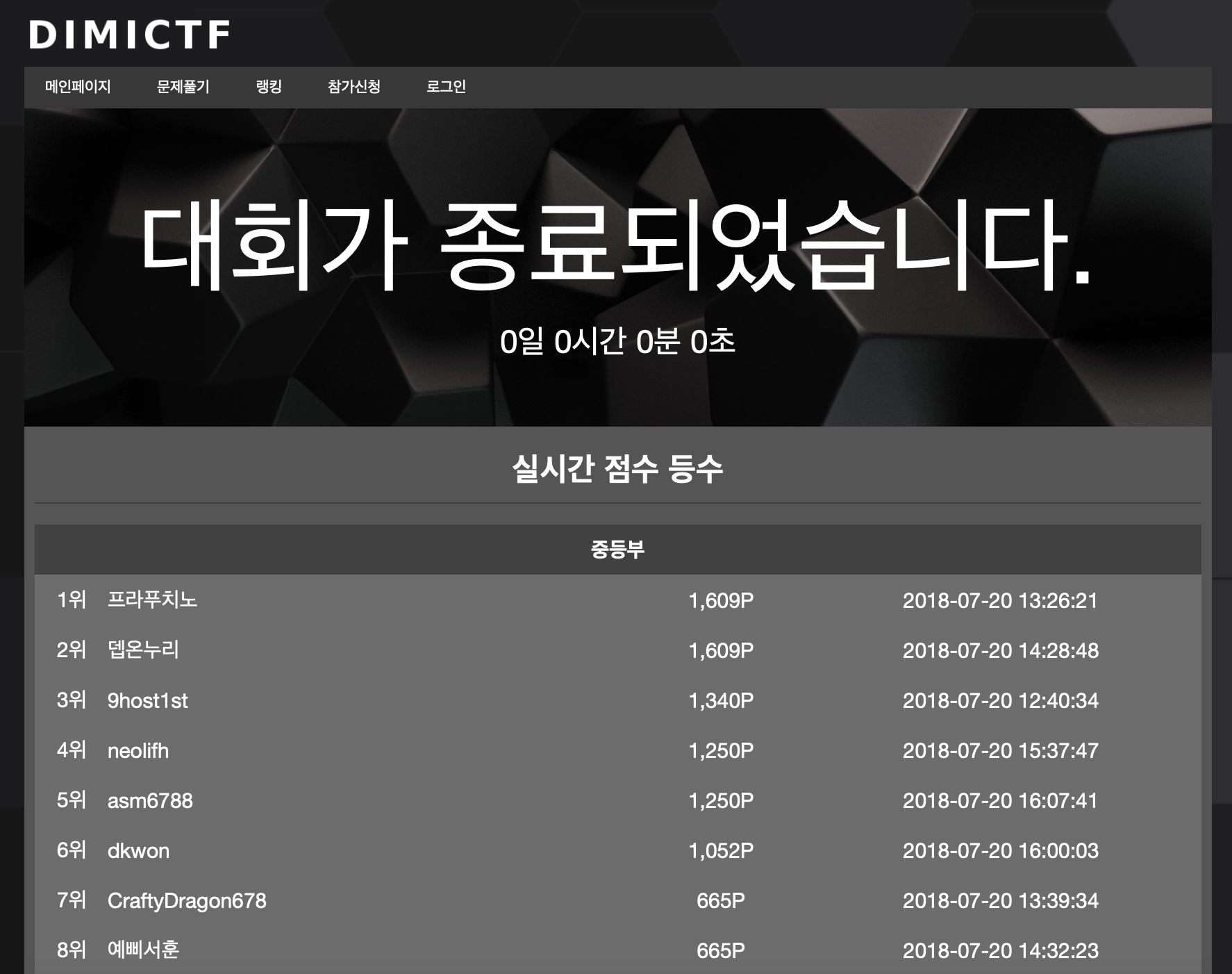
**DIMI CTF 2018 예선 WRITE-UP**

**8위 (예삐서훈)**



**저번 디미고 대회 때는 3위를 했는데, 이번에는 8위로 많이 떨어졌다.**

**대회가 끝나자마자 문제가 닫혀서 자세하게 write-up을 쓸 수는 없겠다.**

**guess\_return(MISC)**

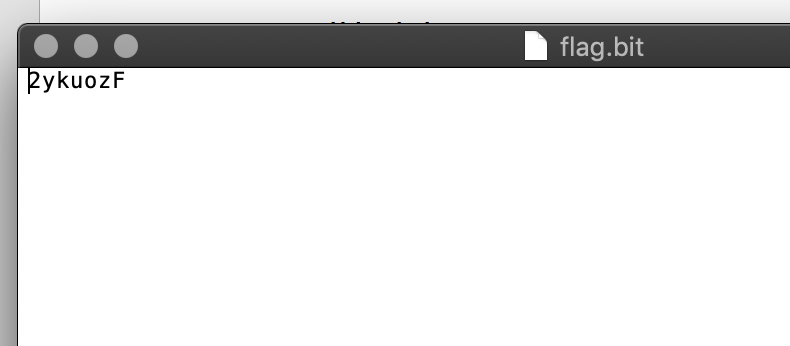
**문제 설명 : Do you remember? This time it is not image, It is just some bit ;)**

**첨부 파일 : flag.bit**

**저번에 나왔던 imgur guess 문제랑 비슷한것 같다**

**이 문제 푸는데 가장 많은 시간을 투자 했던것 같다**

**별거 아닌데,,**



**저번과 비슷하게 파일에 어떤 문자열이 있다**

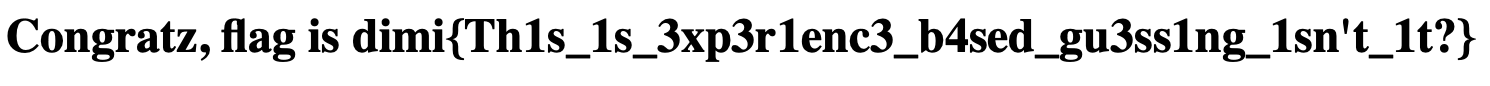
**처음에는 저번과 똑같은 문제 인줄 알고 imgur에서 삽질 하다가**

