

Sécurité des applications PHP

AFUP Paris, France

10 Novembre 2006

Intervenant

- Damien Seguy
 - Editeur de Nexen.net
 - Mission conseils pour nexenservices.com
- damien.seguy@nexen.net
- <http://www.nexen.net/conferences/>

Agenda

- Enjeux
- Sécurité PHP
- Sécurité des applications Web
 - Injections SQL
 - XSS
 - CSRF



Risques encourus

- Exploitation indues des ressources
- Destruction des données
- Publication de données confidentielles
- Détournement de votre site
- Usurpation d'identité
- Ridicule...



Sécurité PHP

- Exploitation des ressources PHP
- Modifier un script en injectant du code PHP



Configuration

- safe_mode, magic_quote,
- register_global
- register_long_arrays
- open_basedir



Configuration

- error_reporting, error_display, html_display, log
- disable_functions, disable_class,
- enable_dl
- memory_limit, max_execution_time, max_post_size, max_upload_size
- expose_php



Sécurité du code PHP

- Éviter les inclusions dynamiques
 - require(), include() + allow_url_fopen
 - `include($_GET['action'].".inc");`
 - PHP 5.2 : allow_url_open_include
- Téléchargement de fichiers PHP
- eval() is evil()!
- Assert()



Sécurité des applications Web

- PHP interagit avec de nombreuses technologies
- PHP peut servir de relais pour attaquer
 - une autre technologie
 - un autre site
- Responsabilité du programmeur



• Injections SQL

• Objectifs :

- contournement de clause WHERE
- **SELECT login FROM USERS**
WHERE email =
'\$_GET['email']';
- **SELECT login FROM USERS**
WHERE email = 'admin' OR
'1'='1';
- déni de service
- corruption de tables



Contrer les injections SQL

- Utilisation de conteneurs
 - Commandes préparées
- `SELECT login FROM USERS WHERE email = ?;`
 - Procédures stockées / Variables SQL
- Protection des données
 - `mysql_real_escape_string()`



Attaque XSS

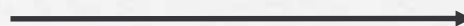
- Cross Site Scripting
 - A l'origine, via les frames
- Une XSS est une attaque de l'application Web, qui ses utilisateurs
- Origine : la possibilité d'injecter du code dans une page HTML



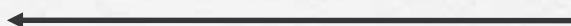
Attaque XSS



URL?XSS



HTML + XSS



Risques des XSS

- Vol de cookie
 - Usurpation d'identité
- Exécution de code JavaScript arbitraire
- Détournement du navigateur



Les voies des XSS

- `echo $_GET['variable'];`
- Balises HTML complètes
 - `PHP<script src="http://www.site.com/hack.js" />`
 - `<A HREF=http://66.102.7.147>PHP</A>`
 - `<A HREF="http://0x42.0x0000066.0x7.0x93/">PHP</A>`
 - `<A
HREF="http://%77%77%77%2E%67%6F%6F%67%6C%65%2E%63
%6F%6D">PHP`
 - `>PHP<script src="//1113982867/hack.js" />`



Les voies des XSS

- Attributs HTML

- `<IMG SRC=javascript:alert('XSS')>`
- `<IMG SRC=JaVaScRiPt:alert('XSS')>`
- `<IMG SRC="javascrip t:alert('XSS');">`
- `<IMG SRC=javascript:alert (String.fromCharCode(88,83,83)) >`
- `<form action="index.php"><xss!><a" method`



Défenses contre XSS

- Concepts à retenir
 - Valider les données entrantes
 - Suivre les données validées
 - Protéger les données sortantes
- Évitez les “, ‘, < et >
 - UTF-8, entité HTML, hexadécimal...

