

2011 SecureKorea 중고생 해킹방어대회 예선 Write-Up

Xero

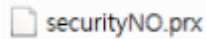
박준혁 (한국디지털미디어고등학교 1학년)

2011-07-10

wnsgurzxc@nate.com

1번 문제

다음과 같은 .prx 형식의 파일이 주어진다.



파일 헤더를 보기 위해 다음과 같이 hexs 에디터로 뜯어보았다.

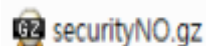
```
1F 8B 08 08 B6 99 FC 4D 00 03 73 65 63 75 72 69 .<...Q^M..securi
74 79 4E 4F 2E 6C 69 62 00 9D 7C 43 AC 28 0A B0 tyNO.lib..|C-|.°
E4 B1 CD DB DC CD DB DC CD DB DC CD DB DC E4 B1 CD DB DC
```

1F 8B 08 를 파일 시그니처라고 생각하고 찾아보니 다음과 같이 gz확장자라는 것을 알게 되었다.

1F 8B 08

GZ, TGZ .<. GZIP archive file

확장자를 다음과 같이 gz으로 바꾸고 압축을 풀어보았다.



그러자 다음과 같이 securityNO.lib 파일이 나왔다.



위의 파일을 hexs 에디터로 뜯어보았다.

```
50 4B 03 04 14 00 00 00 08 00 37 5E C9 3E 39 D0 PK.....7^É>9Đ
1D B7 97 53 00 00 1B AF 00 00 0E 00 08 00 73 65 .-S...-.....se
63 75 72 60 74 70 4E 4E 2E 68 77 70 73 65 04 00 securityNO.lib
```

PK 를 파일 시그니처라고 생각하고 검색하여 ZIP 파일이라는 것을 알아내었다.

50 4B 03 04

PK..
ZIP PKZIP archive file ([Ref. 1](#) | [Ref. 2](#))
Trailer: filename 50 4B 17 characters 00 00 00
Trailer: (filename PK 17 characters ...)

다음과 같이 확장자를 zip으로 바꾸었다.



압축을 푸니 다음과 같이 hwp파일이 나왔다.



헥스 에디터로 뜯어보았다.

```
46 57 53 04 1B AF 00 00 78 00 06 D6 00 00 1B 58 FWS...x..Ö...X
00 00 01 02 00 35 08 01 00 7B 2C 86 5B 8C E4 19 .....5...{,+[æ.
02 00 01 12 9D DB B3 D9 69 33 9A 02 00 21 5F 21 ò ñ³ñ¼³ä 1^1
```

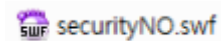
FWS 를 파일 시그니처로 검색하여 SWF 파일이라는 것을 알게되었다.

46 57 53

FWS

SWF Macromedia Shockwave Flash player file

swf로 확장자를 변경후 실행해보았다.



NAHS9229 라는 키 값이 나왔고 인증에 성공했다.

NAHS9229

Key : NAHS9229

2번 문제

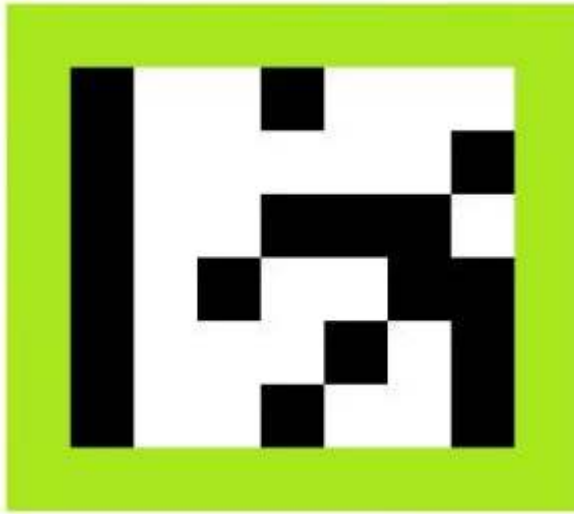
다음과 같은 qr코드가 주어진다.



