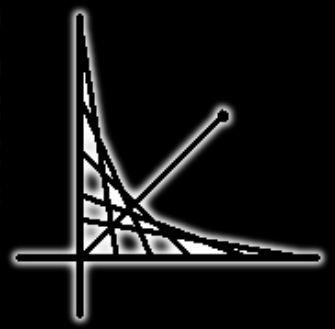
XeeK

La XSS pas si inoffensive que ça



Trance – Emilien Girault
trance@ghostsinthestack.org
www.ghostsinthestack.org
www.emiliengirault.fr

Introduction

- Tout le monde connaît la XSS
- Peu connaissent ses véritables enjeux
- Naissance du projet XeeK
  - « XSS Easy Exploitation Kernel »
  - Framework d'exploitation de XSS
- **Attention :** Projet expérimental !
  - Développement stoppé depuis 3 mois...
  - Soyez indulgents ;)

XSS ?

- XSS = « Cross Site Scripting »
- Faille Web probablement la plus répandue
- Conditions nécessaires :
  - Variables contrôlables par le visiteur
  - Affichage de ces variables sur la page
- Exemple PHP : `<?php echo $_GET['texte']; ?>`

➔ L'utilisateur peut modifier la page

  ➔ Injection de code HTML

  ➔ Injection de code JavaScript

Applications classiques

- Vol de cookie
  - Redirection JS vers un cookie grabber
- Phishing
  - Modifier l'affichage de la page pour tromper le visiteur
    - Formulaire bancaire
- C'est tout ?
  - NON !

Applications avancées

- Une faille, trois cibles
  - Le site faillible (XSRF)
    - Détournement de compte
    - Changement de mot de passe
  - Les autres serveurs
    - Attaques distribuées : DDOS, Botnets
    - En réseau local : Drive by pharming
  - La machine du client
    - Backdoor / Proxy JavaScript
    - Redirection vers site piégé (exploit)
      - Failles applicatives, ActiveX...

Puissance de la XSS

- Seules limites : JavaScript / Ajax
  - Same Origin Policy... ou pas !
  - Manipulation du DOM
    - Récupération du contenu des pages
    - Modification
  - Contrôle du navigateur
    - Envoi de requêtes GET/POST
    - Accès aux frappes clavier → Keylogger
- XSS permanentes
  - Impact encore plus grave !

XeeK

- Buts
  - Démontrer la puissance de la XSS
  - Fournir un outil d'attaque automatisé
  - Être le plus productif possible
    - Coder moins, exploiter plus
- Moyens
  - PHP, MySQL, JS/Ajax
  - Framework Orientée Objet
    - Design Patterns

XeeK – En bref

- L'attaquant installe XeeK sur son serveur
- Il conçoit un exploit à l'aide d'instructions
- XeeK génère un lien piégé pour l'exploit
- L'attaquant trouve une XSS sur un site, y injecte l'exploit et le donne aux victimes
- Les victimes exécutent l'exploit
- L'attaquant récupère les infos

XeeK - Concepts

- L'attaquant crée une « Session » (Exploit)
  - Écriture des « Instructions »
    - Code JS arbitraire ou pré-existant
  - Sélection d'un « Scheduler »
    - Statique : mode « batch » (à la chaîne)
    - Dynamique : exécution au fur et à mesure
- Génération de l'exploit
  - URL à injecter dans une XSS
  - XeeK génère le code JS dynamiquement lors de l'accès des victimes sur la page

