המטרה שלנו: לשנות את המשתנה modified ולתת לו ערך של 0x61626364 (abcd).  
כיוון שמשתמשים בפונקציה gets שכידוע היא פונקציה מסוכנת והיא לא בודקת אם הBuffer שאליו קולטים את הסטרינג הוא בגודל המספיק כדי שלא יהיה overflow.

לכן, נוכל להכניס כקלט תו ארוך כדי שהמתנה modified ישתנה.

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

|  |
| --- |
| buffer |
| .... |
| .... |
| modified |
| Old ebp |
| Ret address |
| ????? |

מה שעשיתי היה לשלוח 64 פעמים a ולאחר מכן את הסטרינג dcba (בהפוך על מנת שנתאים לlittle endian)

EXPLOIT:

./stack1 $(python -c "print 'a'\*64 + 'abcd'")