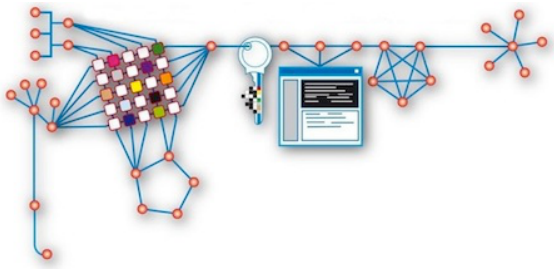

ID de Contribution: **60** Type: **Atelier**

Atelier Sécurité

mardi 27 septembre 2016 11:00 (1h 30m)

Cet atelier permettra aux participants dans une première partie de mettre en évidence des vulnérabilités affectant un serveur Web classique .

Seront évoqués alors :

- Les problèmes de configuration et leurs conséquences : arborescence trop permissive, compromission de données par écritures
- La résistance aux intrusions par injection de code : injections SQL, injection système
- Les failles du type Cross-Site Scripting (XSS)

Une seconde partie sera consacrée à la sécurité de navigateurs courants. Les points abordés seront :

- Cookies traçant (Third-party cookies)
- Traçabilité du navigateur (fingerprinting)
- Détournement et vol de session

Cet atelier disposera de 5 à 6 machines clientes virtuelles, pouvant accueillir chacune un binôme.
Les participants devront simplement disposer d'un pc portable équipé d'un client SSH et d'un serveur X .

Auteurs principaux: M. BOUTHERIN, Bernard (LPSC); M. YAHIA, Fouad (I.P.N.Orsay); M. BARBET, Jean-Michel (Subatech); M. KERMORVANT, Yoann (LPC CAEN); M. ZWOLINSKI, david (cnrs)

Orateurs: M. BOUTHERIN, Bernard (LPSC); M. YAHIA, Fouad (I.P.N.Orsay); M. BARBET, Jean-Michel (Subatech); M. KERMORVANT, Yoann (LPC CAEN); M. ZWOLINSKI, david (cnrs)

Classification de Session: Atelier

Classification de thématique: Ateliers