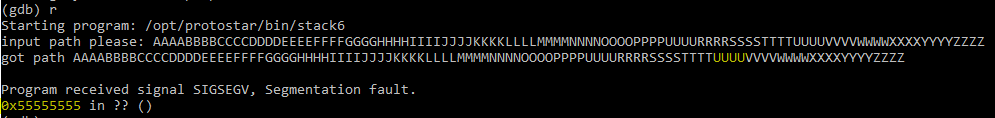
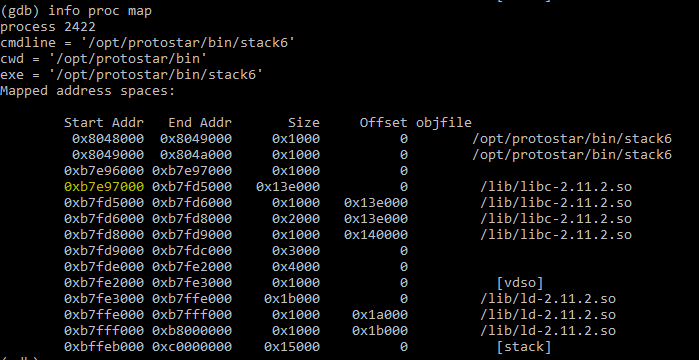
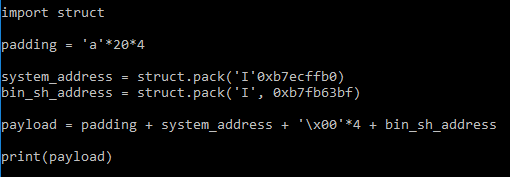
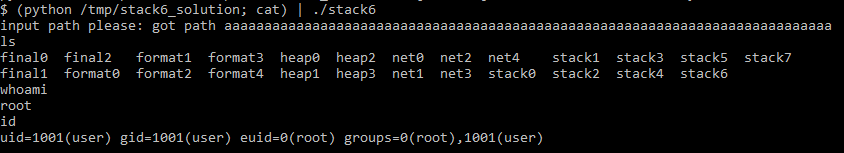
נשים לב שמשתמשים בפונקציה gets, כלומר אין בדיקה על כמה תווים קולטים למשתנה buffer לכן נוכל לכתוב כמה תווים שנרצה. אנו נדרוס את כתובת החזרה ונקפוץ לכתובת של system עם הפרמטר /bin/sh כך שנשיג shell. זה יעבוד כיוון שאין aslr ולכן לא נצטרך להדליף כתובת כלשהי ומשם לחשב את הכתובת של system והסטרינג /bin/sh .

נשתמש בgdb:

* נריץ את התוכנית ובקלט נכניס pattern על מנת לראות מתי אנחנו דורסים את ret 

נשים לב כי אנו מנסים לחזור 0x55555555 (אות U).

* נחפש את הכתובת של system:  
  
* לאחר מכן נחליף את הreturn address לכתובת של system.
* נחפש את הכתובת של המחרוזת /bin/sh:  
    
  המסומן בצהוב זה הoffset של המחרוזת מתחילת libc. כלומר נצטרך למצוא את הכתובת שבה מתחיל libc ולהוסיף את הoffset ונקבל את הכתובת למחרוזת.  
  נמצא את הכתובת בסיס של libc:  
    
    
  בעזרת פייתון – נוסיף את הoffset לכתובת:  
  
* נעבור לפייתון על מנת לכתוב את הקוד שלנו:  
  
* נריץ:  
    
  ויש לנו shell.