2016 순천향대학교 정보보호 페스티벌

예선 풀이

이름 : 이진근

학교 :한세사이버보안고

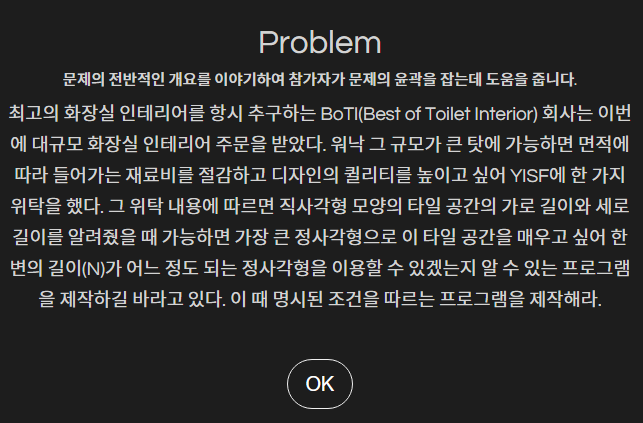
아이디 :iuy1234

닉네임 :Sori

자기 점수 :850

등수 : 18

**Algorithm** 50



유클리드 호제법을 사용하여 C로 소스코드를 짜 컴파일 하였다

#include <stdio.h>

int ucle(int a,int b){

int temp;

int big,small;

if(a<b){

big=b;

small=a;

}

else{

big=a;

small=b;

}

while(small){

temp=big%small;

big=small;

small=temp;

}

return big;

}

int main(void){

int a,b, g,s;

int cas,i;

scanf("%d",&cas);

for(i=1;i<=cas;i++){

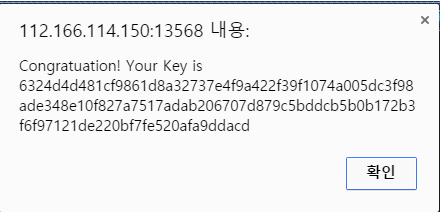
scanf("%d %d",&a,&b);

g=ucle(a,b);

printf("%d\n",g);

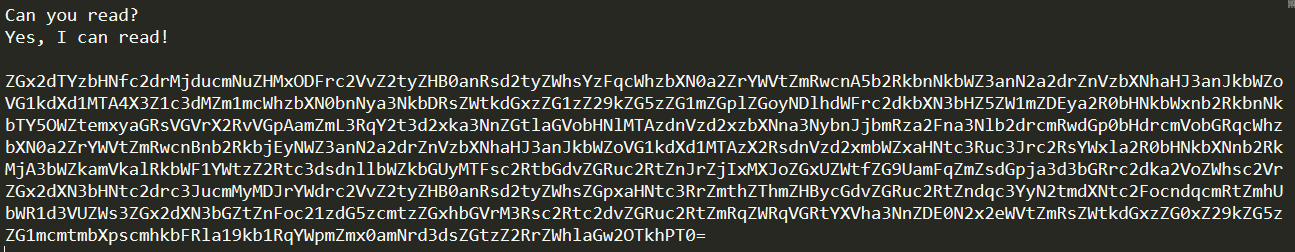
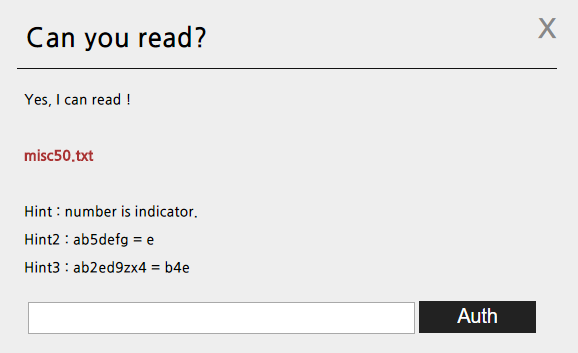
}

}

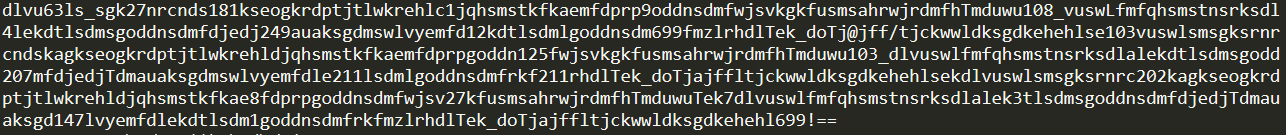


Flag=6324d4d481cf9861d8a32737e4f9a422f39f1074a005dc3f98ade348e10f827a7517adab206707d879c5bddcb5b0b172b3f6f97121de220bf7fe520afa9ddacd

**Misc 50**



base64로 두번 디코딩하면 제공된 플래그가 깨진다. 세번째 힌트가 제공되어야 이해를 하게 되었는데 한번 디코드 한 뒤, 문자열의 숫자번째에 있는 문자를 가져와 조합하면 플래그가 완성될 것 같았다.