XRen QRCode Tool 을 이용해서 디코드를 하니 <http://m.site.naver.com/00UHw> 라는 값이 나왔다.



위의 사이트에 들어가 다음과 같은 사진을 다운받았다.



처음에는 뭔가 했는데 작년 hust 대회와 비슷하다는 생각이 들고 흑을 1로, 백을 0으로 하여 6줄짜리 아스키 코드를 작성해 보았다.

1001000

1000001

1001110

1010011

1000101

1001001

위와 같은 2진수가 나왔고, 계산기를 이용해 10진수로 변환해보니 다음과 같은 값들이 나왔다.

72

65

78

83

69

73

아스키라고 생각하여 변환하니 HANSEI 라는 값이 나왔고 인증에 성공했다.

Key : HANSEI

3번 문제

3번 문제는 대회 도중 운영진들의 협의 결과 취소되었고 4번으로 넘어갔다.

Stage 3

1	2	1	1	2		2	2	2	2	2
2	2	1	2		1					

우연히 책상정리를 하다가 예전 초등학교 때 친구들과 장난삼아 주고받았던 비밀 편지를 발견하였다. 추억에 잠겨 잠시 예전에 썼던 글을 읽어보다 마지막 글귀를 보고 웃고 말았다.

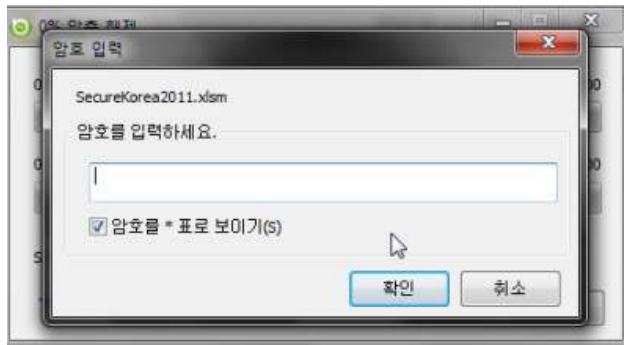
정 답 : 제출하기

4번 문제

다음과 같은 zip 파일이 주어진다.



압축 풀기를 시도했으나 다음과 같이 암호가 걸려 있는 것을 확인 할 수 있다.



압축 암호 크랙을 위해 AZPR 이라는 툴을 사용하였다.



Length를 5로 잡고 브루트포싱을 시작했고, sK2! 라는 비밀번호를 얻었다.



비밀번호를 입력하고 압축을 해제하니 다음과 같은 xlsx 파일이 나왔다.

SecureKorea2011.xlsx

헥스 에디터로 뜯어보았다.

```
50 4B 03 04 14 00 00 00 08 00 00 00 21 00 B5 55 PK.....!.µU
30 23 EB 00 00 00 4C 02 00 00 0B 00 08 00 5F 72 0#ë...L....._f
65 6C 73 2F 2F 72 65 6C 73 73 F5 04 00 B5 03 00 als/relaxÅ n
```

또 다시 PK 라는 파일 시그니처를 발견했고 zip으로 확장자를 바꿔 압축을 풀어 보았다.

```
50 4B 03 04
```

```
ZIP PK..
PKZIP archive file (Ref. 1 | Ref. 2)
Trailer: filename 50 4B 17 characters 00 00 00
Trailer: (filename PK 17 characters ...)
```


압축을 푸니 다음과 같은 파일들이 나타났다.



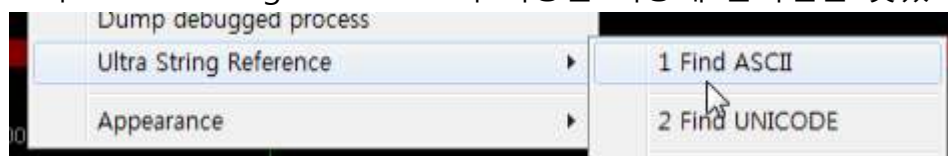
폴더들을 살펴보다가 doc 폴더에 exe가 숨김 파일로 저장되어 있는 것을 발견했다.