**구글링 엄청하고**

**아주 삽질 했다 ㅋㅋㅋ**

**그래서 생각하다가 bit bit bit bit.ly???**

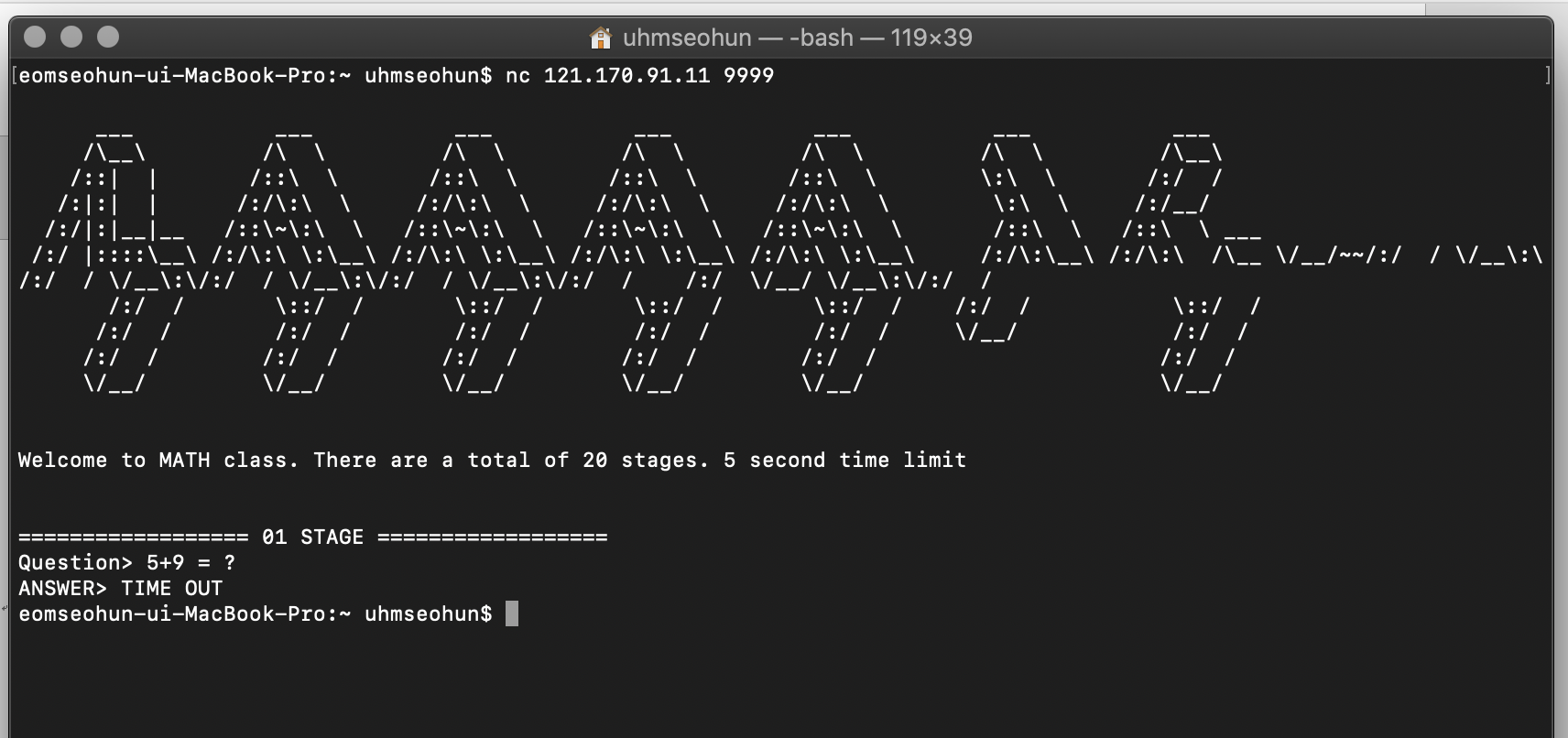
**bit.ly가 떠올라서 bit.ly/2ykuozF에 들어가니 flag가 나왔다**



