

简介

X-Scan 是国内最著名的综合扫描器之一，它完全免费，是不需要安装的绿色软件、界面支持中文和英文两种语言、包括图形界面和命令行方式。主要由国内著名的民间黑客组织"安全焦点"完成，从 2000 年的内部测试版 X-Scan V0.2 到目前的最新版本 X-Scan 3.3-cn 都凝聚了国内众多黑客的心血。最值得一提的是，X-Scan 把扫描报告和安全焦点网站相连接，对扫描到的每个漏洞进行"风险等级"评估，并提供漏洞描述、漏洞溢出程序，方便网管测试、修补漏洞。可以利用该软件对 VoIP 设备、通讯服务器进行安全评估。

软件说明

采用多线程方式对指定 IP 地址段(或单机)进行安全漏洞检测，支持插件功能，提供了图形界面和命令行两种操作方式，扫描内容包括：远程操作系统类型及版本，标准端口状态及端口 BANNER 信息，CGI 漏洞，IIS 漏洞，RPC 漏洞，SQL-SERVER、FTP-SERVER、SMTP-SERVER、POP3-SERVER、NT-SERVER 弱口令用户，NT 服务器 NETBIOS 信息等。扫描结果保存在/log/目录中，index_*.htm 为扫描结果索引文件。

安装与使用

一、下载并解压

到官网下载最新版 x-scan v3.3 或者到多特网下载，地址如下：

<http://www.duote.com/soft/3694.html>

解压后运行 xscan_gui.exe 即可运行 xscan



二、x-scan 界面

X-scan 界面如下图显示，大体分为三个区域，界面上面为菜单栏，界面下方为状态栏。若下载的为英文版，可以在菜单栏的 Language 菜单将语言设置为中文

三、参数设置

点击"设置"菜单，选择"扫描参数"或者直接点击工具栏的蓝色按钮进入扫描参数设置。

检测范围。设置待扫描的 IP，可以按示例方式设置检测范围，或者从文件获取主机列表。

全局设置。用来设置全局的扫描参数，具体如下：

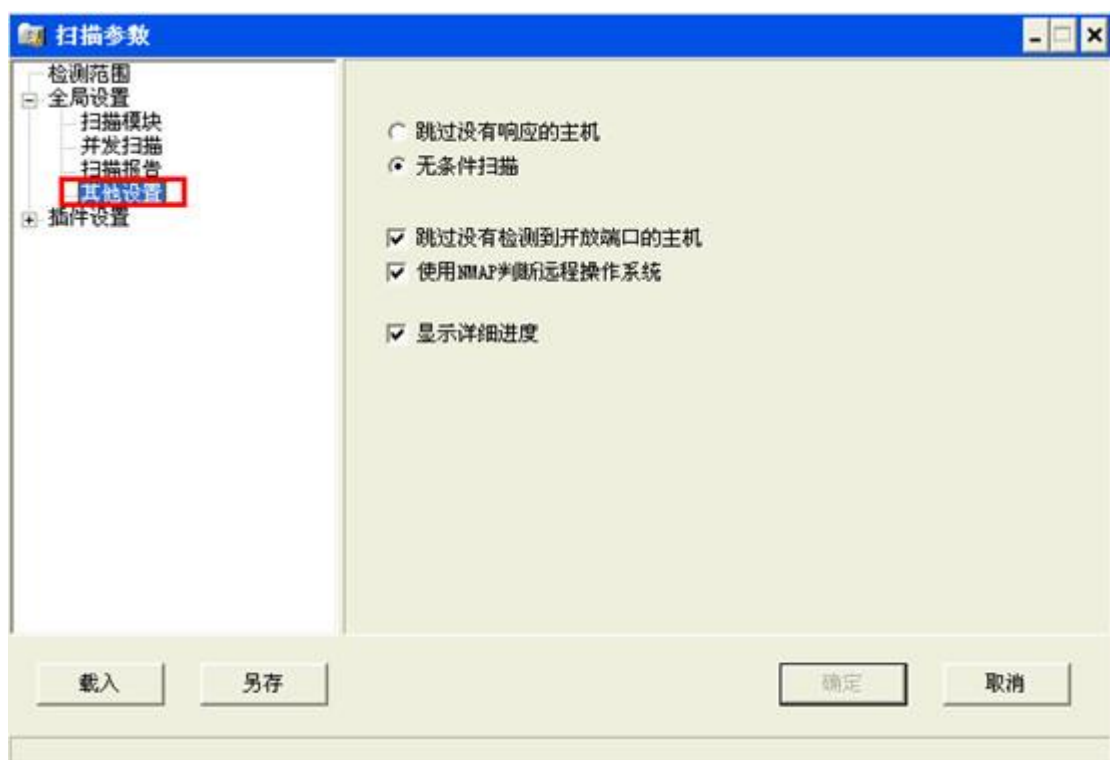
扫描模块：设置需要扫描的模块，对于单台设备的扫描，可以选择全部模块，如果扫描某个范围里面的设备，可以按需勾选需要扫描的模块。