실행시켜보니 다음과 같이 숫자로만 Password를 입력받았다.

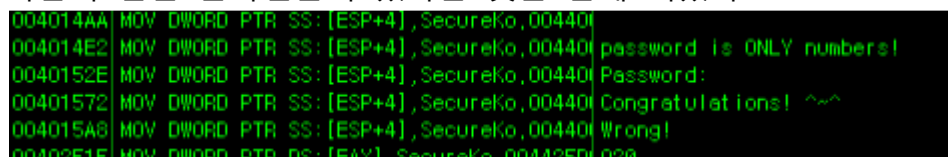


리버싱을 하기 위해 올리디버거로 열어보았다.

그리고 Ultra String Reference 의 기능을 이용해 문자열을 찾았다.



다음과 같은 문자열들이 있다는 것을 알게 되었다.



Wrong! 를 더블클릭하여 해당 주소로 이동하였다.

위로 올려보면 다음과 같이 Congratulations! ^~^ 로 점프하는 구간 위에 CMP 로 비교하는 구간을 볼 수 있다.

```
00401566 . C70424 C0334 MOV DWORD PTR SS:[ESP],SecureKo,004433C0
0040156D . E8 2E8C0200 CALL SecureKo,0042A1A0
00401572 . C74424 04 B8 MOV DWORD PTR SS:[ESP+4],SecureKo,004401572 Congratulations! ^~^
0040157A . C70424 C0334 MOV DWORD PTR SS:[ESP],SecureKo,004433C0
00401581 . E8 C2AC0300 CALL SecureKo,0043C248
00401586 . C70424 60344 MOV DWORD PTR SS:[ESP],SecureKo,00443460
0040158D . E8 AE602000 CALL SecureKo,00425C40
00401592 . EB 34 JMP SHORT SecureKo,004015C8
00401594 > C74424 04 B8 MOV DWORD PTR SS:[ESP+4],SecureKo,0043B8
0040159C . C70424 C0334 MOV DWORD PTR SS:[ESP],SecureKo,004433C0
004015A3 . E8 F88B0200 CALL SecureKo,0042A1A0
004015A8 . C74424 04 CE MOV DWORD PTR SS:[ESP+4],SecureKo,0044015A8 Wrong!
004015B0 . C70424 C0334 MOV DWORD PTR SS:[ESP],SecureKo,004433C0
```

다음과 같이 스택의 값을 77DE5E8C와 비교하는 부분을 찾을 수 있다.

Password가 오직 숫자라고 했으니 16진수인 77DE5E8C 를 10진수로 바꾸면 2011061900이 나온다.

```
00401555 . 817D FC 8C5E CMP DWORD PTR SS:[EBP-4],77DE5E8C
0040155C . 75 96 JNZ SHORT SecureKo,00401594
0040155E . C74424 04 B8 MOV DWORD PTR SS:[ESP+4],SecureKo,0043B8
00401566 . C70424 C0334 MOV DWORD PTR SS:[ESP],SecureKo,004433C0
0040156D . E8 2E8C0200 CALL SecureKo,0042A1A0
00401572 . C74424 04 B8 MOV DWORD PTR SS:[ESP+4],SecureKo,004401572 Congratulations! ^~^
```

다음과 같이 2011061900을 입력하니 Congratulations! 라는 문구가 출력되었고 인증에 성공했다.

```
password is ONLY numbers?

Password: 2011061900

Congratulations! ^~^
```

