi, norme e regolamenti che coinvolgono la sicurezza informatica;
- la definizione di percorsi di formazione per la preparazione e la certificazione delle diverse figure professionali operanti nel settore della sicurezza ICT;
- la promozione dell'uso di metodologie e tecnologie che consentano di migliorare il livello di sicurezza delle varie realtà.

I soci del CLUSIT sono rappresentativi dell'intero "sistema Paese", in particolare della ricerca, dell'industria, del commercio, del settore bancario ed assicurativo, della Pubblica Amministrazione, della Sanità, dei servizi, delle telecomunicazioni e di Internet.

## Copyright e Disclaimer

Copyright © 2006 OWASP-Italy.

Copyright © 2006 CLUSIT

Tutti i diritti sull'Opera sono riservati all'Autore e al Clusit.

Sono tuttavia attribuiti i seguenti diritti:

1. I Soci Clusit fruitori dell'Opera hanno il diritto di utilizzare l'Opera nell'ambito della propria attività professionale purchè: a) riconoscano la paternità dell'Opera in capo all'Autore e al Clusit; b) non la utilizzino per scopi commerciali; c) non creino opere derivate e/o alterino l'Opera e/o la trasformino e/o la sviluppino.
2. I diritti attribuiti ai Soci Clusit sopra riportati sono estesi a tutti i fruitori dell'Opera dopo che la stessa sarà rilasciata in forma elettronica sul sito [www.clusit.it](http://www.clusit.it) in area pubblica.

L'Autore e il Clusit non garantiscono che l'Opera sia esente da errori. Qualora vengano segnalati errori, nel limite del possibile si provvederà a correggerli nelle eventuali edizioni successive.

L'Autore e il Clusit non assumono alcuna responsabilità in relazione al contenuto dell'Opera e/o ai risultati attesi e/o ai risultati conseguenti all'uso della stessa e, pertanto, non risponderanno di eventuali e qualsivoglia danni diretti e/o indiretti che dovessero derivarne. In particolare non viene garantito che il contenuto dell'Opera sia esauriente, completo, preciso o aggiornato.

Il contenuto dell'Opera non costituisce un parere di tipo professionale o legale. Eventuali denominazioni di prodotti e/o aziende e/o i loghi e/o i marchi e/o i segni distintivi eventualmente citati nell'Opera sono di esclusiva proprietà dei rispettivi titolari.

## Abstract

Questo Quaderno CLUSIT si propone di presentare un valido supporto, sia a livello teorico che operativo e pratico, in merito alla tematica della verifica della sicurezza nelle applicazioni *web-based* mediante le risorse fornite dal progetto OWASP.

Il primo capitolo del testo fornisce un'introduzione generica alla problematica della sicurezza nelle applicazioni *web* ed alcuni cenni storici, per passare poi ad illustrare nel secondo capitolo il progetto OWASP (*Open Web Application Security Project*), dalle linee guida agli strumenti *software* messi a disposizione dalla comunità di ricerca internazionale.

Il terzo capitolo, seguendo la traccia indicata nella *OWASP Guide*, vuole invece descrivere i principali aspetti pratici dell'argomento, ovverosia le soluzioni alle diverse problematiche individuate, fornendo per ogni controllo di sicurezza da implementare le relative *best practice* di programmazione sicura e le linee guida necessarie per mitigare il rischio.

Infine, il quarto capitolo fornisce una guida operativa da utilizzare come riferimento durante l'esecuzione di verifiche di sicurezza a livello applicativo, attività definita in letteratura con il termine "*Web Application Security Testing*". Il quaderno termina illustrando nel dettaglio – tramite esempi e riferimenti - il corretto utilizzo degli strumenti *software* messi a disposizione dalla comunità OWASP.

Con questa pubblicazione si è voluto fornire un insieme di validi strumenti a tutti quei soggetti – analisti, sviluppatori *web*, sistemisti e *penetration tester* – che quotidianamente si trovano ad affrontare questa tipologia di problematiche.

Il Gruppo di Lavoro si è inoltre posto l'obiettivo di fornire un documento di riferimento, in lingua italiana, agli operatori del settore IT Security, per facilitarli nella scelta e nella selezione di professionisti della *web-security*, una nicchia di settore in forte espansione e da molti giudicato – per la delicatezza delle informazioni trattate dai siti *web* odierni – ad altissima criticità.

