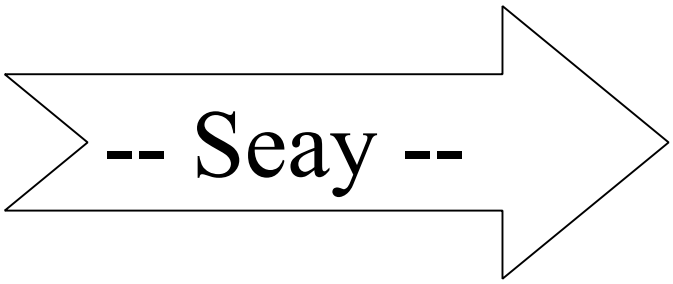
Seay PHP 代码审计工具说明



软件名：	Seay PHP 代码审计工具
软件版本：	Version 2.1
作者：	Seay
博客：	http://www.cnseay.com/
联系方式：	QQ10118157 邮箱：root@cnseay.com
文档编写时间：	2012 年 11 月 12 日

序

本人目前就读重庆某软件学院软件测试专业，将于 2013 年 1 月底毕业，为了扎实基础，于是有时间就会找一些源码研究，有时候想走走捷径，提高下效率，于是开始找一些代码审计的工具，但是目前国内貌似没有发现专业的这类工具，于是就萌发了编写这个 PHP 代码审计工具的想法，并付足于行动。

那为什么写 PHP 的呢？从目前主流的四大动态网页编程(ASP/ASPX/PHP/JSP)语言来分析，目前最火的是 PHP，很多 CMS 等很大一部分是 PHP，安全性最难控制的也是 PHP，怎么难控制就不说了，既然都开始玩代码审计了，应该懂得。

该版本目前支持单个关键字扫描、批量函数扫描、批量正则匹配，其中正则表达式扫描精确度最高，效率最高。

其他功能：

源码浏览：载入程序源码后，可以在最左边的程序文件列表里面点击浏览源码，扫描出包含关键字的源码，也可以在下边的列表点击直接浏览。代码可以直接复制，或者选择用记事本打开。

