ESG TimeMachine Walkthrough

1. Prehistory

힌트를 보면 무엇인가를 찾아야 함을 알 수 있다.



마우스 커서를 사용하거나 개발자 도구, 페이지 소스를 통해 숨겨진 문장을 찾을 수 있다.



I discovered fire 입력하면 클리어

1. Ancient Hieroglyphs

힌트를 보면 주소창에 php?hint=hint를 입력해야 함을 알 수 있다.



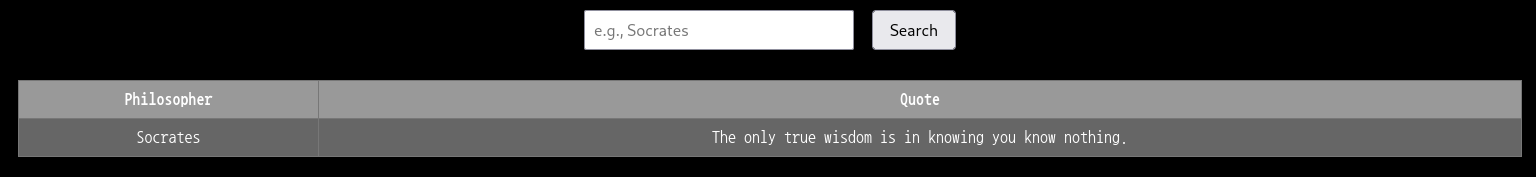
php?hint=hint로 들어가면 각 상형문자에 대응하는 알파벳과 숫자를 알 수 있다.



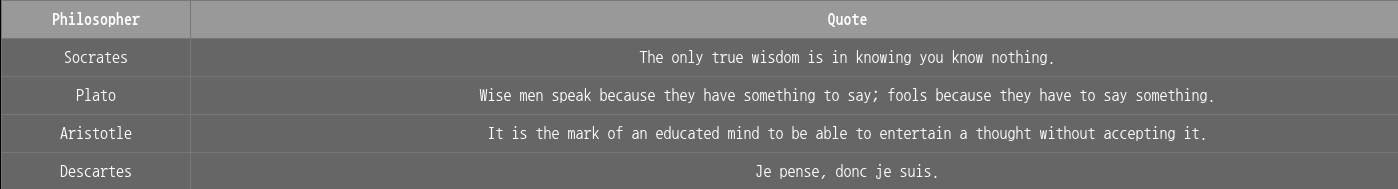
각각 대응해보면 BRING THE NEXT STONE 이 나온다. 이를 입력하면 클리어

1. Ancient Greek Forum

검색창에 주어진 예시처럼 Socrates를 입력하면 다음과 같이 나온다.



sql injection을 시도하기 위해 ‘or 1=1#를 입력하면 데이터가 모두 나온다.



뭔가 다른 거를 적으라고 되어있으므로 Je pense, donc je suis. 입력하면 클리어



1. Middle Age : Witch Hunt

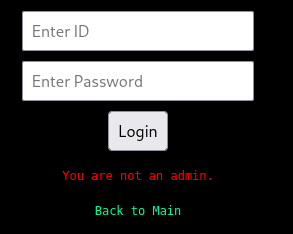
미션을 보면 가입을 해서 admin으로 위장하는 것이 목적이다.



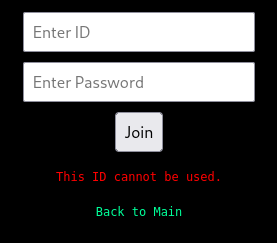
test /1234 로 회원가입 해보자.



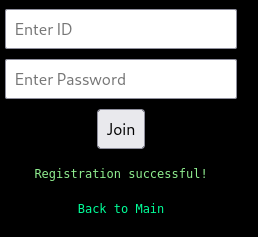
test /1234 로 로그인하면 admin이 아니라고 뜬다.



admin / 1234 로 회원가입 해보자. admin으로는 로그인이 안된다.



admin123 / 1234 로 회원가입 해본다. 회원가입이 성공했다.



admin123 / 1234 로 로그인 하면 성공.

admin+@ 로 로그인 시도하면 성공한다.

1. Scientific Revolution

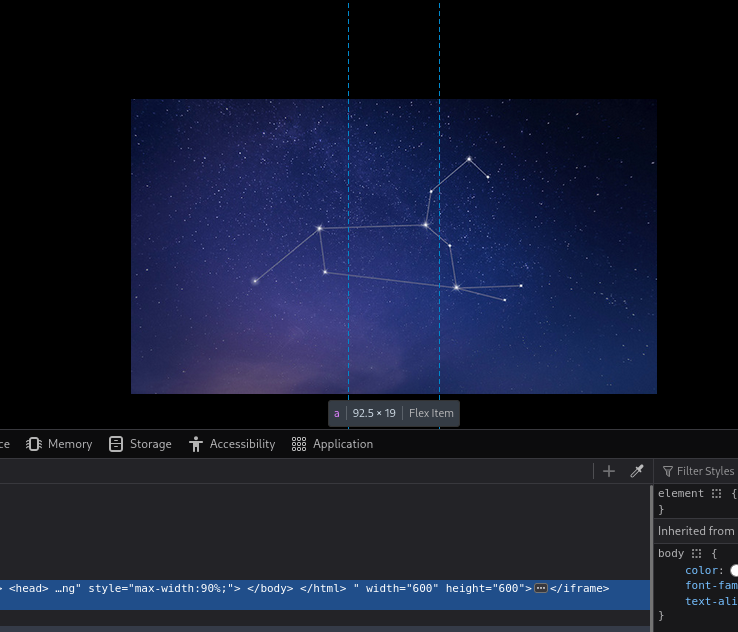
telescope을 사용하라고 되어있다.



개발자모드를 확인하면



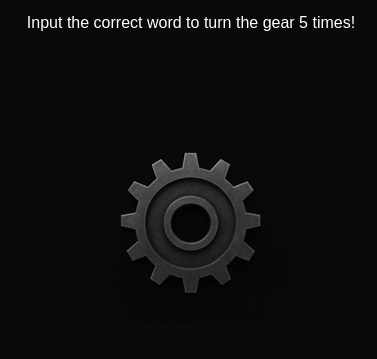
width와 height가 0이므로 숫자를 늘려보면 별자리 이미지가 나온다.



