

网站安全狗 Windows-IIS 版 使用教程



厦门服云信息科技有限公司

leading provider of cloud security services and solutions.

目录

网站安	そ全狗 Windows-IIS 版	1
目	큧	2
1.	软件说明	5
2.	软件安装	5
3.	软件卸载	8
4.	软件运行	12
	4.1 系统要求	12
	4.2 系统运行	12
5.	软件升级	13
6.	软件功能	15
	6.1 网马查杀	15
	6.1.1 查杀方式	16
	6.1.2 网马上报	18
	6.1.3 信任文件上报	18
	6.1.4 隔离文件查看	19
	6.1.5 网马扫描日志	20
	6.1.6 网马扫描结果处理	22
	6.1.7 网马扫描功能设置	22
	6.2 网站防护	23
	6.2.1 漏洞防护	25
	6.2.1.1 HTTP 安全检测	25
	6.2.1.2 上传防护	28
	6.2.2文件防护	29
	6.2.2.1 浏览防护	29
	6.2.2.2 短文件名防护	
	6.2.2.3 目录漏洞防护	
	6.2.2.4 禁止浏览畸形文件	

	6.2.3 行为防护	32
	6.2.3.1 危险组件防护	32
	6.2.3.2 敏感函数防护	34
	6.2.3.3 禁止 IIS 执行程序	
	6.2.3.4 一句话后门防护	
	6.2.3.5 TCP/UDP 发包	43
(6.3 资源防护	44
	6.3.1 内容防护	44
	6.3.1.1 网站后台防护	44
	6.3.1.2 响应内容防护	46
	6.3.2 资源防护	48
	6.3.2.1 资源防盗链	48
	6.3.2.2 特定资源防护	50
	6.3.2.3 环境信息隐藏	52
	6.3.3 流量防护	54
	6.3.3.1 CC 攻击防护	54
	6.3.3.2 下载控制	57
(6.4 IP 黑白名单	
	6.4.1 IP 白名单	60
	6.4.2 IP 黑名单	63
	6.4.2.1 IP 黑名单	64
	6.4.2.2 IP 临时黑名单	65
	6.4.3 爬虫白名单	67
(6.5 防护日志	67
(6.6安全工具	70
	6.6.1 网站加速	70
	6.6.2 网站监控	72
	6.6.2.1 流量监控	73
	6.6.2.2 CPU 监控	74
	6.6.3 批量替换	74

	6.6.4 dede 专杀	76
	6.7 防护等级	77
	6.8 辅助功能	79
	6.8.1版本信息	79
	6.8.2登录	79
	6.8.3皮肤	
	6.8.4系统设置	84
	6.8.4.1 系统常规设置	84
	6.8.4.2 网马扫描设置	
	6.8.4.3 漏洞防护设置	94
	6.8.4.4 文件防护设置	95
	6.8.4.5IP 黑白名单设置	
	6.8.4.6 防护日志设置	97
	6.8.5 防护状态	
	6.8.6 拦截攻击	99
	6.8.7 服务器安全狗	
7.	关于我们	
	7.1 关于我们	
	7.2 联系我们	
	7.2.1 官方网站	
	7.2.2 官方论坛	
	7.2.3 服务与支持	
	7.2.4 市场与合作	

1. 软件说明

网站安全狗系统(IIS版)(以下简称网站安全狗)是为 IDC 运营商、虚拟主机服务商、 企业主机、服务器管理者等用户提供服务器安全防范的实用系统,是集网站内容安全防护、 网站资源防护及网站流量防护功能为一体的服务器工具。作为服务器安全专家,这套软件已 通过公安部信息安全产品检测中心的检测,并获检验合格证书。

功能涵盖了网马查杀、主动防护、.Net设置、流量防护、资源防护、网站加速、网站 监控、IP黑白名单管理以及防护日志查询等模块,能够为用户提供实时的网站安全防护, 避免各类针对网站的攻击所带来的危害。

2. 软件安装

网站安全狗的安装方法与普通应用程序的安装方法相似,安装到带有 IIS 的服务器上即可防护。安装过程需要几分钟时间,请耐心等待。

请根据安装向导提示操作,具体操作如下:

