**Best of Best 11**

**CVE-2022-21882 과제**

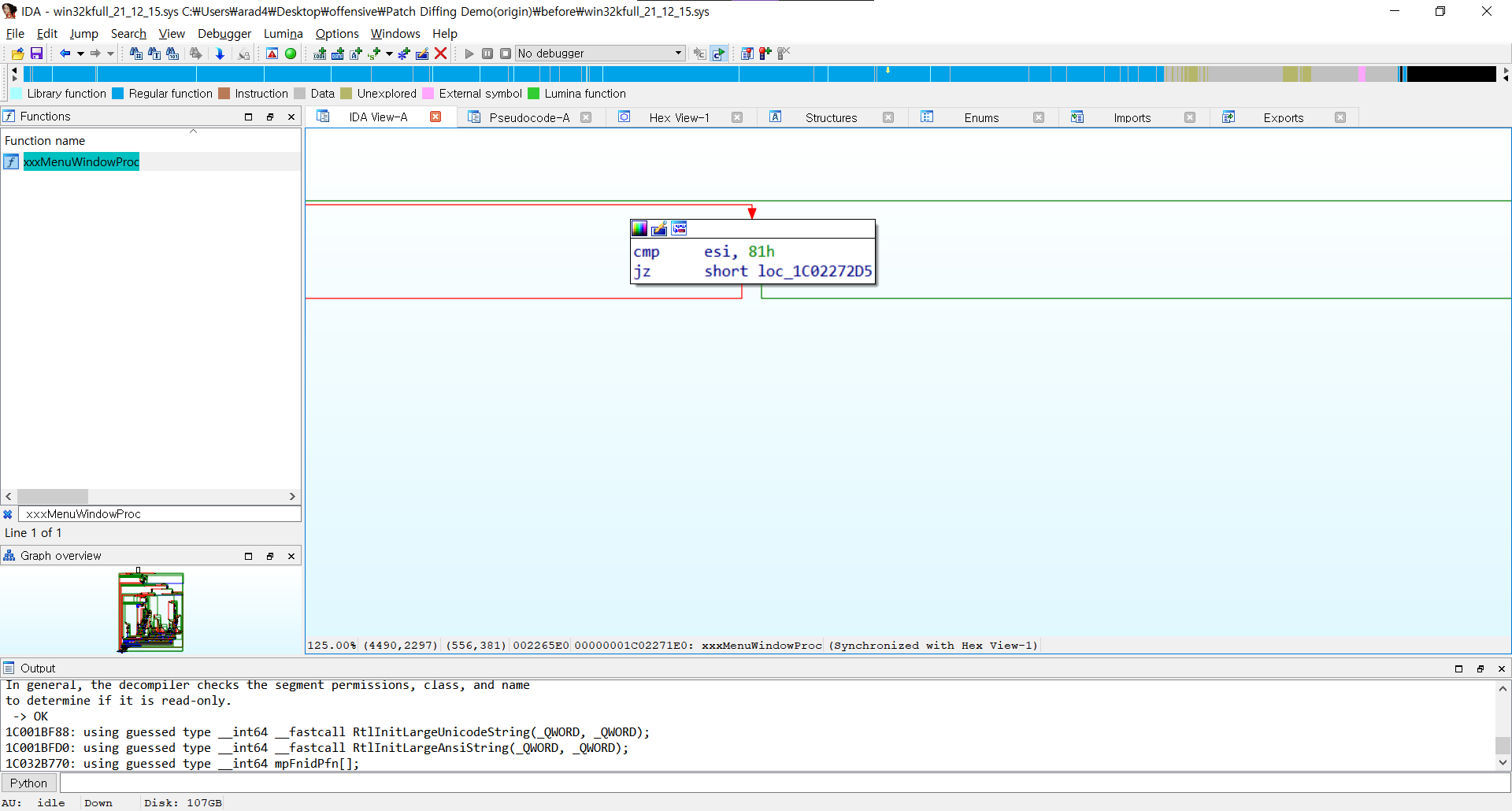