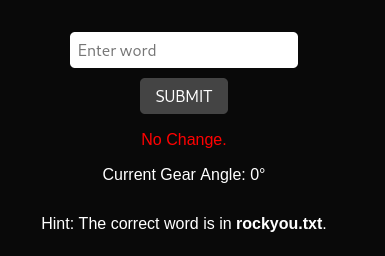
답에서 별자리를 입력하라고 되어 있으므로 사자자리인 leo를 입력하면 성공.

1. Industrial Revolution

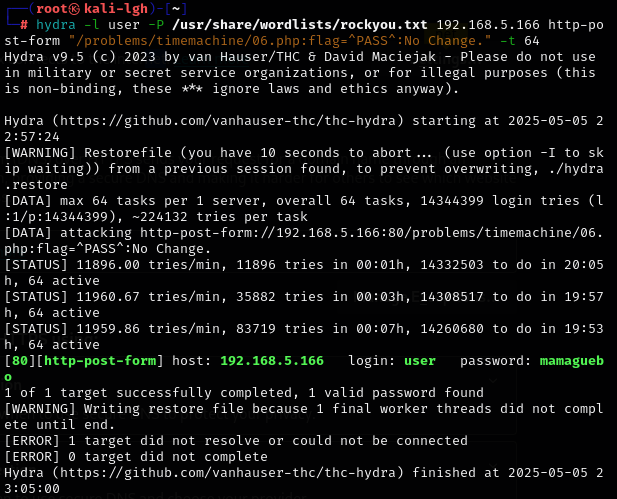
톱니바퀴를 5바퀴 돌려야 한다고 나와있다.



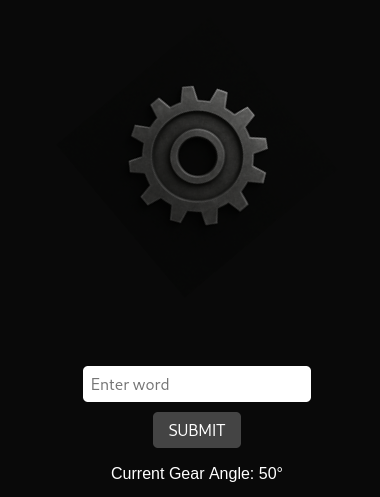
입력칸에 아무 단어나 입력했더니 No change가 뜬다. 힌트로 rockyou.txt에 들어갈 단어가 있다는 것을 알았으니 hydra를 이용해서 보겠다.



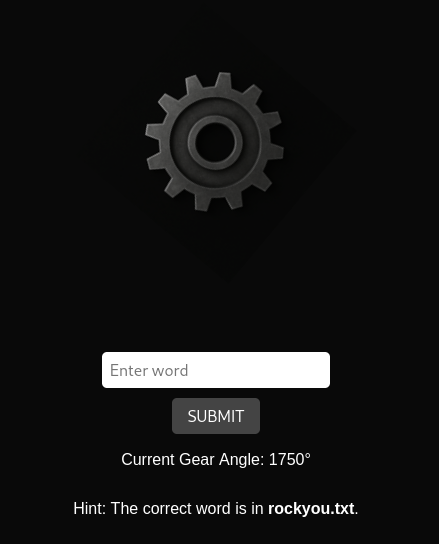
Hydra를 통해 mamaguebo라는 단어를 얻었다.



이를 대입하면 바퀴가 50도 움직인다.



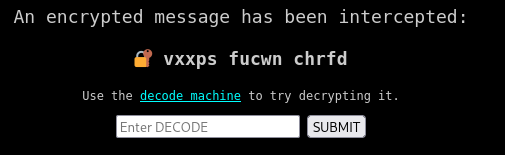
5바퀴는 1800도이므로 35번 더 움직이게 하면 된다. 일일이 복사 붙여넣기 해서 돌려도 되지만 burp suite의 repeater를 이용해서 돌리면 수월하다.



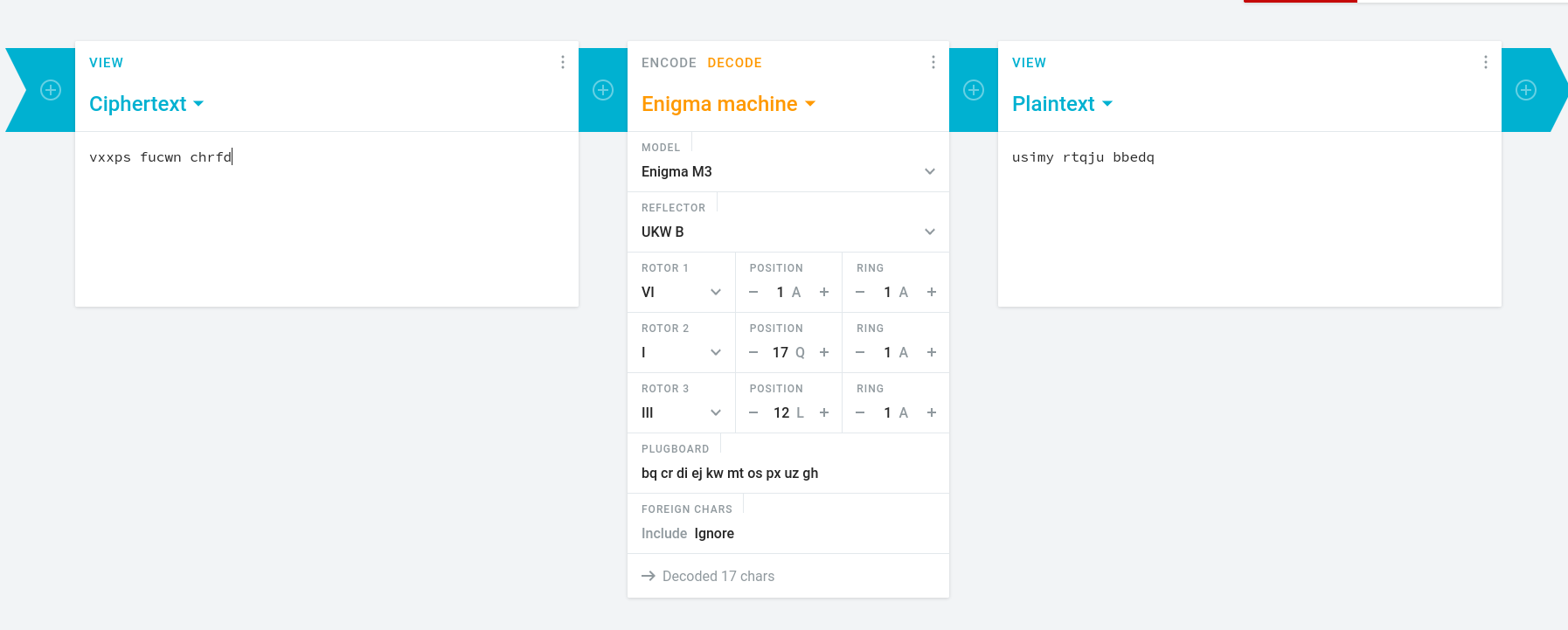
마지막 한번을 더 입력하면 클리어.