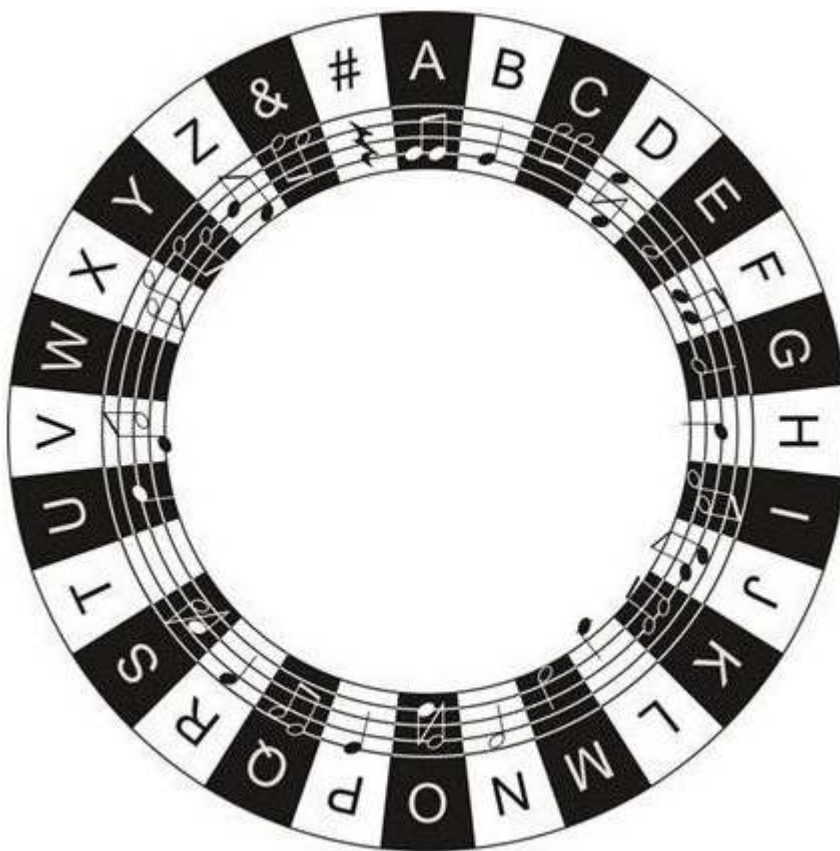
Key : 2011061900

5번 문제

다음과 같은 악보가 하나 주어진다.



암호라는 생각이 들었고 음표암호를 검색, 마타하리 암호라는 것을 알아냈다.
다음은 마타하리 암호표이다.



위의 암호표대로 디코드하니 SEC?RI?Y가 나왔고 계싱을 통해 SECURITY로 인증에 성공하였다.

Key : SECURITY

6번 문제

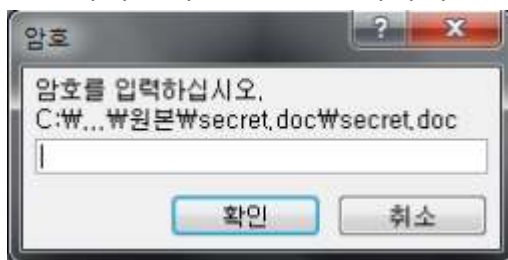
다음과 같이 gz 파일이 하나 주어진다.

