护卫神 • 挂马清理工具

版本：v2.0

编写：2013 年 06 月 19 日

一、软件主要功能介绍

1、本软件为护卫神旗下免费软件，您可以随便使用和传播，但请勿用于商业用途；

2、软件绿色免安装，支持多种 Windows 平台，移植性强；

3、文本文件挂马：自动识别文本的 GBK、UTF8 等编码，自动扫描清理，支持多种规则；

4、Access 数据库挂马：支持 Access 2000/2003 自动扫描清理，支持带日文的数据库，支持多种规则，也可清理数据库中的日文片假名字符；

5、SQL Server 数据库挂马：支持 SQL Server 2000/2005/2008 等，支持操作本地和远程数据库，支持多种规则；

6、MySQL 数据库挂马：支持 MySQL 4.X/5.X，支持操作本地和远程数据库，支持多种规则；

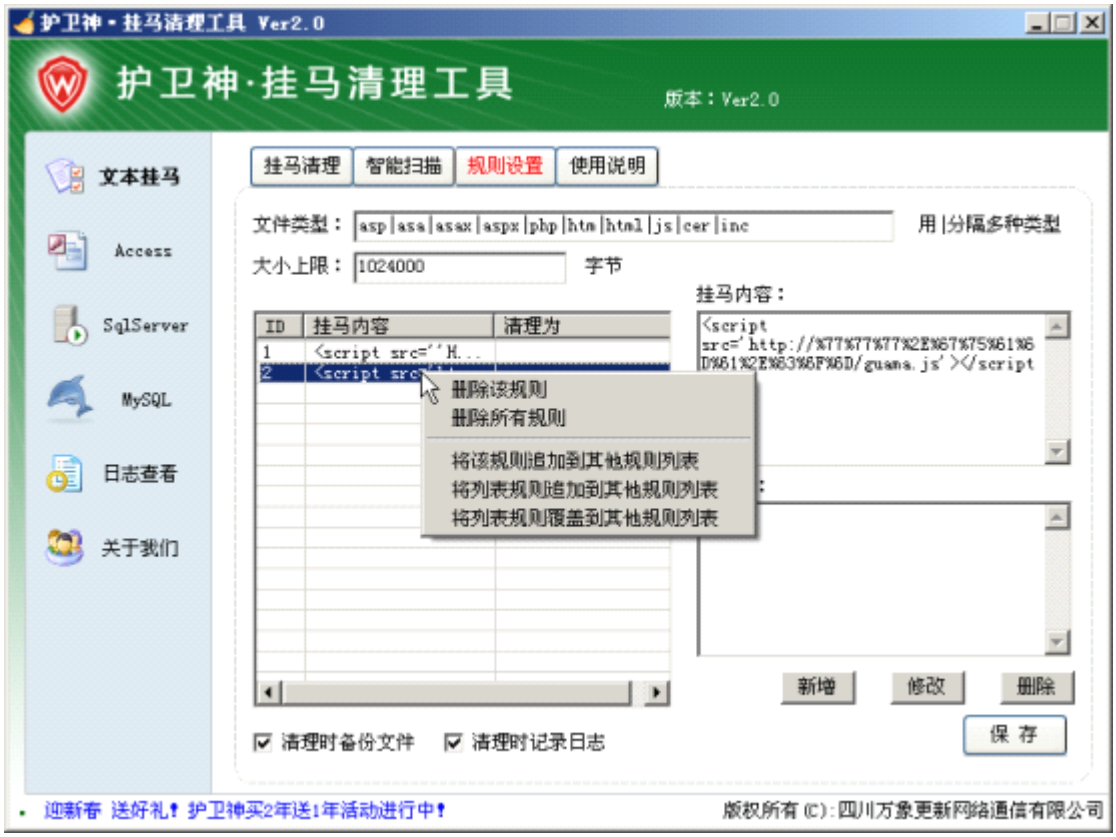
7、各规则之间可以相互转移，使用起来十分方便。

二、文本挂马清理

文本清理，支持对 GBK、GB2312、UTF8 等编码文件的清理。

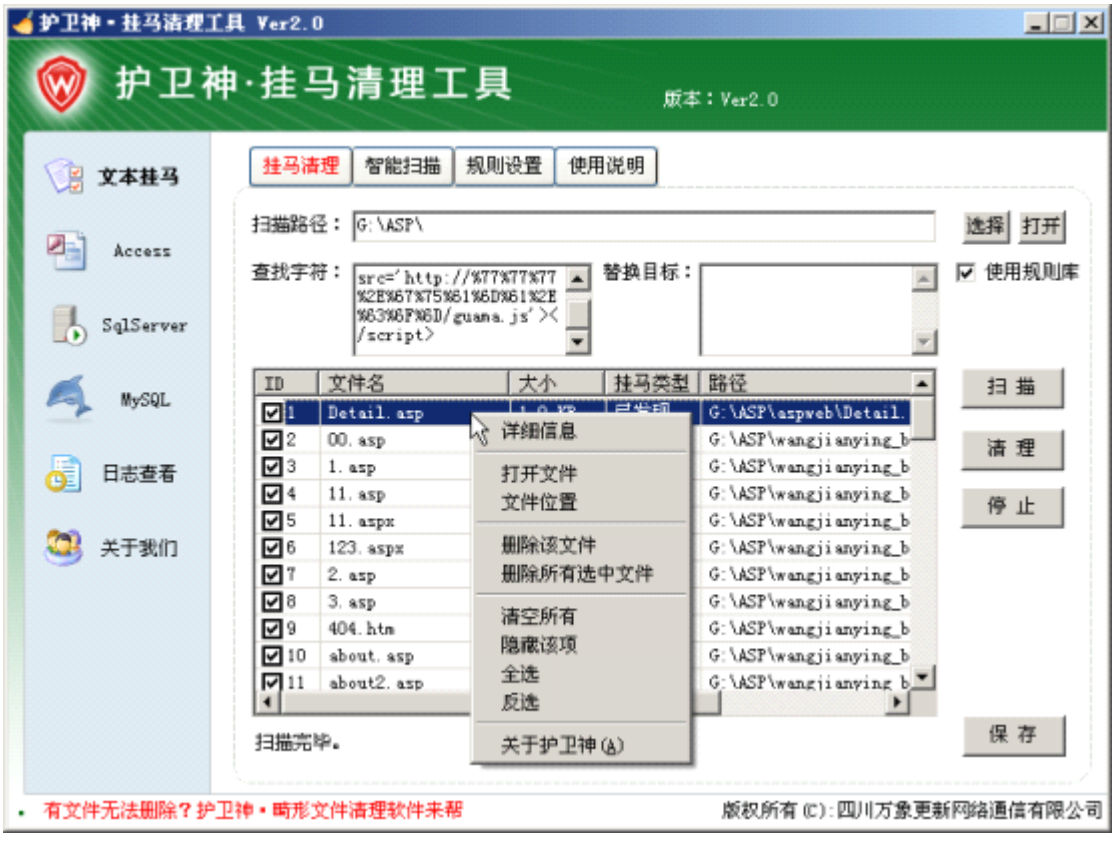
1、规则设置