**남성엽 멘토님 과제 #2 번**

**Best of Best 11기**

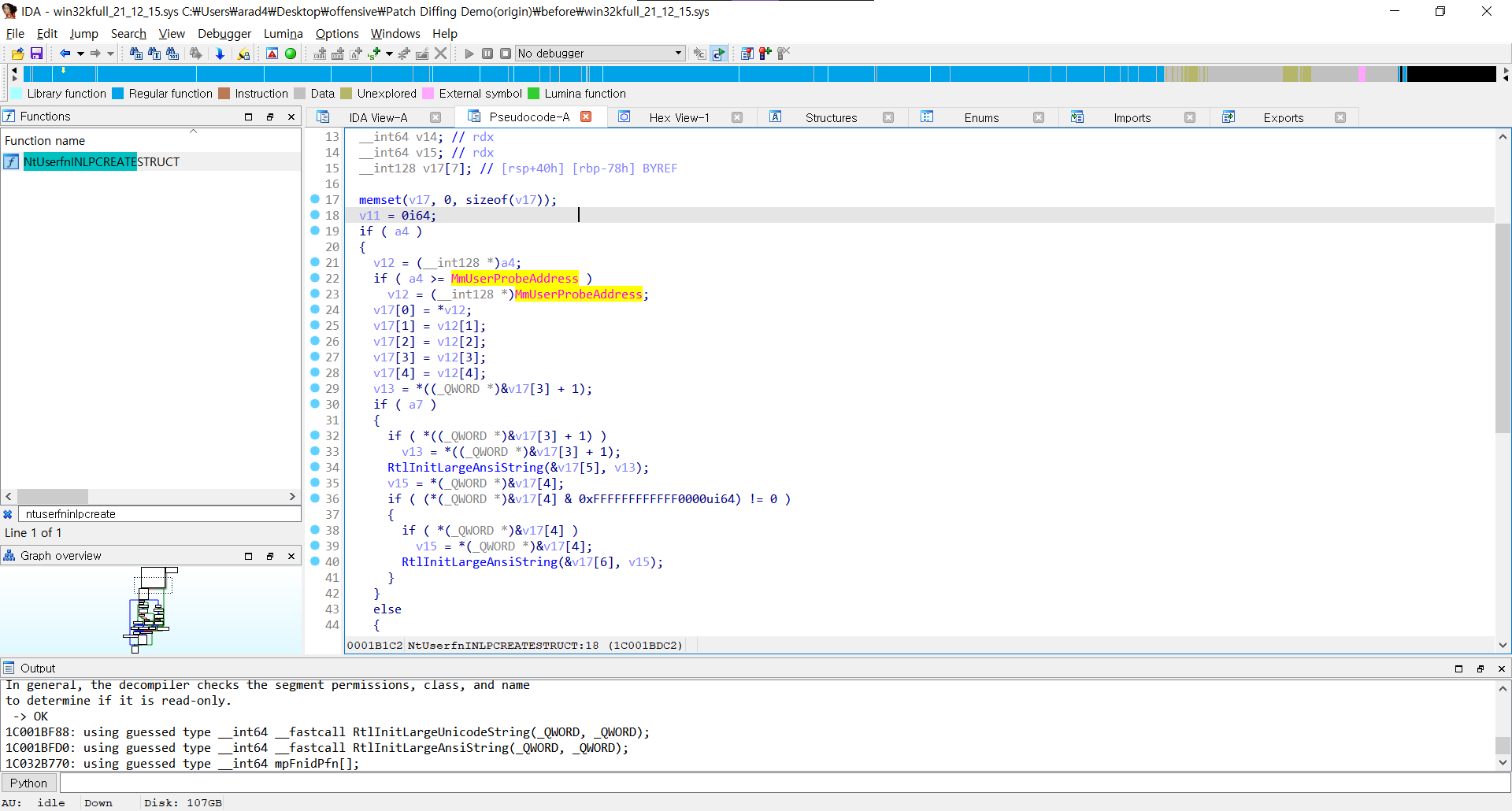
**보안제품 개발 정경재**

