Rapport d'audit Darluok-Server.com

- Fiche consultant
  Pseudo: shp
  Mail: contact@shp-box.fr
  Site web: www.shp-box.fr
- Objet
  Cible: darluok-server.com
  Date: 16/10/2010

I. Injection SQL

- Caractéristiques

Niveau critique: 9/10
Type de vulnérabilité: Injection SQL avec UNION
Contraintes: quotes slashées
Contexte requis: un compte normal + un personnage créé sur un serveur de jeu
Page vulnérable: http://www.darluok-server.com/amelioration/formulaire.html

- Exploitation

Variables concernées: $_POST['subclass'] ; certainement les autres du formulaire également
Proof of concept – variable subclass modifiable avec tamper data:

```
1 AND 1=2 UNION SELECT
0,0,0,0,CONCAT(Host,0x3a,user,0x3a,password),0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 FROM
mysql.user -- -
```

- Sécurisation

Rajouter un quote dans la requête entre les données de la variable
Exemple: "SELECT * FROM item_template WHERE champ='".mysql_real_escape_string($_POST['subclass'])."'"

II. Autres vulnérabilités critiques

1) Accès base de donnée mysql

- Caractéristiques

Niveau critique: 9/10
Utilisateur bdd concerné: web
Accès aux mots de passe et utilisateurs encryptés

- Sécurisation

Laisser les accès à la base de donnée mysql à l'utilisateur root uniquement

2) Mots de passe bdd faibles

- Caractéristiques

Niveau critique: 10/10
Type de vulnérabilité: utilisation cryptage mysql pour le champ Password

- Exploitation

On compile le script c suivant: http://packetstorm.linuxsecurity.com/Crackers/msqlfast.c
Mots de passe jusqu'à 10 caractères cassables en moins de 5 minutes si on optimise le script (ciblage spécifique des caractères ascii)

benjamin : 7c462e7a5c57c42e => avo2k1 (environ 3 secondes avec msqlfast)
Puis connexion avec navicat à distance

- Sécurisation

Changement du type de hash utilisé (mettre à jour la version de mysql)

3) Faille upload

- Caractéristiques

Type de vulnérabilité: faille upload sans vérification de la double extension
Niveau critique: 7/10
Localisation: script d'envoie de preuves dans la page de demande de sanctions

- Exploitation

Protection présente: vérification de l'en-tête jpg, png ou gif
Bypass: on laisse la première ligne d'une image et on insère le code php de notre backdoor dans l'image puis on l'envoie sur le serveur sous l'extension php.jpg
On rajoute des "../../../../" via tamper data dans le filename de l'image pour récupérer le nom du fichier envoyé sous forme de message d'erreur (fichier tout de même envoyé).

Protection présente: htaccess qui empêche l'exécution du fichier
Bypass envisageable: Local File Include

- Sécurisation

Preg_match() sur <?php dans le contenu de l'image, et preg_match sur ".php" dans le nom du fichier

4) Vulnérabilité vol de cookies

- Caractéristiques

Niveau critique: 6/10

- Exploitation

Si on vole les cookies d'un mj avec une faille xss, il suffit de remplacer notre cookie sha_pass_hash et login par les siens pour être connecté automatiquement: aucun log de connexion + droits d'admin

5) Faille XSS permanente

- Caractéristiques

Niveau critique: 6/10
Contexte requis: compte admin web
Localisation: modification d'une news

- Exploitation

Si on modifie une news, on peut rajouter du javascript via tamper data puis obtenir les cookies des autres admins (plus d'accès)
La même faille est présente pour l'ajout d'une news.

- Sécurisation

htmlentities()

6) Faille XSS permanente

- Caractéristiques

Niveau critique: 4/10
Contexte requis: accès en écriture à la base de donnée darluokweb
Localisation: dans la table de la faq

- Exploitation

On peut mettre du javascript qui sera interprété directement sur le site dans les faqs

- Sécurisation

htmlentities()

7) Injection de php

- Caractéristiques

Niveau critique: 7/10
Contexte requis: administrateur avec droit de modifier la configuration sur HESK ticket
Localisation: onglet settings de HESK

- Exploitation

On peut injecter du code php dans la partie settings (j'ai oublié le champ mais il me semble que c'est au niveau de l'email)

8) Faible cryptage mantis

- Caractéristiques

Niveau critique: 3/10
Contexte requis: accès en lecture à la base de donnée darluokweb

- Exploitation

Les mots de passe sont cryptés en md5 pour le logiciel mantis
Scénario: récupération des mots de passe admins

- Sécurisation

Ajout d'un salt lors du cryptage