并发扫描：设置扫描的并发量，默认即可。如果机器性能好，带宽足够，可

以适当增大并发量

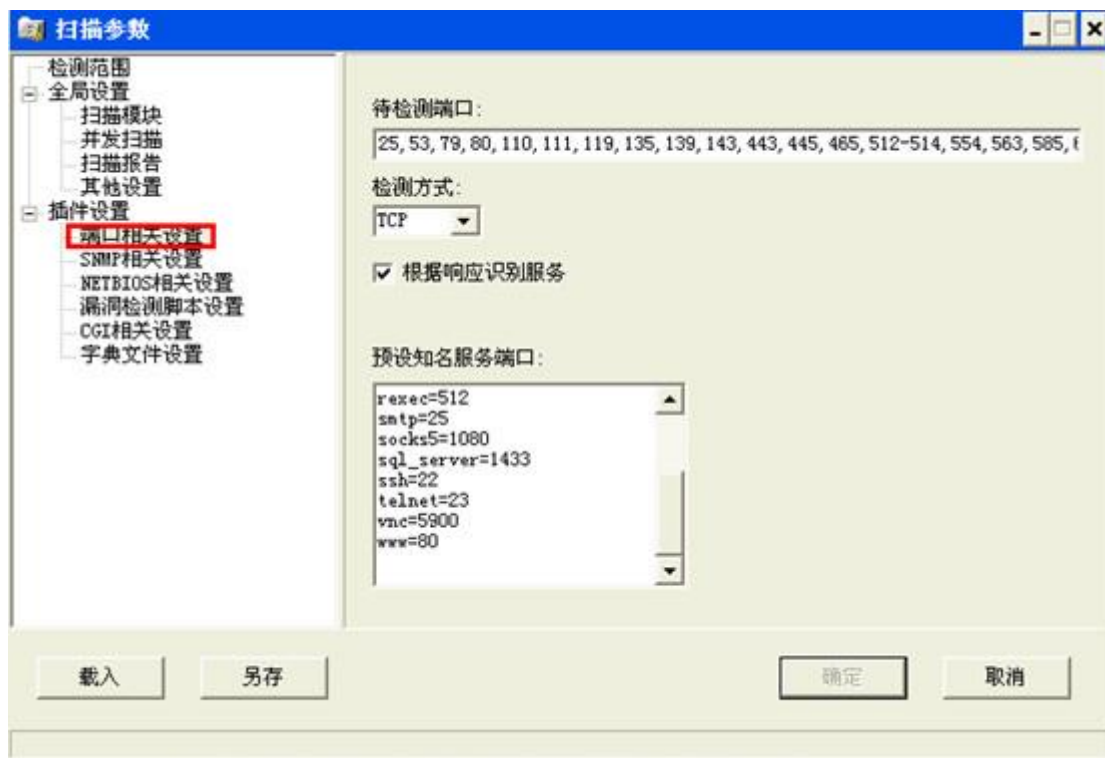
扫描报告：设置扫描报告的名称和类型等

其它设置：设置对目标设备的检测机制等，如果是单个设备，建议使用无条件扫描，因为测试发现 x scan 判断主机是否存活不是很准确。

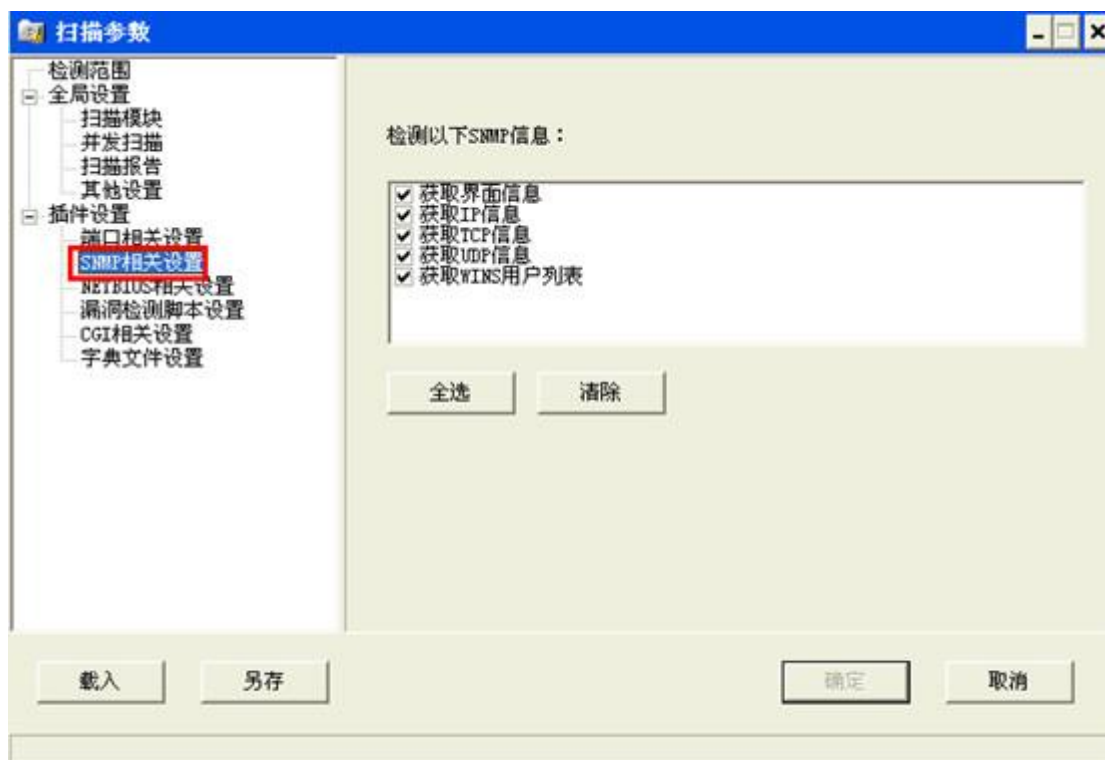