 secret.doc.gz

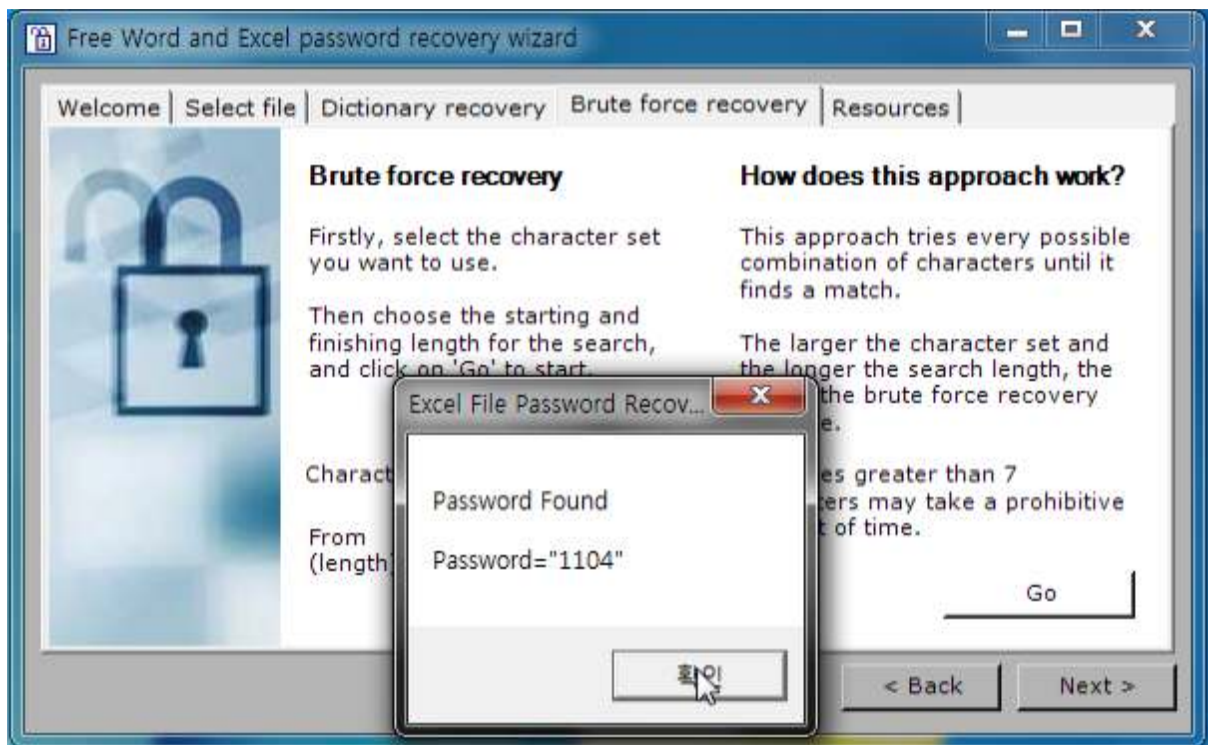
압축을 풀어보면 다음과 같이 doc 파일 하나가 나온다.

 secret.doc

실행시켜보니 암호를 입력하라고 한다.



Free Word and Excel password recovery wizard 툴을 이용해서 비밀번호를 크랙하였다.



비밀번호에 1104를 입력하고 doc 파일을 열어보니 다음과 같은 글이 있었다.

패스워드를 찾으셨군요.

↵

패스워드에서 100을 뺀 값을 답안에 기입해주세요.

1104에서 100을 뺀 1004로 인증에 성공하였다.

Key : 1004

7번 문제

7번 문제는 웹 문제였다.

로그인 폼이 있었고, securekorea 계정으로 로그인하라고 했다.

우선 내 아이디로 로그인 해보았다.

그러자, 쿠키에 user='아이디를 base64로 2번 인코드 한 값' 이 들어갔다.

securekorea를 base64로 2번 인코드 한 값을 쿠키에 넣어주니 다음과 같은 글이 출력되었다.

축하합니다. securekorea 계정으로 로그인 되었습니다.

아래의 코드값을 분석하여 전달하고자 하는 기밀 정보를 알아내시면 정답입니다.


코드값 : 115,101,99,117,114,101,35,107,111,114,101,97,35,95,49,95,67,111,110

코드값을 아스키코드라고 생각하여 디코드하니 secure#korea#_1_Con 라는 값이 나왔고 인증에 성공했다.

