

# HANDS ON HACKING 2



## CORSO DI ETHICAL HACKING: LE APPLICAZIONI WEB



**zone-h**  
unrestricted information

## Argomenti

**Zone-H presenta Hands-on Hacking 2, il corso di ethical hacking destinato ai security manager e professionisti IT dedicato agli aspetti fondamentali della Internet security e alle nuove frontiere dell'hacking: le web application.**

### Le statistiche dimostrano che...

Da anni si registra un incremento costante degli attacchi alle architetture web-based tanto da costituirne oggi la modalità privilegiata. Dagli inizi del 2003 la maggior parte degli attacchi viene messa a segno utilizzando vulnerabilità legate a errori di configurazione delle applicazioni o a fattori intrinseci. La diversificazione e combinazioni possibili rendono gli attacchi ad una architettura web tipica sempre più efficaci e diffusi.

Hands on Hacking 2 nasce con l'intento di mostrare chiaramente come un attacco si possa risolvere nella compromissione di una qualsiasi delle componenti di una architettura web, firewall di protezione perimetrale, webserver, middleware, applicativi, database... Gli scopi? Diversificati, molto spesso il furto di identità...

### Live hacking!

Il corso è composto di un parte teorica e di vari laboratori pratici: inserite all'interno di una vera e propria hacking challenge, una serie di sessioni di live hacking dove, mediante l'esercitazione su casi reali, sarà possibile apprendere insight preziosissimi per la predisposizione di contromisure efficaci.

### Esclusivo materiale a corredo

Al termine del corso verrà fornito a tutti i partecipanti l'aggiornatissimo cd-rom "Security Repository", una vasta collezione di strumenti di sicurezza per Windows e Linux corredata da un'ampia e aggiornata raccolta di exploit specifici.

### A chi è rivolto

Security manager, IT manager, amministratori di rete, responsabili CED, sviluppatori, personale IT.

### Prerequisiti

Background su reti e protocolli TCP/IP.  
Conoscenza Windows/Linux.

### Durata

2 giornate

### Quando

20-21 Novembre 2012

Orario corso: 9.00 - 18.00.

Alla colazione parteciperanno tutti i docenti.

### Dove

Uffici Security Lab - viale Franscini 17 - Lugano - 5° piano

### Offerta speciale

1200 CHF a persona

Per la partecipazione al seminario è necessario compilare la scheda d'iscrizione allegata, inviarla via fax ed effettuare il pagamento.

Dall'osservatorio  
più autorevole  
del crimine  
informatico i corsi  
di hacking etico  
più esaustivi e  
aggiornati



# HANDS ON HACKING 2



## CORSO DI ETHICAL HACKING: LE APPLICAZIONI WEB



## Contenuti

**Introduzione: statistiche sugli attacchi lato server**

**Il protocollo HTTP**

**La struttura di un web server**

**Attacchi alle applicazioni web:**

classificazione  
Autenticazione  
Autorizzazione  
Esecuzione di comandi  
Attacchi lato client  
Information disclosure  
Attacchi logici

**Raccolta informazioni sul bersaglio**

Gli strumenti offerti dai motori di ricerca

**Live session**

**Cross Site Scripting in Depth**

La spiegazione dettagliata di come una tecnica ritenuta banale come XSS consenta in realtà di ottenere risultati eccezionali  
Come evitare questo tipo di attacchi

**Live Session**

**Cookie Manipulation (cURL e Mozilla Firefox)**

**Live session**

**Backdoors with Javascript**

Come installare backdoor utilizzando Javascript

**Remote Files Reading/Inclusion**

**I più comuni errori delle applicazioni PHP**

Esecuzione di codice arbitrario

Esecuzione di comandi

File disclosure

**Live session**

**SQL Injection (simple, blind, advanced)**

Attaccare un sistema utilizzando vulnerabilità di SQL: Form bypassing, Database dump, altri