插件设置：设置各插件的相关选项

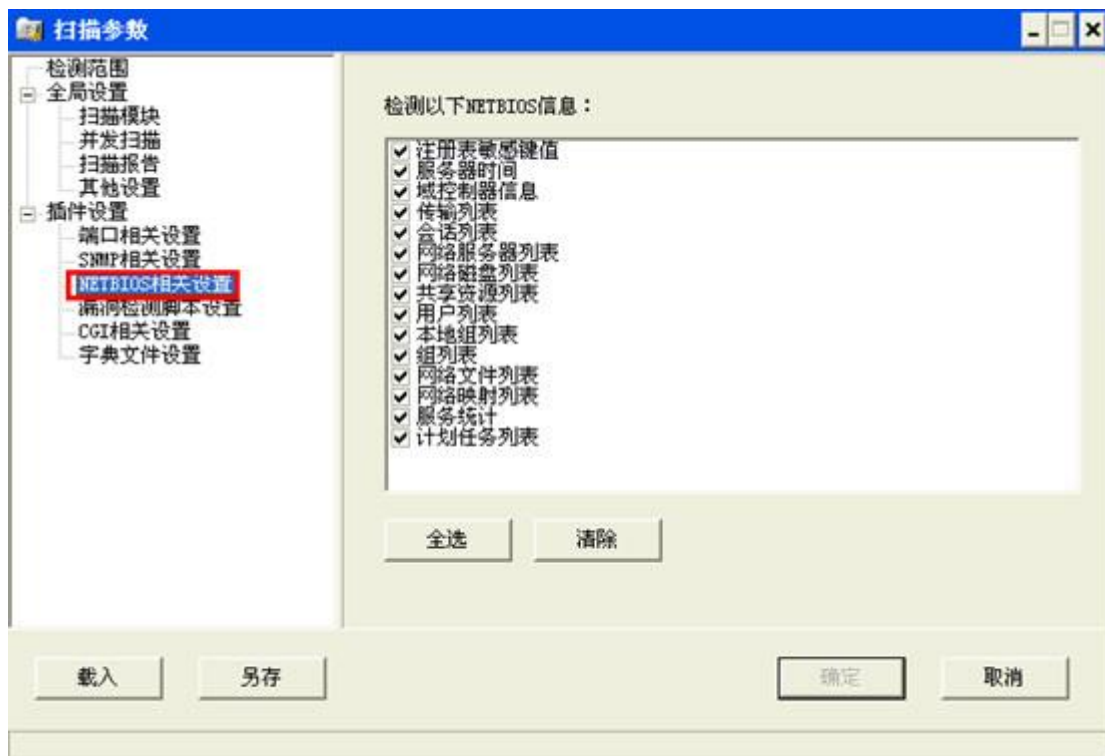
端口相关设置：设置与端口有关的项。待检测端口可以是任意端口的组合。检测方式使用 TCP 能够提高 x-scan 的准确性，但容易被对方的防火墙阻塞，SYN 却相反。根据响应识别服务，x-scan 能够根据响应判断运行的服务，即使端口已被更改。预设知名服务端口，可以自定义某些端口为知名服务端口。