a) 设置需要查杀的文件类型，一般如：asp|asa|asax|aspx|php|htm|html|js|cer|inc 等；
b) 可以设置单条或多条特征码规则，进行批量查找和清理；
c) 在挂马清理功能中，选择【使用规则库】，即可使用规则列表中的特征；
d) 选中【清理时备份文件】，将在执行清理时将文件备份到软件旁边的 backup 目录；
e) 选中【清理时记录日志】，将在执行清理时将操作日志记录到软件旁边的 log 目录。



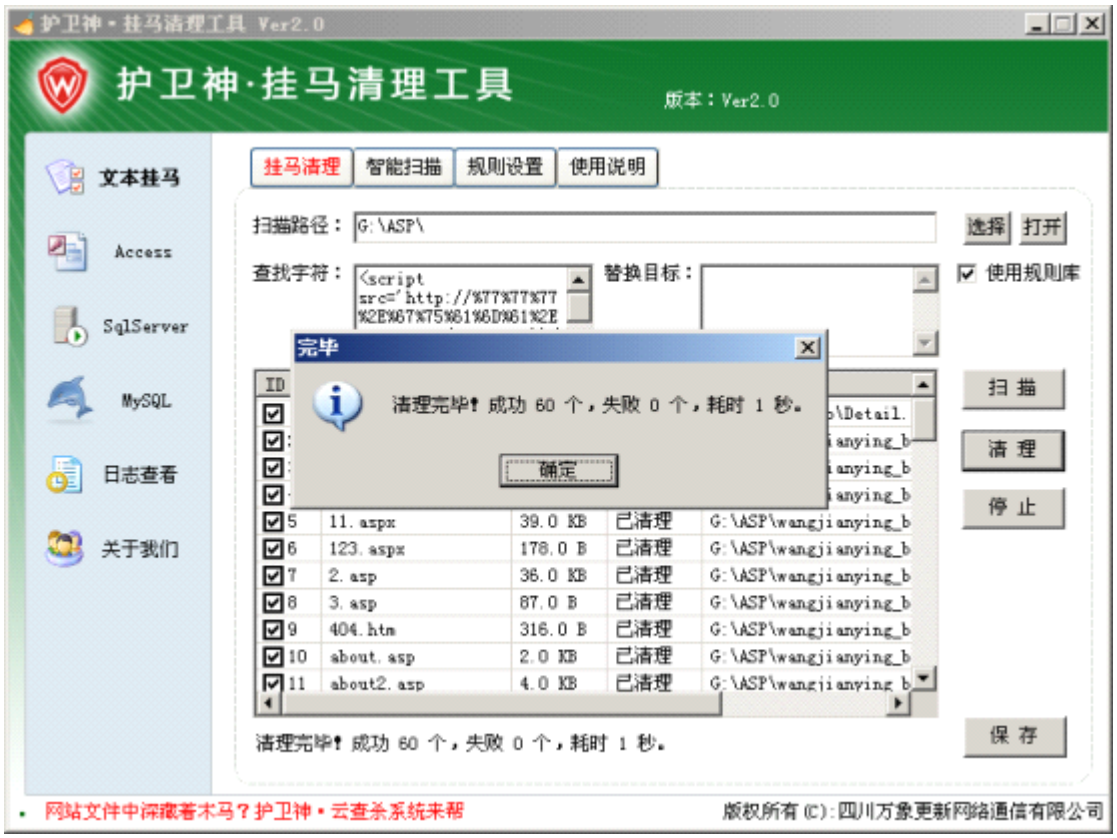
2、挂马清理

a) 选择网页存在的目录，如： D:\wwwroot ，点击【扫描】按钮开始扫描；



b) 根据扫描的结果，在结果列表上点击鼠标右键快捷菜单，或者点击右边的【清理】

按钮，进行清理；



c) 清理之后，如果在【规则设置】中选择了【清理时备份文件】，那么将会在 程序旁边的 backup 目录下找到备份的文件；

d) 如果选择了【清理时记录日志】，那么将会在程序旁边的 log 目录记录相应的日志。

3、智能扫描

a) 智能扫描，按照通常的挂马规则，如 script 和 iframe ，对指定目录下指定的文件类型按照规则进行通配查找，此功能在怀疑网站被挂马，但是无法确定挂马特征是什么的情况；

