**CTF 01 Automation Report**

국어국문학과 2018312567 조명하

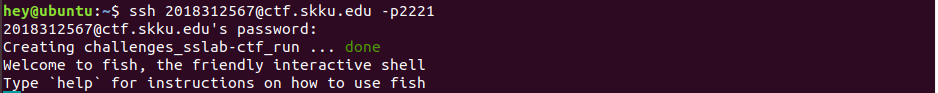
**0. 환경**

OS: Window에서 VMware위에 설치한 Ubuntu 18.04. LST

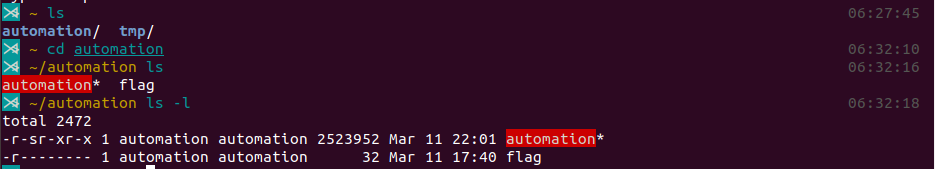
Language: Python 3.8.5



**1. 문제풀이 환경 로그인**



**2. 폴더 구조 파악**



***1) ls – l* 로 automation/ 폴더의 구조 확인**

- automation : 실행 가능 파일임을 확인했다.

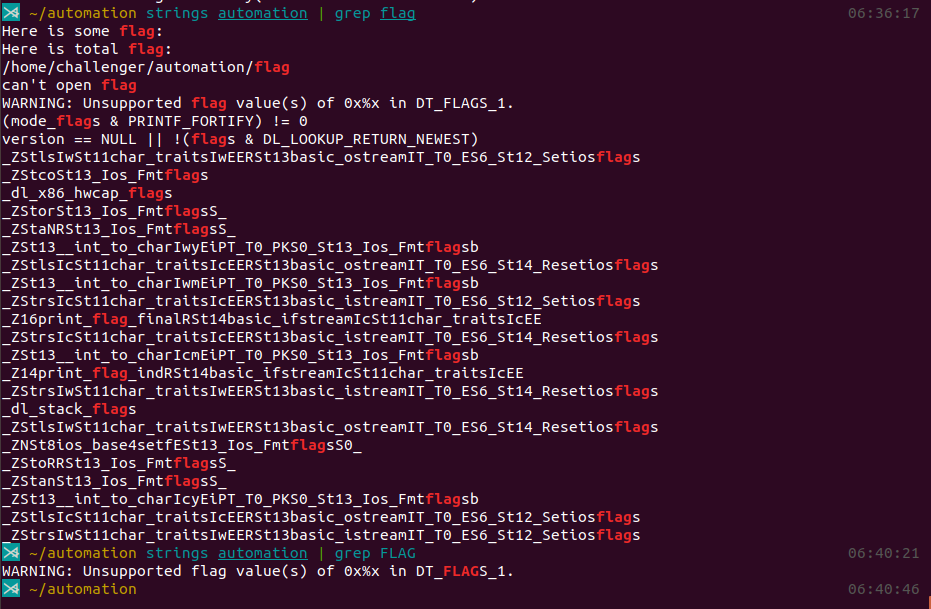
- flag : read-only 파일임을 확인했다.

**3. 파일 조사**



***1) File* 로 automation 확인**

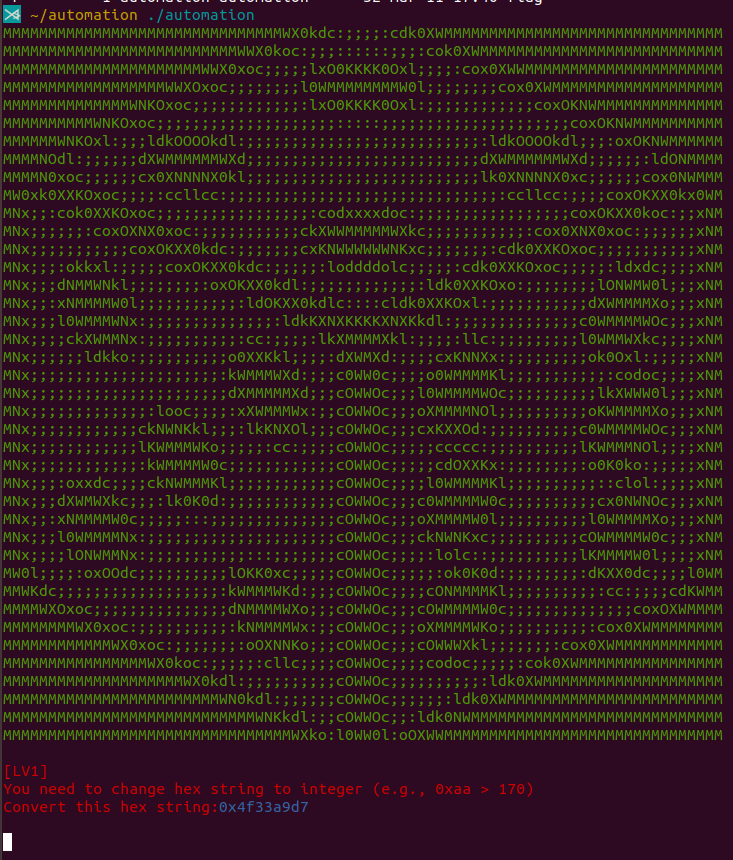
- Executable 파일이라는 것 이외에 문제 해결에 유의미한 정보를 얻지는 못했다.