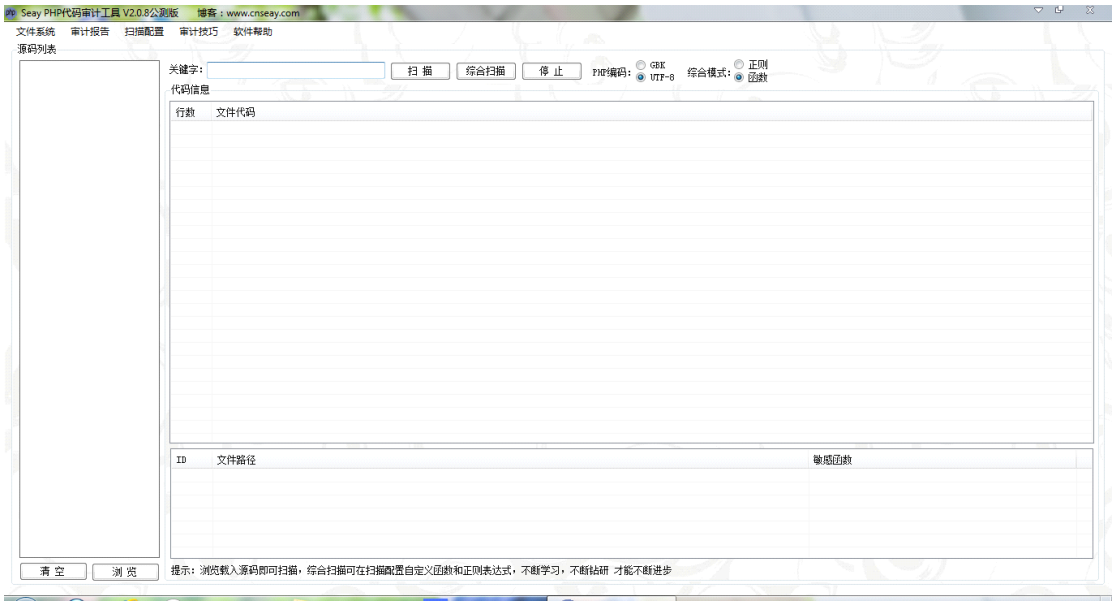
漏洞库：每次做代码审计可以在漏洞库建立一个审计文档，方便以后查阅、管理。

扫描配置：自定义扫描函数和正则表达式规则，针对要扫描的程序可以建立不同的规则，其中正则表达式扫描精确度更高。

审计技巧：收集了一下 PHP 代码审计的资料，提供给新手学习。

程序帮助：一些程序信息和作者信息

程序界面及版本



版本说明：

版本：V1.0
发布时间：2012 年 10 月 9 号
功能说明：只支持单个关键字扫描

版本：V2.0
发布时间：2012 年 10 月 13 号
功能说明：支持单个关键字、批量函数、批量正则表达式扫描、支持审计文档、函数、正则表达式管理

版本：V2.0.3
发布时间：2012 年 10 月 14 号
功能说明：在 2.0 版本的基础上修复 3 个逻辑 BUG

版本：V2.0.4
发布时间：2012 年 10 月 14 号
功能说明：在 2.0.3 版本的基础上修复 1 个逻辑 BUG

版本：V2.0.5
发布时间：2012 年 10 月 14 号
功能说明：在 2.0.4 版本的基础上修复 1 个 BUG，改变代码显示方式，优化正则模式扫描结果