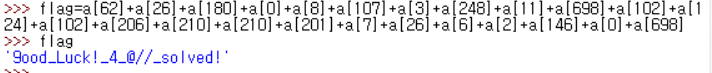


위의 문자열의 숫자들만 추출하면 아래의 숫자들이 나온다

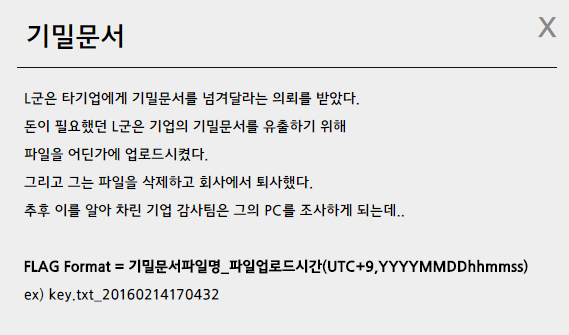
63 27 181 1 9 108 4 249 12 699 103 125 103 207 211 211 202 8 27 7 3 147 1 699 각각 이 숫자번째의 문자를 가져오면 될 것 같았다.

파이썬으로 적절히 추출해보니 아래의 플래그가 나왔다.

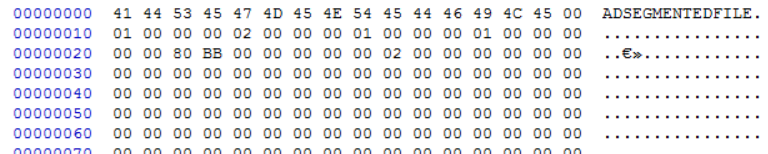
(숫자가 0부터 시작하므로 각각의 숫자에 -1을 해주어야 정상적인 플래그가 나온다)



**Forensic** 50



제공된 파일을 받고 압축을 풀어 헥스에딧으로 까보면 파일시그니쳐 부분이



라고 나온다 adsegmentedfile은 FTK Imager에서 사용하는 이미지 파일이다.

FTK imager로 까보면 어떤 PC의 하드디스크 사본이 나오게 된다.

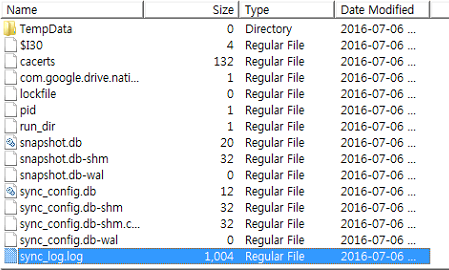
지문에서 어딘가로 업로드 시켰다고 하였다. 이로써 업로드 하는 클라이언트를 생각하여 보았는데 웹을 이용한 업로드와 프로그램을 이용한 업로드가 기억에 났다.

폴더에 가보면 IE, chrome, GoogleDrive가 있다. IE는 실행이 안되었고, 크롬은 문제가 없었다.

구글드라이브로 확신을 짓고 아래의 경로로 이동하였다

\Users\Administrator\AppData\Local\Google\Drive\user\_default

sync\_log라는 로그파일이 있었고, 거기에는 동작하는 로그들이 찍혀있었다.