***2) Strings* *| grep*로 파일 automation에서 flag / FLAG 검색**

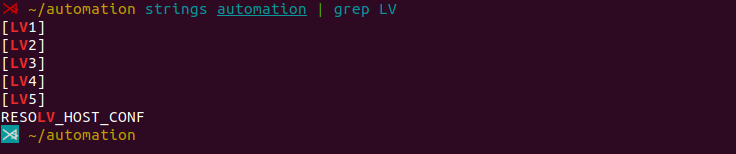
- 접근 불가능하게 막혀 있음 (can’t open flag)을 확인했다.

***3) 파일 automation 실행***



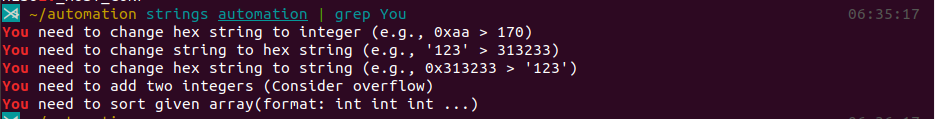
- 위와 같은 형식의 메시지가 출력되었고, **[LV1]**에서 각 단계의 문제를 풀다 보면 flag를 얻을 수 있을 것이라 예상했다.

***4) strings | grep LV으로 총 몇 단계가 있는지 확인***



***- Strings*** 명령어를 사용해 총 5단계의 문제가 있는 것을 확인했다.

***5) strings | grep you로 각 문제 내용 확인***

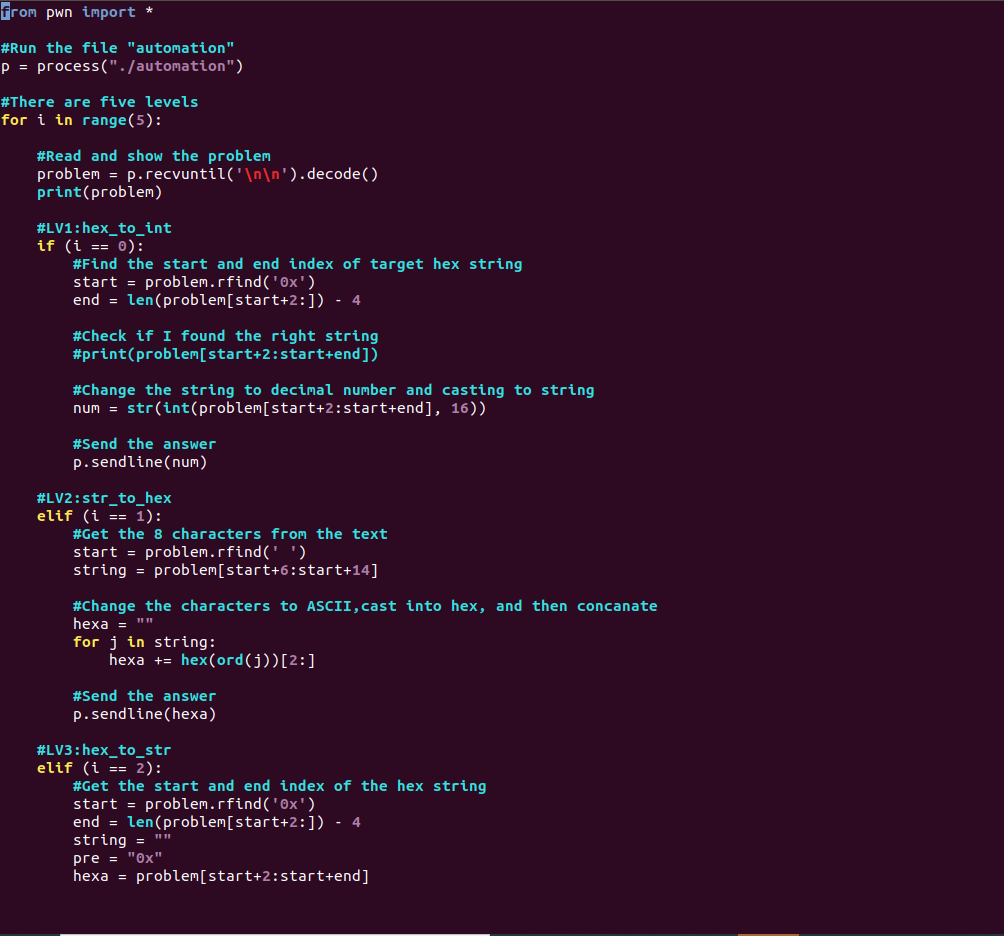


- 문제가 공통적으로 You need to~로 시작할 것이라 생각해 ‘You’를 검색어로 하여 각 단계의 문제 내용도 확인했다.

**4. 단계별 문제 해결하기 위한 코드 작성**



- 문제 Hint에 적혀 있듯이, 1초 안에 답을 전송하지 않으면 timeout으로 틀린 것으로 처리되기 때문에 답을 구하자마자 바로 전송할 수 있도록 ***pwntools*** 모듈을 사용해야겠다고 생각했고, 그래서 *Python3*로 코드를 작성했다.



- 함수 ***process()***로 automation을 실행하도록 했고, 그것을 변수 p에 할당했다.

- 총 5단계의 문제가 출제되므로 문제 decode하는 과정을 5번 반복한다.

- 문제에서 요구하는 대로 제출해야 할 값들을 추출하기 위해 프로그램에서 ***.recvuntil()*** 함수로 전체 텍스트를 받아 ***.decode()*** 함수로 string으로 decode해 problem 변수에 저장했다.