版本：V2.0.6
发布时间：2012 年 10 月 17 号
功能说明：在 2.0.5 版本的基础上修复 1 个 BUG，增加函数库和表达式

版本：V2.0.7
发布时间：2012 年 10 月 27 号
功能说明：在 2.0.6 版本的基础上修复两个 BUG，增加最新版本检测功能，优化扫描速度，增加源码读取停止功能，目前 2.0.7 版本较稳定，动态黑盒漏洞扫描功能正在开发中。

版本：V2.0.8
发布时间：2012 年 11 月 5 号
功能说明：在 2.0.7 版本的基础上修复一个 BUG，大大优化扫描速度，增加扫描速度选择，优化代码，增加几个危险函数。

版本：V2.0.9
发布时间：2012 年 11 月 6 号
功能说明：在 2.0.8 版本的基础上增加区分大小写功能，增加函数导入导出功能，改变函数储存方式，修复审计文档错误问题。

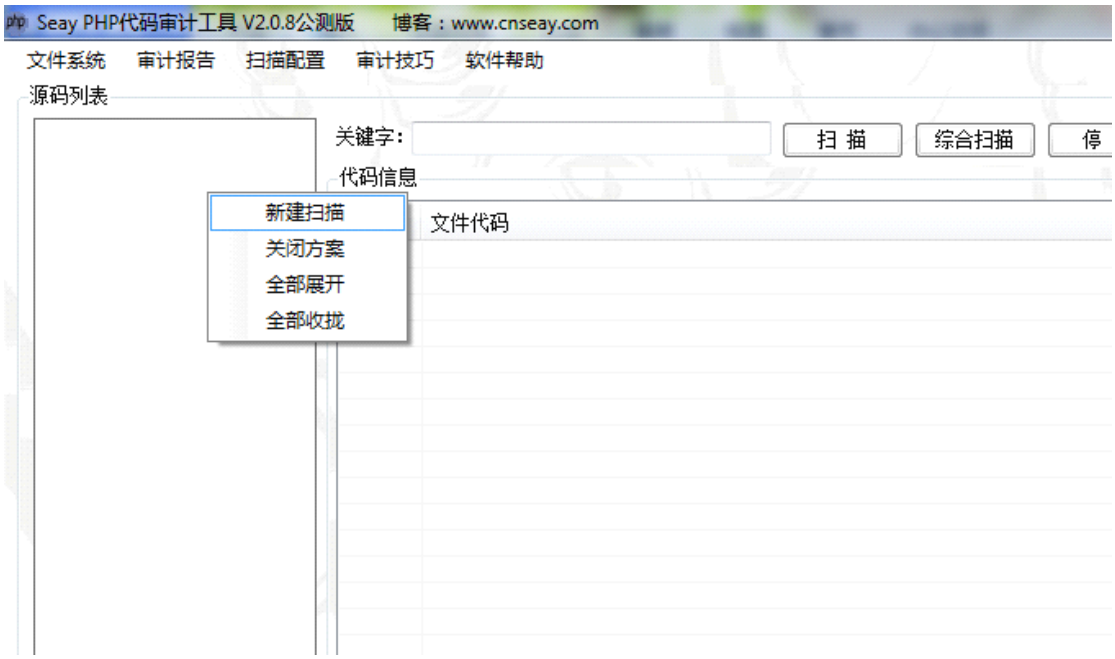
版本：V2.1
发布时间：2012 年 11 月 12 号
功能说明：在 2.0.9 版本的基础上大大优化源码读取速度，改用线程池，大大优化扫描速度，增加一些类似写字板的功能。可直接在本工具上编辑代码，打开、保存文件。