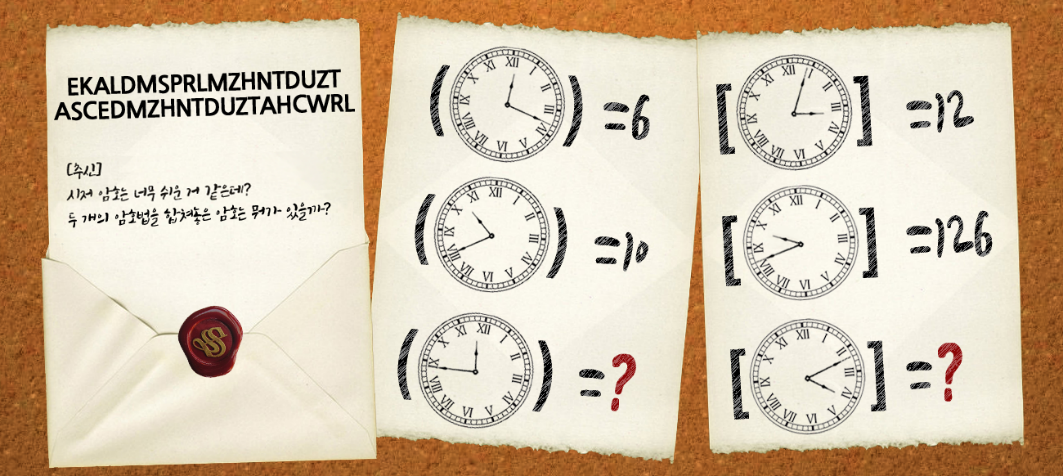


중요한 서류파일을 업로드 했다는 지문에 따라 log파일을 export하여 .docx로 검색하였더니 T0pS2cret.docx 라는 파일이 나왔다. 2016-07-06 16:37:02 에 업로드 하였다고 나온다.

따라서 flag format에 맞추면

Flag = T0pS2cret.docx\_20160706163702

Crypto 50



시계를 정확하게 분단위로 보여준 것이 이상하여 한번 풀어보았다

왼쪽의 시계들은 두 수(시와 분)의 최대공약수, 오른쪽은 두수의 최소공배수였다.

12:18= 6 3:04 12

10:40 = 10 9:42 126

11:44 = 11 4 :12=12

키가 두 개인 암호화, 시저가 너무 쉬운걸?이라는 지문을 보니 지난번 교보문고에서 보았던 책에서 아핀 암호를 다루던 것이 기억이 났다.

http://system.kcu.ac/opendept/crypto/sub/training/affine.html

이곳을 사용하여 아핀암호를 복호화 하였다



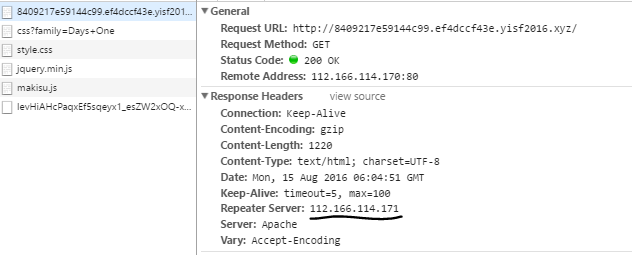
Flag = EOGHLAKFRHANJTDLWNDGKSELANJTDLWNDGJSIRH

Web 50

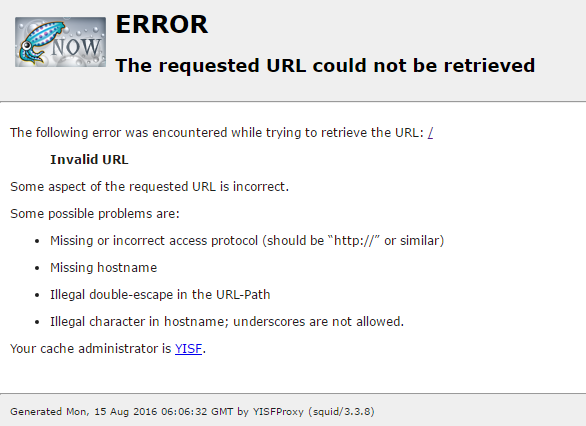


힌트 3번까지 나와야 풀 수 있었던 문제다

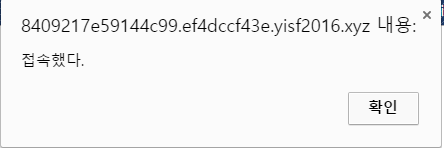
중계기를 영어로 번역해보니 리피터라고 나왔다. 이는 리피터 서버에 무언가 있음을 예상할 수 있었고, 포트가 2000~2999까지 주어졌는데 지문에 응답하라 2016이라고 되어 있어 포트가 2016인 것을 예상할 수 있었고 역시 2016번 포트는 열려있었다.

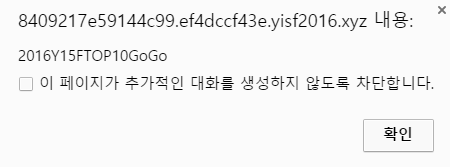


리피터 서버의 주소(112.166.114.171:2016)로 들어가 보면 아래의 화면이 나온다.