**flag : dimi{Th1s\_1s\_3xp3r1enc3\_b4sed\_gu3ss1ng\_1sn't\_1t?}**

**math (MISC)**

**문제 설명 : nc 121.170.91.11 9999**



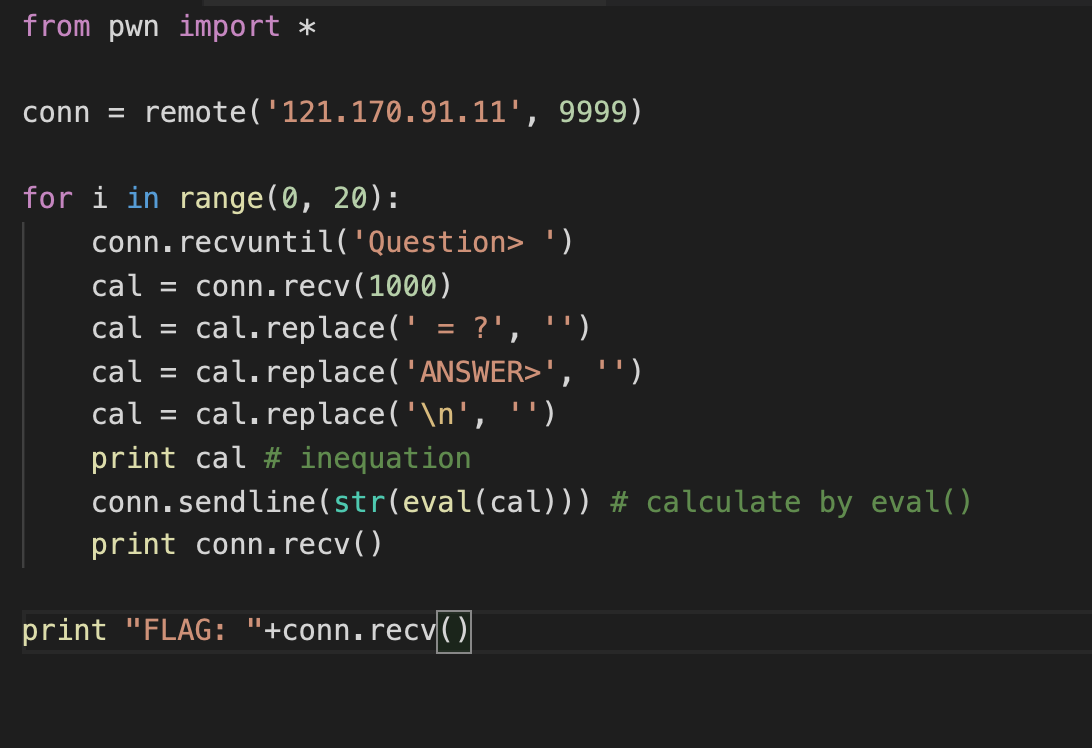
**디미 CTF에서 매년 나오는 문제 형식이다**

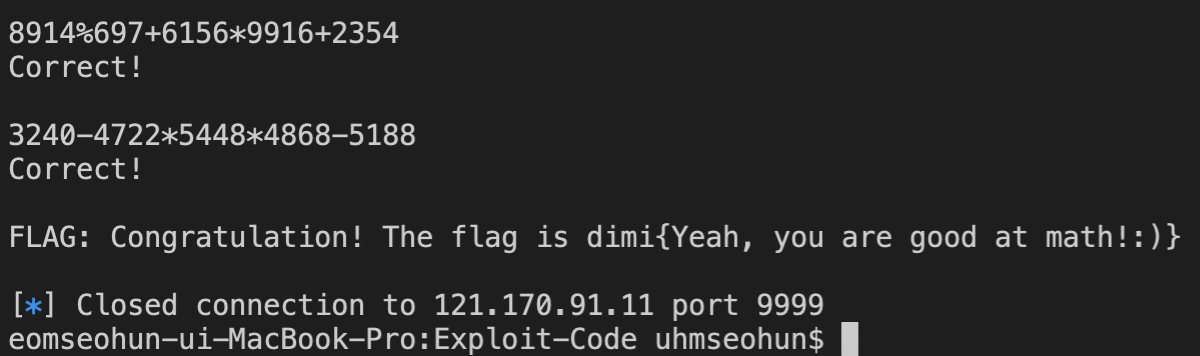
**숫자야구 등등 종류별로 다 나온다**

**이런 문제들을 풀기 위해 pwntools를 공부 했었는데, 쓸모가 있어졌다**

**초반에는 5+9 같이 쉬운 문제들이 나오다가, 후반으로 가면 3240-4722\*5448\*4868-5188 이런 문제도 나온다**

**파이썬으로 