下个版本将推出更多新功能，敬请期待，愿更多朋友来一起完善它。

使用方法

一、**载入源码**：三个地方可以载入源码，分别在主界面的“浏览按钮”，左边文件列表框的右键“新建扫描”和菜单栏的文件系统里面的“新建扫描”。

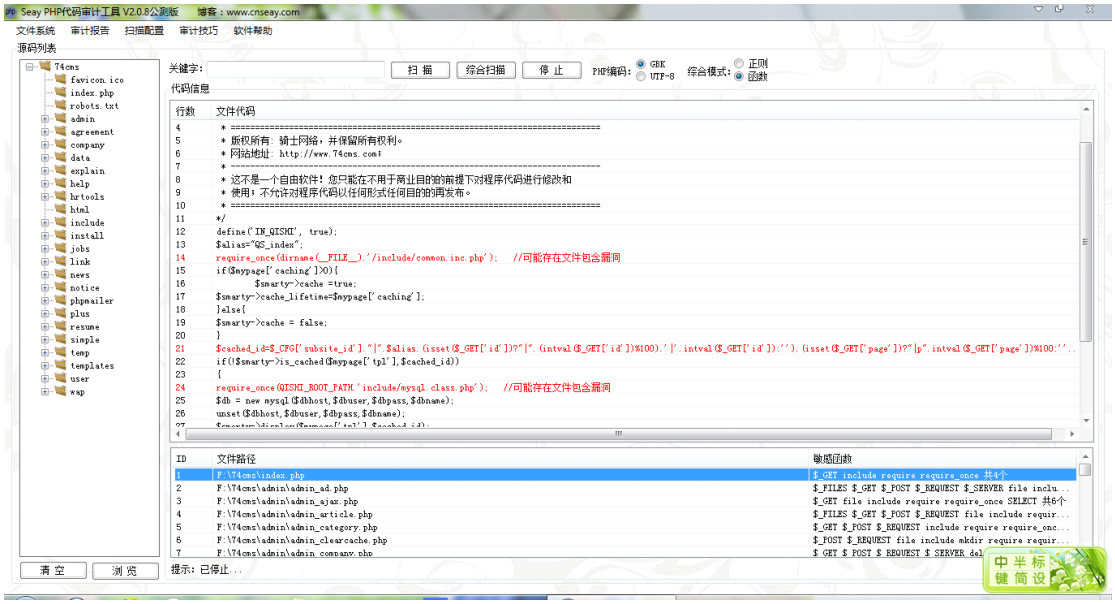
图：



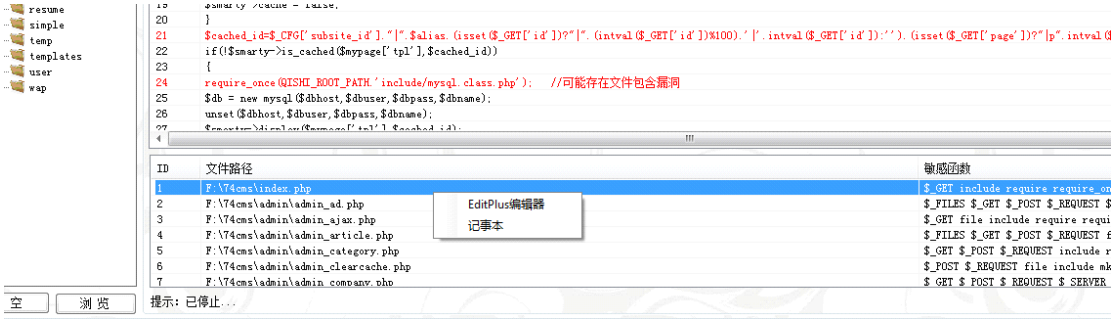
二、**开始扫描**：