***1) LV1: hex to int***

- 주어진 문제에서 바꿔야 할 hex string의 start index와 end index를 추출했다.

- Prefix는 제외하고 구한 hex string을 ***int()*** 함수로 integer로 바꾸고 답을 전송하기 위해 ***str()***으로 캐스팅했다.

- ***.sendline()*** 함수를 사용해 프로그램에 답을 제출했다.

***2) LV2: str to hex***

- 주어진 문제에서 바꿔야 할 string의 start index와 end index를 추출했다.

- 문자열의 앞에서부터 한 글자씩 반복하며 ***ord()*** 함수로 문자를 아스키 코드 값으로 변환한 후 그 값을 다시 ***str()*** 함수로 캐스팅했다.

- ***.sendline()*** 함수를 사용해 프로그램에 답을 제출했다.



***3) LV3: hex to str***

- 주어진 문제에서 바꿔야 할 hex string을 추출한다.

- hex string의 문자를 앞에서부터 두 개씩 묶어서 ***int()***로 아스키 코드 값을 구하고, 그 값을 ***char()***로 캐스팅해 string으로 바꾼 다음 다시 ***str()*** 함수로 캐스팅했다.

- ***.sendline()*** 함수를 사용하여 답을 제출했다.

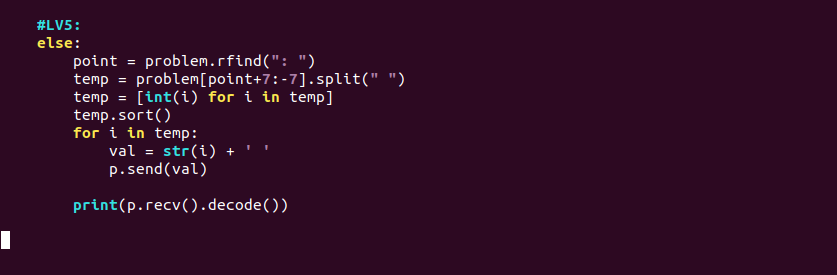
***4) LV4: overflow addition***

- 주어진 문제에서 두 숫자를 추출한다.

- 두 숫자를 ***int()***로 캐스팅해 더한다.

- overflow를 체크한다. int의 범위는 -2147483637 ~ 2147483647 이므로 이 범위를 넘는 값은 over한 만큼 최댓값 혹은 최솟값에서 그만큼을 이동해 실제 값을 구한다.

- ***str()***으로 캐스팅한 후 ***.sendline()***함수를 사용해 답을 제출했다.