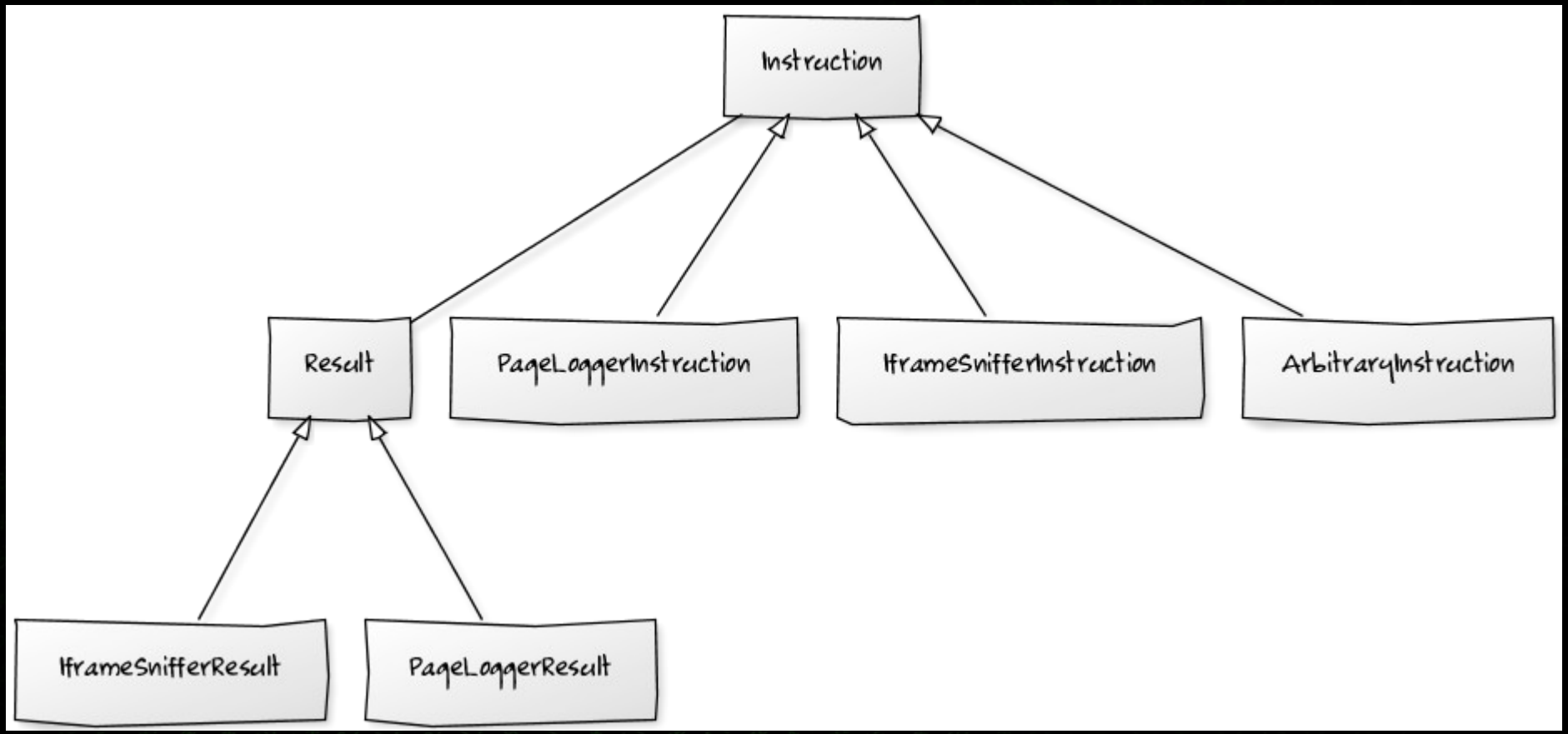
XeeK - Concepts

- Les instructions renvoient des données au serveur XeeK
  - Cookies, contenu des pages, formulaires...
- L'attaquant les visualise en temps réel
  - Si le scheduler dynamique est choisi, il peut voir quelle instruction s'exécute à un instant t chez une victime