프로그램을 짜서 풀었다**





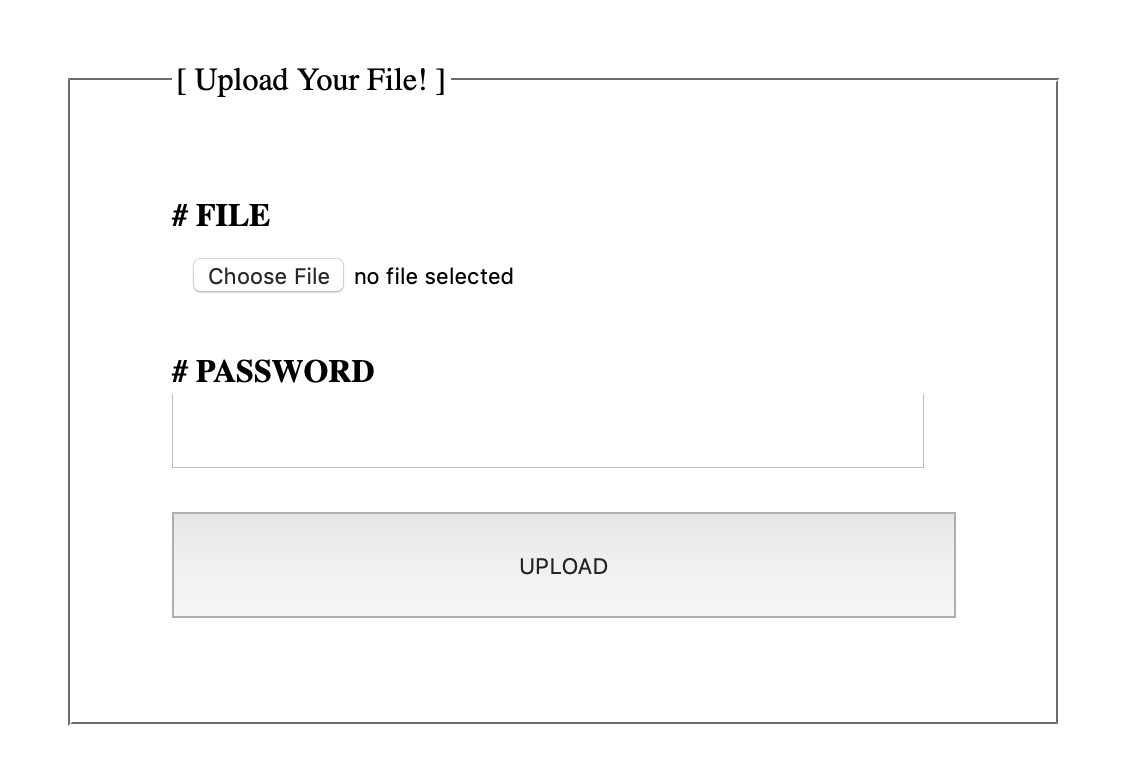
**실행 결과.**

**flag : dimi{Yeah, you are good at math!:)}**

**DimiStorage (WEB)**

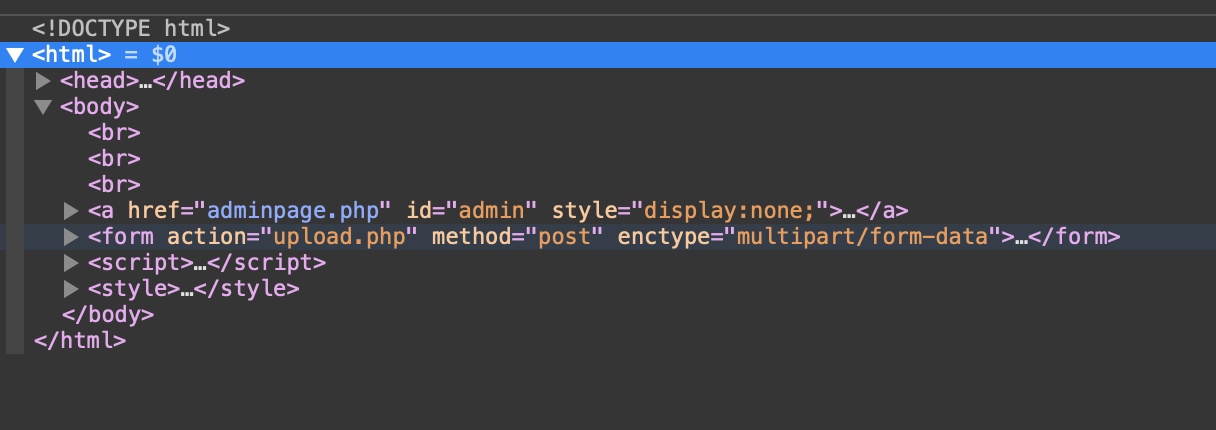
**이번에는 내가 좋아하는 웹 문제가 2문제 밖에 안나왔다**

**우선 링크에 들어가면**

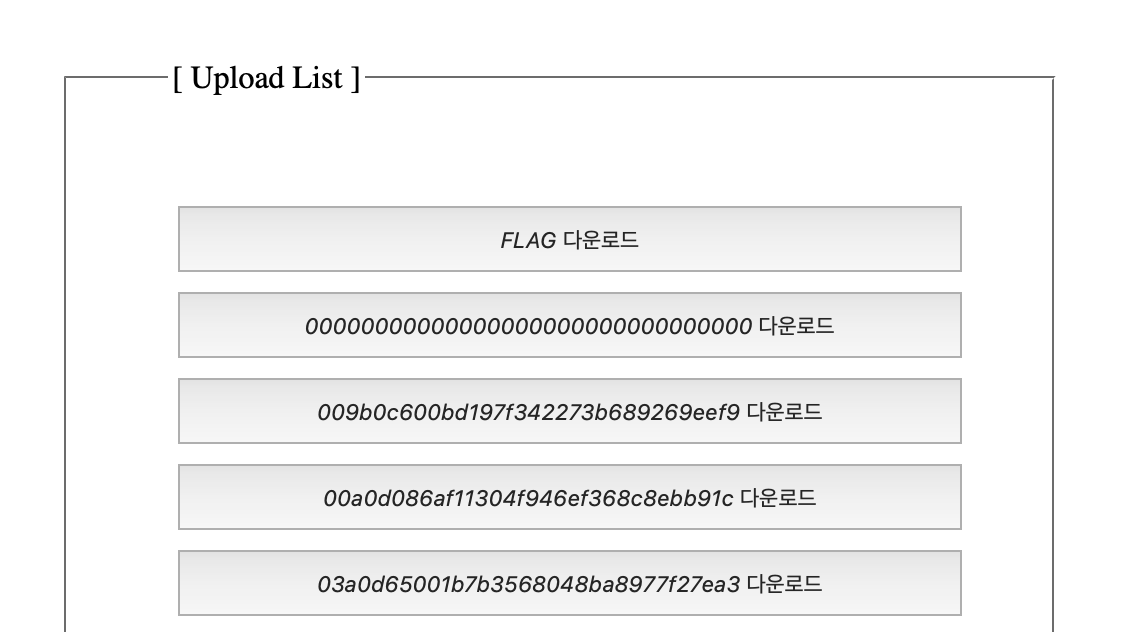


**이런 화면이 나온다**

**요소 검사를 해보니**

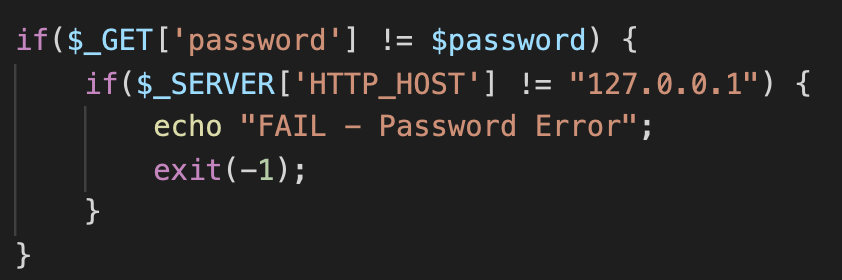