1. Enigma

암호화된 메시지를 해독해야 한다. decode machine 링크를 이용해서 디코딩하자.



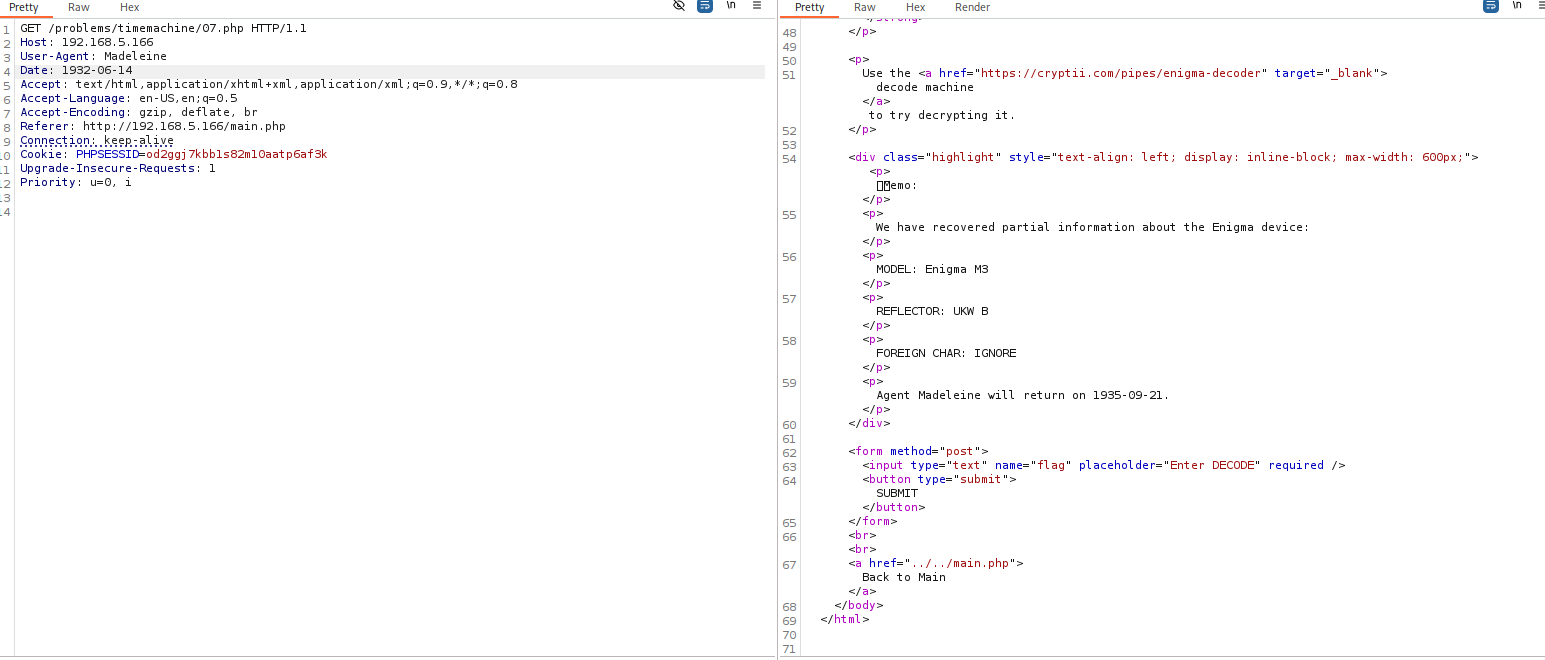
decode machine을 누르면 enigma를 디코딩할 수 있는 사이트가 나오는데 좌측 view에 암호문을 적는다.



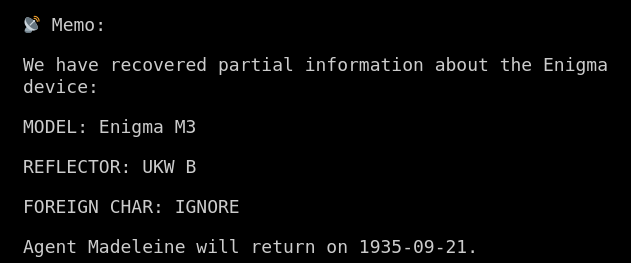
아래 문장에 따라 http 헤더에서 User-Agent는 Madeleine을 입력하고 Date에는 1932-06-14를 입력해보자.