**제출날짜:2022-08-20**

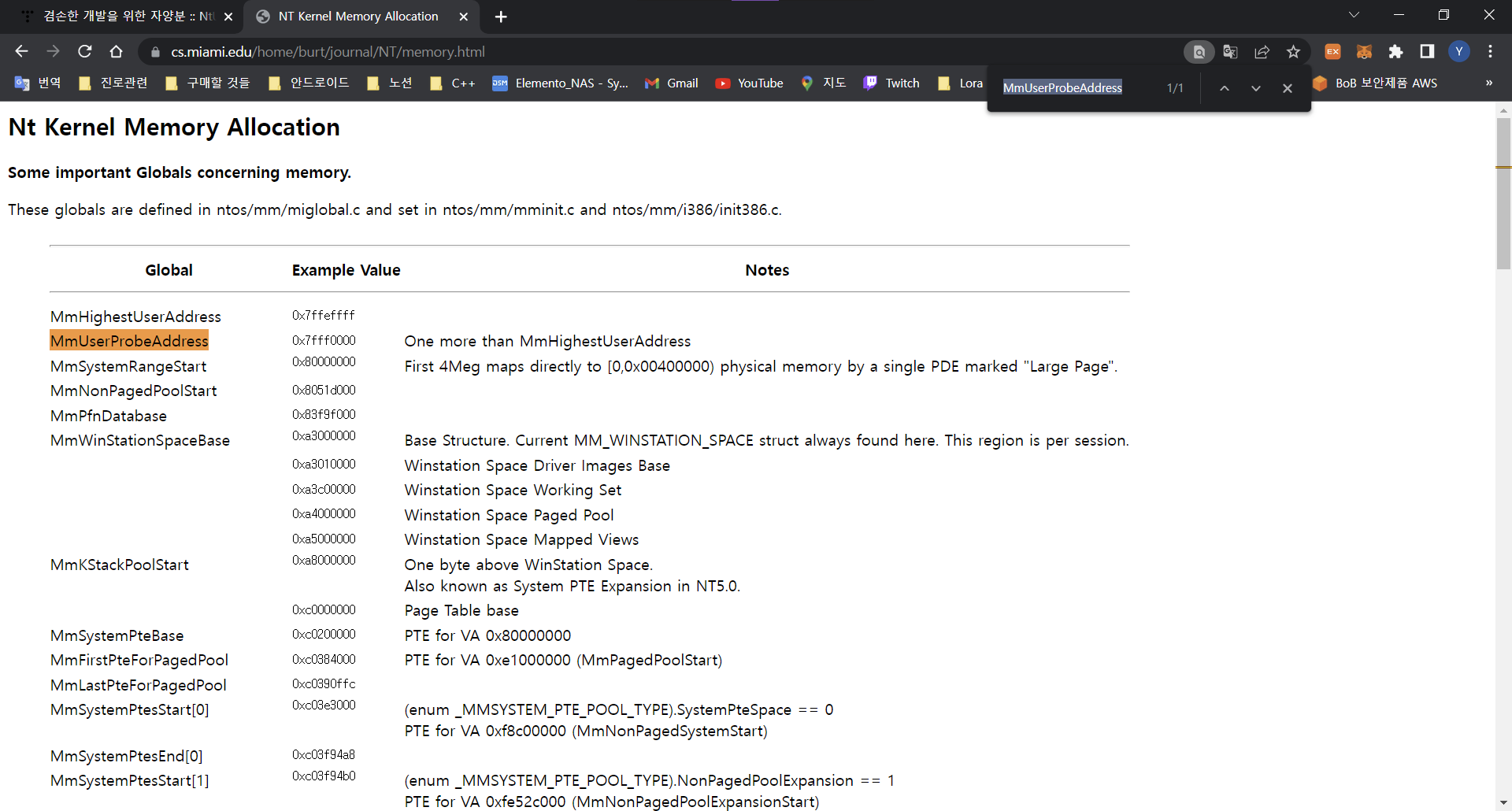
첫번째 ToDo는 멘토님이 주신 사진과 함께 IDA를 리버싱하면서 찾았습니다.