**Live Session**

**Attacchi CSRF/XSRF (Cross Site Request Forgery)**

**Encoding Attacks**

Bypassing IDS; filtering

**Altre vulnerabilità**

AJAX

XPath Injection

LDAP Injection

**HTTP Response Splitting**

Come modificare pacchetti HTTP

**Miniguia alla programmazione sicura: 20 errori da evitare**



# HANDS ON HACKING 2



## CORSO DI ETHICAL HACKING: LE APPLICAZIONI WEB



**zone-h**  
unrestricted information

### Iscrizione

compilare e spedire via fax al n. 0041-91-9226766  
per informazioni: tel. 0041-78-9111260  
e-mail: [alberto.redi@sec-lab.com](mailto:alberto.redi@sec-lab.com)

#### Sede dei corsi:

Uffici Security Lab - viale Franscini 17 - Lugano - 5° piano

#### Data

20-21 Novembre 2012

#### Offerta Speciale

CHF 1200 a persona

#### Modalità di pagamento

L'accettazione dell'iscrizione è subordinata all'avvenuto pagamento dell'intera quota di partecipazione. Il pagamento deve essere effettuato con valuta tassativa della data di inizio corso tramite bonifico bancario anticipato, da allegare alla presente, sul c/c

**Banca:** UBS SA – Lugano

**Conto:** 247-553415.01L

**IBAN:** CH 360024724755341501L

**BIC:** UBSWCHZH80A

**Clearing:** 247

#### Condizioni commerciali

Per iscriversi al corso è necessario compilare in ogni parte il presente modulo e inviarlo a Security Lab Sagl al numero di fax 0041-91-9226766. Le iscrizioni verranno accettate solo al ricevimento della contabile di avvenuto pagamento e secondo l'ordine cronologico di arrivo poiché il numero di posti è limitato. L'eventuale rinuncia da parte dell'interessato dovrà pervenire almeno 10 giorni lavorativi prima dell'inizio del corso; in questo caso verrà reso l'importo versato. Se la rinuncia dovesse avvenire oltre il suddetto limite, non verrà rimborsato alcun importo e la persona sarà iscritta di diritto al corso successivo. Qualora non venga raggiunto il numero minimo di partecipanti, Security Lab Sagl si riserva il diritto di rinviare od annullare il corso. L'eventuale rinvio verrà comunicato via e-mail entro 3 giorni dall'inizio della sessione. In caso di annullamento del corso verrà restituito l'importo versato.

#### Dati del partecipante:

Nome \_\_\_\_\_ Cognome \_\_\_\_\_

Funzione \_\_\_\_\_

Indirizzo \_\_\_\_\_

Cap \_\_\_\_\_ Città \_\_\_\_\_ Prov. \_\_\_\_\_

Tel. \_\_\_\_\_ Cell. \_\_\_\_\_

E-mail \_\_\_\_\_

#### Dati dell'Azienda

Ragione sociale \_\_\_\_\_

Indirizzo \_\_\_\_\_

Cap \_\_\_\_\_ Città \_\_\_\_\_ Prov. \_\_\_\_\_

Tel. \_\_\_\_\_ Fax \_\_\_\_\_

P. IVA./C.F. \_\_\_\_\_

#### Informativa sulla privacy

I dati inseriti in questo modulo saranno trattati con modalità cartacee ed informatiche e saranno utilizzati per (a) dar seguito alle Vostre richieste nonché (b) per tenerla informata, anche mediante strumenti elettronici, in merito a nuovi corsi o seminari organizzati da Security Lab. L'invio dei dati non è obbligatorio, ma necessario per dar seguito alla Vostra richiesta. I dati non saranno comunicati a terzi né saranno diffusi.

Presto il consenso ai trattamenti di cui alla lettera b) dell'informativa

Nego il consenso ai trattamenti di cui alla lettera (b) dell'informativa

Firma del partecipante \_\_\_\_\_

Data \_\_\_\_\_



# HANDS ON HACKING 2



## CORSO DI ETHICAL HACKING: LE APPLICAZIONI WEB



## Team Docenti

### Luigi D'Amato (SecurityWireless) – Italia

“The wireless expert”... Fondatore e admin del primo portale web di tecnologie wireless [www.securitywireless.info](http://www.securitywireless.info), nonché membro di Zone-h. Certificato CWNA, Cisco CCNA e WLAN FE. L'uomo giusto al quale fare tutte le domande sulla sicurezza delle reti wireless.

