三

1.

(1)p[4]

(2)

|  |
| --- |
| buff (p[0]) |
| value (p[1]) |
| a (p[2]) |
| EBP (p[3]) |
| why\_here (p[4],原返回地址) |

2.

(1) “aaaabbbbcc”写入buffer，10写入内存地址0x61616161。

(2)首先将“aaaabbbbcc”写入buffer，然后从堆栈中取下一个参数，由于调用sprintf 时没有传入下一个参数，因而buffer的前四个字节（aaaa对应的地址0x61616161）被当作参数，因此“aaaabbbbcc”的长度10被写入内存地址0x61616161。

3.

攻击步骤：如果虚表里存储的虚函数指针被篡改，程序调用虚函数的时候就会执行篡改后的指定地址的shellcode，发动虚函数攻击。

攻击策略：修改虚表地址，修改虚函数指针。

4.

(1)符号执行三个关键点是变量符号化、程序执行模拟和约束求解。

(2)动态符号执行结合了真实执行和传统符号执行技术的优点，在真实执行的过程中同时进行符号执行，可以在保证测试精度的前提下提升了执行效率。

静态符号执行：不需要运行程序、分析效率高、资源消耗低

动态符号执行：需要运行程序、准确率非常高，误报率很低

5.通过堆溢出覆写了一个空闲堆块的块首的前向指针flink和后向指针blink，我们可以精心构造一个地址和一个数据，当这个空闲堆块从链表里卸下的时候，就获得一次向内存构造的任意地址写入一个任意数据的机会。这种能够向内存任意位置写入任意数据的机会称为Dword Shoot。

6. GET一般用于查询资源信息， POST一般用于更新资源信息。GET请求的数据会附在URL之后；POST把提交的数据则放置在是HTTP包的包体中，POST的安全性要比GET的安全性高。

7.

(1)跨站脚本攻击XSS，XSS主要影响的是Web应用程序的用户，而SQL注入则主要影响Web应用程序自身。

(2)反射式跨站脚本，持久式跨站脚本，反射式跨站脚本主要用于将恶意脚本附加到URL地址的参数中。持久式跨站脚本由Web应用程序进行存储的，并且会将其作为内容显示给浏览用户。（类似：会在Web应用程序的网页中显示未经编码的攻击者脚本。）

四．

（1）

(1)可能出现use-after-free漏洞。

(2) v.free: {\*v} ==> v.useAfterFree

(3)控制流图，漏洞分析

（2）

(1)创建一个符号变量，这个符号变量以8位bitvector形式存在，名称为u

(2)进行符号执行得到想要的状态，即得到满足correct条件且不满足wrong条件的state

(3)获得到state之后，通过solver 求解器，求解u的值

(4)主流的约束求解器主要有两种理论模型：SAT求解器和SMT求解器。

SAT问题（可满足性问题），求解由布尔变量集合组成的布尔表达式，对命题逻辑公式问题适用，但是当前有很多实际应用的问题，并不能直接转换为SAT问题来进行求解。

SMT（可满足性模理论），求解范围从命题逻辑公式扩展为可以解决一阶逻辑所表达的公式。SMT包含很多的求解方法，通过组合这些方法，可以解决很多问题。