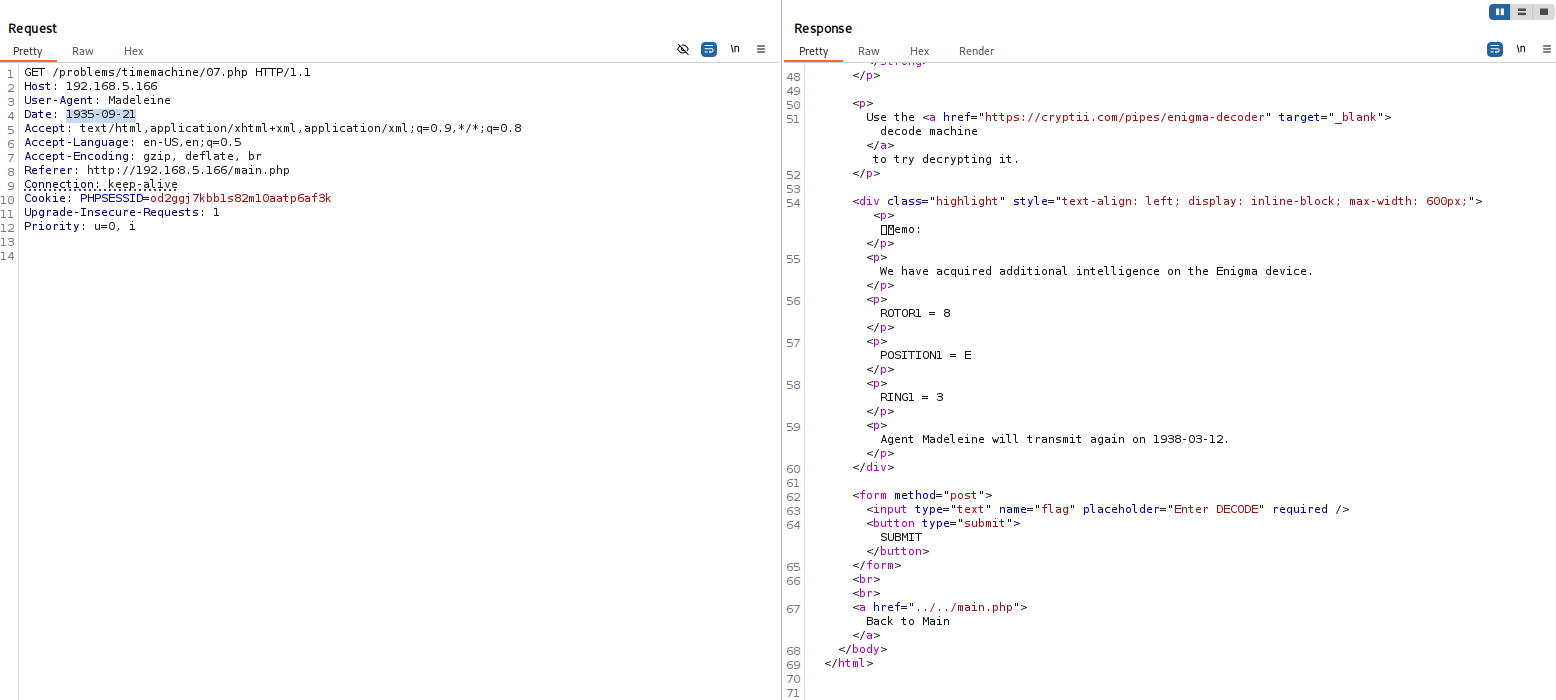
Burp suite를 이용하여 User-Agent와 Date값을 입력한다. Repeater를 이용하면 바로 입력하여 확인할 수 있다.



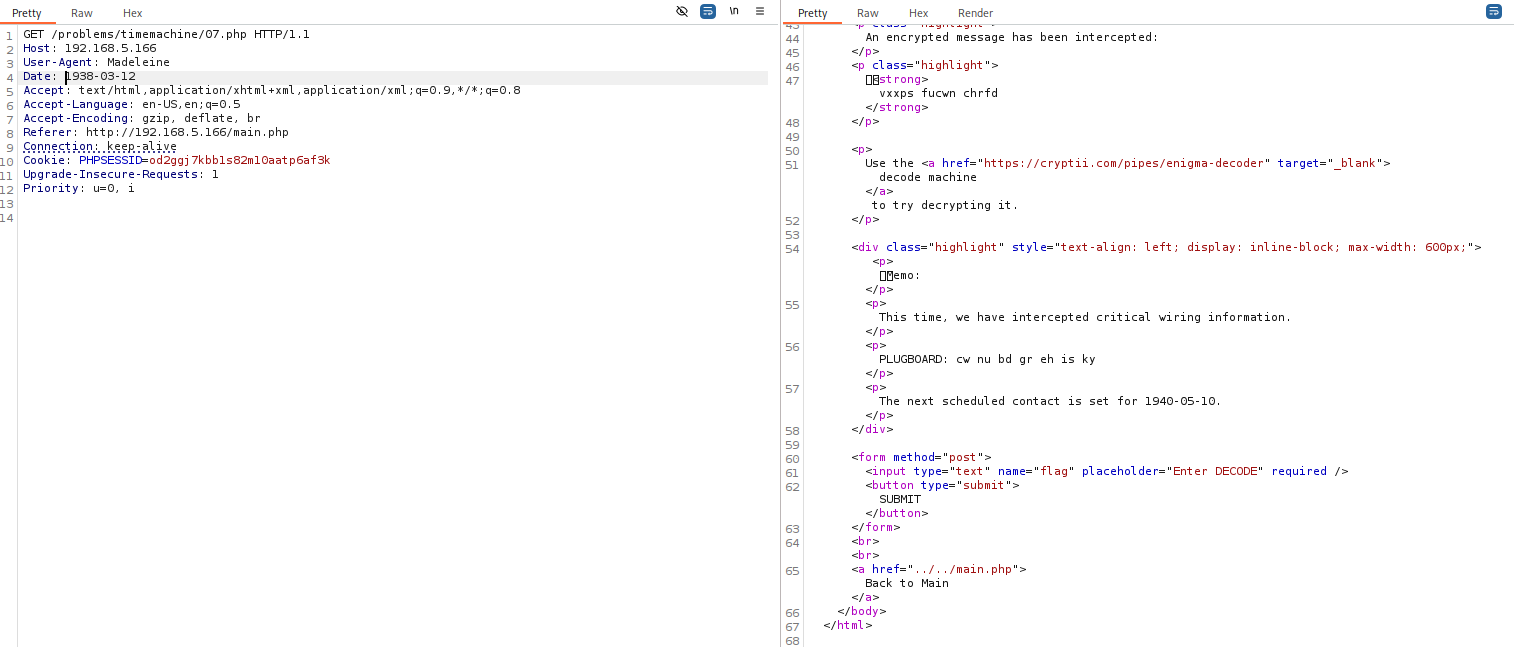
웹에는 다음과 같이 나온다. 힌트에 따라 decode 사이트에서 수정한다.