### Emanuele Mornini (matador) - Italia

IT Security analyst and researcher, conosciuto come “the buffer overflow expert”. Esperto di sicurezza e di penetration testing, ad oggi lavora presso una società estera di sicurezza informatica. Membro del team internazionale di docenza; ha una conoscenza profonda delle tecniche di Hacking e delle loro contromisure.

### Gerardo Di Giacomo (Astharot) – Italia

Tra i cofondatori di Zone-H, si è occupato dapprima dello sviluppo dello stesso per poi entrare nel gruppo di docenti dei corsi di sicurezza informatica che ha tenuto per conto di Zone-H sia a livello nazionale che internazionale. Dal 2005 è a capo del team di sicurezza della release di Linux Ubuntu. Ad oggi è senior analyst presso una società multinazionale di sicurezza informatica.

### Tonu Samuel - Estonia

Senior security analyst e ricercatore. L'attività quotidiana lo vede impegnato come consulente security nelle aree risk analysis, auditing, penetration testing, hardening infrastrutture. Autore di svariati advisory. Relatore Zone-H di lungo corso. Un esperto dal paradiso tecnologico d'Europa: l'Estonia.

### Agris Krusts - Lettonia

Senior security consultant alla guida di società di consulenza lettone, punto di riferimento per la grande impresa e PA locali. Agris è forte di una esperienza decennale nel settore IT; l'attività svolta per Zone-H lo vede impegnato nel team di docenza internazionale. Parla fluentemente inglese e russo, oltre al lettone, la sua lingua madre.

### Uldis Mikelsons - Lettonia

Docente Zone-H in ambito internazionale. L'attività quotidiana come internet security specialist gli garantisce una prospettiva ampia sulle tematiche di sicurezza della Rete. Profondo conoscitore ambienti Windows e \*nix. Uldis parla correntemente inglese e russo, oltre al lettone, la sua lingua madre.

### Boris Mutina - Slovacchia

Docente Zone-H in ambito internazionale, editor e supervisore di Zone-H. L'attività quotidiana lo vede impegnato come consulente security nelle aree risk analysis, auditing, penetration testing, hardening infrastrutture. Boris parla correttamente inglese e tedesco, oltre allo slovacco, la sua lingua madre.

## Zone-H

Zone-H, osservatorio digitale indipendente ed open-source, è oggi la voce più autorevole in Internet in materia di crimine informatico. La home page di [www.zone-h.org](http://www.zone-h.org) registra 35.000 singoli accessi al giorno per un totale di circa 800.000 click.

I siti Zone-H sono attualmente disponibili in inglese, francese e portoghese.

Avalendosi della collaborazione di oltre 50 esperti in tutto il mondo, tra cui figurano professionisti, giornalisti, studenti ed accademici, Zone-H propone una prospettiva realistica e “no-hat” dei flussi che coinvolgono il web.

Informazione ed analisi in tema di cyber terrorismo e cyber crime, servizi per l'implementazione della security e programmi educational vengono elaborati e messi a disposizione della comunità IT che ogni giorno può contare su advisory, statistiche, aggiornamenti e informazioni, frutto di un costante monitoraggio della rete da parte dello staff Zone-H.

I dati prodotti da questa analisi costante del web confluiscono in uno dei più grandi archivi di attacchi digitali al mondo che comprende, ad oggi, più di 3.000.000 di attacchi di cui sono registrati profilo, motivazioni e metodologie.

Il programma educational è frutto del know-how e dell'esperienza di Zone-H che organizza corsi e seminari in tutto il mondo trattando gli aspetti fondamentali della Internet Security, con lo scopo di promuovere la diffusione della filosofia dell'osservatorio di prevenzione e costante aggiornamento dei sistemi di difesa informatici tra i professionisti IT italiani.

[www.zone-h.org](http://www.zone-h.org)