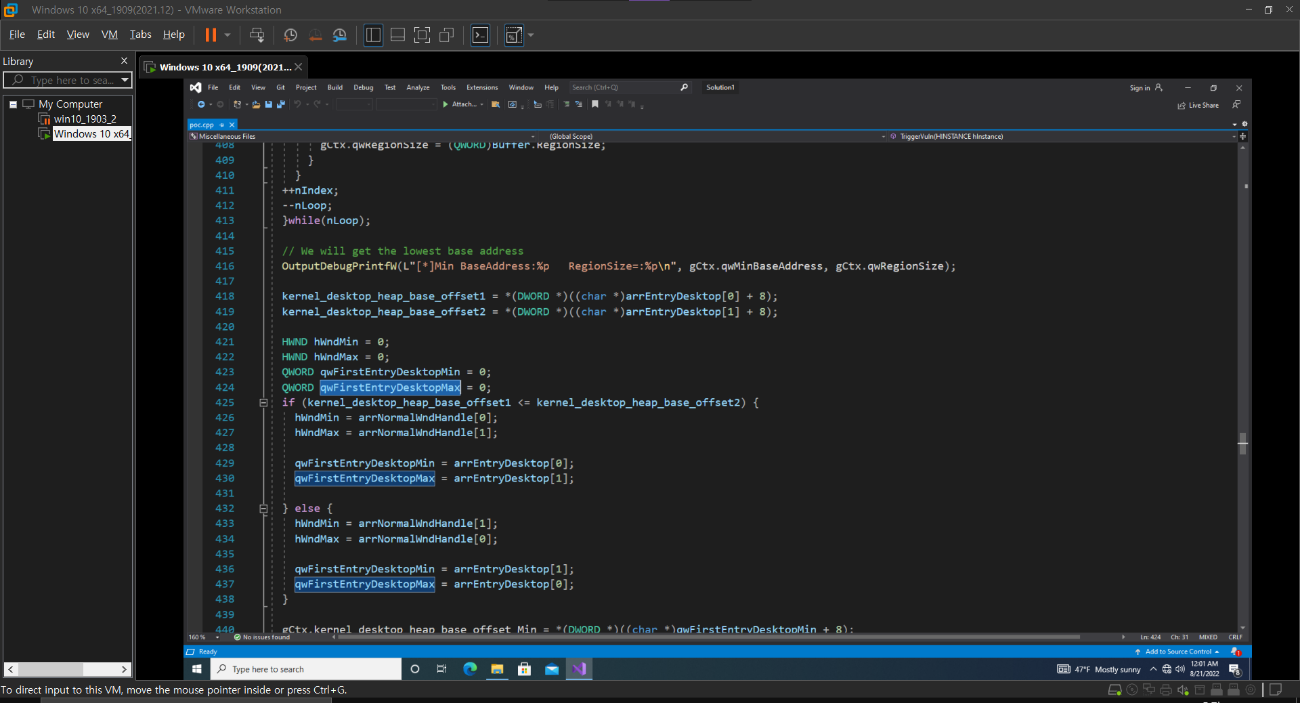


해당 사진에서 보다 싶이 값을 81(hex)와 비교해서 맞다면 우리가 원하는 분기로 아니면 다른 분기로 뛰고 있다는 것을 알아 첫번째 Todo의 값을 0x81로 작성했습니다.



2번째 Todo 역시 a4번이 아래와 같은 조건을 비교하는 것을 보고 인터넷에 검색을 통해 무엇을 하는 함수 있지 확인했습니다.