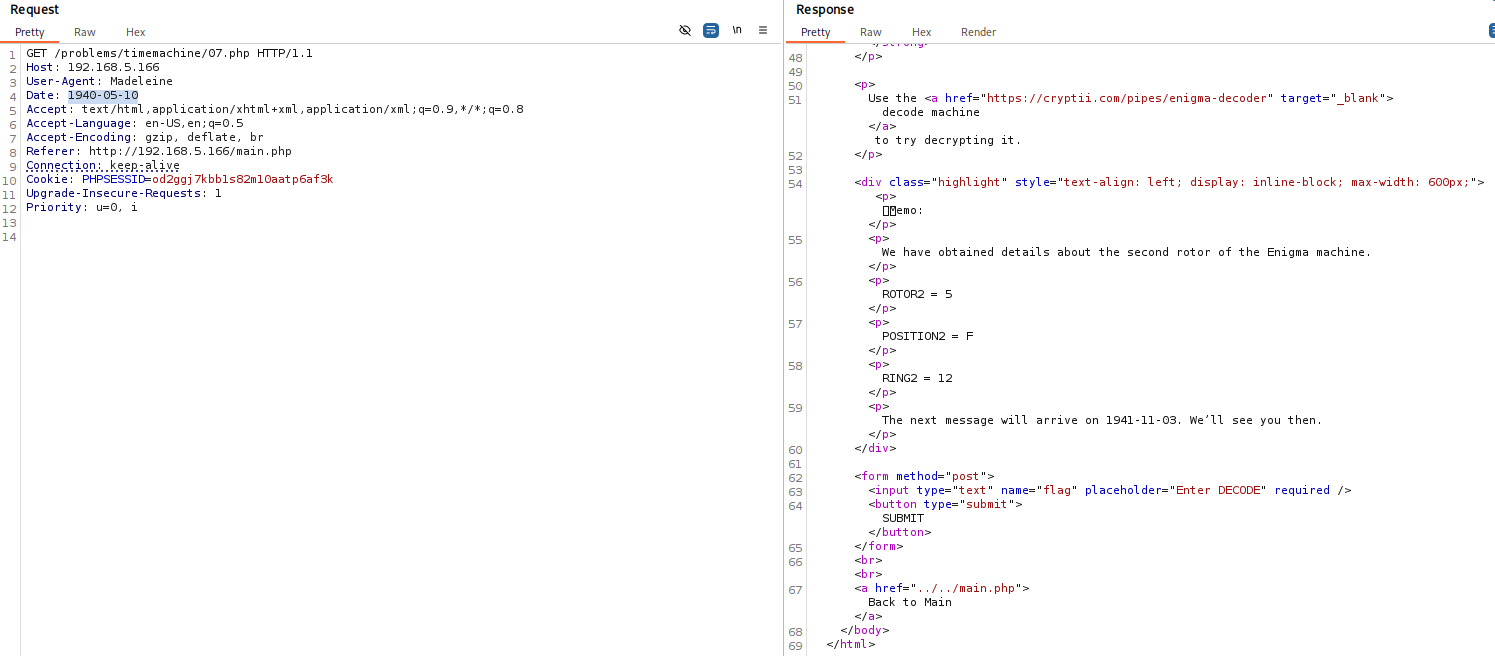
Date 값을 1935-09-21로 수정한다. 힌트에 따라 Rotor1을 8, Position1을 E, Ring1을 3으로 수정한다.



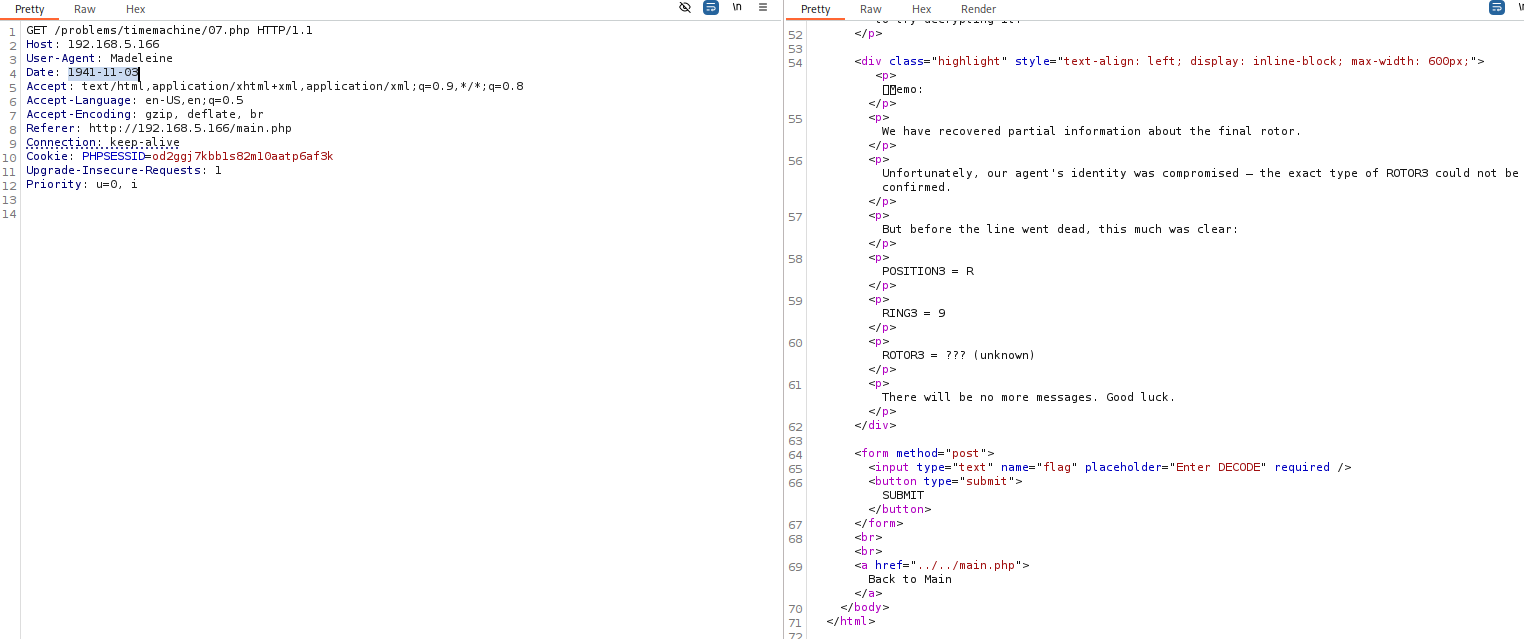
Date값을 1938-03-12로 변경한다. Plugboard 값을 cw nu bd gr eh is ky로 변경한다.



