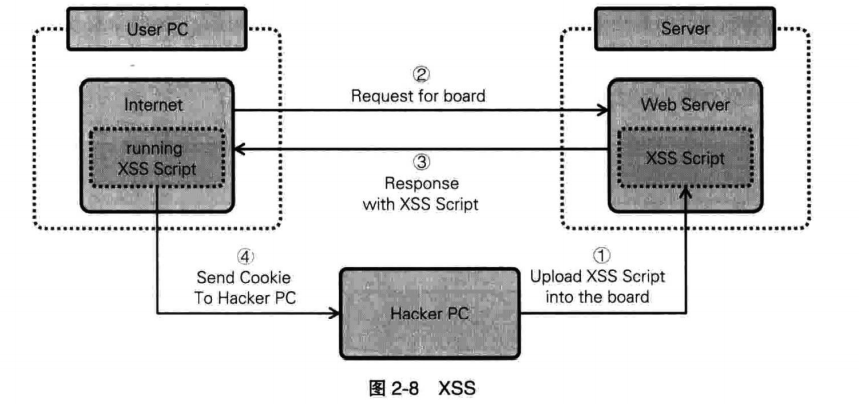
Web系统一般由网络浏览器、Web服务器、数据库三部分组成，各部分功能划分十分明确。

网络浏览器用于处理用户输入，加工来自Web服务器的数据并输出到屏幕。Web服务器用于分析HTTP请求，并执行相应功能。需要处理数据时，Web服务器会连接数据库执行数据处理。数据库用于安全管理数据，支持数据的录入与查询等功能。

黑客会恶意使用Web系统提供的功能。比如利用文件上传功能，将Web shell文件与恶意代码上传到Web服务器，然后运行Web shell文件，获取上传文件所在位置，进而控制Web服务器。黑客利用用户输入功能可以实施SQL注入攻击，通过输入非正常SQL查询语句获取Web服务器的错误信息，并对这些信息加以分析，进而实施攻击。利用文件下载功能，可以将恶意代码散布到网络上的多台PC。网络浏览器中运行的HTML与脚本代码可以被恶意用于开展XSS攻击与CSS攻击。

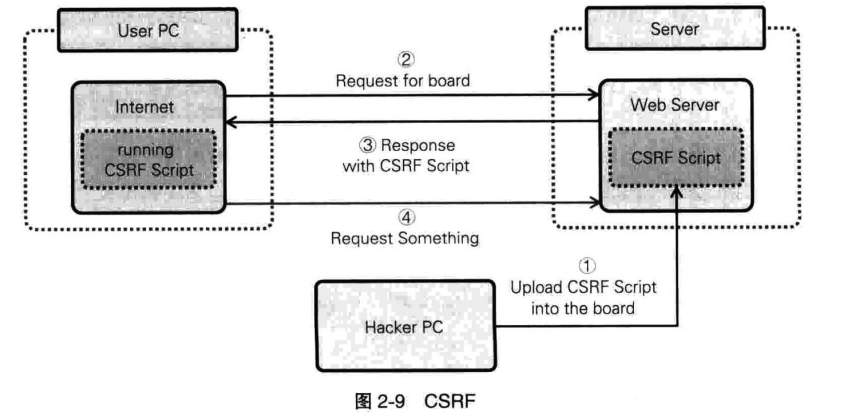
1.XSS

XSS（Cross-Site Scripting，跨站脚本攻击）技术将包含恶意代码的脚本植入布告板的公告，感染阅读公告的用户PC，从中盗取用户个人信息。恶意代码大多数是脚本代码，它读取Cookie，并将其发送到特定URL。用户阅读公告的过程中，其个人信息就会不知不觉地泄露。随着浏览器安全性增强，以及Web防火墙等设备的应用，XSS攻击的成功率已经大幅降低。



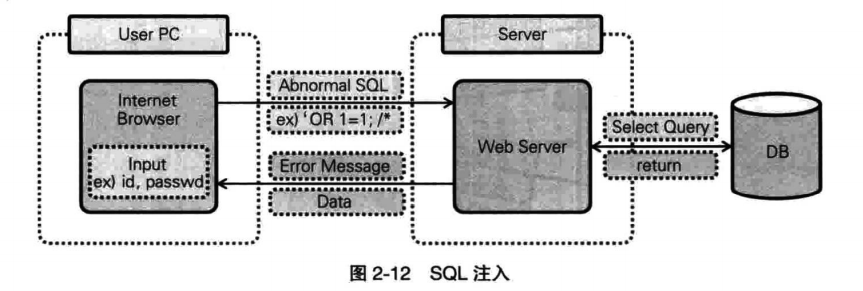
2．CSRF

CSRF（Cross Site Request Forgery,跨站请求伪造）类似于XSS攻击，它也将恶意代码插入公告板，用户阅读相应公告时即受到攻击。XSS攻击主要从用户PC非法盗取个人信息，而CSRF主要通过用户PC对Web服务器发动攻击。就黑客攻击类型而言，CSRF攻击既可以使Web服务器瘫痪，也可以用于盗取敏感信息。



3.SQL 注入

SQL 注入利用HTML input标签发动攻击。为便于各位理解，下面以常见的登录处理过程为例进行说明。首先，浏览器接收用户输入的ID与密码，并将其发送给Web服务器。Web服务器通过SQL语句查询数据库，比对是否存在与输入的ID和密码一致的用户信息。此时，黑客向用户ID与密码中输入的不是正常值，而是一些能够诱使数据库产生错误行为的值。比如，将类似于OR1=1；/\*的值输入ID变量，数据库将忽略条件返回所有值（并非总是如此）。黑客通过反复输入非正常的SQL语句，认真分析数据库返回的数据，从而得到最适合对系统进行攻击的SQL语句。



4. Web shell

Web shell恶意利用了Web提供的文件上传功能。首先，黑客将用于远程操纵服务器的Webshell文件上传到Web服务器，然后找到上传文件所在位置，得到访问Web shell文件的URL地址。然后，通过该URL地址运行Web shell文件，获取可以控制操作系统的超级权限。近来，Web shell与SQL注人都成为实施Web黑客攻击最强大的技术。