**adminpage.php가 보인다. 들어가 보자**



**사람들이 업로드한 파일들이 보인다**

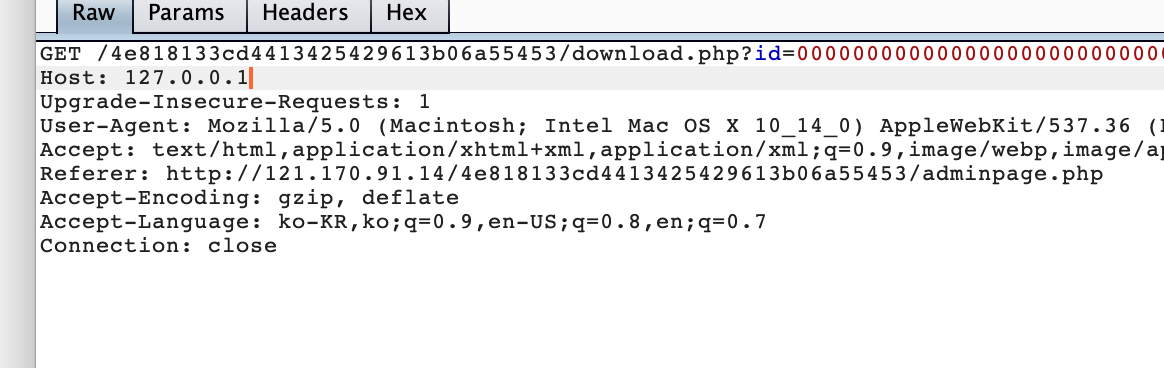
**여기까지 보고, 이제 주어진 소스코드를 보자**



**입력한 password가 맞지 않으면서 $\_SERVER[’HTTP\_HOST’]가 127.0.0.1이 아니라면 실패하고, 아닌건 모두 다운로드 된다.**

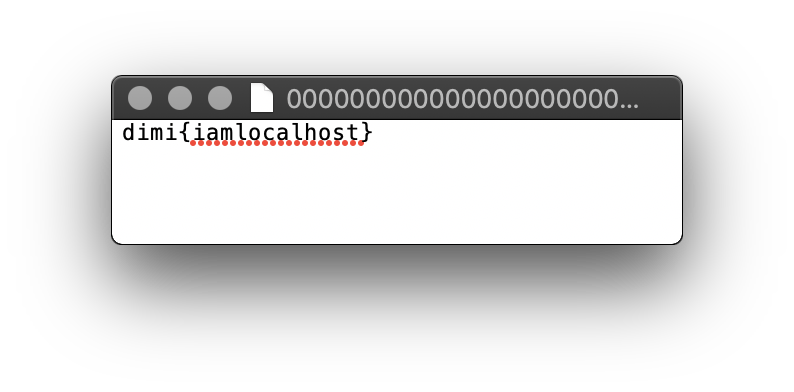
**하드코딩된 password를 알아내는건 거의 불가능 하므로 우리는 $\_SERVER[’HTTP\_HOST’]를 조작해보자**

**$\_SERVER[’HTTP\_HOST’]는 프록시 툴로 간편하게 조작이 가능하**



**위에 있는 사진은 FLAG 다운로드 버튼을 누른후 request 