

Infini45T

박준혁 (한국디지털미디어고등학교 1학년)

2011.07.16

## 1번 문제

1번은 웹 문제였다.

원래 시큐어코리아 사이트와 똑같이 생겼다.

주어진 주소로 들어가서 쿠키를 보면 다음과 같은 쿠키가 보인다.

```
Stago-key=NGQ2YTRkMzE0ZDdhNTkzMTRlNmE0ZDMzNGU1NDYzNzk0ZTZhNTUzMTVhNmE1MjY5NGU2ZDU5MzM0ZDZhNTkzMTRlNmE0NTMxNWE2YTRkNzk0ZDdhNDE3YTRkNTQ0ZDc4NGU1NzU5Nzk0ZDU0NDk3YQ==
```

base64같아서 base64로 디코드를 해보았다.

다음과 같이 hex같은게 나온다.

```
4d6a4d314d7a59314e6a4d334e5463794e6a55315a6a52694e6d59334d6a59314e6a45315a6a4d794d7a417a4d544d784e5759794d54497a
```

헥스에디터에 넣어보니 또다시 base64같은게 나온다.

```
MjM1MzY1NjM3NTcyNjU1ZjRiNmY3MjY1NjE1ZjMyMzAzMTMxNWYyMTIz
```

base64로 디코드하니 또 hex값이 나온다.

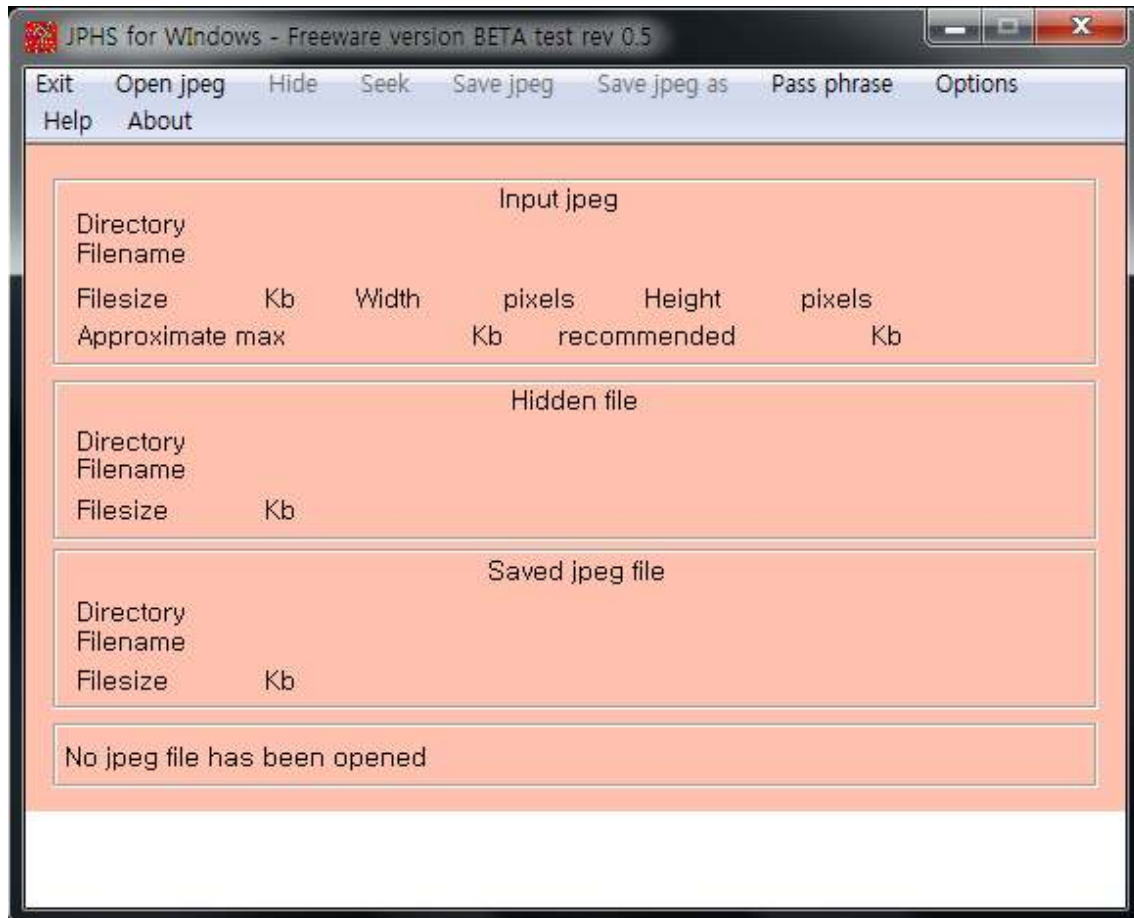
```
235365637572655f4b6f7265615f323031315f2123
```

