模块功能的设计与实现

目录：

爬虫模块的设计与实现

暴力破解漏洞检测模块检测的设计与实现

SQL注入漏洞检测模块的设计与实现

XSS漏洞检测模块的设计与实现

文件上传漏洞检测模块的设计与实现

爬虫模块的设计与实现

简介：爬虫模块(Scan模块)是本程序框架的核心，用于爬取目标网站上的目录，获取所有可能的漏洞点，提供给其他模块使用。是所有模块的基石。

设计：

调用模块：

第三方爬虫库requests

目录爬取的实现：

1. 使用基于深度和广度的算法，完整爬取页面内存在的目录
2. 根据建站经验，扫描一些可能存在的敏感目录，获取可能的隐藏目录或者后台目录。
3. 获取robots.txt目录的内容

在获取完整的目录之后，将目录整合在List中，提供给其他模块使用。

可扩展性:

作为程序的核心模块，提供了多线程等诸多功能，同时也支持第三方扩展。通过调用Scan模块提供的接口，在Scan模块的基础上，加上自己设计的功能，测试其他漏洞或者增强对某一漏洞/目录的扫描能力。

暴力破解漏洞检测模块检测的设计与实现

简介：暴力破解漏洞是原理最为简单的一种漏洞，但是我们并不能忽略这个漏洞。在某些应用场景中，这个漏洞也是有非常大的利用价值。

测试目录：

爬虫模块扫描返回的网页目录

生成字典：

字典是程序用于测试暴力破解漏洞的关键，正确的字典能让暴力破解变得非常轻松。

程序包含多种类型暴力破解的字典，各种用户名和密码的弱口。同时支持外部导入用户自定义的字典。

程序还可以根据用户，输入的关键字，自动生成针对的字典，增加爆破成功率。

可扩展性：

模块也提供接口，给其他模块和第三方插件使用。例如，在SQL盲注的时候，可以使用暴力破解模块，快速爆破出盲注的值，加快漏洞的测试进度。

SQL注入漏洞检测模块的设计与实现

简介: SQL注入攻击是目前最常见的一种WEB漏洞，是以一种基于SQL语句的注入方式。本模块会检测常见的SQL显式注入、盲注等注入漏洞，并且在发现可能注入点之后提供具体的修复方案。

测试目录：

爬虫模块扫描返回的网页目录，发送自己payload

使用GET和POST两种方式发包测试

判断方式设计

（1）显式注入的实现

通过构造两个Payload （例如"1 and 1=1","1 and 1=2"）通过GET/POST发送给服务器

会获得两次回显，如果一次回显式成功获取的ID=1的页面，而第二次报错了，则说明此处的sql语句构造成功，存在明显的SQL注入漏洞。

实现方式则是，判断两个返回页面是否相同，如果不同，则说明存在注入。如果相同，即都报错了，说明这种构造方式被过滤了，构造注入的payload失败了。此模块会提供大量功能齐全的payload，测试各种SQL注入的可能性。并且针对不同的payload注入提供不同的修复建议。

1. 盲注的实现

1.基于报错的盲注

2.基于时间的盲注

XSS漏洞检测模块的设计与实现

简介：

检测常见的XSS漏洞点，并且提供绕过XSS-Filter的选项，并且提供修复漏洞的过滤参数，帮助用户在测试网站安全性的时候做到面面俱到。

测试目录：

爬虫模块扫描返回的网页目录，发送自己的xss测试代码

同样使用GET和POST两种方式发包测试

判断方式设计：

通过植入弹窗代码 #例如<script>alert(’XSS‘);</script>

发送数据包，观察是否弹出含有标签内容（此处即 XSS）的弹窗。

绕过过滤：

程序提供各种绕过绕过XSS-Filter的参数。

文件上传漏洞检测模块的设计与实现

简介：

判断漏洞

使用POST方式上传文件

检测目录中是否包含上传的文件名