Web 攻击技术简介

Web 攻击越来越频繁的今天，下面就对常见的 web 攻击方式做一个简单的介绍，以帮助大家了解 web 攻击，维护网络安全。

1、 xss 跨站攻击技术：

主要是攻击者往网页里嵌入恶意脚本，或者通过改变 html 元素属性来实现攻击，主要原因在于开发者对用户的变量直接使用导致进入 html 中会被直接编译成 js，通常的 get 请求通过 url 来传参，可以在 url 中传入恶意脚本，从而获取信息，解决方法：特殊字符过滤。

2、 sql 注入攻击：

主要是就是通过把 SQL 命令插入到 Web 表单提交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的 SQL 命令，比如 select * from test where username="wuxu" or 1=1，这样会使用户跳过密码直接登录，具体解决方案：1、特殊字符过滤，不要用拼接字符串的方法来凑 sql 语句。2、对 sql 语句进行预编译，比如 java 的 preparedstatement。3、关闭错误信息，攻击者可能会通过不断的尝试来得到数据库的一些信息，所以关闭错误信息变得重要起来。4、客户端对数据进行加密，使原来传进来的参数因为加密而被过滤掉。5、控制数据库的权限，比如只能 select，不能 insert，防止攻击者通过 select * from test ；drop tables 这种操作

3、 os 命令注入攻击：

系统提供命令执行类函数主要方便处理相关应用场景的功能.而当不合理的使用这类函数，同时调用的变量未考虑安全因素，就会执行恶意的命令调用，被

攻击利用。主要原因是服务端在调用系统命令时采用的是字符串连接的方式，比如 a="a.txt;rm -rf *",system("rm -rf {$a}")，这会给服务端带去惨痛的代价

具体防御方案：

1、在程序开发时少用系统命令，执行命令的参数尽量不要从外部获取。

2、参数特殊字符过滤

3、使用外部组建和库

4、http 首部注入攻击：

5、邮件首部注入攻击：

它允许恶意攻击者注入任何邮件头字段,BCC、CC、主题等,它允许黑客通过注入手段从受害者的邮件服务器发送垃圾邮件。主要是利用邮件系统传参的 bug 来进行攻击，解决方法：1、使用正则表达式来过滤用用户提交的数据。例如,我们可以在输入字符串中搜索(r 或 n)。2、永远不要信任用户的输入。

6、目录遍历攻击：

目录遍历是 Http 所存在的一个安全漏洞，它使得攻击者能够访问受限制的目录，并在 Web 服务器的根目录以外执行命令。比如 http://test.webarticles.com/show.asp?view=../../../../../Windows/system.ini，这种 url 会返回 / windows / system.ini 给用户，所以服务器上的重要文件就会遭到泄漏，解决方法：根目录访问，现在主流服务器，比如 nginx，都会有 www 根目录，是网站的根目录，所以用户只能访问该根目录下的文件，不能访问其他目录下的文件，从而实现了权限控制。而目录遍历并不是一个漏洞，而是服务器的一个功能，而因为管理员的疏忽从而变成了漏洞

7、远程目录包含攻击：

原理就是注入一段用户能控制的脚本或代码，并让服务端执行。比如 php 中的 include($filename)，而此 filename 由用户传入，用户即可传入一段恶意脚本，从而对服务其造成伤害，解决方法：当采用文件包含函数的时候，不应动态传入，而应该有具体的文件名，如果动态传入，要保证动态变量不被用户所控制

8、会话劫持：

这是一种通过获取用户 Session ID 后，使用该 Session ID 登录目标账号的攻击方法，此时攻击者实际上是使用了目标账户的有效 Session。会话劫持的第一步是取得一个合法的会话标识来伪装成合法用户，因此需要保证会话标识不被泄漏，通俗一点就是用户在登录时，唯一标示用户身份的 session id 被劫持，使得攻击者可以用这个 session id 来进行登录后操作，而攻击者主要是通过 窃取：使用网络嗅探，XSS 攻击等方法获得。而第一种方式网络嗅探，我们可以通过 ssl 加密，也就是 https 来对报文进行加密，从而防止报文被截获，而第二种方式 xss 攻击，方式在第一种已经给出，不再赘述。此外通过设置 HttpOnly。通过设置 Cookie 的 HttpOnly 为 true，可以防止客户端脚本访问这个 Cookie，从而有效的防止 XSS 攻击，还有就是设置 token 验证。关闭透明化 Session ID。透明化 Session ID 指当浏览器中的 Http 请求没有使用 Cookie 来存放 Session ID 时，Session ID 则使用 URL 来传递。

9、会话固定：

会话固定是会话劫持的一种，区别就是，会话固定是攻击者通过某种手段重置目标用户的 SessionID，然后监听用户会话状态；用户携带 sessionid 进行登录，

攻击者获取 sessionid 来进行会话，解决方案：服务端设置用户登录后的 sessionid 与登录前不一样即可，另外会话劫持的方法也可以用在会话固定上

10、csrf 跨站伪造请求攻击：

其实就是攻击者盗用了你的身份，以你的名义发送恶意请求。

具体方案防御：

1、验证 referer 字段，这个字段主要是反映了访问某个网页只能有 referer 发起请求，所以通过 referer 验证，可以抵御一部分 csrf 攻击。

2、在请求地址中加 token 验证，攻击者发送恶意请求时，通过 token 验证来进行身份验证，而 token 必须是一个攻击者猜不到的，很难去模拟出来的，具体来说可以放在表单的 hidden 字段中。

3、在 htttp 请求头中定义字段，其实就是将 2 中说得 token 字段放入请求头，解决了每次在请求头中加入 token 的不便，同时在其也不会记录在地址栏里，降低了 token 泄露的风险。