b) 扫描到之后，可以在结果列表中，点击鼠标右键菜单，对结果进行有针对性的处理；

c) 此方法已经内置了白名单，放行一些常用的格式，如天气预报、一些统计代码 等。

d) 注：智能扫描会有一定的遗漏和重复，仅作为辅助功能参考使用。

三、Access 数据库挂马清理：

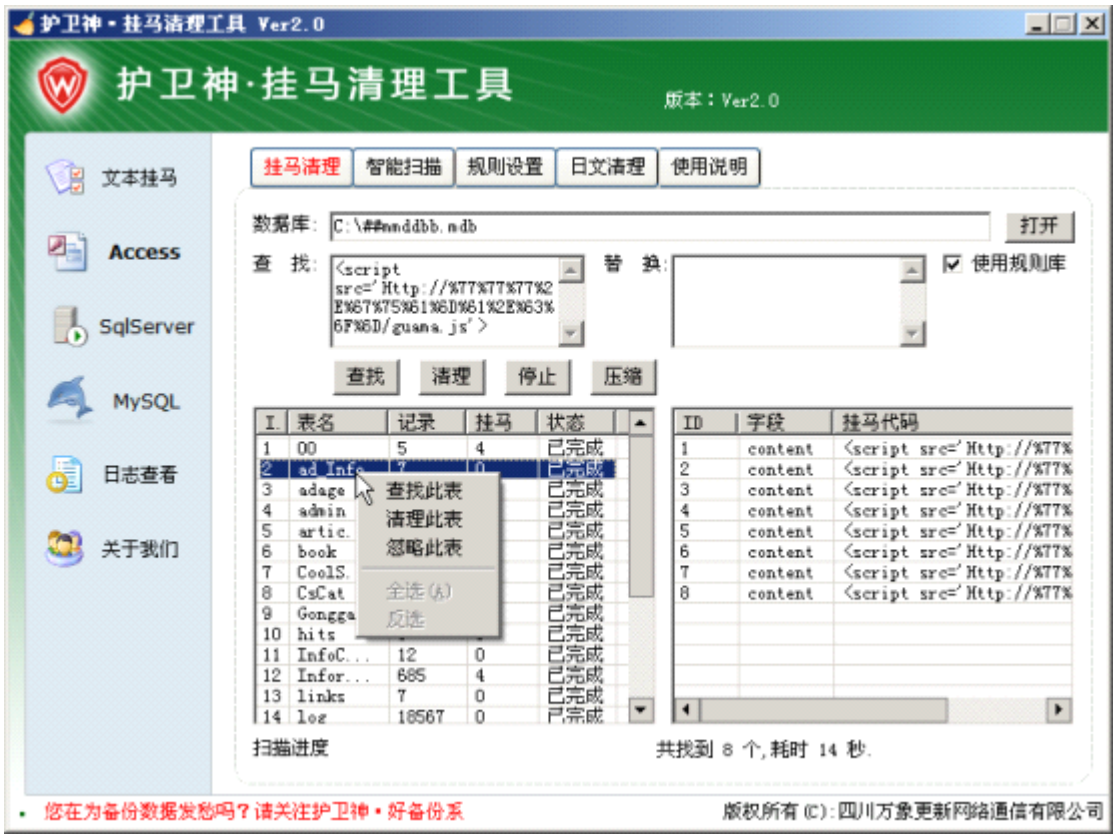
1、规则设置

a) 支持 Access 2000、2002、2003 版本格式，2007、2010 版需要下载对应的数据库驱动组件；
b) 可以设置多条规则，方便进行批量查找和清理；
c) 在挂马清理功能中，选择【使用规则库】，即可使用规则列表中的特征；
d) 注：该功能不区分大小写。

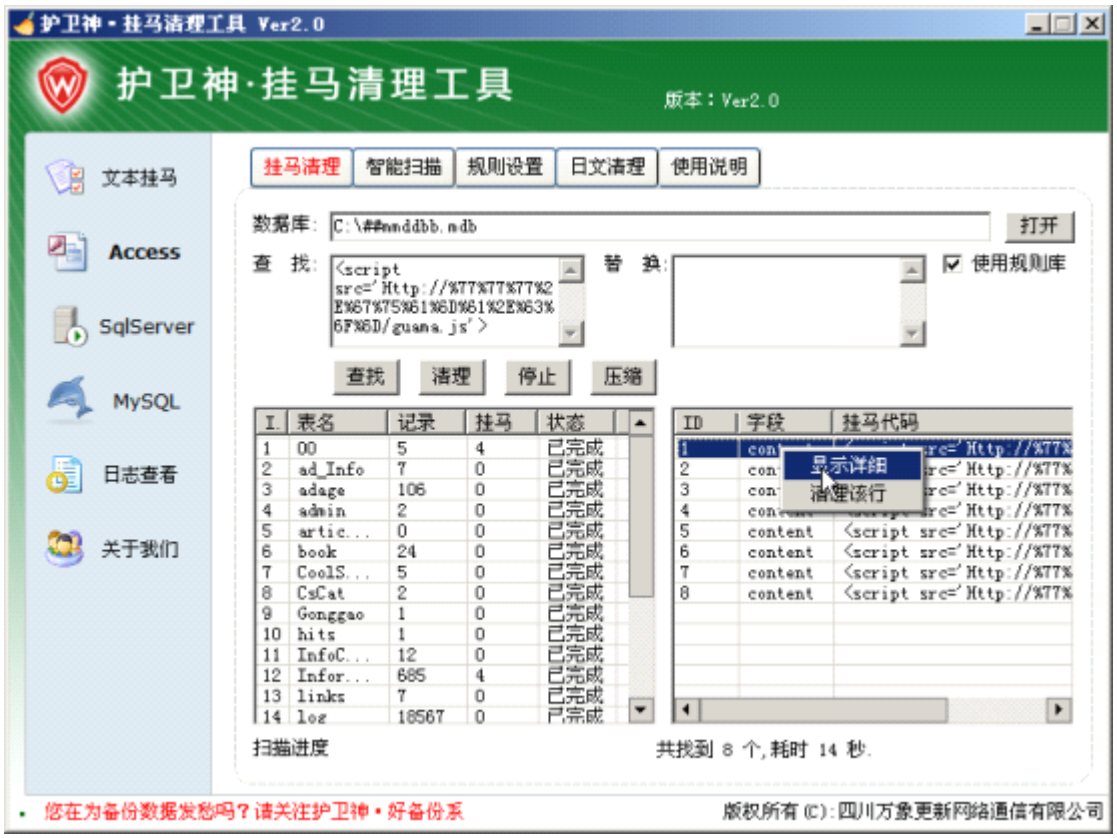
2、挂马清理

a) 选择或鼠标拖入 Access 数据库，系统会自动在左侧列出所有表；
b) 所有表列举完毕后，点击【查找】进行扫描，扫描结果会列在右边列表，可以双击查看，或者鼠标右键单独清理；

