

# HANDS ON HACKING 2



## CORSO DI ETHICAL HACKING: LE APPLICAZIONI WEB



## 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 costituire 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.

### Come

Ogni partecipante avrà a disposizione un computer connesso in rete ed a Internet. Il corso verrà tenuto in lingua italiana; per gli interventi di docenti stranieri è prevista la traduzione contestuale. Alla fine del corso verrà rilasciato un attestato di frequenza.

**Prerequisiti:** Nozioni di programmazione di base.

**Durata:** 2 giornate.

### Quando

6-7 marzo 2008.

Orario corso: 9.00 - 18.00.

Alla colazione parteciperanno tutti i docenti.

### Dove

Presso AONet

Via Riccardo Lombardi 19/6, 20153 - Milano

### Offerta Speciale (IVA esclusa)

1 corso a scelta: € 900

2 corsi: € 1.500 invece di € ~~1.800~~

### L'offerta è relativa ai seguenti corsi:

4-5 marzo 2008 **Hands on Hacking Unlimited**

6-7 marzo 2008 **Hands on Hacking 2, Web Application**

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 esauritivi e aggiornati

**AONet**  
ALWAYS ON NETWORKS

# 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



### Iscrizione

compilare e spedire via fax al n. 02 62685431  
per informazioni: tel. 02 62685401  
e-mail: [info@aonet.it](mailto:info@aonet.it)

#### Sede dei corsi:

Presso AONet – Via Riccardo Lombardi 19/6 20153 Milano.

#### Data

6-7 marzo 2008.

#### Offerta Speciale (IVA esclusa)

1 corso a scelta: € 900  
2 corsi: € 1.500 invece di € ~~1.800~~

#### L'offerta è relativa ai seguenti corsi:

4-5 marzo 2008 **Hands on Hacking Unlimited**  
6-7 marzo 2008 **Hands on Hacking 2, Web Application**

#### Modalità di pagamento

L'accettazione dell'iscrizione è subordinata all'avvenuto pagamento dell'intera quota di partecipazione (IVA compresa). Il pagamento deve essere effettuato con valuta tassativa della data di inizio corso tramite bonifico bancario anticipato.

Coordinate Bancarie: BANCA REGIONALE EUROPEA SEDE DI MILANO,  
ABI: 06906 - CAB: 1600 - CIN: K - C/C: 36818.

Intestato a AONet International srl

#### Condizioni commerciali

Per iscriversi al corso è necessario compilare in ogni parte il presente modulo e inviarlo a AONet International Srl Via Riccardo Lombardi 19/6 20153 Milano al numero di fax 02 62685431. 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, AONet International S.r.l. 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. \_\_\_\_\_

#### Vorrei partecipare ai seguenti corsi:

- Hands on Hacking Unlimited, 4-5 marzo 2008  
 Hands on Hacking 2, Web Application, 6-7 marzo 2008

#### Informativa ai sensi dell'art.13 del D.lgs 196 del 2003

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 AONet International S.r.l. 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. Per richiedere la modifica, l'aggiornamento o la cancellazione dei dati, ai sensi dell'art 7 del D.lgs 196/03, può rivolgersi al Titolare dei Trattamenti, scrivendo a AONet International S.r.l. – Via Riccardo Lombardi 19/6 20153 Milano.

- 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 del mirror Zone-H in slovacco. 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 16 lingue diverse: inglese, italiano, francese, russo, portoghese, slovacco, spagnolo, giapponese, sloveno, turco, tedesco, lettone, croato, polacco, arabo e indonesiano. Avvalendosi 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 educativi 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 2.200.000 di attacchi di cui sono registrati profilo, motivazioni e metodologie.

Il programma educativo 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.