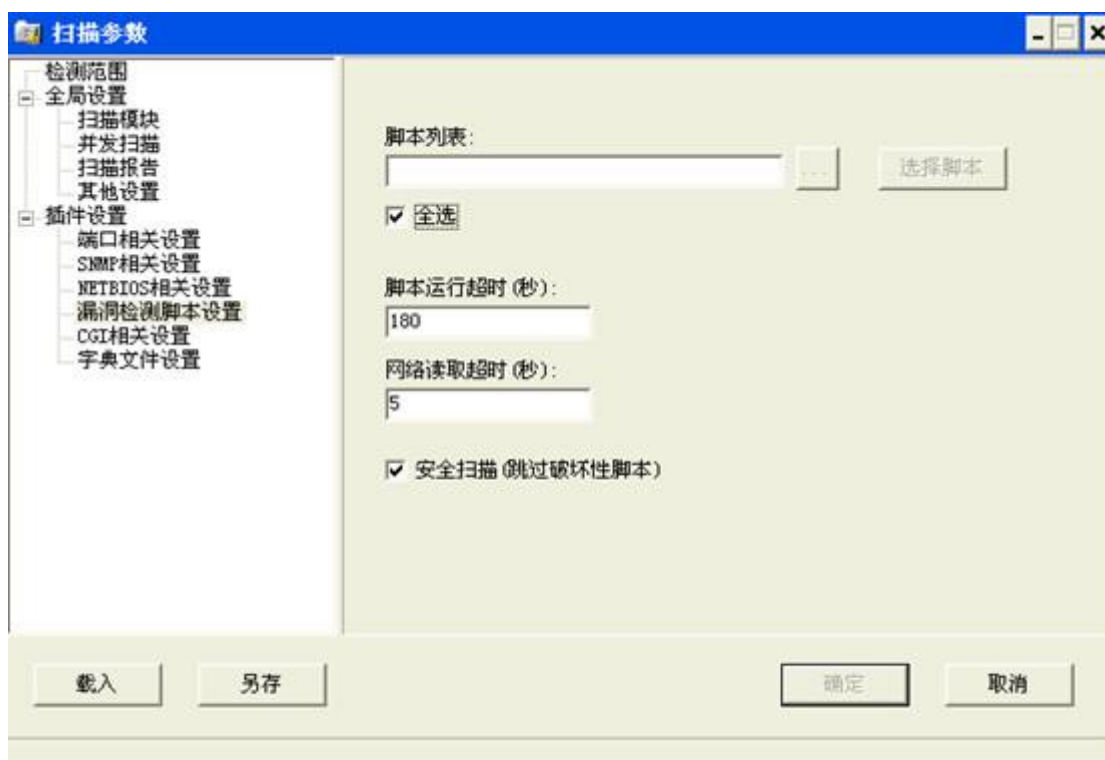
SNMP 相关设置：设置 SNMP 协议检测项，建议全选。



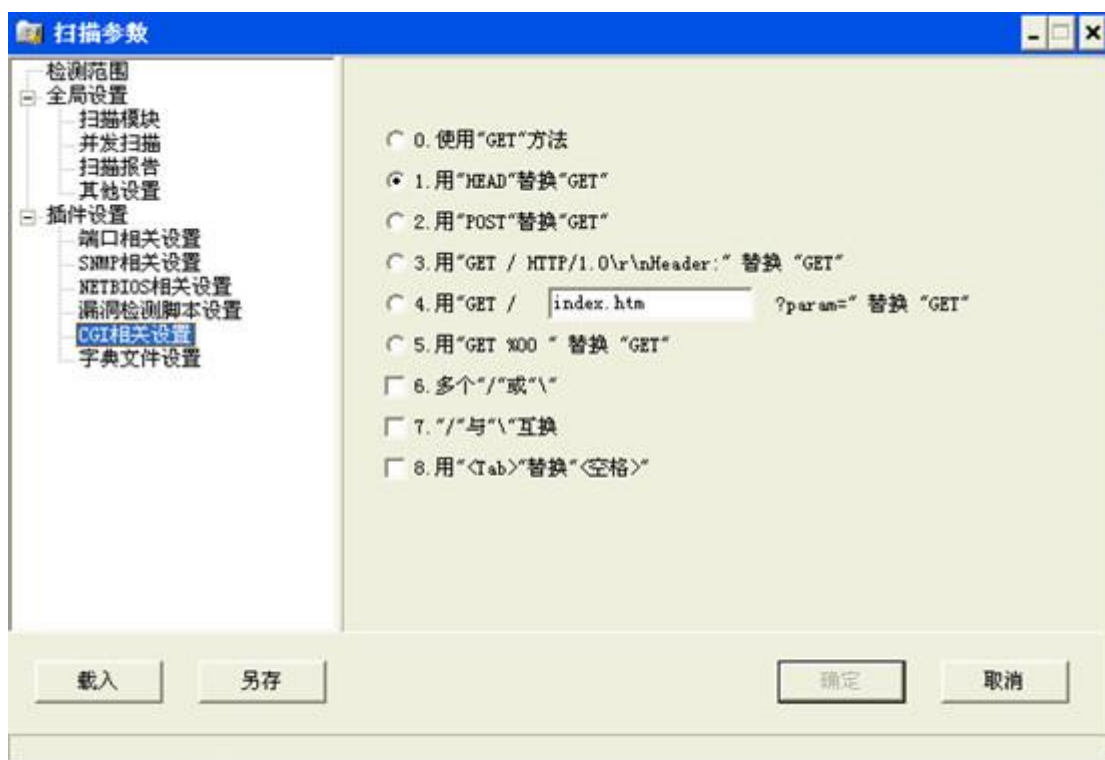