载入程序后，我们可以输入关键字点击主界面“扫描”按钮即可，如果选择的是综合扫描，将自动调用综合模式里面选择的模式进行扫描，如函数模式、正则模式。

Seay PHP 代码审计工具 V2.1　博客：http://www.cnseay.com/

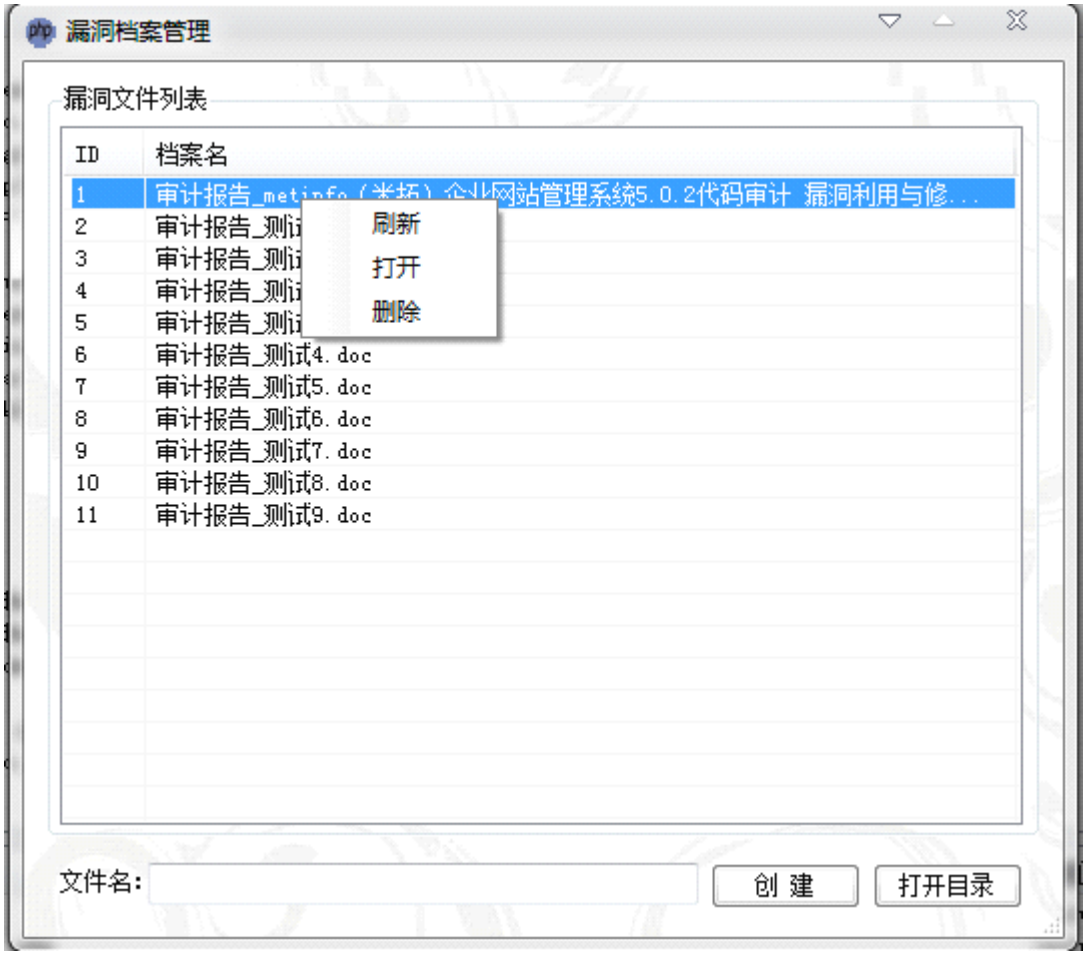


我们可以选择用自定义编辑器打开源码：



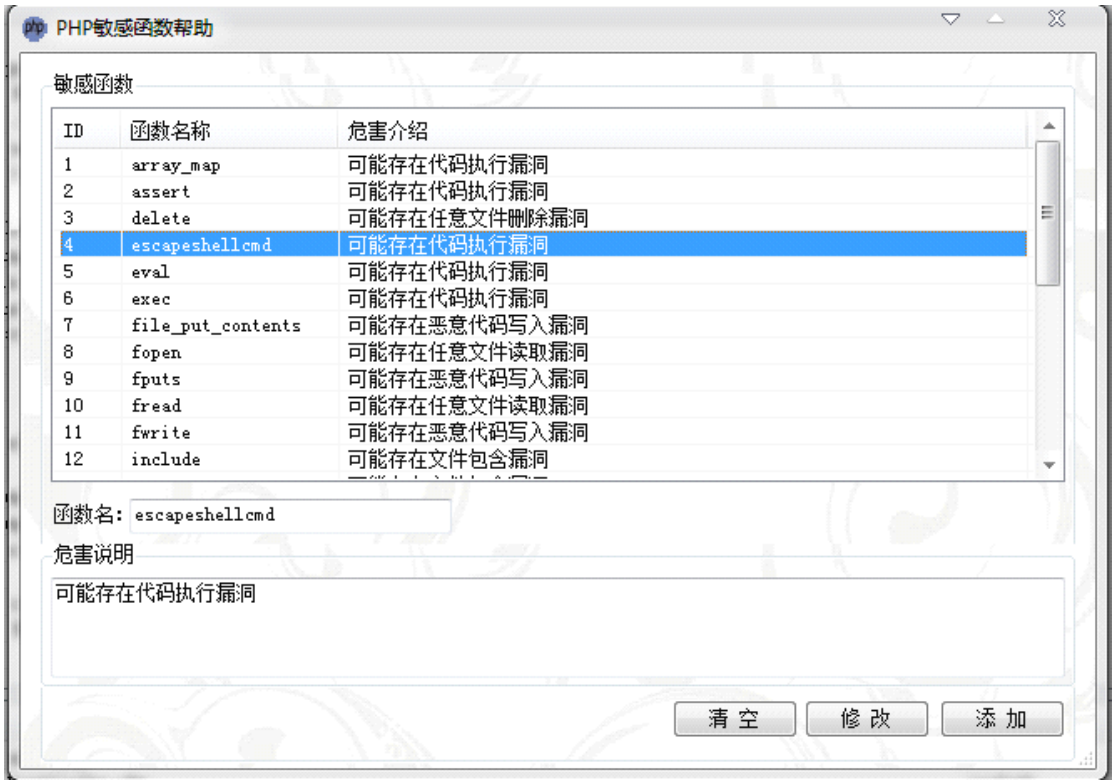
三、**漏洞仓库**：在这可以对审计文档进行管理。包括新建、打开、修改、删除操作。

