



## OWASP - Séminaire sécurité

La gestion de la qualité, sécurité et continuité d'activité



**Nous sommes à un moment singulier. L'informatique pénètre « partout ». Nous modifions notre système d'information avec l'introduction de bouleversement en termes de management, ouvertures vers des partenaires, nouveaux outils de développement. Au niveau mondial les attaques sur Internet ne cessent d'augmenter, les développeurs créent des applications web de plus en plus vulnérables, sans respecter les normes de développements sécurisé et ce quelques soit le langage ou la méthode de développement utilisée.**

**Les technologies utilisées dans ces applications web représentent de réels risques et des fragilités :**

- ✓ Existence de failles connues exploitables par les outils de hacking en libre-service sur Internet.
- ✓ Arrivé de nouveaux vecteurs d'attaques comme les réseaux mobiles avec les smartphones.
- ✓ Virus transmis en pièce jointe dans les messageries personnelles et Professionnelles.
- ✓ Saturation des systèmes par l'envoi de messages répétés.
- ✓ Usurpation d'identité facilitée.
- ✓ Le réseau manipulant des flux financiers (paiement d'actes, feuille de soins électronique,...)

**L'OWASP organise un séminaire pour exposer ces risques et ces attaques, ainsi que la méthodologie préconisée pour mettre en œuvre les techniques de protections adéquates.**

**Plusieurs experts dans le domaine de la sécurité des systèmes d'informations vont présenter les démarches, les techniques, les outils avec des démonstrations à la clef pour exploiter les failles et pour mettre en œuvre les techniques pour les corriger ou pour réduire la surface des attaques.**

### Programme du séminaire

09:00-09:30 Welcome  
09:30-09:45 OWASP Presentation ( Azzeddine RAMRAMI )  
09:45-10:00 Security Awareness ( Tarik EL AOUADI )  
10:00-10:30 OSSTMM v3.0 a PenTest Methodlogy - Overview ( Intissar EL MEZROUI )  
10:30-10:45 PAUSE  
10:45-11:30 How to conduct a Web Application Pen Testing ( Hamza WARAKI )  
11:30-12:00 OWASP WebGoat & Attack Example (A virtual Hacking Environment) (Nawfal Makdad )  
12:00-14:30 PRIERE DE VENDREDI  
14:30-15:30 OWASP WebGoat & Attack Example (A virtual Hacking Environment) (Nawfal Makdad )  
15:30-16:15 Smartphone Security (Tarik EL AOUADI)  
16:15-16:30 PAUSE  
16:30-17:00 Smartphone Security (Tarik EL AOUADI)  
17:00-17:45 Writing Secure Code : Java Principles ( Azzeddine RAMRAMI )  
17:45-18:00 Questions & Answer

### PARTICIPANTS CONCERNES

- Directeurs d'établissement, direction SI, Responsable Sécurité SI, Gestionnaire des risques, Médecins, Pharmaciens, etc.
- Cadres de l'Agence Régionale de Santé, de l'Assurance Maladie
- Industriel de l'informatique et de l'électronique de Santé, et SSII
- Toute personne intéressée par le management hospitalier et la qualité-sécurité des systèmes d'information en Santé

### Dates

Vendredi le 18 mai 2012

De 9h00 à 18h00

L'inscription est obligatoire :

<https://www.owasp.org/index.php/Morocco>

### Lieu du séminaire

Ecole VINCI

Adresse :  
10,Rue Al Yamama (Aproximité de la gare Rabat-Ville)  
Rabat

Tél: 05 37 70 69 05  
E-mail: [vinci@vinci.ac.ma](mailto:vinci@vinci.ac.ma)



### Sponsors

L'OWASP remercie les sponsors suivants :

- ECOLE VINCI (Rabat)
- FIDENS (PARIS)
- LEXSI (PARIS)
- AXEL TELECOM (Casablanca)