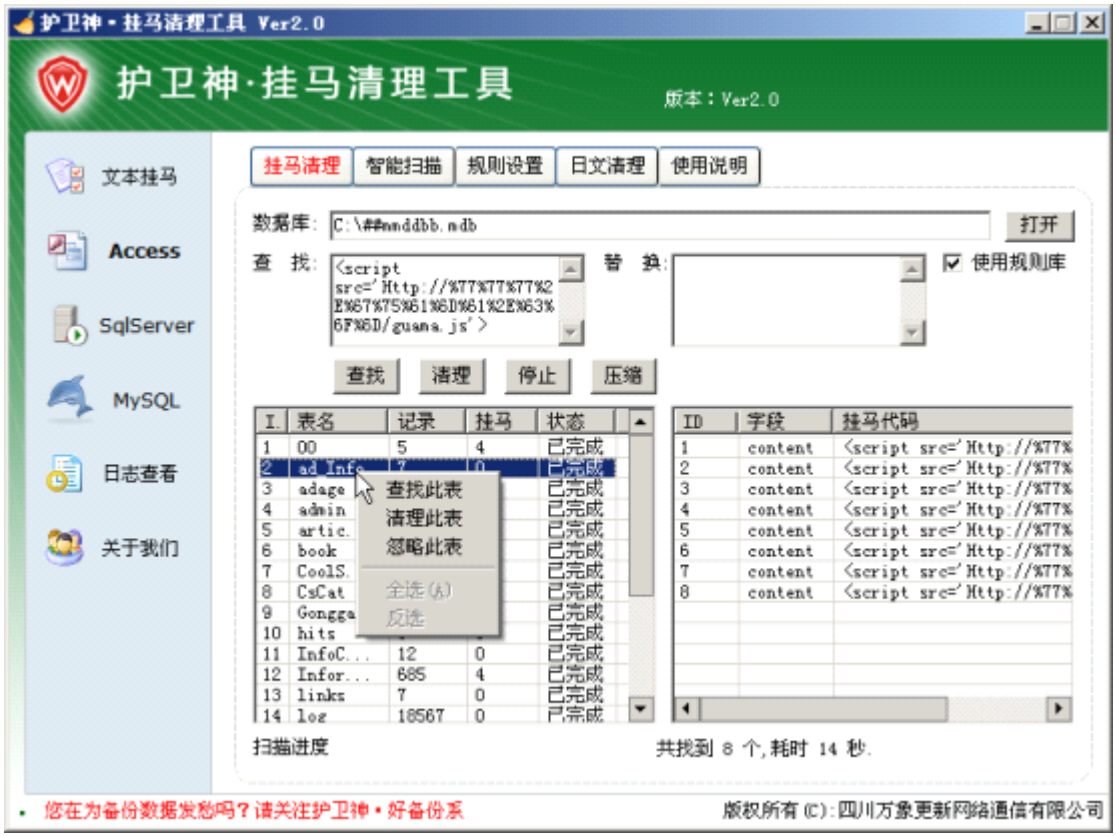
c) 可以单独查找某个表，也可以单独清理某个表，或者忽略某个表；



d) 在扫描结果列表中，可以点击右键或双击，查看某项详细内容，方便管理员审核：



e) 也可以点击【清理】按钮，直接一次性全部清理（注意：数据表若无主键，则会失败）；



3、智能扫描

a) 智能扫描，按照通常的挂马规则，如 script 和 iframe ，对指定表中的数据按照规则进行通配查找，此功能在怀疑网站被挂马，但是无法确定挂马特征是什么的情况；

b) 扫描到之后，可以在结果列表中，点击鼠标右键菜单，对结果进行有针对性的处理；

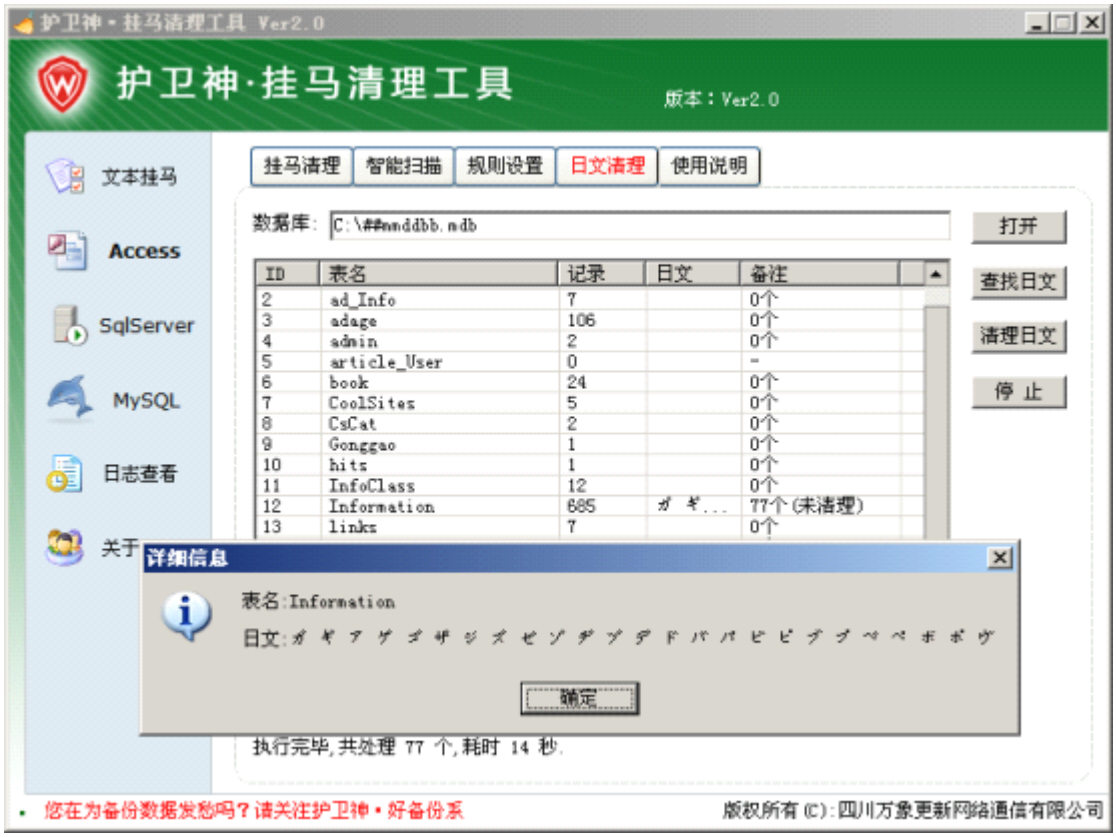
c) 此方法已经内置了白名单，放行一些常用的格式，如天气预报、一些统计代码 等。

d) 注：智能扫描会有一定的遗漏和重复，仅作为辅助功能参考使用。

e) 双击结果，可以查看详细的关联信息：

4、日文清理

由于 Access 本身的问题，如果您的 Access 数据库中含有日文字符，那么您的应用程序在使用过程中，可能会造成故障，因此可以用该功能清理掉数据库中的所有日文片假名字符。

