* **WEB攻击**

**WEB应用攻击原理**

Web应用攻击是攻击者通过浏览器或攻击工具，在URL或者其它输入区域（如表单等），向Web服务器发送特殊请求，从中发现Web应用程序存在的漏洞，从而进一步操纵和控制网站，查看、修改未授权的信息。

**信息泄露漏洞**

信息泄露漏洞是由于Web服务器或应用程序没有正确处理一些特殊请求，泄露Web服务器的一些敏感信息，如用户名、密码、源代码、服务器信息、配置信息等。造成信息泄露主要有以下三种原因:

Web服务器配置存在问题，导致一些系统文件或者配置文件暴露在互联网中；

Web服务器本身存在漏洞，在浏览器中输入一些特殊的字符，可以访问未授权的文件或者动态脚本文件源码；

Web网站的程序编写存在问题，对用户提交请求没有进行适当的过滤，直接使用用户提交上来的数据。

**目录遍历漏洞**

目录遍历漏洞是攻击者向Web服务器发送请求，通过在URL中或在有特殊意义的目录中附加“../”、或者附加“../”的一些变形（如“..\”或“..//”甚至其编码），导致攻击者能够访问未授权的目录，以及在 Web 服务器的根目录以外执行命令。

**命令执行漏洞**

命令执行漏洞是通过URL发起请求，在Web服务器端执行未授权的命令，获取系统信息，篡改系统配置，控制整个系统，使系统瘫痪等。 命令执行漏洞主要有两种情况：

通过目录遍历漏洞，访问系统文件夹，执行指定的系统命令；

攻击者提交特殊的字符或者命令，Web程序没有进行检测或者绕过Web应用程序过滤，把用户提交的请求作为指令进行解析，导致执行任意命令。

**文件包含漏洞**

文件包含漏洞是由攻击者向Web服务器发送请求时，在URL添加非法参数，Web服务器端程序变量过滤不严，把非法的文件名作为参数处理。这些非法的文件名可以是服务器本地的某个文件，也可以是远端的某个恶意文件。由于这种漏洞是由PHP变量过滤不严导致的，所以只有基于PHP开发的Web应用程序才有可能存在文件包含漏洞。

**SQL注入漏洞**

SQL注入漏洞是由于Web应用程序没有对用户输入数据的合法性进行判断，攻击者通过Web页面的输入区域(如URL、表单等) ，用精心构造的SQL语句插入特殊字符和指令，通过和数据库交互获得私密信息或者篡改数据库信息。SQL注入攻击在Web攻击中非常流行，攻击者可以利用SQL注入漏洞获得管理员权限，在网页上加挂木马和各种恶意程序，盗取企业和用户敏感信息。

**跨站脚本漏洞XSS**

跨站脚本漏洞是因为Web应用程序时没有对用户提交的语句和变量进行过滤或限制，攻击者通过Web页面的输入区域向数据库或HTML页面中提交恶意代码，当用户打开有恶意代码的链接或页面时，恶意代码通过浏览器自动执行，从而达到攻击的目的。跨站脚本漏洞危害很大，尤其是目前被广泛使用的网络银行，通过跨站脚本漏洞攻击者可以冒充受害者访问用户重要账户，盗窃企业重要信息。

根据前期各个漏洞研究机构的调查显示，SQL注入漏洞和跨站脚本漏洞的普遍程度排名前两位，造成的危害也更加巨大。

* **WEB应用攻击处置方式**

直接拦截黑客的入侵行为，返回493状态码拦截页面，不封锁攻击者ip，并且是立刻进行拦截，不存在检测时间。