# ADF

# Aide à la Détection des Faiblesses d'un site WEB

formation nationale ANGD organisée par l'UREC

La Grande-Motte, 15-17 septembre 2008

*(Magali Contensin, Sylvain Corcoral, Marie-Claude Quidoz )*

*rediffusion/adaptation à Marseille DR12 - Janv. 2009*

*M. Contensin , K. Poutrain, T. Dostes, M. Libes*

# Population concernées par cette formation

- 53 participants (ASR et développeurs)
  - *47 CNRS ; 2 CERTA ; 2 Académie ; 1 INRIA ; 1 IFREMER*
- 14 intervenants
  - *10 CNRS ; 2 CERTA ; 2 Académie*
- 70 pré-inscriptions pour 40 places
  - Taux de sélection voisin de 60 %
  - Volonté d'avoir une population « mixte »
    - *Développeur d'application (40 %)*
    - *Administrateur système et réseau (60 %)*

# Pourquoi la formation ADF ?

- Why Web applications are at High Risk ? http://honeynet.org/papers/webapp
- From an attacker's viewpoint, a Web application is an interesting target for several reasons. First, the *quality of the source code as related to security is often rather poor*, as numerous bug reports show.
- Every week hundreds of vulnerabilities are being reported in these web applications, and are being actively exploited. The number of attempted attacks every day for some of the large web hosting farms range from hundreds of thousands to even millions."

- *WebCalendar includedir remote code-inclusion, around 230,000 publicly accessible installations.*
- *PHPBB viewtopic code injection, (the flaw that Santy exploited), around 1,500,000 publicly accessible.*
-

# Pourquoi la formation ADF ?

- ...Les bulletins hebdomadaires des CERTs
  - semaine du 20/06/08 au 26/06/08, 5 cas de compromissions ....
    - dont 3 cas de modification de sites Web signalées ....
  - semaine du 24/07/08 au 31/07/08, 4 cas de compromissions ...
    - dont quatre serveurs victimes d'attaques de type "SQL injection ....
- Les sites web :
  - sont devenus les principaux supports d'information et de communication de nos Laboratoires et systèmes d'information.
  - Leur disponibilité, fiabilité et intégrité sont primordiales ....

# Un avis de stats du CERT

compromission de la semaine

Cette semaine 48 sites webs compromis ont été mis au jour.Deux d'entre eux toujours en cours d'analyse ont vu leur page d'accueil modifiée.

Les attaques ont porté sur des sites web utilisant des versions vulnérables du CMS Joomla, du CMS spip et d'autres application PHP.  Une fois compromis tous ces sites ont été utilisés pour mettre en ligne de faux sites de ventes (a propos de pilules colorées dont le viagra, cialis, levitra et autres...).

L'analyse de plusieurs cas a révélé des traces d'attaques provenant de l'adresse 195.5.117.252 ainsi que l'ajout de trois scripts déposés à la racine permettant la création des pages frauduleuses.

*- -rw-rw-rw-  1 apache apache  7079 dec 23 18:25 generate.php*

*- -rw-rw-rw-  1 apache apache  3286 dec 23 18:24 _http.php*

*- -rw-rw-rw-  1 apache apache  4065 dec 23 18:25 skins.php*

# Pourquoi la formation ADF ?

- Statistiques Sophos : Conclusions du rapport de sécurité 2009
  - ”Spam-related webpages” : 1 page nouvelle compromise par du spam toute les 15 secondes

Le Web est désormais le premier facteur par lequel les cybercriminels infectent les ordinateurs.. Les Malwares injectés sur les sites ne sont plus seulement dus aux failles Microsoft

Les routeurs et parefeu protégent désormais assez bien les sites.. Les cybercriminels exploitent désormais les failles relatives aux serveurs Web..

Les codes injectés attendent d'infecter les ordinateurs clients

# Objectifs de la formation ADF

- Connaitre et/ou Comprendre  les principales vulnérabilités relatives à l'utilisation de la technologie ”LAMP” ou WAMP
  - ➔ Présenter des outils de détection des vulnérabilités pour tester la solidité de nos systèmes Web
  - ➔ Acquérir des méthodes pour sécuriser nos sites et nos applications web
  - ➔ Acquérir des éléments *[architecture, filtrage]* pour améliorer leur protection
- Proposer des solutions complémentaires de sécurisation aux conseils donnés en général (pas forcément aisés à appliquer dans tous les cas)

# Programme dela formation ADF

- Introduction : Contenu et Objectifs de la formation
  - Typologie des menaces
    - *Injection de code, XSS, injection SQL, CSRF*
  - Rappels sur la sécurisation d'Apache
  - Conseil en utilisation et écriture de scripts Mysql, PHP
  - Outils de détection et recherche de vulnérabilités
    - *pixy, rats, spike, phpsecinfo, TemperData*
    - *Scanner de vulnérabilités : Webscarab, SQLix; Nikto, Wapiti*
  - TP détection de vulnérabilités

# Programme de la formation ADF

- Sécurisation de site Web
  - Architecture réseau avec différents types de  filtrage
    - *Exemple de filtrage sur site web avec iptables*

- Présentation reverse proxy &TP sur ”reverse_proxy”
- Présentation d'un filtrage HTTP avec ”mod_security” & TP sur ”mod_security”

- Architecture : rappel utilisation des logs centralisés
- Utilisation d'empreinte systemes : exemple avec ”tripwire”
- Procédures a suivre en cas d'incidents (rappel A2IMP)