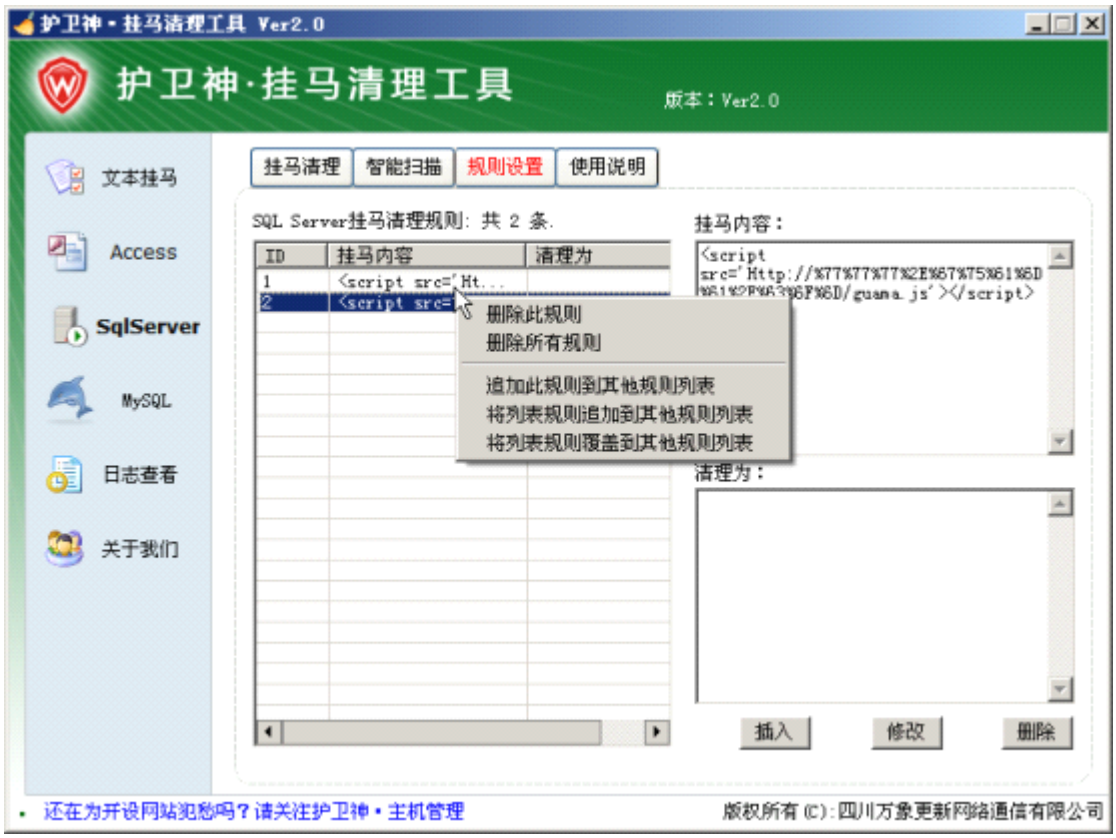


查找出来之后，点击【清理日文】即可完成清理。

四、SQL Server 数据库挂马清理

支持 MS SQL Server 2000/2005 版，其余没有测试。

1、规则设置



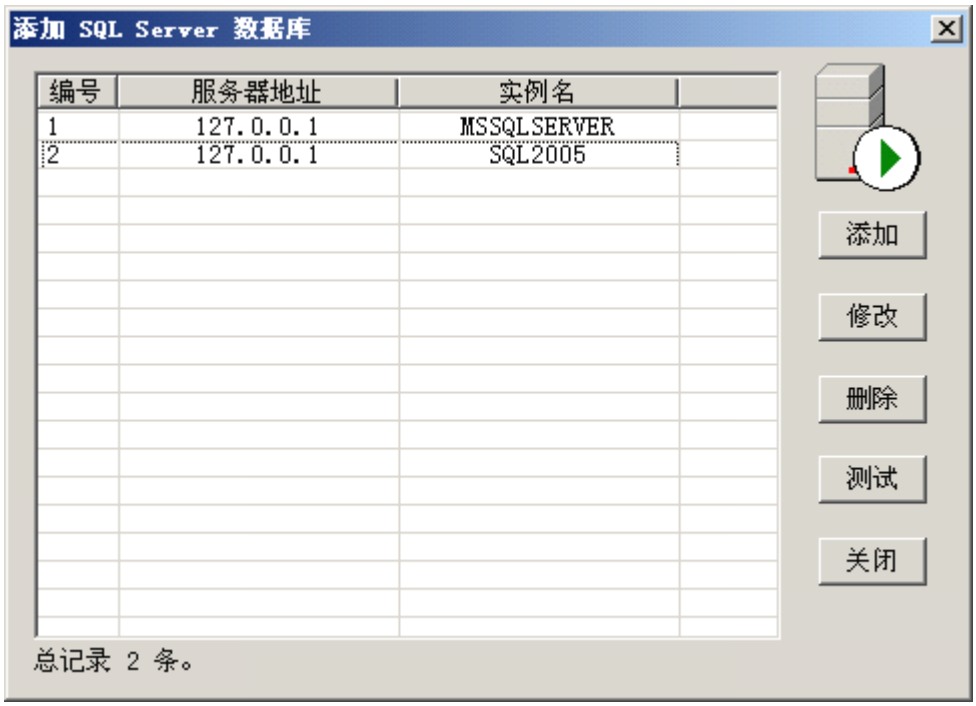
a) 添加 SQL Server 数据库，必须填写地址、实例、端口、管理账号等基本信息，然后测试连接以及保存；