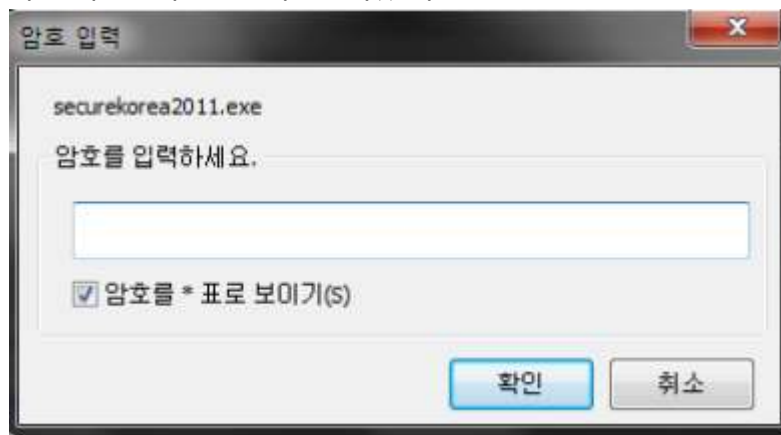
Key : secure#korea#_1_Con

8번 문제

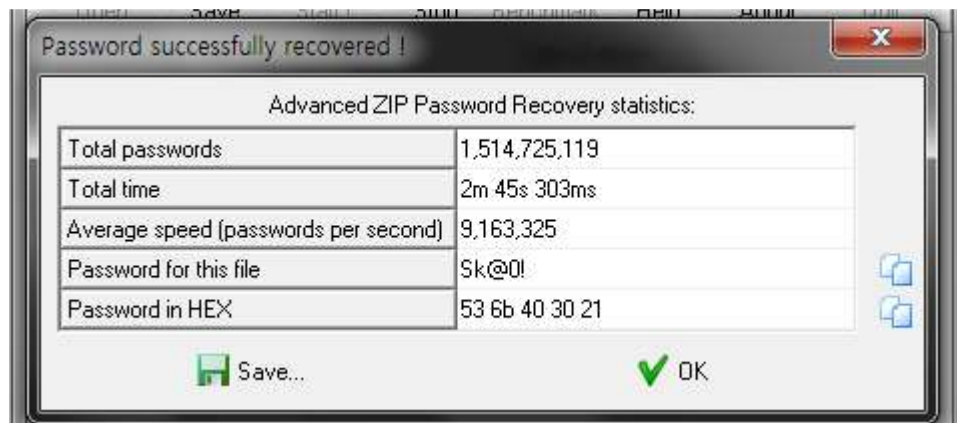
8번 문제는 아무도 풀지 못하였고, 푸는 도중 대회가 끝났었다.
다음과 같은 zip 파일을 준다.

 SecureKorea2011-Reversing.zip

다음과 같이 암호가 걸려있다.



또 다시 AZPR 툴을 이용해 비밀번호를 크랙해 Sk@0! 라는 비밀번호를 얻었다.



압축을 풀면 다음과 같은 파일 하나가 나온다.

 securekorea2011.exe

압축을 푸니 securekorea2011-1.exe 라는 파일이 나왔다.

 securekorea2011-1.exe

다음과 같이 아무 값이나 입력했더니 Fail! 이라는 문장이 출력되었다.

```
=====
Secure Korea 2011 해킹방어대회
=====

KEY를 입력하세요 : 1234
Fail!

KEY를 입력하세요 :
```

올리디버거로 열어서 보면 다음과 같이 패킹되었다는 것을 알 수 있다.

