WEB开发中常见的漏洞

# 一、SQL注入漏洞 （1）

SQL注入攻击（SQL Injection），简称注入攻击、SQL注入，被广泛用于非法获取网站控制权，是发生在应用程序的数据库层上的安全漏洞。在设计程序，忽略了对输入字符串中夹带的SQL指令的检查，被数据库误认为是正常的SQL指令而运行，从而使数据库受到攻击，可能导致数据被窃取、更改、删除，以及进一步导致网站被嵌入恶意代码、被植入后门程序等危害。

通常情况下，SQL注入的位置包括：

（1）表单提交，主要是POST请求，也包括GET请求；

（2）URL参数提交，主要为GET请求参数；

（3）Cookie参数提交；

（4）HTTP请求头部的一些可修改的值，比如Referer、User\_Agent等；

（5）一些边缘的输入点，比如.mp3文件的一些文件信息等。

常见的防范方法

（1）所有的查询语句都使用数据库提供的参数化查询接口，参数化的语句使用参数而不是将用户输入变量嵌入到SQL语句中。当前几乎所有的数据库系统都提供了参数化SQL语句执行接口，使用此接口可以非常有效的防止SQL注入攻击。

（2）对进入数据库的特殊字符（’”<>&\*;等）进行转义处理，或编码转换。

（3）确认每种数据的类型，比如数字型的数据就必须是数字，数据库中的存储字段必须对应为int型。

（4）数据长度应该严格规定，能在一定程度上防止比较长的SQL注入语句无法正确执行。

（5）网站每个数据层的编码统一，建议全部使用UTF-8编码，上下层编码不一致有可能导致一些过滤模型被绕过。

（6）严格限制网站用户的数据库的操作权限，给此用户提供仅仅能够满足其工作的权限，从而最大限度的减少注入攻击对数据库的危害。

（7）避免网站显示SQL错误信息，比如类型错误、字段不匹配等，防止攻击者利用这些错误信息进行一些判断。

（8）在网站发布之前建议使用一些专业的SQL注入检测工具进行检测，及时修补这些SQL注入漏洞。

# 二、跨站脚本漏洞 （2）

跨站脚本攻击（Cross-site scripting，通常简称为XSS）发生在客户端，可被用于进行窃取隐私、钓鱼欺骗、窃取密码、传播恶意代码等攻击。

XSS攻击使用到的技术主要为HTML和JavaScript，也包括VBScript和ActionScript等。XSS攻击对WEB服务器虽无直接危害，但是它借助网站进行传播，使网站的使用用户受到攻击，导致网站用户帐号被窃取，从而对网站也产生了较严重的危害。

XSS类型包括：

（1）非持久型跨站：即反射型跨站脚本漏洞，是目前最普遍的跨站类型。跨站代码一般存在于链接中，请求这样的链接时，跨站代码经过服务端反射回来，这类跨站的代码不存储到服务端（比如数据库中）。上面章节所举的例子就是这类情况。

（2）持久型跨站：这是危害最直接的跨站类型，跨站代码存储于服务端（比如数据库中）。常见情况是某用户在论坛发贴，如果论坛没有过滤用户输入的javascript代码数据，就会导致其他浏览此贴的用户的浏览器会执行发贴人所嵌入的Javascript代码。

Document.append

Eval()

（3）DOM跨站（DOM XSS）：是一种发生在客户端DOM（Document Object Model文档对象模型）中的跨站漏洞，很大原因是因为客户端脚本处理逻辑导致的安全问题。

常用的防止XSS技术包括：

（1）与SQL注入防护的建议一样，假定所有输入都是可疑的，必须对所有输入中的script、iframe等字样进行严格的检查。这里的输入不仅仅是用户可以直接交互的输入接口，也包括HTTP请求中的Cookie中的变量，HTTP请求头部中的变量等。

（2）不仅要验证数据的类型，还要验证其格式、长度、范围和内容。

（3）不要仅仅在客户端做数据的验证与过滤，关键的过滤步骤在服务端进行。

（4）对输出的数据也要检查，数据库里的值有可能会在一个大网站的多处都有输出，即使在输入做了编码等操作，在各处的输出点时也要进行安全检查。

（5）在发布应用程序之前测试所有已知的威胁。

# 三、弱口令漏洞

弱口令(weak password) 没有严格和准确的定义，通常认为容易被别人（他们有可能对你很了解）猜测到或被破解工具破解的口令均为弱口令。设置密码通常遵循以下原则：

（1）不使用空口令或系统缺省的口令，这些口令众所周之，为典型的弱口令。

（2）口令长度不小于8个字符。

（3）口令不应该为连续的某个字符（例如：AAAAAAAA）或重复某些字符的组合（例如：tzf.tzf.）。

（4）口令应该为以下四类字符的组合，大写字母(A-Z)、小写字母(a-z)、数字(0-9)和特殊字符。每类字符至少包含一个。如果某类字符只包含一个，那么该字符不应为首字符或尾字符。

