HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

SSTIC 2009 – Rump Session

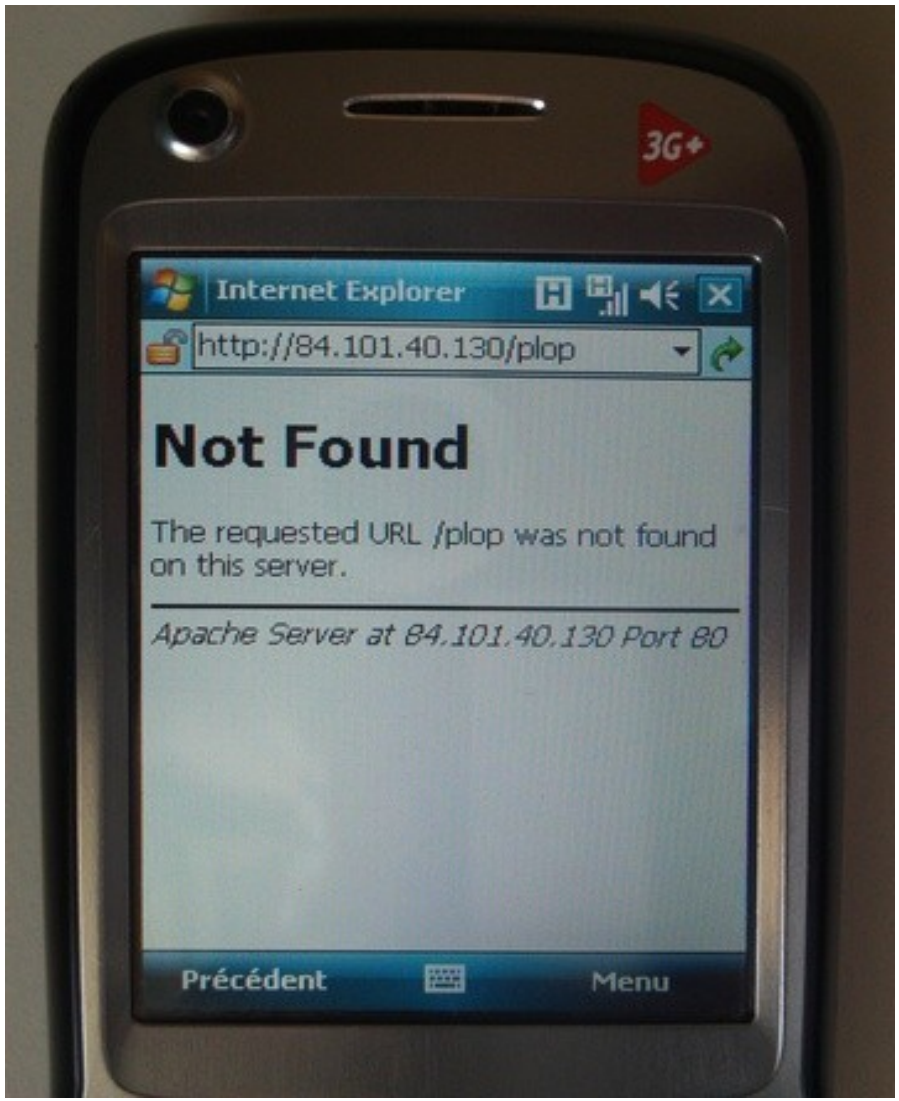
Jeudi 4 juin 2009

Intrusion Web par SmartPhone WM

Yves Le Provost
<Yves.Le-Provost@hsc.fr>

Prises d'informations

- Moyens classiques : page d'erreur, navigation



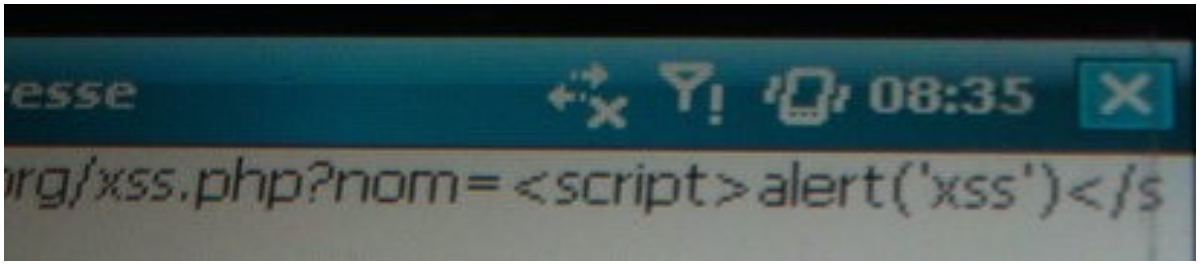
Outils standards adaptés

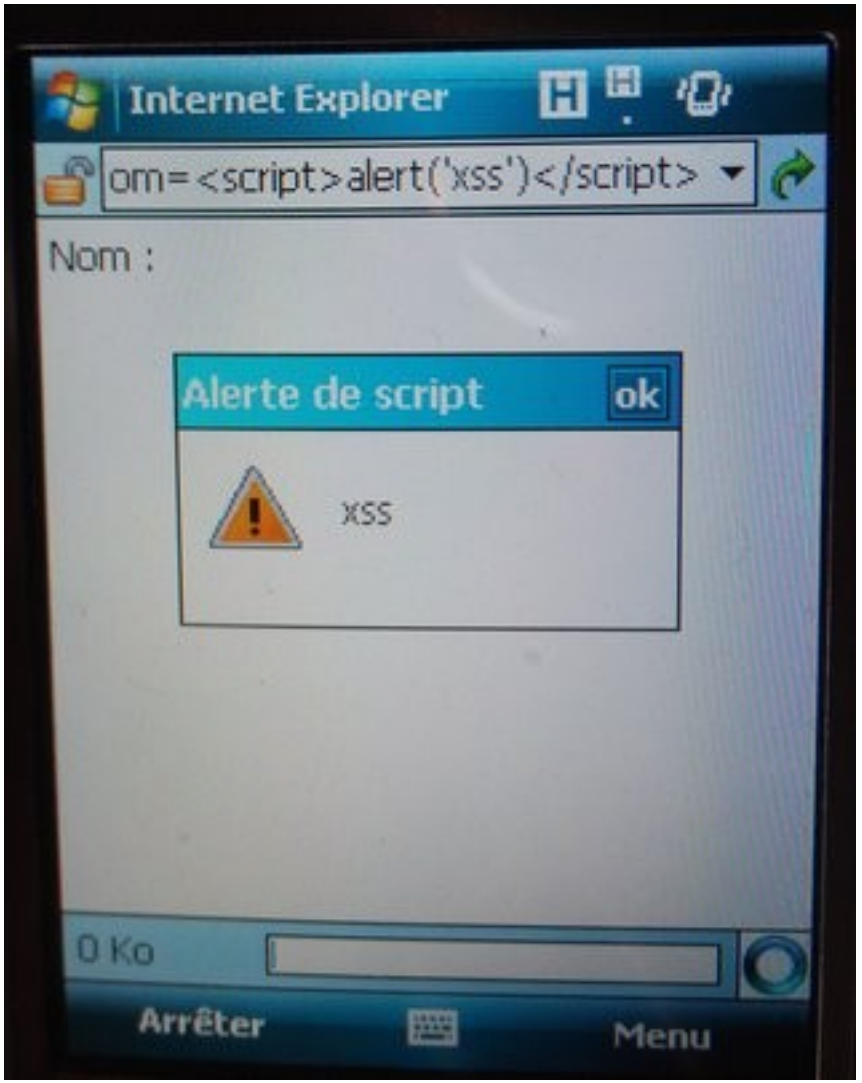
- Moyens adaptés : Nikto / Wfuzz
  - Pas d'interpréteur Perl disponible pour Windows Mobile 6
  - Utilisation de PythonCE
  - Nikto : écrit en Perl, base de données dans un fichier texte
    - ↳Écriture rapide d'un moteur en Python
  - Wfuzz : écrit en python, mais utilise des bibliothèques absentes de PythonCe
    - ↳Réécriture en simplifiant certaines fonctions