## Gli autori

### **Raoul Chiesa (OPST, OPSA, ISECOM Trainer)**

Socio fondatore del CLUSIT, membro del Comitato Direttivo e del Comitato Tecnico-Scientifico, partecipa attivamente a tutte le attività dell'Associazione ed è il fautore, lato CLUSIT, dell'alleanza CLUSIT-OWASP, siglata nel dicembre del 2005.

Fondatore e direttore tecnico di @ Mediaservice.net Srl, Raoul ricopre il ruolo di *Director of Communications* nell'ISECOM (*Institute for Security and Open Methodologies*) e nel capitolo italiano dell'OWASP, oltre che referente per il Sud-Europa di TSTF.net (Telecom Security Task Force) e membro attivo dell'Italian ISMS Chapter<sup>1</sup> sulla nuova ISO 27001.

Come docente e relatore, ha prestato la sua opera presso svariati eventi pubblici e privati, tra cui: CLUSIT, IDC, ISACA, AICA, Poste Italiane, Istituto di Ricerca Internazionale, Learning Resources Associates, Systems Technology Institute, Università (Torino, Biella, Milano, Udine, Trento, Bologna, Pisa, Roma, Cosenza), ISESTORM (Spagna), EUROSEC (Francia), Ticino Communications Forum (Svizzera), Hack in the Box (Malesia), InterOp (Russia).

### **Lorenzo De Santis (CISSP, CISA, OPST)**

Lavora da diversi anni nel campo della ICT *Security*, durante i quali ha partecipato come consulente e progettista ad attività di analisi dei rischi, di *system integration* e di sviluppo *software*.

Laureato in fisica, ha svolto per tre anni attività di ricerca come *Ph.D. student* presso la *International School of Advanced Studies* di Trieste, dove ha conseguito un *Ph.D.* in materia condensata.

Attualmente è responsabile della consulenza tecnologica presso Business-e, e partecipa attivamente al progetto OWASP. Ha conseguito le certificazioni CISSP, CISA e OPST.

### **Massimiliano Graziani (OPSA, BSI Lead Auditor, CCNA)**

Con oltre 10 anni di esperienza nello sviluppo delle applicazioni web, Massimiliano Graziani oltre ad essere un vero e proprio appassionato della sicurezza delle informazioni, è anche dotato delle certificazioni professionali "Vignette FT1" e "Vignette VAP" (per lo sviluppo di portali ad alte prestazioni e di CMS), ISECOM OPSA, BSI Lead Auditor 7799:2, Cisco CCNA.

Ha recentemente conseguito il Master in Information Security Management del Politecnico di Milano (CEFRIEL), dove ha ideato e sviluppato il project work "E-Forensics Best Practices"; ed attualmente si occupa dei Piani di Sicurezza per le *Web Application* e dei Piani di Sicurezza Infrastrutturali presso un noto operatore di telefonia mobile.

Massimiliano, inoltre, è un attivo ricercatore antivirus sin dal 1990 (suo il primo test comparativo sugli antivirus pubblicato in Italia) ed è membro dell'OWASP *Italian Chapter* e socio del CLUSIT.

---

<sup>1</sup> L'International User Group (IUG) riunisce gli utilizzatori dei sistemi di gestione della sicurezza delle informazioni (ISMS) secondo lo standard ISO 27000 (ex BS7799) e norme collegate.

## **Luca Legato (OPST)**

Luca Legato è una di quelle rare figure che inizia il suo percorso professionale come *sviluppatore web* (di quelli che “facevano HTML a manina”, come si dice in gergo) per passare poi a dedicarsi esclusivamente alla sicurezza delle informazioni e, nello specifico, alla verifica sul campo della sicurezza degli applicativi web.

*Senior Web Application Penetration Tester* presso il *Tiger Team* di @ Mediaservice.net Srl sin dal 2001, Luca nutre una forte passione per la *web security*, maturata e sviluppata durante anni di “pentest” verso molteplici settori quali Finance ed E-Banking, Industria, P.A., Telecomunicazioni e, negli ultimi tempi, verso il settore del “Black-box Security Testing” su dispositivi hardware (e le interfacce che li “gestiscono”).