（5）口令中不应包含本人、父母、子女和配偶的姓名和出生日期、纪念日期、登录名、E-mail地址等等与本人有关的信息，以及字典中的单词。

（6）口令不应该为用数字或符号代替某些字母的单词。

（7）口令应该易记且可以快速输入，防止他人从你身后很容易看到你的输入。

（8）至少90天内更换一次口令，防止未被发现的入侵者继续使用该口令。

# 四、HTTP报头追踪漏洞

HTTP/1.1（RFC2616）规范定义了HTTP TRACE方法，主要是用于客户端通过向Web服务器提交TRACE请求来进行测试或获得诊断信息。当Web服务器启用TRACE时，提交的请求头会在服务器响应的内容（Body）中完整的返回，其中HTTP头很可能包括Session Token、Cookies或其它认证信息。攻击者可以利用此漏洞来欺骗合法用户并得到他们的私人信息。该漏洞往往与其它方式配合来进行有效攻击，由于HTTP TRACE请求可以通过客户浏览器脚本发起（如XMLHttpRequest），并可以通过DOM接口来访问，因此很容易被攻击者利用。

防御HTTP报头追踪漏洞的方法通常禁用HTTP TRACE方法。

# 五、Struts2远程命令执行漏洞

ApacheStruts是一款建立Java web应用程序的开放源代码架构。Apache Struts存在一个输入过滤错误，如果遇到转换错误可被利用注入和执行任意Java代码。

网站存在远程代码执行漏洞的大部分原因是由于网站采用了Apache Struts Xwork作为网站应用框架，由于该软件存在远程代码执高危漏洞，导致网站面临安全风险。CNVD处置过诸多此类漏洞，例如：“GPS车载卫星定位系统”网站存在远程命令执行漏洞(CNVD-2012-13934)；Aspcms留言本远程代码执行漏洞（CNVD-2012-11590）等。

修复此类漏洞，只需到Apache官网升级Apache Struts到最新版本：http://struts.apache.org

# 六、文件上传漏洞 （3）

文件上传漏洞通常由于网页代码中的文件上传路径变量过滤不严造成的，如果文件上传功能实现代码没有严格限制用户上传的文件后缀以及文件类型，攻击者可通过 Web 访问的目录上传任意文件，包括网站后门文件（webshell），进而远程控制网站服务器。

因此，在开发网站及应用程序过程中，需严格限制和校验上传的文件，禁止上传恶意代码的文件。同时限制相关目录的执行权限，防范webshell攻击。

# 七、私有IP地址泄露漏洞

IP地址是网络用户的重要标示，是攻击者进行攻击前需要了解的。获取的方法较多，攻击者也会因不同的网络情况采取不同的方法，如：在局域网内使用Ping指令，Ping对方在网络中的名称而获得IP；在Internet上使用IP版的QQ直接显示。最有效的办法是截获并分析对方的网络数据包。攻击者可以找到并直接通过软件解析截获后的数据包的IP包头信息，再根据这些信息了解具体的IP。

针对最有效的“数据包分析方法”而言，就可以安装能够自动去掉发送数据包包头IP信息的一些软件。不过使用这些软件有些缺点，譬如：耗费资源严重，降低计算机性能；访问一些论坛或者网站时会受影响；不适合网吧用户使用等等。现在的个人用户采用最普及隐藏IP的方法应该是使用代理，由于使用代理服务器后，“转址服务”会对发送出去的数据包有所修改，致使“数据包分析”的方法失效。一些容易泄漏用户IP的网络软件(QQ、MSN、IE等)都支持使用代理方式连接Internet，特别是QQ使用“ezProxy”等代理软件连接后，IP版的QQ都无法显示该IP地址。虽然代理可以有效地隐藏用户IP，但攻击者亦可以绕过代理，查找到对方的真实IP地址，用户在何种情况下使用何种方法隐藏IP，也要因情况而论。

# 八、未加密登录请求

由于Web配置不安全，登陆请求把诸如用户名和密码等敏感字段未加密进行传输，攻击者可以窃听网络以劫获这些敏感信息。建议进行例如SSH等的加密后再传输。

# 九、敏感信息泄露漏洞

SQL注入、XSS、目录遍历、弱口令等均可导致敏感信息泄露，攻击者可以通过漏洞获得敏感信息。针对不同成因，防御方式不同，其中有一个源码泄漏方式只要由运维人员在做系统部署升级时候，把升级的war包等留在了服务器上，建议进行排查并全部删除。

# 十、CSRF （跨站请求伪造）

http://www.cnblogs.com/hyddd/archive/2009/04/09/1432744.html