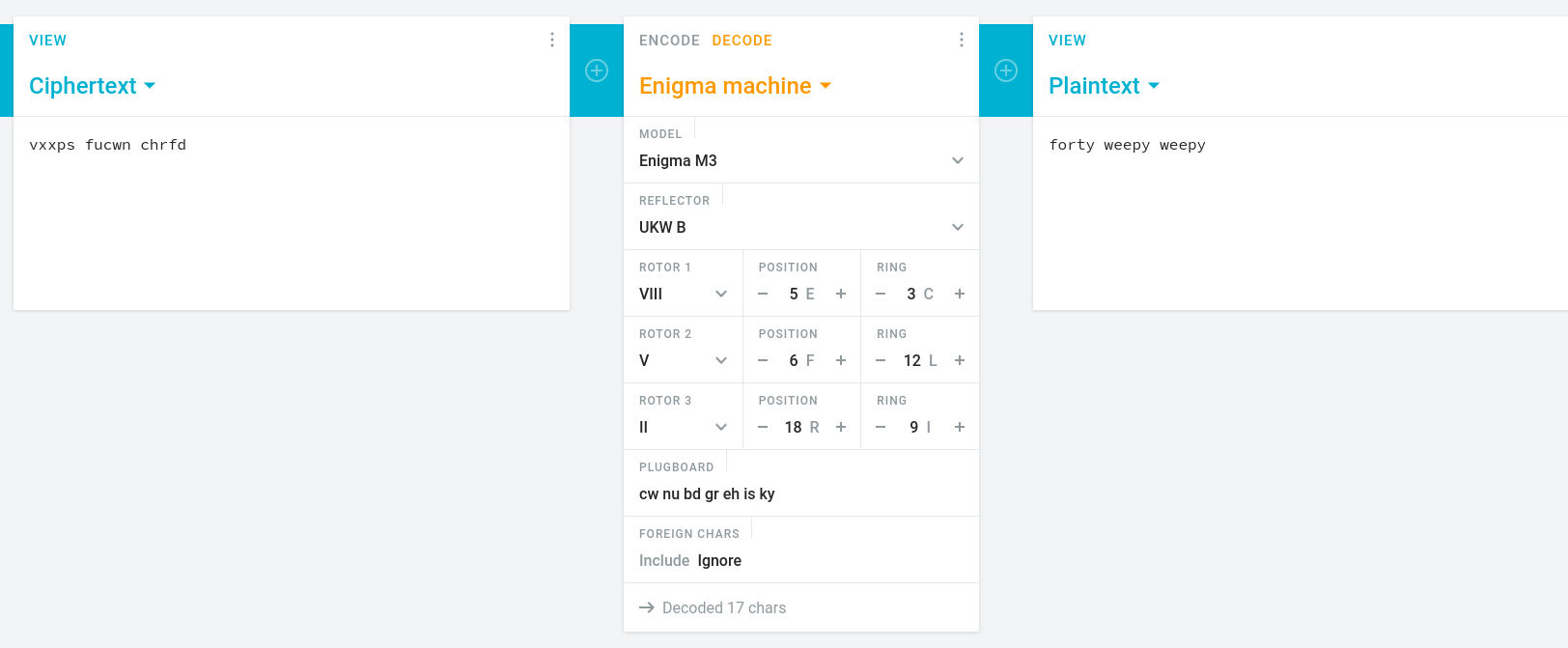
다음으로 Date값을 1940-05-10로 변경한다. Rotor2를 5, Position2를 F, Ring2를 12로 변경한다.



Date 값을 1941-11-03으로 변경한다. Position3 값은 R, Ring3은 9로 변경한다. 내용을 보니 마지막 힌트이다. Roter3값은 직접 대입해서 구한다.



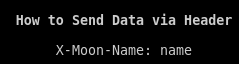
하나씩 대입하다보면 forty weepy weepy라는 단어들이 나온다.



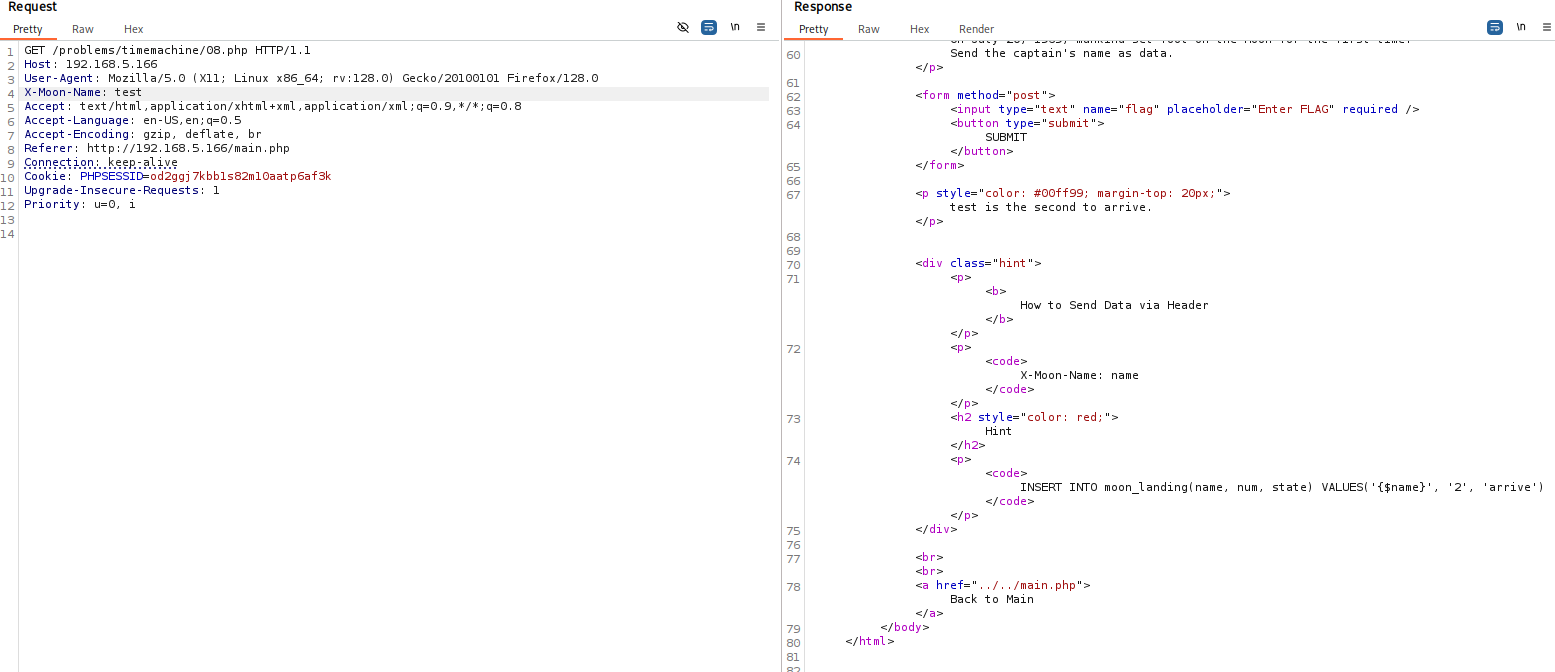
이것을 입력하면 정답.