Address	Hex dump	Disassembly	Comment
00409720	60	PUSHAD	
00409721	BE 00804000	MOV ESI,secureko,00408000	
00409726	8DBE 0090FFFF	LEA EDI,DWORD PTR DS:[ESI+FFFF9000]	
0040972C	57	PUSH EDI	
0040972D	EB 0B	JMP SHORT secureko,0040973A	
0040972F	90	NOP	
00409730	8A06	MOV AL,BYTE PTR DS:[ESI]	
00409732	46	INC ESI	
00409733	8B07	MOV BYTE PTR DS:[EDI],AL	
00409735	47	INC EDI	
00409736	010B	ADD EBX,EBX	

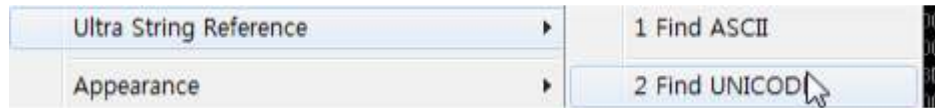
다음과 같이 마지막의 JMP 구간에 브레이크포인트를 걸어 수동으로 언패킹하였다.

Address	Hex dump	Disassembly	Comment
00409891	57	PUSH EDI	
00409892	FFD5	CALL EBP	
00409894	58	POP EAX	
00409895	61	POPAD	
00409896	8D4424 80	LEA EAX,DWORD PTR SS:[ESP-80]	
0040989A	6A 00	PUSH 0	
0040989C	39C4	CMP ESP,EAX	
0040989E	75 FA	JNZ SHORT secureko,0040989A	
004098A0	83EC 80	SUB ESP,-80	
004098A3	E9 F07EFFFF	JMP secureko,00401798	
004098A8	48	DB 48	CHAR 'H'

언패킹을 하여 실제 엔트리 포인트로 왔다.

Address	Hex dump	Disassembly	Comment
00401798	E8 7B040000	CALL secureko,00401C18	(Initial CPU
0040179D	E9 9FFDFFFF	JMP secureko,00401541	
004017A2	8BFF	MOV EDI,EDI	
004017A4	55	PUSH EBP	
004017A5	8BEC	MOV EBP,ESP	
004017A7	81EC 28030000	SUB ESP,328	
004017AD	A3 48614000	MOV DWORD PTR DS:[406148],EAX	
004017B2	890D 44614000	MOV DWORD PTR DS:[406144],ECX	
004017B8	8915 40614000	MOV DWORD PTR DS:[406140],EDX	

Ultra String Reference를 이용해 UNICODE를 찾아보았다.



그러자 다음과 같이 문자열들이 떴다.

2735f2c54e255f10ba7f03b6e318b843 이라는 md5값이 보인다.

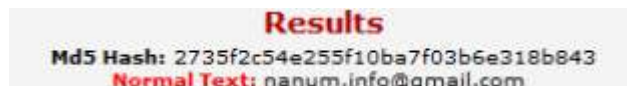
Address	Disassembly	Text String
00402DC6	PUSH secureko,004042B8	2735f2c54e255f10ba7f03b6e318b843
00402E7B	MOV ESI,secureko,00404244	TTqP0/SoJReLPD0eRg7WJSSSWDqh0JuVvheLqT6SKQGw_BR2RCB6MN :
00402EC9	PUSH secureko,00404290	C:₩₩₩Windows₩System32
00402FF8	PUSH secureko,004042DC	%02x
004030B4	PUSH secureko,004041A4	cls=====₩n
004030C2	PUSH secureko,004041A8	=====₩n
004030D5	PUSH secureko,004041CC	Secure Korea 2011 해킹방어대회 ₩n
004030E9	PUSH secureko,004041F0	=====₩n₩n
0040310A	PUSH secureko,00404214	KEY를 입력하세요 : Success!
004031C9	PUSH secureko,00404228	Success!
004031E4	PUSH secureko,00404234	pause
00403236	PUSH secureko,0040423C	Fail!

md5 디코드 사이트에서 위의 md5값을 디코드 해봤다.



그러자 다음과 같이 nanum.info@gmail.com 이라는 메일 주소가 나왔다.

위의 메일 주소가 답이거나 메일을 보내 어떻게 문제를 더 푸는 것 같았으나 대회가 종료되어 더 이상 풀 수 없었다.



후기

다음과 같이 7문제를 풀고 11등을 하였다.