해당 정보를 통해 MmHighestUserAddress 보다 크면 된다는 정보를 얻고 소스코드에서 

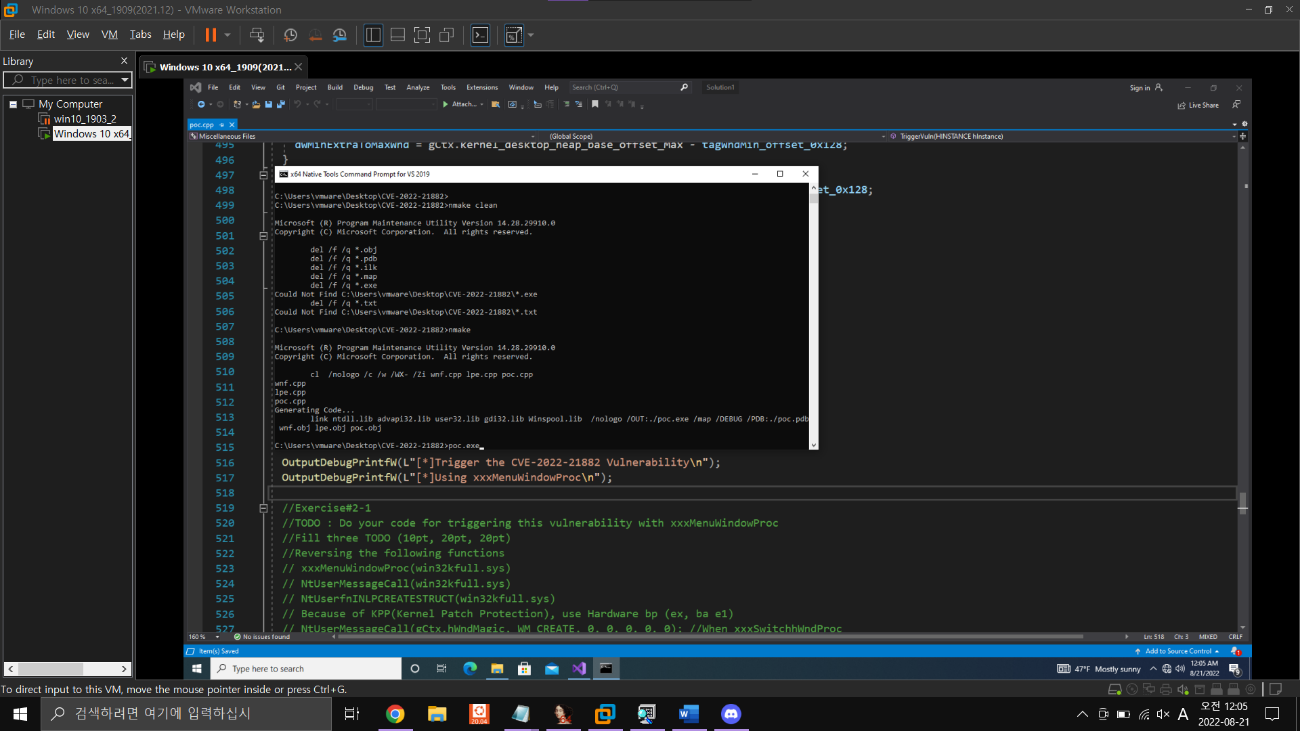
찾다 보니 max값을 가지는 변수를 발견해 해당 변수를 사용했습니다.