    - ↳ **DEMO Nikto et Wfuzz**

Détection classique des XSS

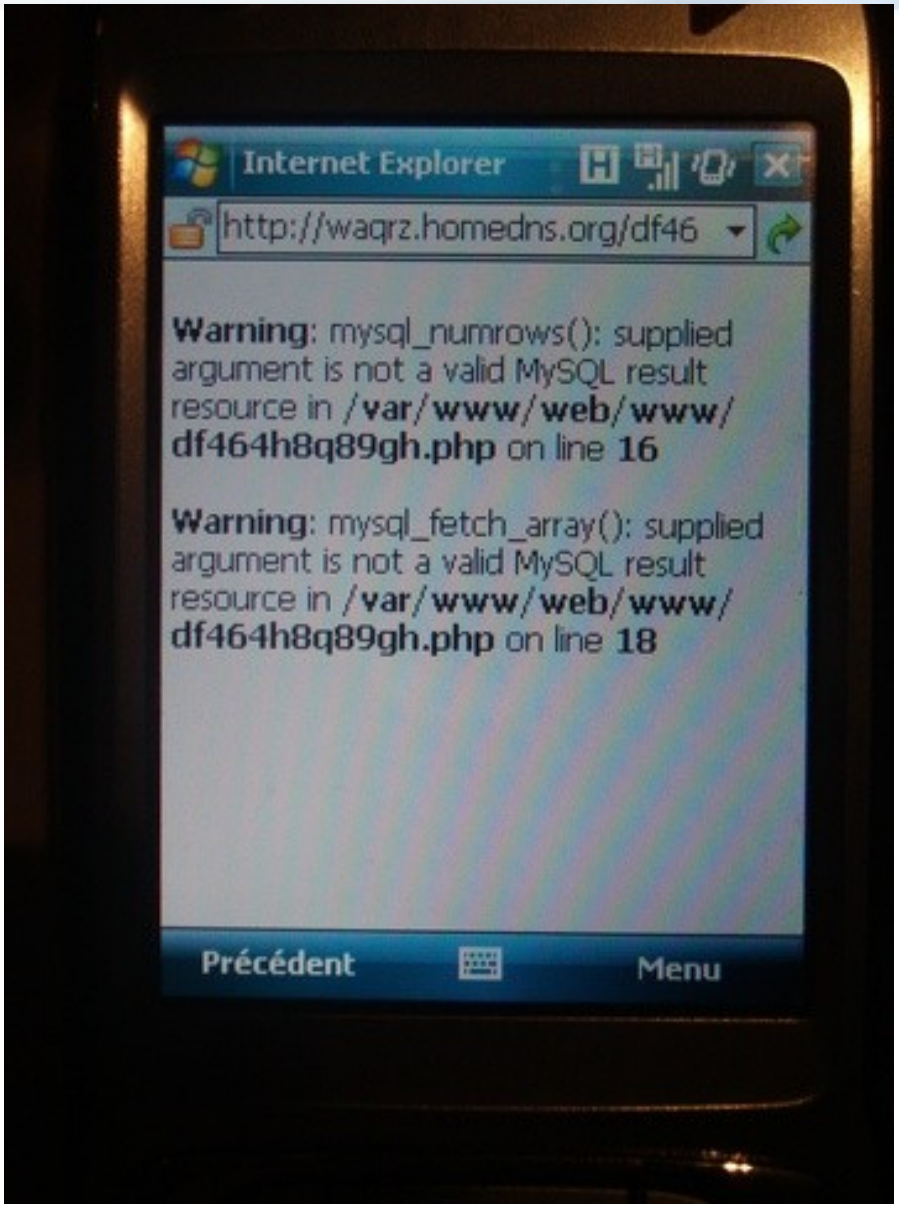
- Dans le navigateur





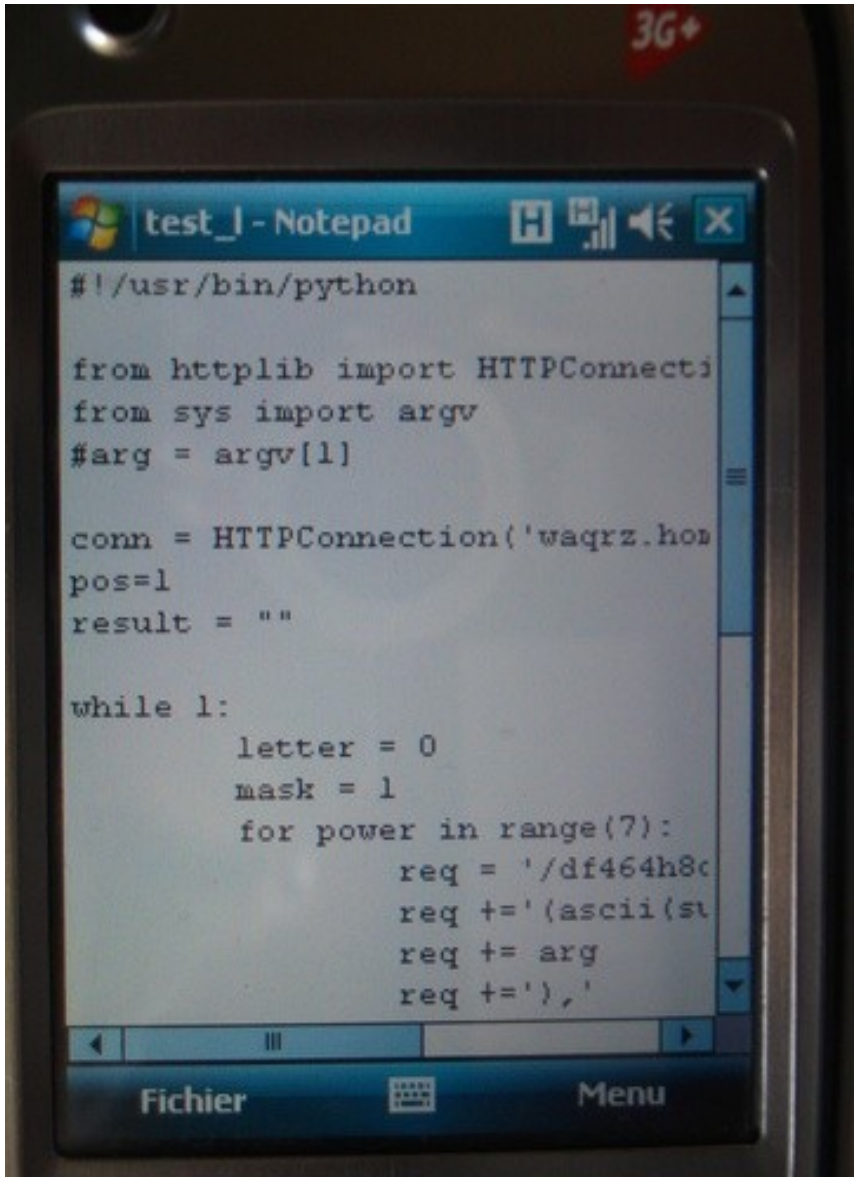
Injections SQL

- Détection classique



Exploitation injections SQL

- Écriture de script python



- **DEMO injection SQL**

Références

- PythonCE : http://pythonce.sourceforge.net/
- Nikto : http://www.cirt.net/nikto2
- Wfuzz : http://www.edge-security.com/wfuzz.php