b) 如果第一次使用并且计算机本身已经安装了 SQL Server，则系统会自动识别并添加默认连接；

c) 要增加，双击空白，或点击【添加】按钮，填写后保存即可；

d) 要修改，双击需要修改的项目，或者选中项目后点击右边的【修改】按钮，编辑后保存即可；

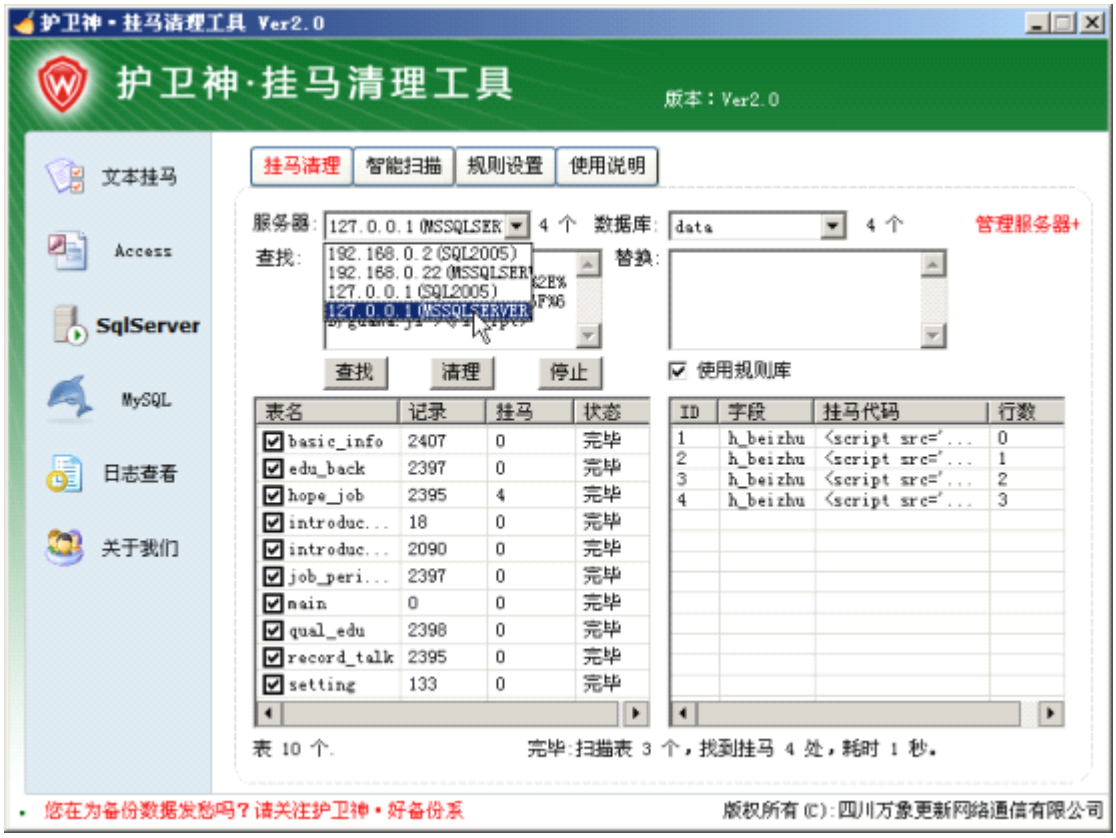
e) 如果要删除，则选中某项，点击【删除】即可删除。



2、挂马清理

a) 填写好连接项后，保存，打开【挂马清理】菜单；
b) 选择需要查杀的服务器，系统会自动进行连接，若连接信息填写正确，会显示连接成功，此时在数据库中就会显示所有的用户数据库；
c) 选中需要查找的数据库，如“data”，软件会将该数据库的所有用户表列表到左侧的列表框中；
d) 点击【查找】按钮，软件将按照指定查杀规则进行扫描，并将扫描结果列到右侧的列表框中；
e) 用户点击各项，右键查看详细挂马信息，确认无误后，点击【清理】按钮，或者右键菜单的【清理】菜单清理；
f) 双击扫描结果，则会提示对应的关联信息，方便管理员审核；

g) 注：该功能不区分大小写。



3、智能扫描

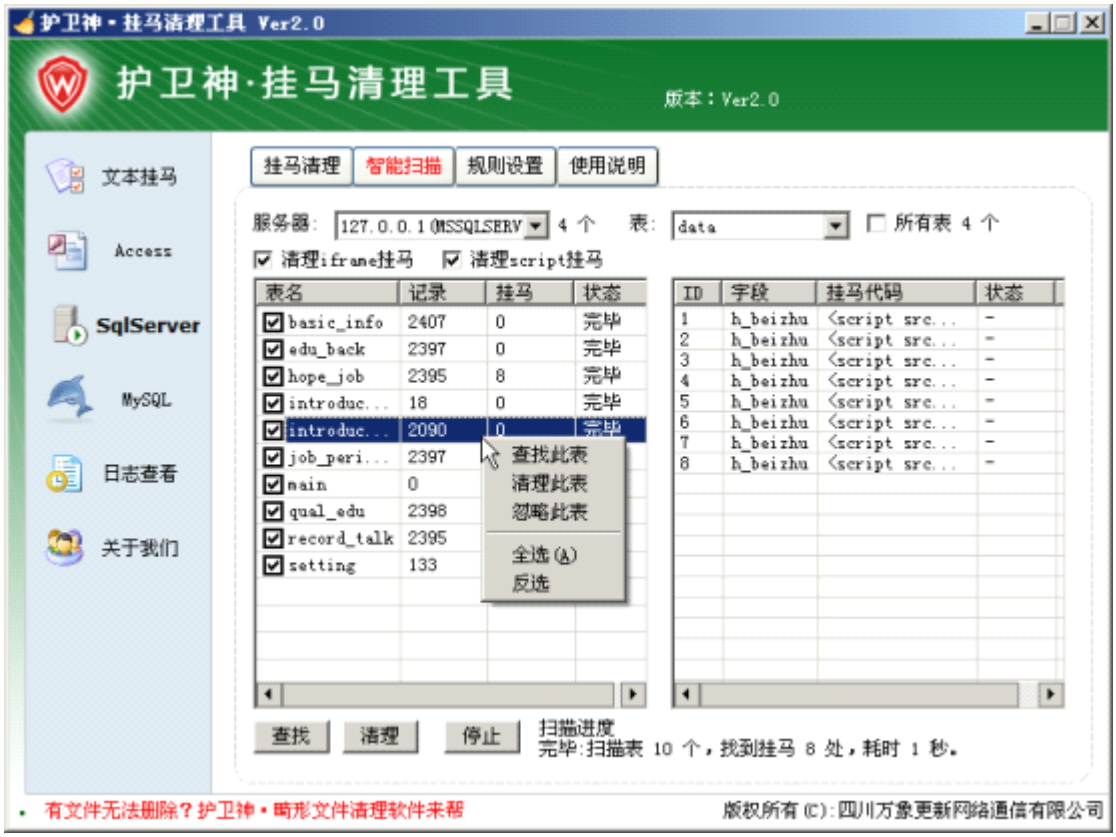
a) 智能扫描，按照通常的挂马规则，如 script 和 iframe ，对指定表中的数据按照规则进行通配查找，此功能在怀疑网站被挂马，但是无法确定挂马特征是什么的情况；

