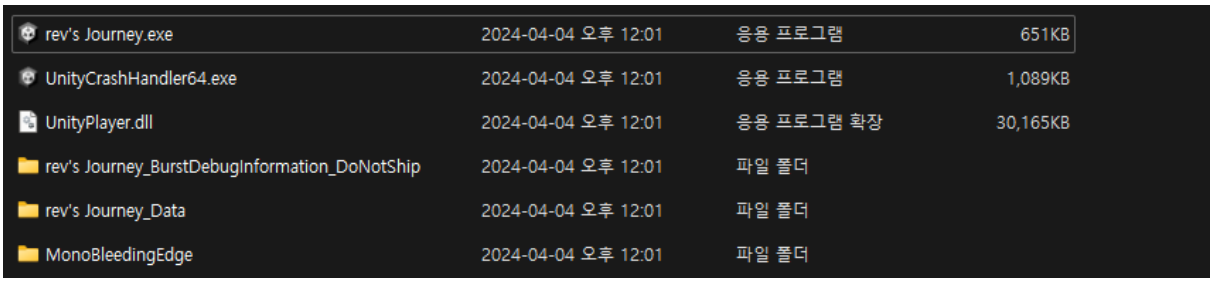
rev’s journey

생성자	R Rena231
생성 일시	@2024년 5월 20일 오후 3:12
태그	

1. 문제

처음 문제를 다운로드 받은 후 파일 안의 내용을 살펴보면 UnityPlayer.dll과 실행파일의 아이콘을 보고 Unity Engine으로 구성된 것을 확인할 수 있습니다.



게임을 실행시 5초~6초 단위로 Strength, Agility, Intelligence 셋중하나가 랜덤으로 1씩 증가하는걸 확인할 수 있습니다.

오른쪽에 아이콘에 커서를 올려보면 각각 10000이상의 능력치가 필요하며 전부합산해서 50000이상의 능력치가 있어야 마지막 아이콘을 클릭할 수 있다고 합니다.

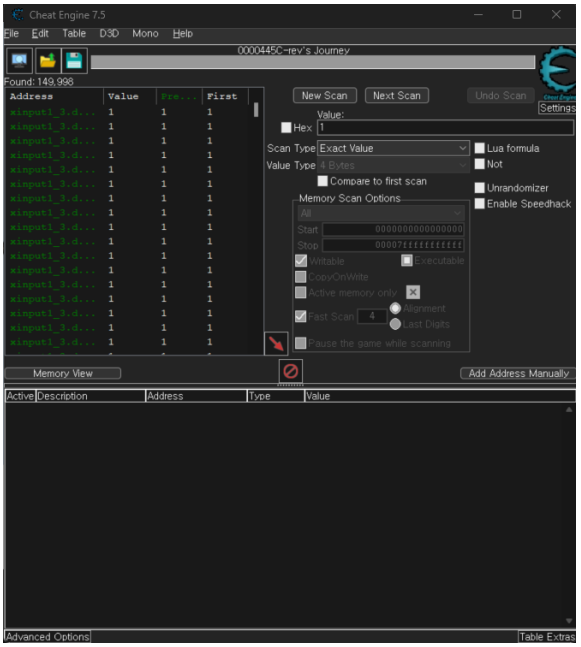
이는 시간적으로 대략 250000초 정도가 걸리며 일반적인 방법으로 풀기에는 무리가 있다는걸 확인할 수 있습니다.

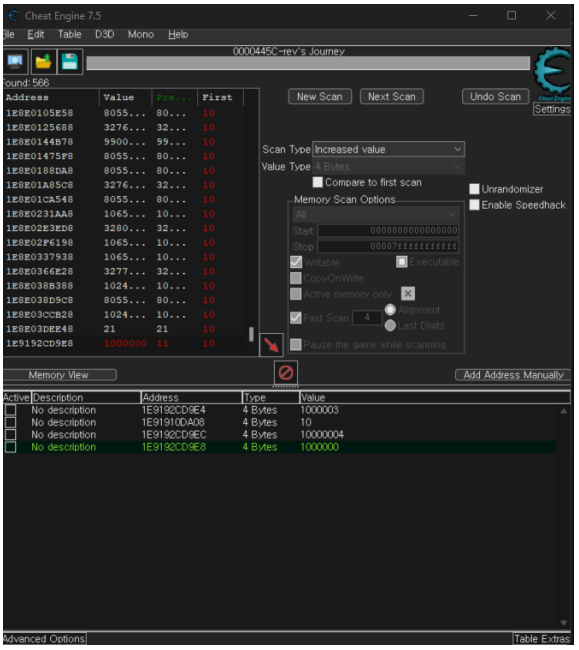
2. 풀이

Unity Engine은 따로 변수나 상수의 저장을 교차검증하는 트리거를 가지고 있지 않습니다. 개발자가 만들지 않는다면 말이죠.

이를 통해서 만약 교차검증 트리거가 존재하지 않는다는 가정을 해보면 간단한 메모리 변조 툴인 Cheat Engine을 통해 각 변수의 값을 변조할 수 있습니다.

특히 각각의 변수를 잡을때에는 게임 엔진의 특성상 기본적으로 실행되는 트리거들이 존재해 0에서 1로 변하는 메모리의 벨류값을 육안으로 확인하기란 매우 어렵습니다. 그래서 대략적으로 능력치가 10~ 이상정도되는 구간에서 Exact Value를 한다음 1이 올랐을때 멈춘 후 increase value를 통해 값을 찾아내는게 효율적입니다.





각값의 메모리 주소를 변조하게되면 트리거가 변수 변경을 위해 참조할 경우 변조된 메모리의 벨류값을 불러오게 됩니다.

이미지 파일로 flag 값이 출력되며 base64 인코딩이 되어있는것을 확인할 수 있습니다.


rev's Journey
Congratulations, here's Flag! Decode to base64.U09USXt0aDFzXzFzX1VuMXR5X0VuZzFuZX0=
Agility 1000001
Intelligence 10000005