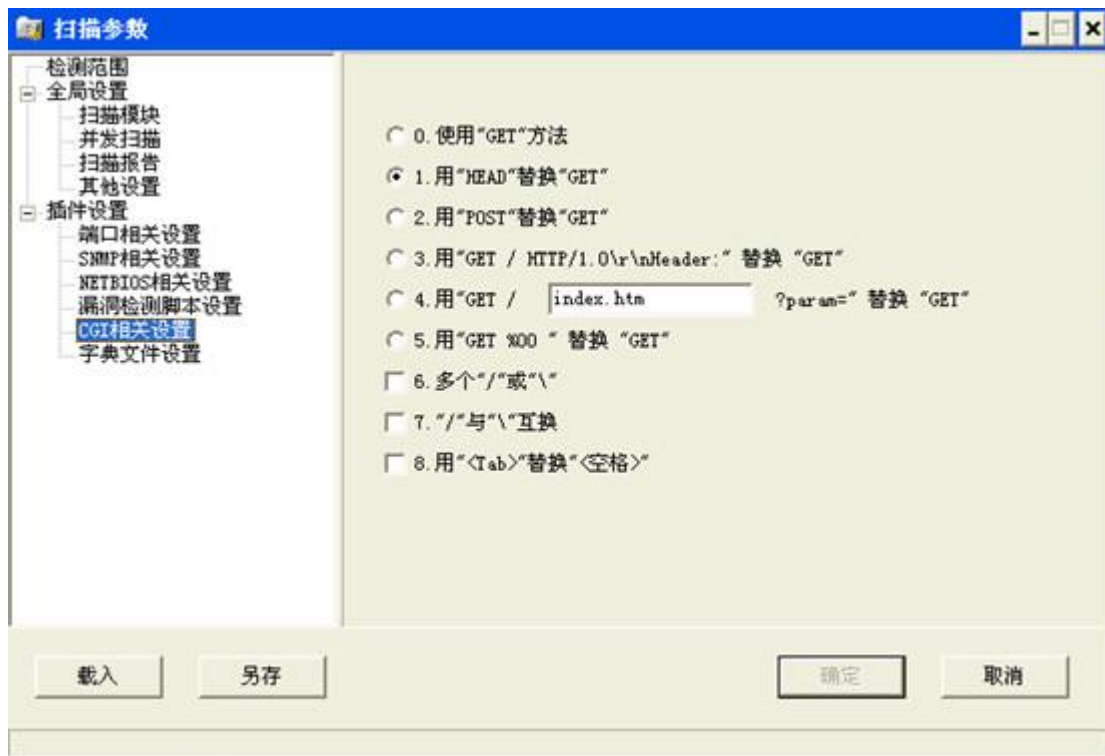
NETBIOS 相关设置：设置检测的 NETBIOS 信息，主要是针对 windows 系统的 NETBIOS 的检测，单个非 windows 设备测试时勾选也无所谓。