1. First Moon Landing

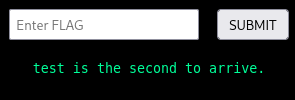
Data를 보내기 위해서는 http header를 이용하여 X-Moon-Name에 name값을 입력하면 된다고 한다.



Burp suite를 통해 header에 X-Moon-Name: test를 입력하면 test is the second to arrive. 라는 문장이 나온다.



화면에는 다음과 같이 나온다.



Captain의 이름을 전달해야 하므로 name 값으로 Armstrong으로 해보자.

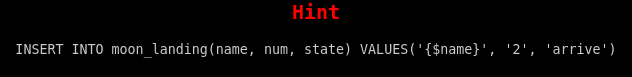
X-Moon-Name: Armstrong



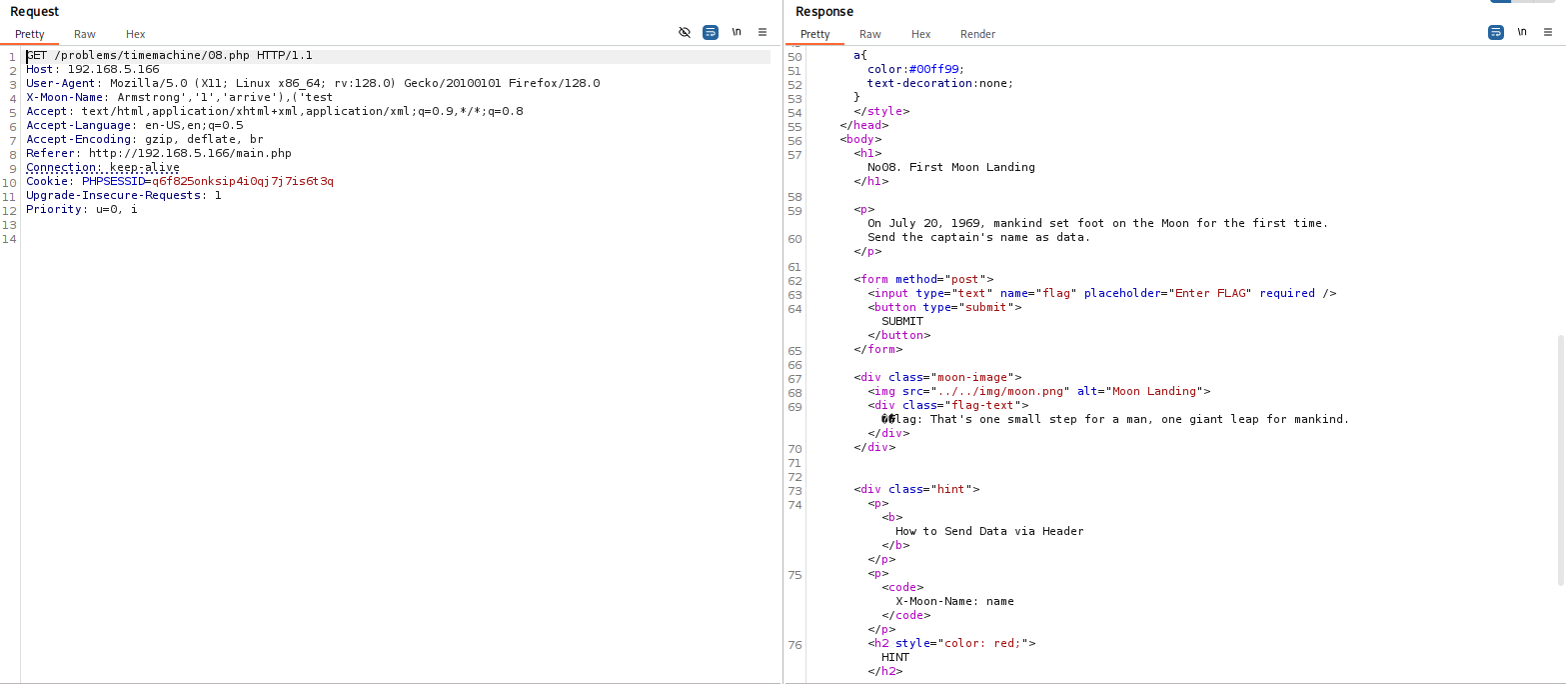
Armstrong을 입력하면 다음과 같은 문장이 나온다.



힌트를 보면 insert 구문을 통해 입력된 값에 따라 출력됨을 알 수 있다. Num에 해당하는 값을 1로 수정해야 한다.



X-Moon-Name: Armstrong','1','arrive'),('test 를 입력하면 Flag: ~ 가 나온다.



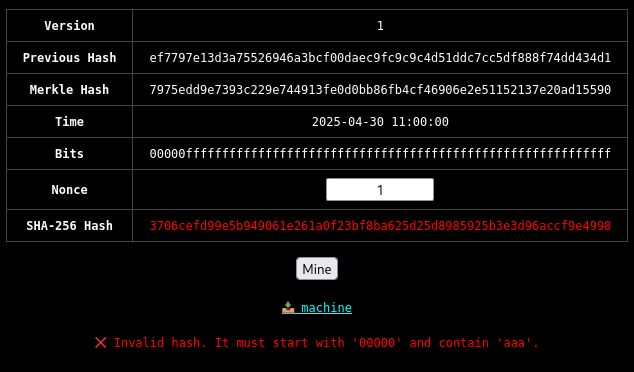
화면에는 다음과 같이 나온다.