헥스에디터에 넣으니 #Secure\_Korea\_2011\_!# 라는 값이 나온다.

답으로 생각했지만 인증이 계속 되지 않았다.

몇 시간 후에 스테가노그래피 문제라는 힌트가 주어졌다.

여러 스테가노그래피 툴들을 찾다가 JPHS 라는 툴을 발견했다.



다음과 같이 jpg파일을 선택 한 후 Seek 버튼으로 숨겨진 파일을 찾았다.



그러자 숫자로 구성된 텍스트 파일이 나왔다.

일정한 패턴을 발견했고 그 패턴들을 없애니 다음의 텍스트가 나왔다.

32333533363534333735353236353566346236663532363534313566333234303231323132643  
665363136653735366432653639366536366634303637366436313639366332653633366636

헥스 에디터에 넣으니 다음의 값이 나왔다.

235365437552655f4b6f5265415f324021212d6e616e756d2e696e666f40676d61696c2e636f6d

위의 값을 다시 헥스 에디터에 넣으니 다음의 값이 나왔고 인증에 성공했다.

#SeCuRe\_KoReA\_2@!!-nanum.info@gmail.com

## 2번 문제

2번은 확장자가 없는 파일이 하나 주어진다.

파일 헤더를 보니 `0x00000000` 였고 파일 시그니처에 검색 결과 다음과 같이 패킷 캡처 파일이었다.

`D4 C3 B2 A1`

`0x00000000`  
n/a WinDump (winpcap) capture file (Windows)

와이어샹크로 열어 보니 wep 크랙 문제라는 것을 알 수 있었고 Aircrack -ng 툴로 풀기로 했다.

Aircrack -ng 툴을 켜고 후에 파일을 선택하고 Launch 버튼을 누르면 다음과 같이 크랙을 시작한다.

잠시 후에 KEY FOUND! 라는 문자열과 함께 키가 나온다.

KEY에서 콜론을 뺀 다음의 값을 인증에 성공하였다.

2D997A157ECCB52F139CD07B94

```
관리자: C:\windows\System32\cmd.exe

Aircrack-ng 1.1

[00:00:00] Tested 676 keys (got 49922 IVs)

KB    depth  byte(vote)
0     11/ 14  3A<56320> F2<55552> 20<55296> 21<55296> F0<55040>
1     24/  1  EC<55040> 33<55040> 4A<54784> 7E<54784> 8F<54784>
2      0/  1  40<71424> C6<57600> A3<57600> CC<57088> 51<57088>
3      2/  3  CD<59648> EA<58624> C3<58368> 6F<58368> 81<58112>
4      0/  3  D3<71680> AB<60928> 0C<59904> 3E<58880> 9B<58112>

KEY FOUND! [ 2D:99:7A:15:7E:CC:B5:2F:13:9C:D0:7B:94 ]
Decrypted correctly: 100%

2 [main] aircrack-ng 9260 fork: child -1 - CreateProcessW failed, errno 2

D:\Sonic\유틸리티&툴-W\aircrack-ng-1.1-win\bin>
```

### 3번 문제

3번 문제는 쉬운 웹 문제였다.

소스를 보면 `rand()%100` 함수로 0~99까지의 100가지의 난수를 생성시킨 후 입력 값과 비교시킨다.

한 값만 대입하는 프로그램을 코딩 후 실행시키면 다음의 답이 출력된다.

`#SeCuReK@ReA@)1!`