图：

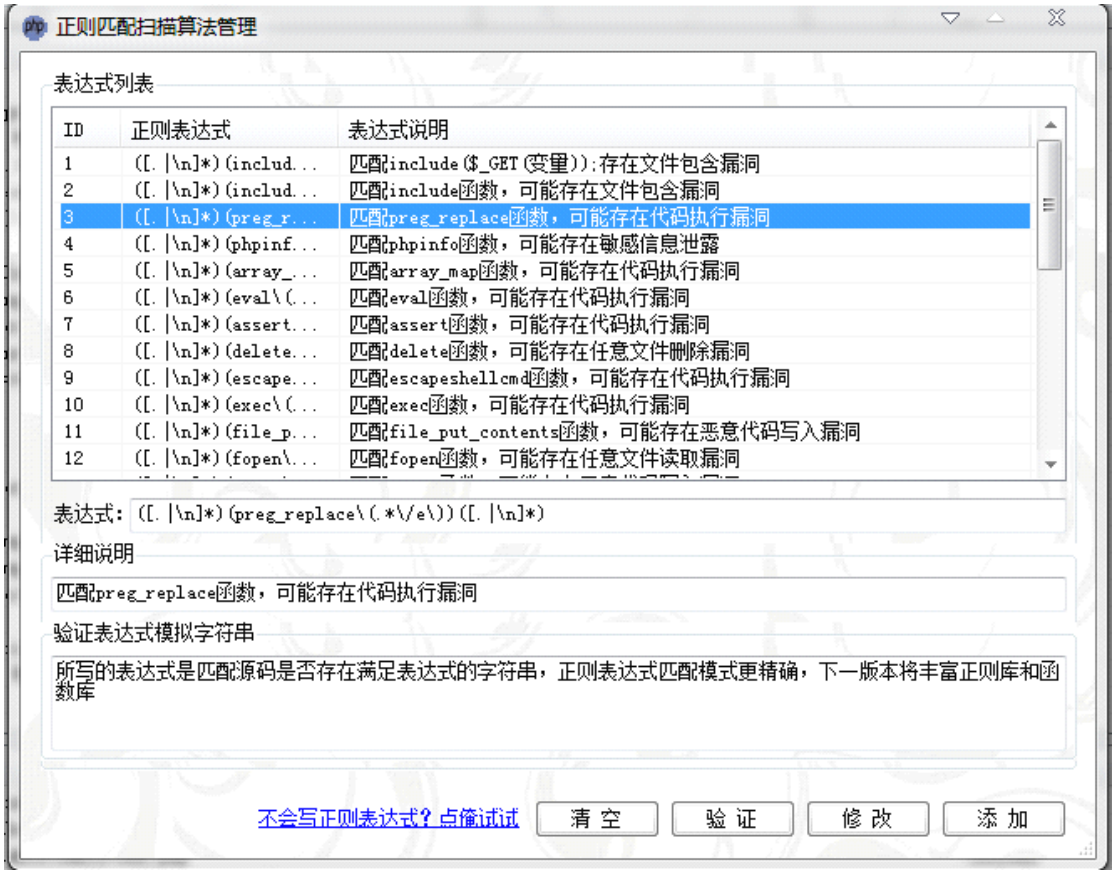


四、**扫描配置**：可以对综合扫描要用到的函数、正则表达式进行管理。包括查看、新增、修改、删除。

图：函数管理


PHP敏感函数帮助
敏感函数
ID 函数名称 危害介绍
1 array_map 可能存在代码执行漏洞
2 assert 可能存在代码执行漏洞
3 delete 可能存在任意文件删除漏洞
4 escapeshellcmd 可能存在代码执行漏洞
5 eval 可能存在代码执行漏洞
6 exec 可能存在代码执行漏洞
7 file_put_contents 可能存在恶意代码写入漏洞
8 fopen 可能存在任意文件读取漏洞
9 fputs 可能存在恶意代码写入漏洞
10 fread 可能存在任意文件读取漏洞
11 fwrite 可能存在恶意代码写入漏洞
12 include 可能存在文件包含漏洞
函数名: escapeshellcmd
危害说明
可能存在代码执行漏洞
清 空
修 改
添 加