步骤1. 下载软件安装包(exe 安装包),下载得到 safedogwzIIS. exe 安装包。

步骤 2. 双击下载后的安装包 "safedogwsIIS. exe",按照安装向导提示,一步步执行 安装操作,如下图 2.1 所示。



图 2.1 安装向导

步骤 3. 完成安装后,出现如下提示,如下图 2.2 所示。点击完成,即可进入网站安全 狗主界面。



图 2.2 安装成功提示

✤ 注意事项

(1) 如果服务器有麦咖啡(Mcafee)软件的,请先停止防护功能。

(2) 尽量不要把程序安装在系统盘,以免受杀毒软件的文件夹监控的影响。

(3) 若是 IIS7 以上的版本,请确保安装 IIS6 管理兼容性,否则 IIS 插件会安装 失败。

(4) 如果未安装 IIS 服务器,系统会弹出如下图 2.3 所示对话框。

9 网站安全狗(IIS版) V4.(0 正式版 安
您机器上未装有IIS服务。	

图 2.3 未安装 IIS 提示

(5) 若上一次卸载有保留历史记录,则会弹出如下图 2.4 所示对话框。

◎ 网站安全狗(IIS版)	V4.0 正式版 安装向导	X
2 检测到上个	版本的网马查杀和隔离记录,是否这	个版本使用?
	是(Y)	否(N)

图 2.4 检测到网马查杀、隔离记录提示

3. 软件卸载

卸载过程需要几分钟时间,请耐心等待。

步骤1. 关闭"网站安全狗"所有程序。

步骤 2. "开始"→"程序"→"网站安全狗"→"卸载网站安全狗"。如下图 3.1 所示。

🏉 Internet Explorer 🏈 Internet Explorer (64 位) 🚰 Windows Update 🖃 Windows 联系人	
	Administrator 文档
 ◎ 网站安全狗(IIS版) ○ 网站安全狗主页 ◎ <u>卸载网站安冷狗(IIS版)</u> ● 方案和升级 	计算机 网络
 ▶ 服务器安全狗 ▶ 附件 ▶ 管理工具 > 白油 	控制面板 管理工具 ▶
	帮助和支持 运行
▲ 返回	
开始搜索	0 🔒 🔸

图 3.1 软件卸载



步骤 3. 按照提示一步步执行卸载操作。如下图 3.2、图 3.3 所示。

图 3.2 确认卸载提示



图 3.3 卸载选项

步骤4. 卸载完成后,会出现以下提示框,如下图3.4 所示。



图 3.4 卸载成功提示

步骤 5. 点击卸载完成,完成软件卸载,或点击我要吐槽,前往用户卸载反馈页面 提交您的卸载反馈。

◆ 在卸载过程中,会询问用户是否保留网马扫描的历史记录,用户可根据需要选择是否保留,建议您保留历史记录以备下个版本使用。如下图 3.5 所示。

网站安全狗(IIS版) V4.0	正式版 卸载	X
2 是否保留网	马扫描及隔离历史记录,以备下	个版本使用?
	是①	否(N)

图 3.5 保留历史记录提示框

4. 软件运行

4.1 系统要求

系统硬件要求如下表 4.1 所示。

表 4.1 硬件需求表

参数	基本配置	推荐配置
CPU	Pentium II 处理器及以上	Pentium III 处理器及以上
内存	>256MB	>512MB
硬盘	剩余空间>100MB	剩余空间>1GB

运行环境的要求如下表 4.2 所示。

表 4.2 运行环境需求表

参数	基本配置
操作系统	微软服务器操作系统
IIS	IIS5.0以上版本

4.2 系统运行

软件运行自动区分 32 位系统或者 64 位系统,无需您的介入。直接双击安装后的网站安 全狗快捷方式,即可打开界面,如下图 4.1 所示。

 ● 网站安全狗(IIS版) V4.0 正式版 ● 未登录 	$\Im \equiv - \times$
上次扫描未发现风险,请保持 上次扫描时间:2016-06-14 11:28:30 立即扫描	1天 持续保护网站 0 个
◎防护等级自定义 ② 拦截攻击 0次	IP黑白名単
	服务器安全狗 🔂 工具箱

图 4.1 软件主界面

5. 软件升级

网站安全狗(IIS版)软件有更新版本的时候,用户通过如下所示的设置可以选择软件自动更新或者提醒模式更新。

步骤1. 打开"网站安全狗"主页面,单击"检查更新",如下图5.1 所示:

● 网站安全狗 (IIS版) V4.0 正式版 ● 未登录	$\Im \equiv - \times$
 ③ 主程序版本: V4.0.14139 ② 四马库版本: 2016-06-12 ⑥ 松宮更新 辺风险,请保持 	1工
上次扫描时间:2016-06-14 11:28:30 立即扫描	上入 持续保护网站 0 个
◎防护等级自定义 ② 拦截攻击 0次	IP黑白名单
	务器安全狗

图 5.1 检查更新 1

也可以通过设置界面检查更新,点击"检测更新",如下图 5.2 所示:

♥ 网站安全狗 (IIS版) V4.0 正式版 ④ 未登录 上次扫描未发现风险,请保持	 ・ ・ × ・ ・ ・ ・ ・ ・
上次扫描时间: 2016-06-14 11:28:30 立即扫描	本 へ
● 防护等级 自定义 ② 拦截攻击 0次 ● 防护等级 自定义 ② 拦截攻击 0次 网站防护	
10入服云	S 服务器安全狗 工具箱