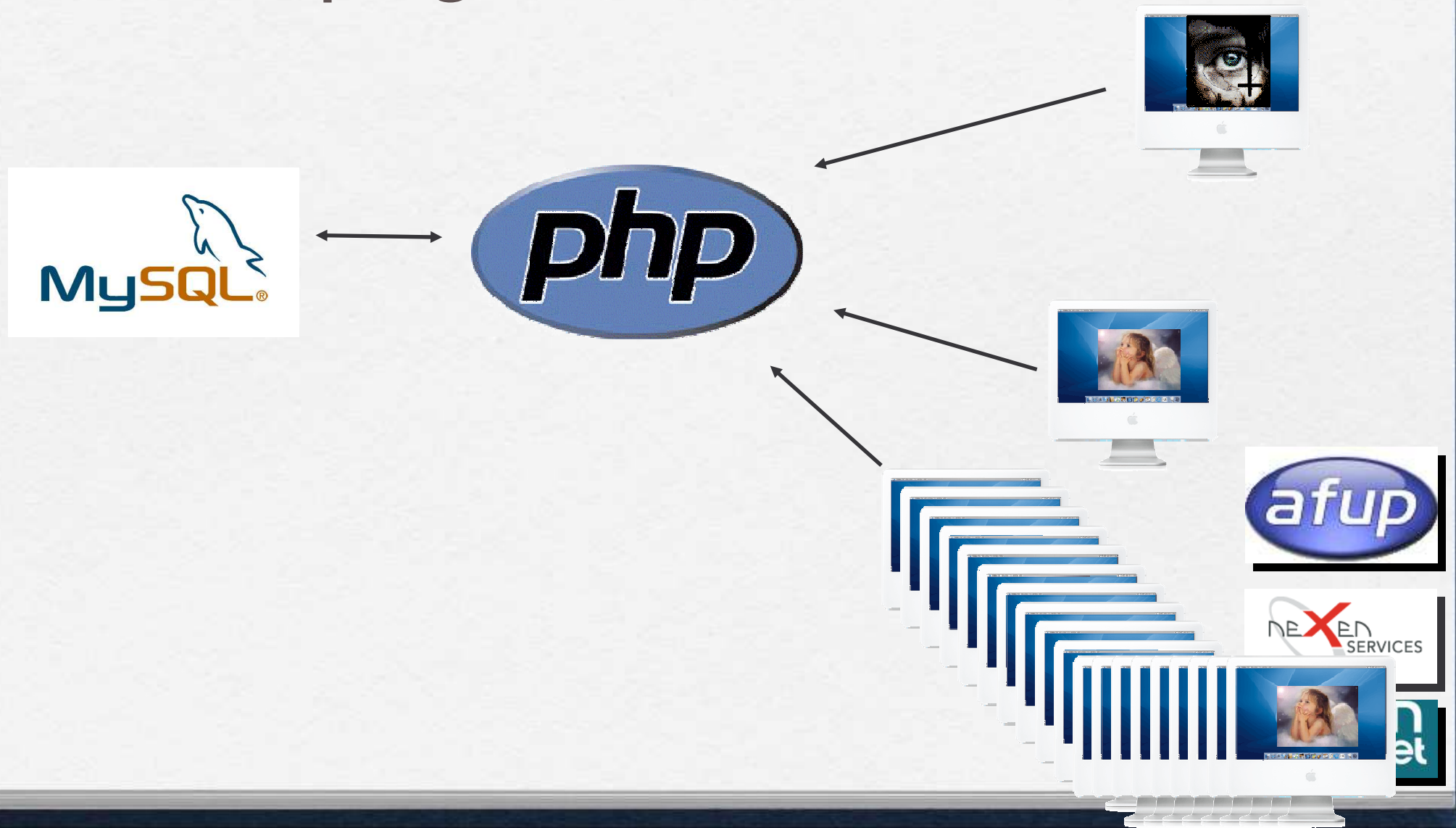


Virus XSS?

- XSS sauvée en base de données
 - XSS retardées
 - XSS publiées
 - XSS administrateur



