常见的安全漏洞

一，SQL注入

SQL注入（SQL Injection）是最常见的漏洞，具有多种影响。 攻击者将SQL命令插入Web表单以提交或输入域名或页面请求的查询字符串，并最终诱使服务器执行恶意SQL命令，从而入侵数据库以执行任意查询。

SQL注入可能造成的危害是：篡改了网页和数据，窃取了核心数据，攻击了数据库所在的服务器，并使之成为a主机。

例如，某些网站不使用预编译的SQL，并且用户在界面上输入的某些字段将添加到SQL。 这些字段可能包含一些恶意SQL命令。 例如：password =“ 1'OR'1'='1”; 即使您不知道用户密码，也可以正常登录。

测试方法：

在需要查询的页面上，输入简单的SQL语句，例如正确的查询条件和1 = 1，然后检查响应结果。如果结果与正确的查询条件相符，则表明该应用程序尚未筛选用户输入，并且可以初步判断它存在。 SQL注入漏洞

二，XSS跨站点脚本攻击

SS（跨站点脚本）类似于SQL注入，XSS通过网页插入恶意脚本。使用的主要技术是前端HTML和JavaScript脚本。当用户浏览网页时，将实施一种控制用户浏览器行为的攻击方法。

成功的XSS可以获取用户的cookie，并使用该cookie窃取用户在网站上的操作权限。它还可以获取用户的联系人列表，并使用攻击者的身份将大量垃圾邮件发送到特定的目标组。 ，还有很多。

XSS分为三类：存储（持久XSS），反射（非持久XSS）和DOM。

测试方法：

在数据输入界面上，输入：保存成功后，弹出对话框，提示存在XSS漏洞。

或更改url请求中的参数。如果页面上弹出对话框，则表明存在XSS漏洞。

三，CSRF跨站伪造请求攻击

CSRF(Cross Site Request Forgery)，利用已登录的用户身份，以用户的名义发送恶意请求，完成非法操作。

例如，如果用户浏览并信任具有CSRF漏洞的网站A，则浏览器会生成相应的cookie，并且用户访问危险的网站B而不退出网站。

危险网站B要求访问网站A并提出要求。 浏览器使用用户的cookie信息访问网站A。 由于网站A不知道是用户自身发出的请求还是危险网站B发出的请求，因此将处理危险网站B的请求，从而完成了用户操作目的的模拟。 这是CSRF攻击的基本思路。

测试方法：

同个浏览器打开两个页面，一个页面权限失效后，另一个页面是否可操作成功，如果仍然能操作成功即存在风险。2.使用工具发送请求，在http请求头中不加入referer字段，检验返回消息的应答，应该重新定位到错误界面或者登录界面。

四，文件上传漏洞

文件上传攻击是指攻击者将可执行文件上传到服务器并执行该文件时。

这种攻击方法是最直接，最有效的。 上载的文件可以是病毒，特洛伊木马，恶意脚本或Webshell。

Webshell是Web文件（例如asp，php，jsp或cgi）形式的命令执行环境。 也可以说是Web后门。 攻击者阻止或在受影响的系统上插入Web Shell之后，他可以轻松地通过Web Shell访问系统以控制Web服务器。

测试方法：

严格检查上传文件的类型和大小，禁止上传带有恶意代码的文件。

检查相关目录的执行权限。 您可以通过浏览器访问Web服务器上的所有目录，并检查是否返回了目录结构。 如果显示目录结构，则可能存在安全问题。

五，URL跳转漏洞

URL跳转漏洞，即未经验证的重定向漏洞，是指Web程序直接跳转到参数中的URL，或者在页面中引入了任意开发者的URL，将程序引导到不安全的第三方区域，从而导致安全问题。

测试方法：

1.使用数据包捕获工具捕获请求。

2.抓住302 URL，修改目标地址，然后查看它是否可以跳转。

ps：但是现在很多跳转都添加了引荐来源验证，这导致攻击者无法跳转。