图 5.2 检查更新 2

步骤 2. 弹出"智能升级程序"窗口,如下图 5.3 所示:

⑦ 安全狗升级中心−升级提示		×
	智能升级程序3.0 感谢您使用本系统! 以下产品或组件已安装在您的系统上: 网站安全狗(IIS版)4.0.14139	
	您现在用的版本已是最新的!当前版本:	4.0.14139 取消C)

图 5.3 智能升级程序窗口

6. 软件功能

6.1 网马查杀

用于网页木马、网页挂马、黑链和畸形文件扫描,及时发现并清除各类木马文件。



图 6.1.1 网马查杀

6.1.1 查杀方式

网马扫描方式可以分为全站扫描、自定义网站扫描与自定义路径扫描,如下图 6.1.2 所示。

e	返回				
	€) m ™	马查杀 时本机进行过网马查杀,建议	尽快进行扫描		
		全站扫描	… 「「」 自定义网站扫描	自定义路径扫描	
已后	3月网马引擎:	*		上报 信任区 隔	寄区 日志

图 6.1.2 网马查杀类型

(1)全站扫描:对 IIS 服务器上的所有站点,包括运行中和未运行的站点进行扫描。 目前支持第一级的虚拟目录。

(2) 自定义网站扫描:扫描选择的本地网站。需选择扫描的网站域名,点击"确定" 开始扫描。如下图 6.1.3 所示。

◎ 选择需要扫描的网站		×
	Q <u>L</u> -^ <u>T</u> -^	刷新
网站域名	网站路径	状态
192.168.147.128:8088	C:\inetpub\Dvbbs8.2.0_Ac\Dvbbs8.2.0_Ac\Dvbbs8.2.0_Ac\Dvbbs8.	•• 运行
192. 168. 147. 128	C:\inetpub\www.oot	运行
	THAILAN	arte sale
	十項扫描	

图 6.1.3 自定义网站扫描

(3) 自定义路径扫描:支持扫描指定的文件路径。选择好需要扫描的路径后,点击"确定"开始扫描。如下图 6.1.4 所示。

⑧ 请选择站点下目录。						×
🌀 🕞 - 📕 • 安全狗 •		+	经 搜索			
- 组织 ▼] 视图 ▼	📑 新建文件夹					0
收藏夹链接 ■ 桌面 ● 计算机 ● 文档 ● 图片 ● 音乐 ● 最近的更改 ● 捜索 ● 公用	名称	修改日期 ▼ 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21 2011/9/21	▲型文文文文文文文文文文文文文文文文文文文文文文文文文文文文文文文文文文文文	•] 大小	标记	
文件夹 ^ 文件夹: 5	安全狗					
			选	择文件夹		

图 6.1.4 自定义路径扫描

◆ 注意:选择路径时必须选择网站部署的路径,否则容易出现误报情况。

6.1.2 网马上报

当发现网马文件或可疑文件时,可以将文件上传至安全狗云端,系统将利用云端强大智能引擎进行分析、确认,并进行相应处理。如下图 6.1.5 所示。

● 网马上报	×	<
上报可疑的文件	文件大小	
C:/Users/qiuyb/Desktop/网马全/array_map_1(1).php	48 B	
☆ 全选 删除 添加文件	上报	1 Per-

图 6.1.5 网马上报

6.1.3 信任文件上报

提供设置信任文件功能,将不需要进行查杀的文件添加到信任文件列表,网马扫描过程 中,系统将自动忽略列表内的文件,不进行任何扫描。如下图 6.1.6 所示。

❷ 信任文件	×
信任的文件	文件大小
C:/Program Files/SafeDog/SafeDogSiteIIS/msvcm90.dll	220.00 KB
C:/Program Files/SafeDog/SafeDogSiteIIS/msvcp90.dll	559.50 KB
	VT (->- /)
	<u>添加文件</u>

图 6.1.6 信任文件

6.1.4 隔离文件查看

◆ 隔离文件查看:网马查杀处理完成后,被隔离的文件统一转移至隔离区。

✤ 隔离文件恢复:在隔离文件查看列表中的文件,可以通过恢复功能被还原到原始位置并再次允许执行,恢复前请确认该文件风险性。

\diamond	隔离文件清除:	在隔离文件查看列表中清除的文件	,将不能再被恢复,	请谨慎处理。
------------	---------	-----------------	-----------	--------