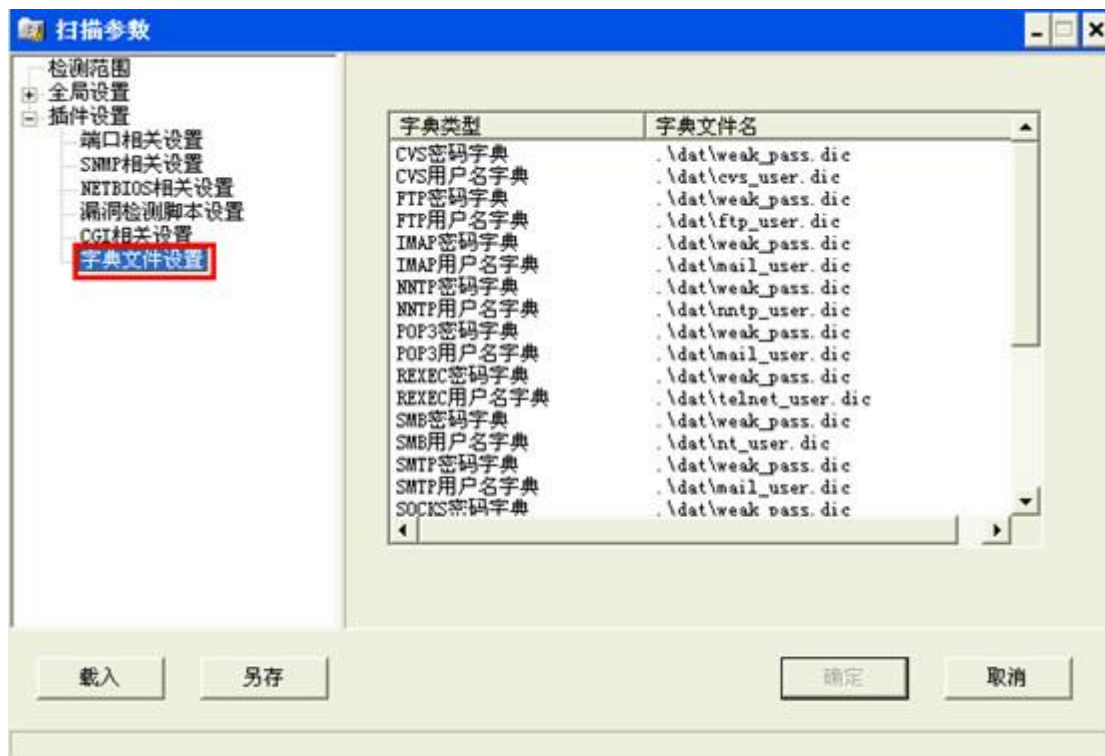
漏洞检测脚本设置：默认即可




CGI 相关设置：设置 CGI（公用网关接口）的扫描策略，主要是针对 web 服务器的扫描。一般默认。



字典文件设置：设置扫描弱口令时用到的字典，可以编辑字典以自定义弱口令



四、开始扫描

保存好配置后，点击工具栏的开始按钮  即可进行扫描，x-scan 界面具有详细的扫描状态，扫描时间视扫描的深度和广度而定。

五、扫描结果

扫描结束后，x-scan 会自动弹出扫描结果，结果会详细列出漏洞情况和解决建议，高危漏洞会以红色字体标出。如图：