Luca Legato è inoltre stato tra i primi professionisti a conseguire la certificazione ISECOM OPST nel nostro Paese, ed è un attivo contributore della metodologia OSSTMM e dell'OWASP *Italian Chapter*.

## **Matteo Meucci (CISSP)**

Fondatore e *Chair* del capitolo italiano del progetto OWASP, coordina le attività dell'iniziativa, mantiene i rapporti con la OWASP *Foundation* e con il *network* dei capitoli internazionali. Si propone di diffondere la cultura sulla *Web Application Security* mediante la scrittura di articoli e la partecipazione a seminari e conferenze come relatore presso IDC, ISACA, Master presso l'Università di Bologna, Workshop sul Computer Crime, SMAU e-Academy.

È laureato in Ingegneria Informatica, possiede la certificazione CISSP (*Certified Information System Security Professional*). Matteo è responsabile dell'area *Application Security* presso Business-e (una società del gruppo ITWay), contribuisce a diversi progetti OWASP ed in particolare alla realizzazione della nuova metodologia di *Web Application Penetration Testing* insieme ad Alberto.

## **Alberto Revelli**

Laureato in Ingegneria Informatica al Politecnico di Milano con una Tesi sperimentale su tecniche ricorsive di analisi di sicurezza di rete, ha lavorato per Intesis (divisione *Security Lab*) e per McKinsey & C., prima di approdare in Spike Reply, dove attualmente è a capo del team di *Ethical Hacking*. Ha collaborato con la rivista Inter.Net scrivendo articoli divulgativi sulle tecniche di attacco informatico e sulle relative contromisure.

Collabora dal 2005 con il chapter italiano di OWASP, in cui ricopre attualmente la carica di *Technical Director*.

# INDICE

<b>SEZIONE I</b> .....	<b>11</b>
<b>INTRODUZIONE ALLA WEB APPLICATION SECURITY</b> .....	<b>11</b>
Perché interessarsi alla sicurezza degli applicativi web? .....	14
Lo sviluppo di un applicativo web .....	15
Quali sono i rischi a cui è esposto un servizio web.....	16
Un approccio diverso: sicurezza e flussi di “verifica sul campo” negli applicativi web-based.....	17
<b>SEZIONE II</b> .....	<b>19</b>
<b>IL PROGETTO OWASP</b> .....	<b>19</b>
Il progetto OWASP .....	21
Linee guida per lo sviluppo degli applicativi web .....	23
La lista delle dieci vulnerabilità più critiche delle applicazioni web .....	24
Linee guida per la verifica della sicurezza degli applicativi .....	27
Gli strumenti OWASP .....	27
<b>SEZIONE III</b> .....	<b>29</b>
<b>LINEE GUIDA PER LO SVILUPPO “SICURO” DI APPLICATIVI WEB</b> .....	<b>29</b>
Introduzione alla Guida OWASP per lo sviluppo di applicativi web sicuri .....	31
Linee guida di design architetturale e principi di sicurezza .....	31
Thread Modeling di un applicativo web .....	34
Meccanismi di autenticazione .....	38
Autorizzazione e metodi di controllo degli accessi.....	42
Validazione dei dati di input .....	45
Gestione delle sessioni web.....	48
Riservatezza delle informazioni e crittografia .....	50
Insecure Configuration Management .....	52
La gestione degli errori, auditing e logging .....	53
Denial of Service e Phishing .....	54
<b>SEZIONE IV</b> .....	<b>57</b>
<b>COME SI REALIZZA UN’ANALISI DI SICUREZZA PER GLI APPLICATIVI WEB</b> .....	<b>57</b>
Tecniche di Web Application Penetration Test.....	59
Il tool Web Scarab e la metodologia OWASP .....	77
OWASP WebGoat.....	78
<b>APPENDICE A – Riferimenti</b> .....	<b>81</b>

CLUSIT

**Associazione Italiana per la Sicurezza Informatica**

Sede legale presso:

Dipartimento di Informatica e Comunicazione

Università degli Studi di Milano

Via Comelico 39 - 20135 MILANO

[www.clusit.it](http://www.clusit.it) – [info@clusit.it](mailto:info@clusit.it)

tel. 347 23 19 285