b) 扫描到之后，可以在结果列表中，点击鼠标右键菜单，对结果进行有针对性的处理；

c) 此方法已经内置了白名单，放行一些常用的格式，如天气预报、一些统计代码 等；

d) 双击扫描结果，则会提示对应的关联信息，方便管理员审核；

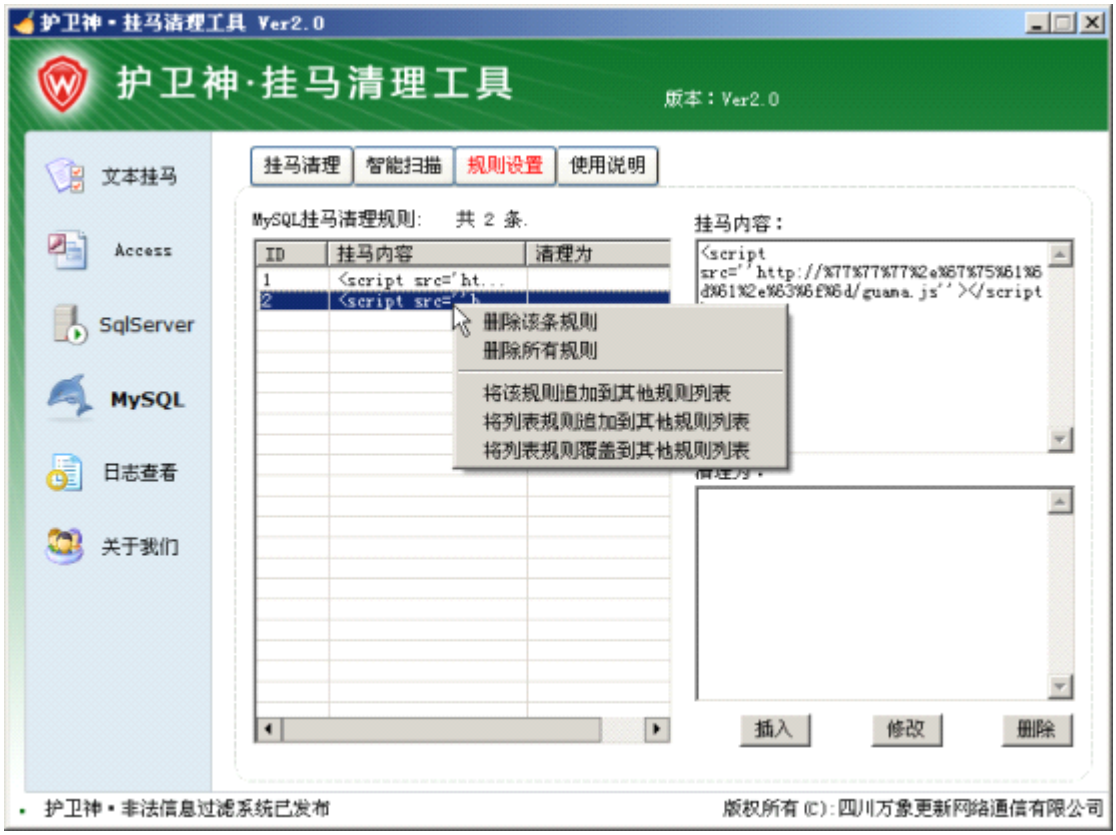
e) 注：智能扫描会有一定的遗漏和重复，仅作为辅助功能参考使用。


护卫神·挂马清理工具 Ver2.0
护卫神·挂马清理工具
版本：Ver2.0
文本挂马
Access
SqlServer
MySQL
日志查看
关于我们
挂马清理
智能扫描
规则设置
使用说明
服务器: 127.0.0.1(MSSQLSERV 4 个
表: data
所有表 4 个
清理iframe挂马
清理script挂马
表名 记录 挂马 状态
basic_info 2407 0 完毕
edu_back 2397 0 完毕
hope_job 2395 8 完毕
introduc... 18 0 完毕
introduc... 2090 0 完毕
job_peri... 2397
main 0
qual_edu 2398
record_talk 2395
setting 133
查找此表
清理此表
忽略此表
全选(A)
反选
ID 字段 挂马代码 状态
1 h_beizhu <script src... -
2 h_beizhu <script src... -
3 h_beizhu <script src... -
4 h_beizhu <script src... -
5 h_beizhu <script src... -
6 h_beizhu <script src... -
7 h_beizhu <script src... -
8 h_beizhu <script src... -
查找
清理
停止
扫描进度
完毕:扫描表 10 个，找到挂马 8 处，耗时 1 秒。
有文件无法删除？护卫神·晴彤文件清理软件来帮
版权所有(C):四川万象更新网络通信有限公司

