缓冲区溢出

缓冲区是内存那种的一个片段，之所以出现漏洞，是因为计算机是动态的，他可以执行任何东西，这就导致了xss和sql等漏洞的产生。而这往往都是因为没有做严格的限制而诞生的，而解决的方法就是加上过滤。

缓冲区溢出就是当程序限制不严格的时候，由于数据传入所导致的的程序运行错误，导致缓冲区溢出。而溢出的有可能会修改内存数据，也可能会造成进程劫持，执行恶意代码，获取服务器控制权等相关后果

Windows缓冲区溢出
FUZZER
SLMail 5.5.0 Mail Server
POP3 PASS命令存在缓冲区溢出漏洞
无需身份验证实现远程代码执行
DEP：阻止代码从数据页被执行
ASLR:随机内存地址加载执行程序和DLL，每次重启地址变化