نرگس سیداخلاقی H2

2 . بررسی کنید که کامپایلرهای جدید برای جلوگیری از buffer overflowاز چه مکانیزمی استفاده میکنند؟

کامپایلر یک مقدار تصادفی را در **Stack** بین متغیرهای محلی و آدرس بازگشت یک تابع قرار می‌دهد. به این مقدار **Stack Cookie**می‌گویند. اکنون اگر مهاجم یک حمله از نوع سرریز بافر را به منظور بازنویسی آدرس بازگشت تابع انجام دهد در واقع **Stack Cookie**را هم نیز بازنویسی کرده است در نتیجه مقدار آن تغییر می‌کند. حال هنگامی که تابع به پایان کار خود می‌رسد **Cookie**قرار داده شده قبل از فراخوانی آدرس بازگشت کنترل می‌شود و اگر مقدار آن با مقدار گذاشته شده اولیه برابر نباشد برنامه به طور غیر عادی خاتمه می‌یابد.

به منظور پیشگیری از اینکه مهاجم بتواند متغیرها و آرگیومنت‌های مورد استفاده یک تابع را بازنویسی کند کامپایلر چیدمان داخل **Stack**را تغییر می‌دهد به اینصورت که بافر رشته‌ها را در بالاترین آدرس نسبت به هر متغیر دیگری قرار می‌دهد. این عمل از عدم بازنویسی هر متغیر محلی در هنگام **String Buffer Overflow** اطمینان حاصل می‌کند.آرگیومنت‌های تابع که شامل اشاره‌گرها و بافرهای رشته‌ای هستند توسط اختصاص یک فضای اضافی در **Stack** به منظور کپی کردن مقادیرشان در آن، که در پایین متغیرهای محلی قرار دارد، محافظت می‌شوند.مقادیر اصلی آرگیومنت‌ها که بعد از آدرس بازگشت قرار گرفته‌اند در بقیه کد استفاده نمی‌شوند.