그리고 힌트 2번에 나왔던 8080포트가 주어졌는데, 난 처음에 다른 웹 서버인줄 알았는데 구글에 검색해 보니 proxy server라고 나왔고, 인터넷 옵션에서 프록시 설정을 바꾸고 문제에 주어졌던 페이지를 다시 들어가면,

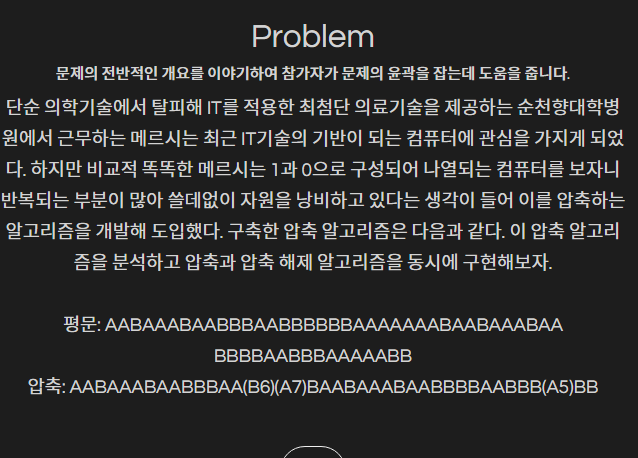




정상적인 플래그가 출력이 되게 된다.

Flag = 2016Y15FTOP10GoGo

**Algorithm** 100



문자열 검색하는 것이 인덱스로 찾는 방법과 정규표현식을 사용하여 찾는 방법을 알고있었는데, 정규표현식은 내가 재대로 잘 사용을 못해서 인덱스로 짰었다. 자바의 replace가 기억이 나서 자바로 코드를 짰는데 그러자



시간이 부족하였다. 인덱싱하여 replace하는 것이었는데 시간이 매우 오래걸렸던 것 같다.

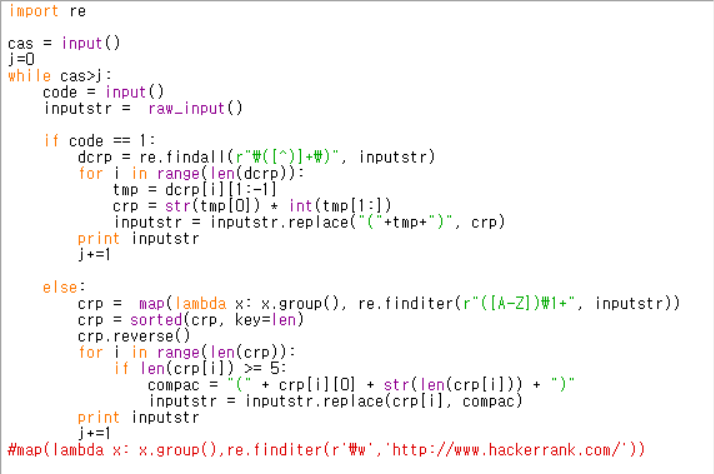
할 수 없이 구글에 정규표현식을 검색하고 검색한 문서를 보니 람다 함수를 사용하면 쓸때없는 조건문과 반복문이 생략된다고 한다.

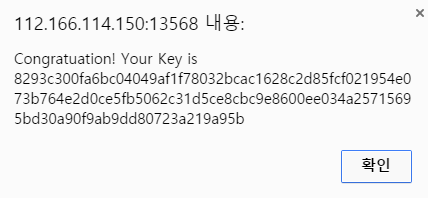
람다 사용법은 stackoverflow.com에서 본

https://www.hackerrank.com/challenges/re-findall-re-finditer

이곳을 참고하였다.

자바로 짜기엔 시간이 너무 오래 걸려서 구글에 정규표현식과, 람다함수 예제를 많이 참고하여서 파이썬 코드를 짜서 돌렸다





Flag= 8293c300fa6bc04049af1f78032bcac1628c2d85fcf021954e073b764e2d0ce5fb5062c31d5ce8cbc9e8600ee034a25715695bd30a90f9ab9dd80723a219a95b

수고 많으셨습니다.

풀이보고서는 [yisf.sch@gmail.com](mailto:yisf.sch@gmail.com) 으로 보내주시면 됩니다.