常用的几种web攻击方式

# 一、Dos攻击（Denial of Service attack）

是一种针对服务器的能够让服务器呈现静止状态的攻击方式。有时候也加服务停止攻击或拒绝服务攻击。其原理就是发送大量的合法请求到服务器，服务器无法分辨这些请求是正常请求还是攻击请求，所以都会照单全收。海量的请求会造成服务器停止工作或拒绝服务的状态。这就是Dos攻击。

# 二、SOL注入攻击

　　是指通过对web连接的数据库发送恶意的SQL语句而产生的攻击，从而产生安全隐患和对网站的威胁，可以造成逃过验证或者私密信息泄露等危害。

　　SQL注入的原理是通过在对SQL语句调用方式上的疏漏，恶意注入SQL语句。

　　SQL注入常见的两个例子：

　　　　1、私密信息泄露

　　　　　　　假如一个出版书籍的网站，具有根据作者姓名查询已出版书籍的功能，作者未出版的书籍不能被普通用户看到，因为版权属于隐私的问题。那么假设请求是用HTTP的GET请求来完成的，其地址栏请求内容为：www.book.com?serach=echo

　　　　　　　完成此功能的SQL语句为简单的根据条件查找：select \* from book where author = 'echo' and flag = 1; flag等于1代表书籍已出版。

　　　　　　　这时如果有的用户直接地址栏里输入www.book.com?serach=echo'--   这样请求会发生什么？？

　　　　　　　这样的请求传到服务器里的状态会是这样子的 select \* from book where author = 'echo' -- and flag = 1;在SQL语句中--代表注释，会自动忽略掉后面的内容，所以这个请求是骗过服务器把作者为echo的已出版和未出版的书籍全部显示在网页上。造成网站违背开发者的意图，造成信息泄露。

# 三、跨站点请求伪造（CSRF，Cross-Site Request Forgeries）

　　是指攻击者通过已经设置好的陷阱，强制对已完成认证的用户进行非预期的个人信息或设定信息等某些状态的更新。属于被动攻击。更简单的理解就是攻击者盗用了你的名义，以你的名义发送了请求。

　　一个CSRF最简单的例子就是用户A登录了网站A在虚拟账户里转账了1000块钱，用户A在本地生成了网站A的cookie，用户A在没有关闭网站A的情况下有访问了恶意网站B，恶意网站B包含请求A网站的代码，利用了本地的cookie经过身份验证的身份又向网站A发送了一次请求，这时你就会发现你在网站A的账户又少了1000块。这就是基本的CSRF攻击方式。

# 四、XSS攻击（Cross-Site scripting）

　　跨站脚本攻击，是指在通过注册的网站用户的浏览器内运行非法的HTML标签或javascript，从而达到攻击的目的，如盗取用户的cookie，改变网页的DOM结构，重定向到其他网页等。

# 五、点击劫持(Click Jacking)

在我们浏览网页时经常会出现一些令人讨厌的信息，比如一些中奖通知或者色情信息，但在网页中散布这些内容却是不法分子用来诱惑被攻击者点击的常用手段，

点击劫持就是利用透明的iframe或者被覆盖的iframe，通过诱骗用户在该网页上点击某些按钮，触发iframe页面上的点击操作

### 防御方法：

#### 1. 既然点击劫持的核心是iframe的嵌套，那么完全可以通过写一段javascript代码来禁止iframe的嵌套：

|  |
| --- |
| <script type="text/javascript">  if (window!=top) // 判断当前的window对象是否是top对象  top.location.href =window.location.href; // 如果不是，将top对象的网址自动导向被嵌入网页的网址</script> |

注：此段代码来自阮一峰老师的文章   
[《防止网页被嵌入框架的代码》](http://www.ruanyifeng.com/blog/2008/10/anti-frameset_javascript_codes.html" \t "http://blog.csdn.net/adrianzqt/article/details/_blank)

#### 2. X-FRAME-OPTIONS是目前最可靠的方法。

X-FRAME-OPTIONS是微软提出的一个http头，专门用来防御利用iframe嵌套的点击劫持攻击。

并且在IE8、Firefox3.6、Chrome4以上的版本均能很好的支持。

这个头有三个值：

* DENY // 拒绝任何域加载
* SAMEORIGIN // 允许同源域下加载
* ALLOW-FROM // 可以定义允许frame加载的页面地址