20등 안에 들어 본선에 진출하게 되었다. 첫 대회임에도 좋은 성적을 거두어서 좋았다. 앞으로도 노력해야겠다.

시큐어코리아 중고생 해킹방어대회 랭킹보기

※ 문제당 100점이며 동점일 경우 문제를 먼저 푼 참가자가 우선순위를 먼저 가짐
참고 : 순위를 명확하게 보이기 위해 timestamp 값을 출력함

순위	아이디	총점수	문제1	문제2	문제3	문제4	문제5	문제6	문제7	문제8	문제9	문제10
1	hkdiw0823	700	20110619125357	20110619125403	20110619183434	20110619183444	20110619183613	20110619183624	20110619183629	X	X	X
2	ppark	700	20110619125517	20110619130154	20110619183926	20110619184241	20110619185846	20110619191123	20110619191748	X	X	X
3	pyutic	700	20110619125518	20110619125529	20110619183509	20110619183924	20110619184539	20110619191007	20110619192044	X	X	X
4	chldktjd1024	700	20110619125519	20110619125524	20110619130300	20110619153757	20110619154815	20110619161045	20110619192454	X	X	X
5	tester	700	20110619130817	20110619130823	20110619184406	20110619190542	20110619190654	20110619192245	20110619192524	X	X	X
6	BillyHerrington	700	20110619130255	20110619130307	20110619183400	20110619183913	20110619190249	20110619191401	20110619193358	X	X	X
7	lokihardt	700	20110619130122	20110619130127	20110619183626	20110619184117	20110619185837	20110619190850	20110619193832	X	X	X
8	pwn3r	700	20110619130235	20110619130245	20110619183718	20110619183827	20110619192120	20110619193443	20110619194107	X	X	X
9	nagi	700	20110619125427	20110619125433	20110619185859	20110619190258	20110619192612	20110619193355	20110619194556	X	X	X
10	parkayun	700	20110619130203	20110619130208	20110619190232	20110619190240	20110619193725	20110619193734	20110619195453	X	X	X
11	smith	700	20110619125518	20110619130253	20110619190220	20110619191026	20110619193054	20110619195246	20110619195620	X	X	X
12	h3jin	700	20110619125438	20110619125516	20110619185858	20110619190320	20110619193736	20110619195343	20110619200326	X	X	X
13	gggg	700	20110619125500	20110619125507	20110619190520	20110619191015	20110619193114	20110619200341	20110619201502	X	X	X
14	rest	700	20110619142921	20110619190157	20110619190209	20110619191032	20110619193120	20110619200457	20110619201659	X	X	X
15	vio	700	20110619130333	20110619130403	20110619185840	20110619190527	20110619194132	20110619200547	20110619201833	X	X	X
16	name1588	700	20110619130440	20110619130501	20110619185849	20110619190258	20110619193819	20110619195609	20110619202119	X	X	X
17	hanmanseong	700	20110619125415	20110619125422	20110619185830	20110619185943	20110619191459	20110619191716	20110619202125	X	X	X
18	baleen	700	20110619125400	20110619125405	20110619185920	20110619190304	20110619193727	20110619200658	20110619202151	X	X	X
19	n0m	700	20110619152921	20110619184349	20110619185923	20110619192756	20110619194307	20110619200645	20110619202223	X	X	X
20	dlcjf95	700	20110619130452	20110619130458	20110619185957	20110619190529	20110619195421	20110619200923	20110619202606	X	X	X
21	jaction02	700	20110619130436	20110619130445	20110619185855	20110619190258	20110619194933	20110619194940	20110619202942	X	X	X
22	deiph	700	20110619125350	20110619125354	20110619192752	20110619195139	20110619200732	20110619201320	20110619203408	X	X	X
23	deiph	700	20110619125350	20110619125354	20110619192752	20110619195139	20110619200732	20110619201320	20110619203408	X	X	X