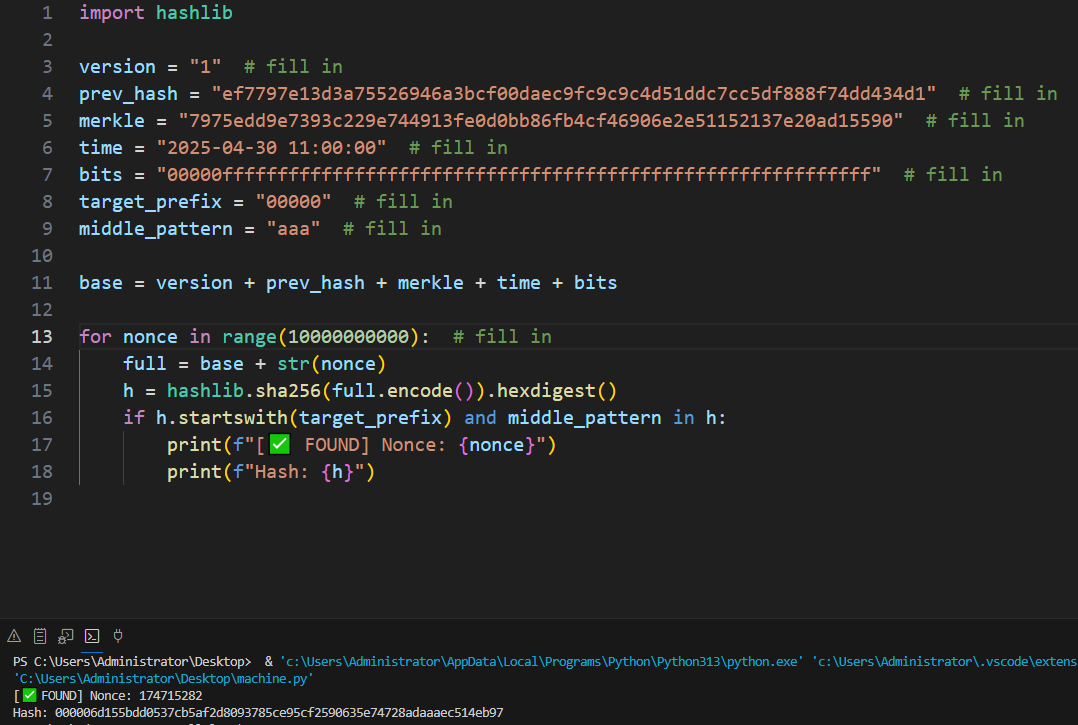
이제 Flag 입력칸에 That's one small step for a man, one giant leap for mankind. 를 입력하면 클리어.

1. Cryptocurrency Mining

Nonce 값에 1을 입력했더니 00000으로 시작해야 하고, aaa값이 있어야 한다고 나온다.



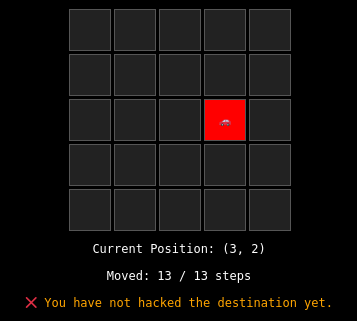
Machine 다운로드 링크를 통해 파이썬 파일을 받고 빈칸에 맞는 값을 입력한다.



나온 값을 입력하고 mine 버튼을 누르면 클리어.

1. Autonomous Driving

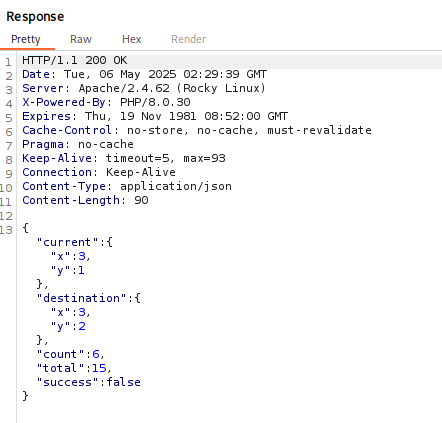
Move to destination 버튼을 누르면 자동차 이미지가 이동하는데 아래와 같은 실패 메시지가 나온다.



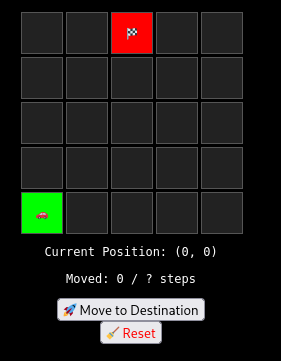
힌트를 보면 좌표를 해킹해야 한다.



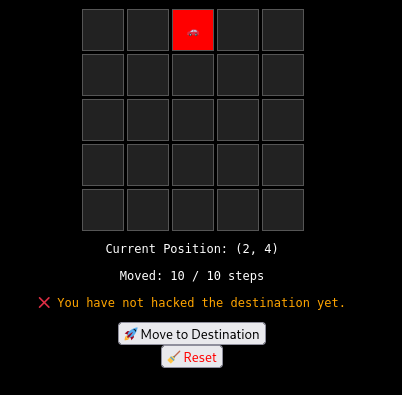
Burp suite를 통해 확인하면 destination 값을 확인할 수 있다.



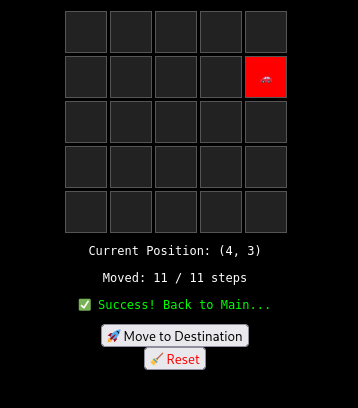
Reset을 한 번 누른 뒤 새로고침을 하여 Burp suite로 intercept할 때 reset=1이 있는데 이를 지우고 x=2&y=4 와 같은 임의값을 넣어본다. 그러면 목적지의 위치가 바뀐다.



(2,4)는 정답이 아님을 알 수 있다.



정답인 목적지 좌표를 찾을 때까지 좌표를 움직이며 확인한다.



(4,3)일 때 클리어.