***5) LV5: sort integers***

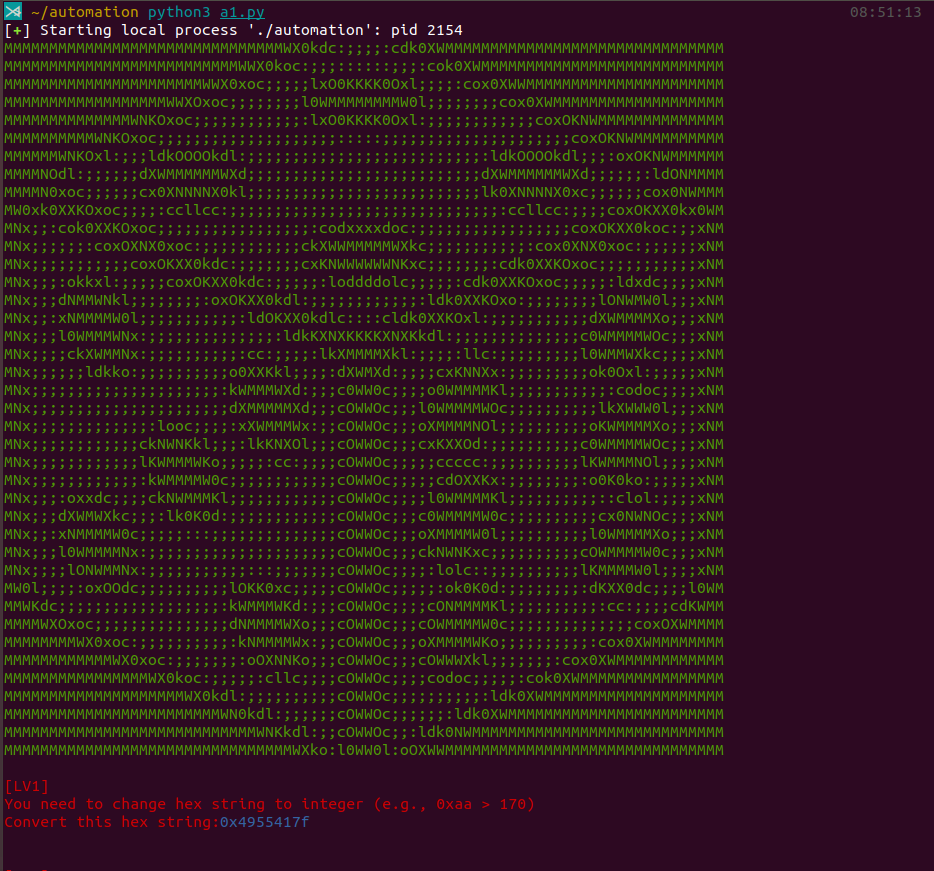
- 주어진 문제에서 숫자들을 추출해 temp라는 배열에 저장한다.

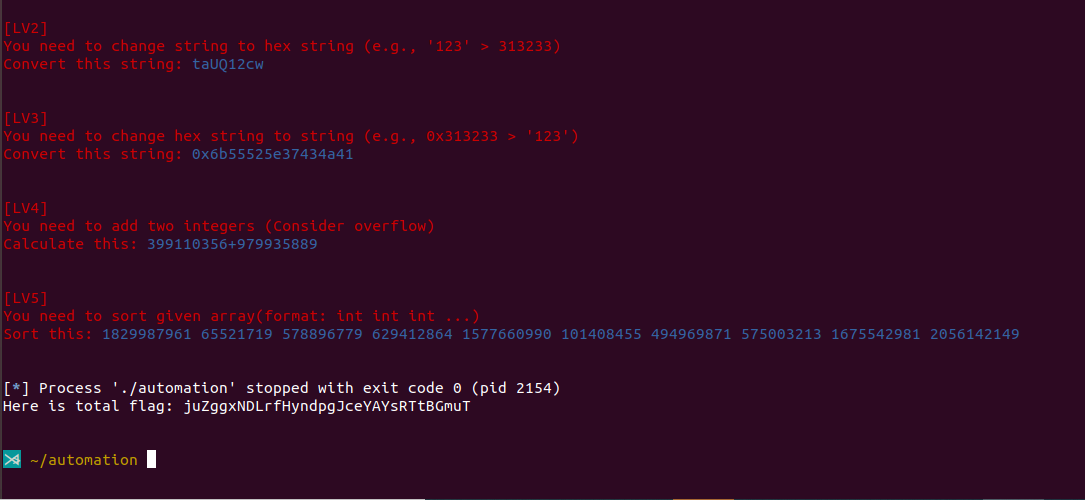
- temp에 저장된 문자열들을 ***int()***로 캐스팅한 후, ***sort()*** 함수로 정렬한다.

- 한 칸씩 띄어서 전송해야 하므로 temp의 값들을 각각 ***str()***으로 변환한 것에 **‘ ’**을 더하여 답으로 제출한다.

- 다섯 문제를 다 풀었으므로 flag가 공개될 것이다.

**5. 문제 풀기**





**Flag가 *‘juZggxNDLrfHyndpgJceYAYsRTtBGmuT’* 임을 확인했다.**