图：正则表达式管理

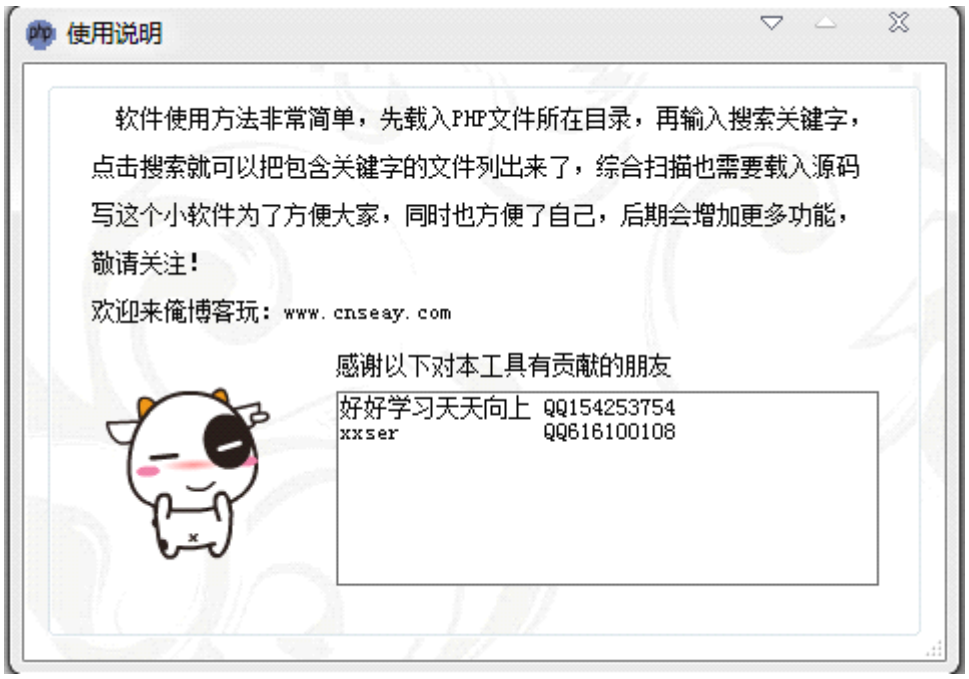

正则匹配扫描算法管理
表达式列表
ID 正则表达式 表达式说明
1 ([. |\n]*)(includ... 匹配include($_GET(变量));存在文件包含漏洞
2 ([. |\n]*)(includ... 匹配include函数，可能存在文件包含漏洞
3 ([. |\n]*)(preg_r... 匹配preg_replace函数，可能存在代码执行漏洞
4 ([. |\n]*)(phpinf... 匹配phpinfo函数，可能存在敏感信息泄露
5 ([. |\n]*)(array_... 匹配array_map函数，可能存在代码执行漏洞
6 ([. |\n]*)(eval\(... 匹配eval函数，可能存在代码执行漏洞
7 ([. |\n]*)(assert... 匹配assert函数，可能存在代码执行漏洞
8 ([. |\n]*)(delete... 匹配delete函数，可能存在任意文件删除漏洞
9 ([. |\n]*)(escape... 匹配escapeshellcmd函数，可能存在代码执行漏洞
10 ([. |\n]*)(exec\(... 匹配exec函数，可能存在代码执行漏洞
11 ([. |\n]*)(file_p... 匹配file_put_contents函数，可能存在恶意代码写入漏洞
12 ([. |\n]*)(fopen\... 匹配fopen函数，可能存在任意文件读取漏洞
表达式: ([. |\n]*)(preg_replace\(.*\/e\))([. |\n]*)
详细说明
匹配preg_replace函数，可能存在代码执行漏洞
验证表达式模拟字符串
所写的表达式是匹配源码是否存在满足表达式的字符串，正则表达式匹配模式更精确，下一版本将丰富正则库和函数库
不会写正则表达式？点俺试试
清 空
验 证
修 改
添 加

