**跨站脚本攻击**(xxs也就是通过HTML或JS动态生成而造成的)

跨站脚本攻击（Cross-Site Scripting，XSS）是指通过存在安全漏洞的 Web 网站注册用户的浏览器内运行非法的 HTML 标签或 JavaScript 进行的一种攻击。动态创建的 HTML 部分有可能隐藏着安全漏洞。就这样，攻击者编写脚本设下陷阱，用户在  
自己的浏览器上运行时，一不小心就会受到被动攻击。  
跨站脚本攻击有可能造成以下影响。  
1、利用虚假输入表单骗取用户个人信息。  
2、利用脚本窃取用户的 Cookie 值， 被害者在不知情的情况下， 帮助攻击者发送恶意请求。  
3、显示伪造的文章或图片。

**HTTP首部注入攻击**(在HTTP头部进行攻击，进而修改cookie,重定向url)

HTTP 首部注入攻击（HTTP Header Injection）是指攻击者通过在响应首部字段内插入换行，添加任意响应首部或主体的一种攻击。属于被动攻击模式。  
向首部主体内添加内容的攻击称为 HTTP 响应截断攻击（HTTP Response SplittingAttack）。  
HTTP 首部注入攻击有可能会造成以下一些影响。  
*设置任何 Cookie 信息  
重定向至任意 URL  
显示任意的主体（ HTTP 响应截断攻击）*

**SQL 注入攻击**(植入sql到数据库，进而篡改或查看数据，或规避认证==)

*会执行非法 SQL 的 SQL 注入攻击*  
SQL 注入（SQL Injection）是指针对 Web 应用使用的数据库，通过运行非法的 SQL 而产生的攻击。该安全隐患有可能引发极大的威胁，有时会直接导致个人信息及机密信息的泄露。  
Web 应用通常都会用到数据库，当需要对数据库表内的数据进行检索或添加、删除等操作时，会使用 SQL 语句连接数据库进行特定的操作。如果在调用 SQL 语句的方式上存在疏漏，就有可能执行被恶意注入（Injection）非法 SQL 语句。  
SQL 注入攻击有可能会造成以下等影响。  
1、非法查看或篡改数据库内的数据  
2、规避认证  
执行和数据库服务器业务关联的程序等

**OS 命令注入攻击**

OS 命令注入攻击（OS Command Injection）是指通过 Web 应用，执行非法的操作系统命令达到攻击的目的。只要在能调用 Shell 函数的地方就有存在被攻击的风险。  
可以从 Web 应用中通过 Shell 来调用操作系统命令。倘若调用 Shell 时存在疏漏，就可以执行插入的非法 OS 命令。  
OS 命令注入攻击可以向 Shell 发送命令，让 Windows 或 Linux 操作系统的命令行启动程序。也就是说，通过 OS 注入攻击可执行 OS 上安装着的各种程序。

**不正确的错误消息处理**(利用web抛出的错误，进一步利用)

不正确的错误消息处理（Error Handling Vulnerability）的安全漏洞是指，Web 应用的错误信息内包含对攻击者有用的信息。与 Web 应用有关的主要错误信息如下所示。  
1、W eb 应用抛出的错误消息  
2、数据库等系统抛出的错误消息  
Web 应用不必在用户的浏览画面上展现详细的错误消息。对攻击者来说，详细的错误消息有可能给他们下一次攻击以提示。

**开放重定向**(在利用开放的重定向redirect进一步利用攻击)

开放重定向（Open Redirect）是一种对指定的任意 URL 作重定向跳转的功能。而于此功能相关联的安全漏洞是指，假如指定的重定向 URL 到某个具有恶意的 Web 网站，那么用户就会被诱导至那个 Web 网站。  
*开放重定向的攻击案例*  
我们以下面的 URL 做重定向为例，讲解开放重定向攻击案例。该功能就是向 URL 指定参数后，使本来的 URL 发生重定向跳转。  
http://example.com/?redirect=http://www.tricorder.jp  
攻击者把重定向指定的参数改写成已设好陷阱的 Web 网站对应的 连接，如下所示。  
http://example.com/?redirect=http://hackr.jp  
用户看到 URL 后原以为访问 example.com，不料实际上被诱导至 hackr.jp 这个指定的重定向目标。  
可信度高的 Web 网站如果开放重定向功能，则很有可能被攻击者选中并用来作为钓鱼攻击的跳板。

**点击劫持**(将恶意网站弄成透明按钮，放到正规网站上，隐瞒使用者点击而劫持)

点击劫持（Clickjacking）是指利用透明的按钮或链接做成陷阱，覆盖在 Web 页面之上。然后诱使用户在不知情的情况下，点击那个链接访问内容的一种攻击手段。这种行为又称为界面伪装（UI Redressing）。  
已设置陷阱的 Web 页面，表面上内容并无不妥，但早已埋入想让用户点击的链接。当用户点击到透明的按钮时，实际上是点击了已指定透明属性元素的 iframe 页面。  
*点击劫持的攻击案例*  
下面以 SNS 网站的注销功能为例，讲解点击劫持攻击。利用该注销功能，注册登录的 SNS 用户只需点击注销按钮，就可以从 SNS 网站上注销自己的会员身份。  
攻击者在预料用户会点击的 Web 页面上设下陷阱。上图中钓鱼游戏页面上的 PLAY 按钮就是这类陷阱的实例。  
在做过手脚的 Web 页面上，目标的 SNS 注销功能页面将作为透明层覆盖在游戏网页上。覆盖时，要保证 PLAY 按钮与注销按钮的页面所在位置保持一致。  
由于 SNS 网站作为透明层被覆盖，SNS 网站上处于登录状态的用户访问这个钓鱼网站并点击页面上的 PLAY 按钮之后，等同于点击了 SNS 网站的注销按钮。

**DoS 攻击**(DOS攻击是针对web，服务器等进行攻击，比较难防止DOS攻击)

DoS 攻击（Denial of Service attack）是一种让运行中的服务呈停止状态的攻击。有时也叫做服务停止攻击或拒绝服务攻击。DoS 攻击的对象不仅限于 Web 网站，还包括网络设备及服务器等。  
主要有以下两种 DoS 攻击方式。  
1、集中利用访问请求造成资源过载， 资源用尽的同时， 实际上服务也就呈停止状态。  
2、通过攻击安全漏洞使服务停止。  
其中，集中利用访问请求的 DoS 攻击，单纯来讲就是发送大量的合法请求。服务器很难分辨何为正常请求，何为攻击请求，因此很难防止 DoS 攻击。  
  
多台计算机发起的 DoS 攻击称为 DDoS 攻击（Distributed Denial of Serviceattack）。DDoS 攻击通常利用那些感染病毒的计算机作为攻击者的攻击跳板。  
内容来自：