Aufgabe 04

Simon Kramer

June 27, 2023

1 Aufgabe

Es soll ein Trainer erstellt werden für das Spiel AssaultCube. Dieser Trainer soll ermöglichen durch das drücken von den NumPad Tasten gewisse Funktionen zu aktivieren. So soll, wenn Numpad 1 gedrückt wird auf das bisherige Leben 100 aufaddiert werden. Bei Numpad 2 soll auf die bisherige Ammo 20 aufaddiert werden. Optionale aufgaben sind zudem das Implementieren von NoRecoil, beidem die Aufwärtsbewegung der Kamera gepatched werden soll, dass diese nicht beim schießen ausgeführt wird.

2 MaxHealth/Ammonition

Durch die Vorlesung war der Baselevel pointer vom Spieler bereits gegeben, von dort aus muss man nur noch das Offset bestimmen zur den gewünschten Spieler Werten. Normal würde man sowas über einen Pointer Scan machen. Es war jedoch möglich in CheateEngine die Base Adresse anzugeben und das Offset so lange weiter zu klicken, bis ein Wert erschien, der den gleichen Wert hatte, wie Health oder Ammonition. So konnten die Offsets schnell bestimmt werden und nieder geschrieben werden.

Nach dem man den Wert ermittelt hat, konnte man mit ReadMemory, den Orginalen Pointer auslesen und den Wert für den nächsten ReadMemory Befehl nutzten um auf den Health Value zu kommen. Danach wird der Health Value ausgelesen. Der ausgelesene Wert wird anschließend +100 gerechnet und mit WriteMemory in die gewünschte Adresse geschrieben. Das vorgehen ist bei Ammo gleich.

3 NoRecoil

Für diese Implementation, war es zuerst nötig, herauszufinden, in welchem Speicher die Nick Rotation steht. Dafür wieder über CheatEngine, Memory-Scans machen und Values verändern, bis man den passenden Wert hat. CheatEngine hat das Feature, dass es einem die Code-Regionen ausgeben kann, welche auf die Speicher Adresse schreiben. Dort hat sich herausgestellt, dass wenn man

90 Grad nach oben schaut, eine separate Funktion beim schießen überprüft, ob man diesen Wert überschreitet. Diesen Code habe ich mir genauer angeschaut und über trial and error die Funktionen gefunden, die initial den Recoil-Wert schreiben. Im Trainer konnte ich einfach die CodeAdresse angeben und mit den Werten 0x90 überschreiben (NoOperation).