CLASS 8

SQL Injection Lab 2

吴瑞欣-E41614059

1、网上搜索并且阅读 Four different tricks to bypass StackShield and StackGuard protection 这篇文章，描述这些现有保护机制的弱点。

StackGuard is a compiler that emits programs hardened against ”stack smashing” attacks.

StackGuard 是一个编译器，可以发出针对“堆栈”强化的程序粉碎“攻击。

limitations: Only protecting data located higher in memory than the first safe-guarded address. And, what we think is worse, checking for attacks only after the function finishes, and right before returning from it. In addition to this,StackGuard and StackShield have an implementation or technical flaw: They protect the stack starting at the return address, leaving the saved frame pointer unprotected.

限制：仅保护位于内存中比第一个安全位置更高的数据守卫地址。并且，我们认为更糟糕的是，仅在检查攻击之后函数完成，并在返回之前完成。除此之外，StackGuard 和 StackShield 有一个实现或技术缺陷：他们保护堆栈从返回地址开始，留下保存的帧指针保护。

2、阅读下面这篇文章：

Bypassing non-executable-stack during exploitation using return-to-libc.

http://www.infosecwriters.com/text_resources/pdf/return-to-libc.pdf

返回 libc 是一种在系统上利用缓冲区溢出的方法有一个不可执行的堆栈，它非常类似于标准的缓冲区溢出返回地址被更改为指向我们可以的新位置控制。 但是，由于堆栈上不允许执行任何代码，我们不能只是 shellcode 中的标记。这就是我们使用返回 libc 技巧并利用函数的原因由图书馆提供。 我们仍然用 a 中的一个覆盖返回地址 libc 中的函数，传递正确的参数并为我们执行。由于这些函数不驻留在堆栈上，我们可以绕过堆栈保护和执行代码。

3、阅读这个链接的第 3 章，解释怎样构造 return2libc 的

http://www.phrack.org/issues.html?issue=58&id=4

Return-to-libc 攻击（缩写：ret2libc），即“返回至 C 标准库攻击”，是一种计算机安全攻击。这种攻击方式一般应用于缓冲区溢出中，其堆栈中的返回地址被替换为另一条指令的地址，并且堆栈的一部分被覆盖以提供其参数。这允许攻击者调用现有函数而无需注入恶意代码到程序中。

4、阅读这个链接

https://bbs.pediy.com/thread-224643.html

一般的思路是先 leak 出 canary 的 cookie，然后在 payload 里，

把原来的 canary 位置的 cookie 用我们 leak 出的正确的 cookie 写入，之后就是正常的 rop。

这题有 fork，因而可以直接爆破。