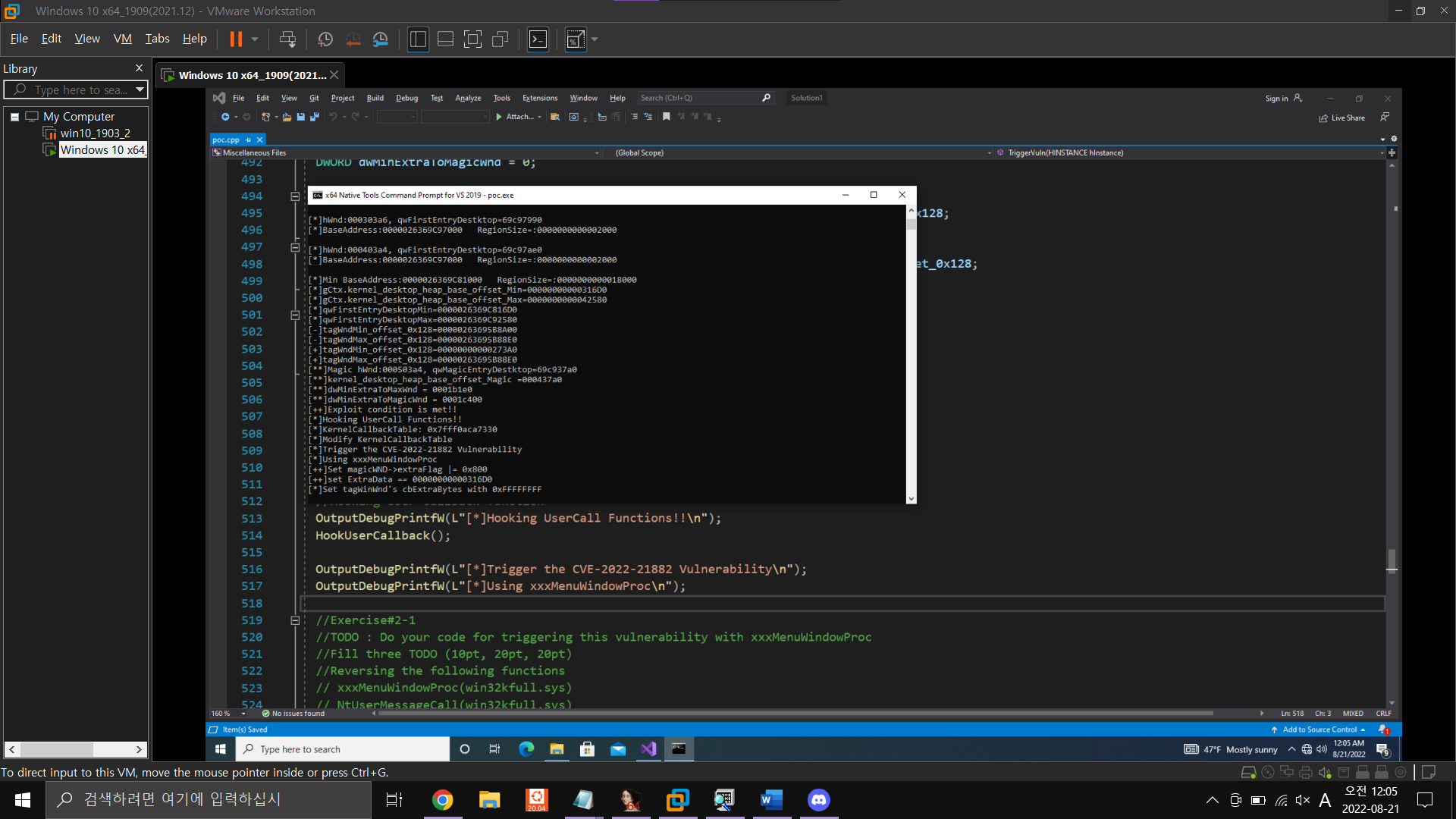
마지막 Todo도 역시 멘토님이 주신 사진과 인터넷 검색을 통해 정답을 얻었습니다.

멘토님이 주신 사진을 통해 값이 -4라는 정보는 얻었지만 이에 대한 값을 확신할 수 없어 인터넷에 검색을 통해 같은 값인 0X29C를 찾아 맞다는 것을 확인하고 해당 값을 사용했습니다.



해당 값을 사용해 성공적으로 POC를 했습니다.

코드를 만드는 과정



실제 코드를 동작시킨 사진

텍스트, 스크린샷, 모니터, 전자기기이(가) 표시된 사진

자동 생성된 설명