



请解释下 **referer** 是什么，并任意描述一些与之相关的攻击场景或安全漏洞。

HTTP Referer 是 **header** 的一部分，当浏览器向 **web** 服务器发送请求的时候，一般会带上 **Referer**，告诉服务器我是从哪个页面链接过来的，服务器籍此可以获得一些信息用于处理。

如果是 **CSRF** 攻击传来的请求，**Referer** 字段会是包含恶意网址的地址，这时候服务器就能识别出恶意的访问。

分类列举 **sql** 注入常用判断方法？

参考答案

1. 整形参数判断

通常 **news.asp** 中 **SQL** 语句原貌大致如下：

select * from 表名 where 字段=xx，所以可以用以下步骤测试 **SQL** 注入是否存在。
最简单的判断方法

http://xxx/news.asp?id=xx'(附加一个单引号)，

1. 字符串型参数判断

通常 **news.asp** 中 **SQL** 语句原貌大致如下：

select * from 表名 where 字段='xx'，所以可以用以下步骤测试 **SQL** 注入是否存在。

http://xxx/news.asp?id=xx'(附加一个单引号)，此时 **news.asp** 中的 **SQL** 语句变成了 **select * from 表名 where 字段=xx'**，**news.asp** 运行异常；

http://xxx/news.asp?id=xx and '1'='1'，**news.asp** 运行正常，

而且与 **http://www.hackbase.com/news.asp?id=xx** 运行结果相同；

http://xxx/news.asp?id=xx and '1'='2'，**news.asp** 运行异常；

如果以上满足，则 **news.asp** 存在 **SQL** 注入漏洞，反之则不能注入

根据不同的维度，描述软件测试可以划分的种类。例如,根据软件的生命周期，我们可以将测试划分为：单元测试，集成测试，系统测试，验收测试.....请至少根据两种不同的依据，说出 2-3 软件测试方式。(不包含举例的内容)

参考答案

从测试设计方法分类，分为黑盒测试，白盒测试和灰盒测试。

从获得测试数据形式上分：穷尽法；等价类划分法；边界值分析法。

有如下 2 个文件:**test.cpp**,**test.hpp**，简述下 **g++** 编译器将其编译成 **binary** 的工程中都做了哪些事情？

参考答案

预处理，编译，汇编，连接。

获取更多资料礼包！

微信关注：白熊求职



如何用一枚硬币等概率地产生一个 1 到 3 之间的随机整数?如果这枚硬币是不公正的呢?

参考答案

如果是公正的硬币,则投掷两次,“正反”为 1,“反正”为 2,“正正”为 3,“反反”重来。如果是不公正的硬币,注意到出现“正反”和“反正”的概率一样,因此令“正反反正”、“反正正反”、“正反正反”分别为 1、2、3,其余情况重来。另一种更妙的办法是,投掷三次硬币,“正反反”为 1,“反正反”为 2,“反反正”为 3,其余情况重来。

简述对称密钥密码体系与公钥密码体系的区别

参考答案

1. 对称密钥密码体系

对称密钥密码体系也叫密钥密码体系,它是指消息发送方和消息接收方必须使用相同的密钥,该密钥必须保密。发送方用该密钥对待发消息进行加密,然后将消息传输至接收方,接收方再用相同的密钥对收到的消息进行解密。这一过程可用数学形式来表示。消息发送方使用的加密函数 encrypt 有两个参数:密钥 K 和待加密消息 M ,加密后的消息为 E , E 可以表示为 $E=\text{encrypt}(K, M)$ 消息接收方使用的解密函数 decrypt 把这一过程逆过来,就产生了原来的消息:

$M=\text{decrypt}(K, E)=\text{decrypt}(K, \text{encrypt}(K, M))$

2. 非对称密钥密码体系

非对称密钥密码体系又叫公钥密码体系,它使用两个密钥:一个公共密钥 PK 和一个私有密钥 SK 。这两个密钥在数学上是相关的,并且不能由公钥计算出对应的私钥,同样也不能由私钥计算出对应的公钥。这种用两把密钥加密和解密的方法表示成如下数学形式。假设 M 表示一条消息, $\text{pub}-a$ 表示用户 a 的公共密钥, $\text{prv}-a$ 表示用户 a 的私有密钥,那么:

$M=\text{decrypt}(\text{pub}-a, \text{encrypt}(\text{prv}-a, M))$

现在有 10 个人被一个魔鬼逮住了。魔鬼对于直接把人杀掉的方法不感兴趣了。于是,他就想了一个杀人的新花样。是这样的,一天晚上,魔鬼向着十个人宣布了游戏规则,即明天早上他要把 10 个人排成一排,然后从一堆既有无限多的白帽子混着无限多黑帽子的帽子堆为每个人随机抽取一顶帽子,给他们 10 个人都戴上帽子。因为 10 个人是排成一排的,所以排在第 10 个人的人可以看到前面 9 个人帽子的颜色,排在第 9 个人的人可以看到前面 8 个人的帽子的颜色,....以此类推。然后,魔鬼会从排在第 10 个人开始,问他,你头上的帽子的颜色是白色还是黑色,如果答对了,就放他走;如果答错了,就被杀掉。然后同样问排在第 9 位的人,然后问排在第 8 位的人,....以此类推。在这其中,10 个人所能做的只有当他被魔鬼问到的时候,答白色或者黑色。不能有超越此范围的任何行动,不然,魔鬼会把它们 10 个人全部杀死。



现在魔鬼给他们 10 个人一晚上的时间去商量一个对策，使得他们中能存活下来的人越多越好。请问，你会有什么样的对策，请计算出按照你的对策执行时最坏的情况下，他们中能有多少人能 100%够活下来？期望能活下来的人数又是多少？

参考答案

我们将白色帽用 0 表示，黑色帽用 1 表示，每个人都将他所见到的帽子颜色进行异或运算。第 10 人以他所见到的 9 顶帽子颜色异或处理后的结果，他有 50% 的机会活下来。第 9 人听到他的回答后，结合自己看到的 8 顶帽子颜色异或处理后的结果，可以知道自己帽子颜色，如实作答，有 100% 的机会存活下来。第 8 人听到前面两人的回答后，结合自己看到的 7 顶帽子颜色经过异或处理后的结果，也可以知道自己帽子颜色，如实作答，有 100% 的机会存活下来。……依此类推，前面 9 个人都可以活下来，第 10 个人存活的几率是 50%。