값에서 HOST 값을 127.0.0.1로 바꾼 상태 이다**

**이렇게 조작하고 forward를 누르면 flag가 다운로드 된다**



**flag : dimi{iamlocalhost}**

**Waiting (REV)**

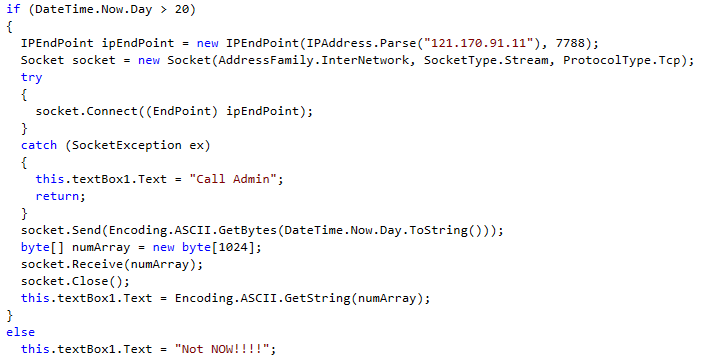
**정확한 문제 명은 기억나지 않지만 실행파일 이름이 Waiting.exe로 되어있어서 waiting 이었던것 같다**

**실행하면 Not NOW!! 라고 뜬다.**

**이걸로 시간이랑 뭔가 연관이 있는 프로그램이라는 것을 알아냈다**

**이 프로그램을 DotPeek으로 디컴파일 해보니 오늘의 날짜가 20보다 크다면 소켓으로 무언갈 가져와 출력해주는 것 같다**

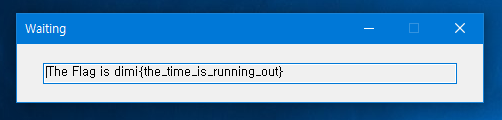
**20보다 크지 않다면 아까처럼 Not NOW!!를 출력한다**



**그래서 나는 윈도우의 날짜를 21일로 바꿨다**



**그러니 flag가 나왔다**



**flag : dimi{the\_time\_is\_running\_out}**

**이번에 내가 푼 문제는 4문제 인데, 더 공부해야겠다는 생각이 들게 했다**

**MISC의 image는 어느정도 guessing이 필요하긴 했다지만 감도 못잡았고,**

**pwnable의 uaf는 뭔지 대충 이해는 가는데 exploit 방법을 몰라 풀지 못했다**

**이제 내일 dis ctf 대회 끝나고 pwnable 열심히 공부해야겠다!!**

**최종 순위 8등. 아쉽당**