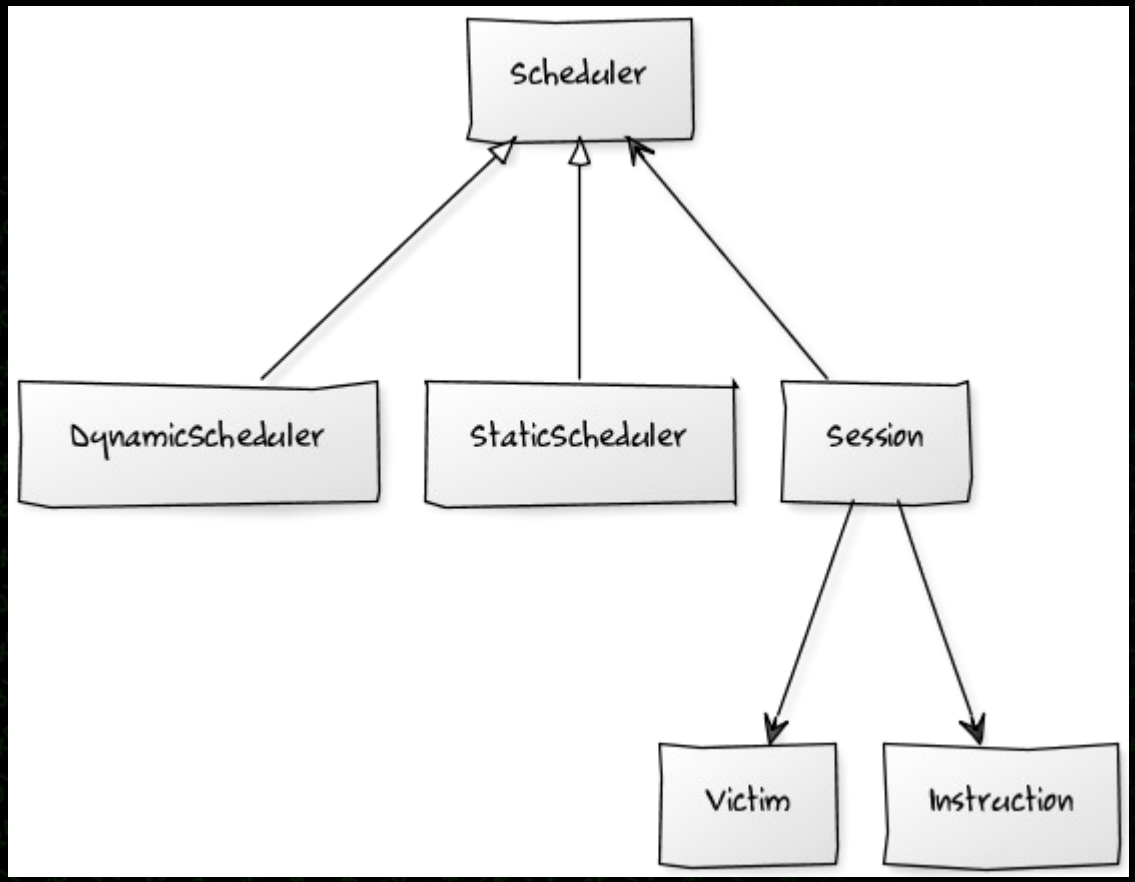
→ Interface ressemblant à un debogueur

XeeK – Entrailles (1)

XeeK – Entrailles (2)



XeeK – Entrailles (3)



Modularité

- XeeK = XSS Easy Explioitation **Kernel**
- Noyau supportant des modules
- A la « Metasploit »
  - Nouvelles instructions
  - Nouveaux visualisateurs de résultats
  - Nouvelles fonctionnalités
    - Encodeur JS, faux formulaire, ...

Exemple : IframeSniffer

- Principe : Encapsuler la page courante dans une frame
  - 100 % de l'écran
    - Invisible
  - Toujours actif même si la victime change de page
  - Sniffeur de visite
    - Récupération et modification du contenu des pages, formulaires

État d'avancement

- Noyau plus ou moins fonctionnel
  - 3 instructions de base
  - Partie exploitation fonctionnelle sous FF
    - Bientôt sous IE 7
- Interface d'admin
  - Encore au stade d'ébauche...
  - Utilise Phico (PHP + Comet)
  - Ajax « manuel »
    - Mériterait d'utiliser des frameworks
      - jQuery / Prototype...

Démo

Conclusion

- Encore loin de Metasploit...
- Devrait s'améliorer dans un futur proche
- Release très probablement en GPL
  - Plugins développables par tous !
- Questions / Idées ?