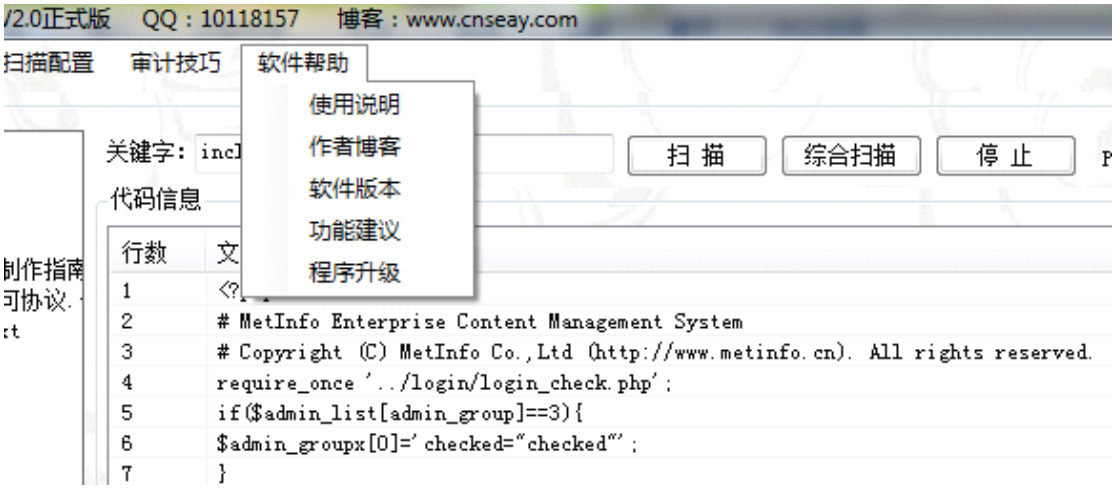
五、审计技巧：提供大量代码审计技巧资料，审计实例，供新手借鉴。

图 ：

名称	修改日期	类型	大小
asp代码审计.pdf	2012/8/18 星期...	Kankan PDF 图像	917 KB
LAMP安全审计之PHP代码审计_paper.p...	2012/8/18 星期...	Kankan PDF 图像	590 KB
PHP安全基础详解.pdf	2012/8/18 星期...	Kankan PDF 图像	356 KB
PHP安全问题：远程溢出、DoS、safe_...	2012/8/18 星期...	Kankan PDF 图像	172 KB
PHP程序的常见漏洞攻击分析.zip	2012/6/15 星期...	WinRAR ZIP 压缩...	8 KB
php代码审核.pdf	2012/6/15 星期...	Kankan PDF 图像	278 KB
PHP代码审计.pdf	2012/8/4 星期六 ...	Kankan PDF 图像	644 KB
PHP函数功能.txt	2012/8/18 星期...	文本文档	3 KB
PHP漏洞全解.pdf	2012/6/20 星期...	Kankan PDF 图像	145 KB
PHP漏洞全解1-9.pdf	2012/8/4 星期六 ...	Kankan PDF 图像	1,072 KB
web代码安全边缘性问题_.pdf	2012/6/15 星期...	Kankan PDF 图像	6,450 KB
WEB代码审计与渗透测试.ppt	2012/6/15 星期...	Microsoft Power...	2,453 KB
代码审计参考资料.txt	2012/8/4 星期六 ...	文本文档	1 KB
二次漏洞审计.pdf	2012/8/4 星期六 ...	Kankan PDF 图像	1,523 KB
高级PHP应用程序漏洞审核技术.pdf	2012/6/15 星期...	Kankan PDF 图像	155 KB
脚本安全的本质.pdf	2012/6/15 星期...	Kankan PDF 图像	142 KB
浅谈web漏洞挖掘—特殊变量fuzz.pdf	2012/6/15 星期...	Kankan PDF 图像	88 KB
上传代码.txt	2012/8/4 星期六 ...	文本文档	2 KB
上传验证绕过.pdf	2012/8/4 星期六 ...	Kankan PDF 图像	2,266 KB
实例分析讲解为您敲开代码审计大门.doc	2012/8/3 星期五 ...	Microsoft Word ...	411 KB
小脚本，大用场浅谈WEB攻击.pdf	2012/6/16 星期...	Kankan PDF 图像	291 KB
执行漏洞总结.zip	2012/6/15 星期...	WinRAR ZIP 压缩...	2 KB
重燃你的PHP安全之火.pdf	2012/7/9 星期一 ...	Kankan PDF 图像	155 KB

六、**软件帮助**：一些帮助信息，版本信息，有俩可爱的牛牛在动哦。





结束

好了，现在可以开始你的代码审计工作了，目前版本实现功能较少，下一版本主要致力于扫描的速度和精确度，请关注俺的博客 http://www.cnseay.com/ 获取最新版本。欢迎上报程序 BUG 和提出功能建议，本人联系方式：QQ10118157 邮箱：root@cnseay.com

By：Seay
于 2012 年 10 月 27