五、MySQL 数据库挂马清理

支持 MySQL 4.X/5.X 版本，其余未测试。

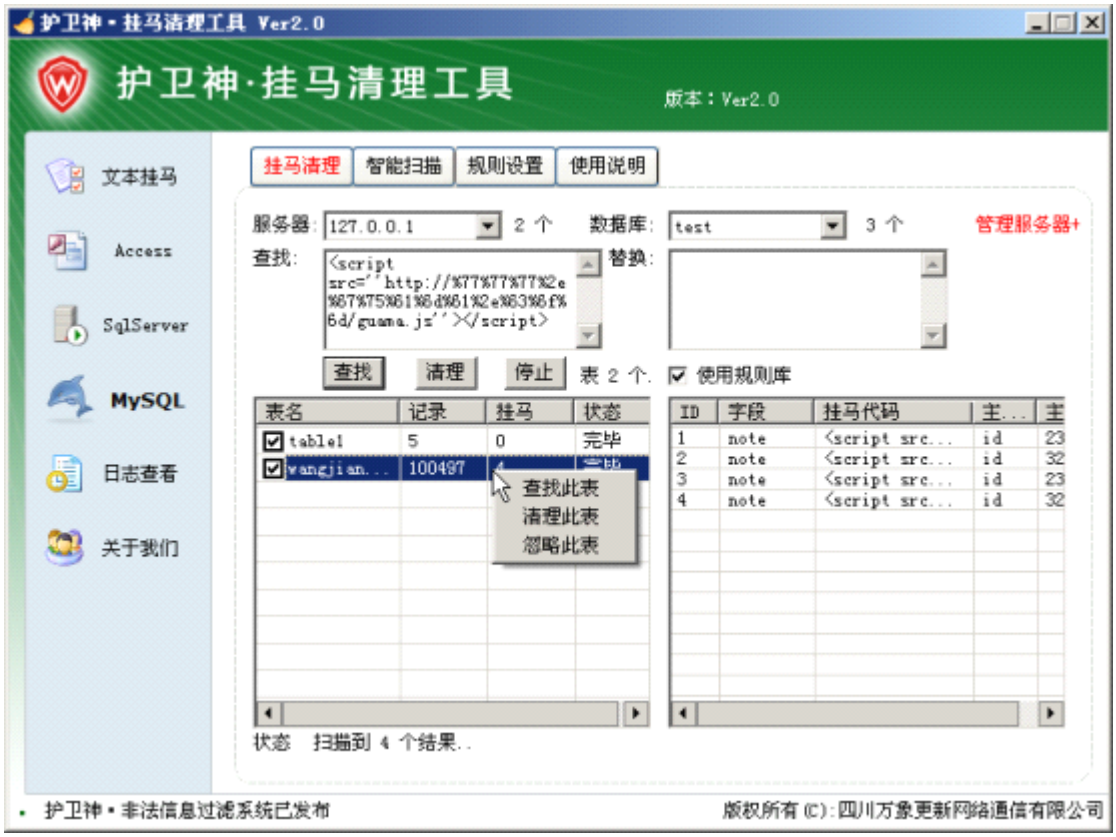
1、规则设置



a) 添加 MySQL 数据库，必须填写地址、端口、管理账号等基本信息，然后测试连接以及保存；
b) 如果要修改，双击某项弹出编辑框，编辑后，点击【保存】按钮保存即可；
c) 如果要增加，点击【添加】按钮，弹出添加对话框，填写信息后点击【保存】即可；
d) 如果要删除，则选中某项，点击【删除】即可删除。

2、挂马清理

a) 填写好连接项后，保存，打开【挂马清理】菜单；
b) 选择需要查杀的服务器，系统会自动进行连接，若连接信息填写正确，会显示连接成功，此时在数据库中就会显示所有的用户数据库；
c) 选中需要查找的数据库，如“test”，软件会将该数据库的所有用户表列表到左侧的列表框中；
d) 点击【查找】按钮，软件将按照指定查杀规则进行扫描，并将扫描结果列到右侧的列表框中；
e) 用户点击各项，右键查看详细挂马信息，确认无误后，点击【清理】按钮，或者右键菜单的【清理】菜单清理；
f) 双击扫描结果，则会提示对应的关联信息，方便管理员审核；
g) 注：该功能不区分大小写。



3、智能扫描

a) 智能扫描，按照通常的挂马规则，如 script 和 iframe ，对指定表中的数据按照规则进行通配查找，此功能在怀疑网站被挂马，但是无法确定挂马特征是什么的情况；
b) 扫描到之后，可以在结果列表中，点击鼠标右键菜单，对结果进行有针对性的处理；
c) 此方法已经内置了白名单，放行一些常用的格式，如天气预报、一些统计代码 等；
d) 双击扫描结果，则会提示对应的关联信息，方便管理员审核；
e) 注：智能扫描会有一定的遗漏和重复，仅作为辅助功能参考使用。

六、日志管理

日志查看：能够详细记录每一步的操作日志，方便检查。

七、联系我们

官方网站: http://www.huweishen.com

24 小时服务热线：028-65886111

我们提供的不只是软件，还有丰富的技术服务。如有问题或建议，请登录我们的论坛: http://home.huweishen.com/

八、附：关于护卫神

护卫神成立于 2004 年，是国内最大的服务器软件供应商，隶属于四川万象更新网络通信有限公司。

自成立以来，护卫神一直专注服务器领域；拥有强大的开发团队和技术团队，并拥有自己的核心技术。

经过 8 年的技术沉淀，我们积累了丰富的服务器管理经验；凭借强大的研发实力，截止 2013 年 6 月，护卫神已开发出 20 多款服务器应用软件，完全免费开放，帮助广大管理员更好的管理服务器。

公司配置了完善的客服、技术、开发等部门，能为用户提供强大的技术支持和优质的售后服务。

根据公司强大的技术和实力，我们的“护卫神 • 安全套装”产品上线，从根本上杜绝网站挂马问题。

另外，我们开展的服务器代维服务，也深受广大企业用户喜爱和推广，邀您共享。

公司网址：www.huweishen.com

四川万象更新网络通信有限公司
2013 年 06 月 19 日