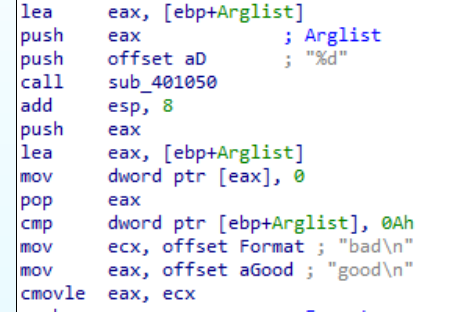
פתרון CHEATER רז אברג'ל



לאחר שנגיע למיין נראה שאנחנו תמיד נקבל bad עבור כל קלט אפשרי

הסיבה היא כיוון שהקלט שנכנס למשתנה המקומי ARGLIST תמיד יאופס

ומכאן שהוא לעולם יהיה קטן בהשוואה בינו לבין הערך 10

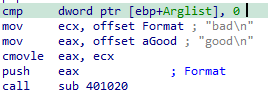
ולכן הפקודה CMOVLE תבצע את הזזה (פקודה זו מבצעת הזזה במקרה שתוצאת ההשוואה הקודמת בקוד היא קטנה או שווה) של המחרוזת BAD לתוך EAX

כדי למנוע את המצב הזה נרצה לבצע שני פצ'פוצ'ים

הראשון על מנת לדלג מעל האיפוס של הarglist

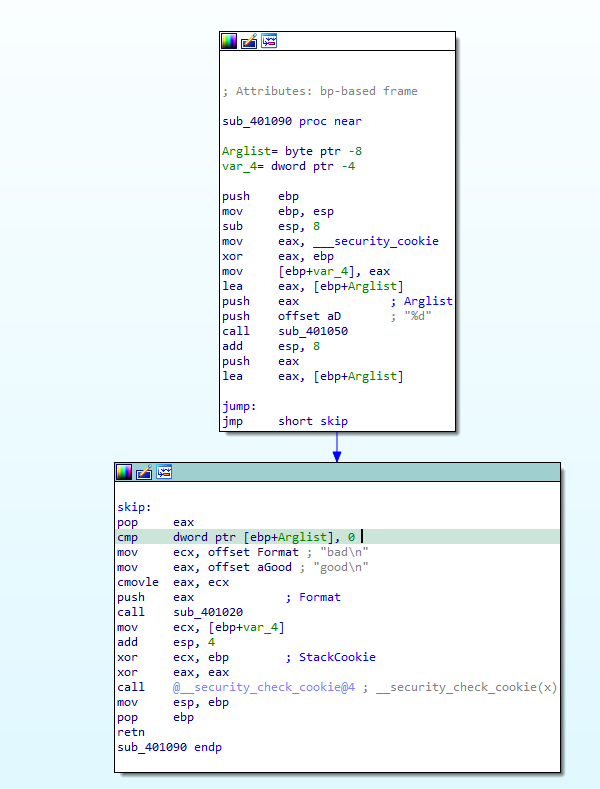
והשני הוא לשנות את הערך שיש בהשוואה מ10 ל0 ככה שכל הקלטים החיובים יתנו לי את הפלט GOOD

השינוי של השוואה כך שנשווה את ARGLIST עם 0 במקום עם 10



דילוג מעל האיפוס של המשתנה המקומי שמקבל את הקלט

בעזרת יצירת תווית וקפיצה אליה



וככה רימנו את הרמאי כך שעבור קלטים חיובים נקבל GOOD