Propagation d'une XSS

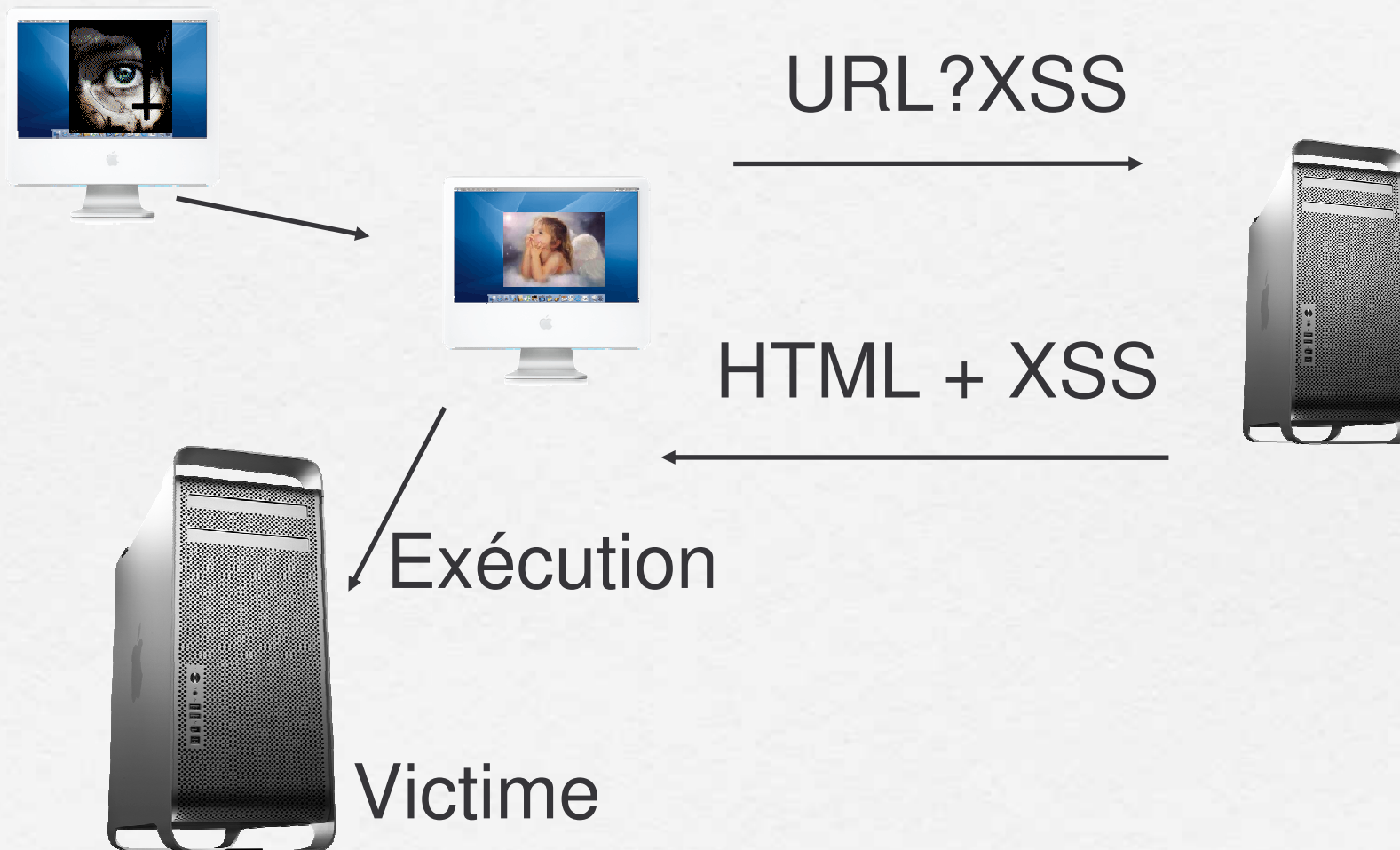


CSRF

- Cross Site Request Forgery
- Exploite un site vulnérable pour qu'un utilisateur de ce site attaque un autre site
 - Ou le même site!
- La seule protection de la victime est l'identification de l'utilisateur
- Aucun contact entre le pirate et le site



Attaque CSRF



CSRF

- Site victime
 - <http://admin.site.com/efface.php?id=33>
- Site vulnérable
 - ``



CSRF

- Il faut se méfier d'un utilisateur qu'on a déjà identifié
 - Faire des identifications fréquentes
 - Réduire les temps de sessions
 - Exploiter GET / POST



Questions?



Autres attaques

- Spam et emails
- Injections HTTP
- Injections LDAP, ABAP, etc
- Exécution de commandes
- Téléchargement de fichiers
- AJAX!



Autres défenses

- Chiffrement et signatures
- Pot de miel pour attirer les abeilles
- CAPTCHA
- Gestion des mots de passe



Sessions

- Sensibles aux XSS (vol de cookie)
- Fixation de session
- Attention aux hébergements partagés
- Changer l'identifiant régulièrement
- Relier la session au navigateur

