信息安全探测研究

1. **绪论**

1.1 研究背景

目前国内非常重视信息安全，国家也大力支持信息产业，对国内的安全产业要求也越来越高，由于5G的到来，信息技术可能又要迎来新一轮的快速发展，特别是物联网的发展，又会迎来新一轮的安全挑战，所以信息安全的重要性不言而喻，对于国内的web安全，目前较少有全面信息收集的工具，有位大牛曾说：渗透测试的本质是信息收集，由此可见信息收集在渗透测试中所占的比重，且由于目前全球网络互通，各个国家与企业都要加强自己的安全建设，防止数据与信息的泄露、系统的崩溃，目前国内外信息安全对于信息收集这方面的工具大多偏重于一个方面，且大多数据放在了网页中提供查询，我们要在网上获取很多信息是非常繁琐的，那么我们是否可以通过一个工具来对这些操作进行简化，可以同时抓取到很多网站关于该目标的数据

1.2 研究的目的与意义

1.2.1 研究的目的

渗透测试的两种基本类型有：黑盒测试：即渗透测试者对客户的任何信息一无所知的情况下进行测试；白盒测试：即渗透测试者对客户的任何信息一无所知的情况下进行测试。对于生活在信息时代的我们来说，学会侦查与探测是非常重要的，对于渗透测试人员或者黑客来说都是必不可少的。因为目前的时代特点，使得信息收集对其他非专业人员来说是非常无趣的步骤。很多刚学习渗透测试的白帽子可能会认为信息收集没有挑战性。但是真正出色的信息收集即可扫描出系统漏洞并获取权限。通常我们在知道测试目标时大多对目标知之甚少，那么我们就要通过各种途径取获得测试站点的信息，只有我们获得了足够的信息后，才能通过信息指定一些测试计划和编写漏洞利用代码，有时当我们久攻主站不下时，我们也可以换一个思路，攻击信息收集到的旁站，通过旁站获得主服务器的权限，毕竟在大多数情况下，比较大的网站很难做到对自己的所有资产进行完美的加固，那么我们就可以根据这个原因，对该站点的资产收集整理，使用扫描器和手动测试一起进行漏洞扫描。

随着网络技术的发展，web应用的范围也越来越广泛，但在web应用范围扩大的情况下，各种安全问题也随之而来，在早期时，web因为攻击手段和防护手段的限制，攻击成功获取到的权限也比较低，获取敏感数据也比较少，大多数人较于偏向于挖掘二进制漏洞，但随着信息技术的飞速发展以及攻击与防御的相辅相成，各种web安全问题接踵而来,其中以OWASP公布的top10出现次数为例，XSS(Cross-Site Scripting)跨站脚本攻击、XXE(XML External Entity attack)XML外部实体注入攻击、文件上传、文件包含、命令执行、SQL注入、SSRF(Server-Site Request Forgery)服务器端请求伪造、因配置不当造成的信息泄露(git泄露、SVN泄露、hg源码泄露、WEB-INF泄露)、CSRF(Cross-Site Request Forgery)跨站请求伪造、JSONP劫持、CORS跨域请求漏洞、反序列化漏洞，因为目前大多数网站的后端大多是通过“世界上最好的语言”PHP编写的，PHP语言是以C语言为基础的，所以有些C语言的特性也保留了下来，比如00截断，且PHP在比较时也会因为程序员的一些疏忽导致产生PHP弱类型比较等漏洞（PHP进行“==”比较时，会先进行转化类型再进行比较，所以可能会导致一些恶意代码逃过WAF），由于目前web攻防技术的快速提升、各种新型漏洞不断爆出，类似于目前大火的python语言中flask模块，因为其轻量型和可定制的特点，已经超越了Django成为了目前最多人使用的网站模块，而flask中也有未过滤注入导致的悲剧(如:SSTI注入)即渲染模板时未对用户输入进行限制，敏感信息的泄露会导致系统面临严重威胁，有可能导致渗透测试者直接获得源代码，目录遍历或敏感文件泄露都对系统的防御带来了严峻的挑战，目前web安全对社会的稳定性有着非常重要的作用，比如大型电商企业因JSONP、CORS和SQL注入导致用户数据被窃取，酒店数据、身份信息被纰漏在了“大名鼎鼎”的社工库，这样又导致了一个新的安全问题，即社会工程学攻击，因为目前密码的设置如果过于复杂可能会导致记不住，所以用户常常会使用123456或者自己的身份信息和名字简称等作为密码，且多个平台的密码基本是相同的，如果身份信息泄露，则既有可能导致你的密码被社会工程学攻击，自己密码被破解的几率大大上升，且因为多个平台通常使用同一个密码，导致破解了一个密码则可以获取更大的攻击面，个人信息安全也面临严重威胁。因为网络远程登录控制能够非常方便快捷的控制远程个人电脑或服务器，因为有些用户设置的密码过于简单，可以通过弱口令爆破的方式获取远程登录的账号密码，导致用户的设备不安全

通过爬虫技术实现对于目标信息的爬取，解决由于目标信息分布过广但是收集信息步骤过于繁琐和复杂，弥补了因为人工收集信息可能导致的收集信息遗漏无法对资产进行全面性评估，无法对己方资产进行有效保护

1.2.2 研究的意义

目前国内非常重视信息安全，国家也大力支持信息产业，对国内的安全产业要求也越来越高，由于5G的到来，信息技术可能又要迎来新一轮的快速发展，特别是物联网的发展，又会迎来新一轮的安全挑战，所以信息安全的重要性不言而喻，对于国内的web安全，目前较少有全面信息收集的工具，有位大牛曾说：渗透测试的本质是信息收集，由此可见信息收集在渗透测试中所占的比重，且由于目前全球网络互通，各个国家与企业都要加强自己的安全建设，防止数据与信息的泄露、系统的崩溃。特别是对于信息战来说，信息量越大，获取速度越快，攻击面也就越广，所以对于自动化的信息搜集是非常有必要的

1.3 国内外研究现状