	×
隔离文件名	文件大小
☐ O:/服务器测试工具/双击测试/oday.php	124.13 KB
□ 全选 删除	恢复文件

图 6.1.7 隔离文件

6.1.5 网马扫描日志

 ● 査杀记录 × 					
总数	网页挂马	畸形文件	开始时间	结束时间	是否终止
10932	7	6	2016-06-16 16:26:57	2016-06-16 17:01:01	是
18	0	0	2016-06-16 16:26:05	2016-06-16 16:26:12	是
6	0	0	2016-06-16 16:24:57	2016-06-16 16:25:04	是
□ 全选					清除

通过查看扫描日志,了解历次扫描结果及查杀详情等相关信息。如下图 6.1.8 所示。

图 6.1.8 网马查杀记录

◆ 打开日志详情:在查杀记录列表上双击需要查看的记录,展开日志详情界面。如下图 6.1.9 所示。

● 详情	×
扫描目录 0:/新建文件夹 (2)/网马全/新建文件夹	
详情 查杀日期: 2016-06-24 15:09:30 网马库版本: 12.2 最后更新日期: 2016-06-16	
是否查杀网马木马: 是 是否查杀挂马/黑链: 是 是否查杀畸形文件: 是	
网页木马: 389 0:/新建文件夹 (2)/网马全/新建文件夹/1.aspx 0:/新建文件夹 (2)/网马全/新建文件夹/1.php 0:/新建文件夹 (2)/网马全/新建文件夹/123(1).php 0:/新建文件夹 (2)/网马全/新建文件夹/123.php 0:/新建文件夹 (2)/网马全/新建文件夹/abouttus(1).asp 0:/新建文件夹 (2)/网马全/新建文件夹/abouttus.asp 0:/新建文件夹 (2)/网马全/新建文件夹/abouttus.asp 0:/新建文件夹 (2)/网马全/新建文件夹/array_map_1(1).php 0:/新建文件夹 (2)/网马全/新建文件夹/array_map_1.php 0:/新建文件夹 (2)/网马全/新建文件夹/array_map_2(1).php	
	导出

图 6.1.9 网马查杀记录

◆ 导出详情功能:通过点击网马扫描日志界面上的导出按钮,可以将本次扫描结果及 详细信息以文本的形式存储到指定路径下。或在每次扫描结束后的扫描结果界面上,点击导 出详情按钮,同样可以实现扫描结果及详细信息的导出,如下图 6.1.10 所示。

e 返回	≡ - ×
扫描完成,发现12个安全风险 扫描文件:58350个 用时:00:33:35	与出详情 暂不处理 一键处理
☑ 🕘 网页木马 发现9个风险	添加信任
☑ C:/Users/qiuyb/Desktop/网马全/1.aspx	详情
☑ C:/Users/qiuyb/Desktop/网马全/1.php	详情
☑ C:/Users/qiuyb/Desktop/网马全/123(1).php	详情
☑ C:/Users/qiuyb/Desktop/网马全/123.php	详情
☑ C:/Users/qiuyb/Desktop/网马全/abouttus(1).asp	详情
✓ C:/Users/qiuyb/Desktop/网马全/abouttus.asp	详情
☑ C:/Users/qiuyb/Desktop/网马全/array_map_1(1).php	详情
☑ C:/Users/qiuyb/Desktop/网马全/array_map_1.php	详情
☑ C:/Users/qiuyb/Desktop/网马全/array_map_2(1).php	详情 🗸
已启用网马引擎: 🐲	上报信任区隔离区日志

图 6.1.10 网马扫描进度

6.1.6 网马扫描结果处理

网马扫描结束后,通过界面相关操作提示,可以对网马扫描结果采取进一步处理。如下 图 6.1.11 所示。

		=	- ×
扫描完成,发现679个安全风险 扫描文件:801个 用时:00:02:04 <u> 母描文件</u> :801个 用时:00:02:04 <u> <u> </u> <u> </u> <u> </u> <u> </u> <u> </u> <u> </u> <u> </u> <u> </u> <u> </u> <u> </u> <u> </u> <u> </u> </u>	暂不处理	- 健久	业理
☑ 🕘 网页木马 发现389个风险	添加信何	Ŧ	
☑ O:/新建文件夹 (2)/网马全/新建文件夹/1.aspx		详情	
☑ O:/新建文件夹 (2)/网马全/新建文件夹/1.php		详情	
☑ O:/新建文件夹 (2)/网马全/新建文件夹/123(1).php		详情	
☑ O:/新建文件夹 (2)/网马全/新建文件夹/123.php		详情	
✓ O:/新建文件夹 (2)/网马全/新建文件夹/abouttus(1).asp		详情	
✓ 0:/新建文件夹 (2)/网马全/新建文件夹/abouttus.asp		详情	
✓ O:/新建文件夹 (2)/网马全/新建文件夹/array_map_1(1).php		详情	
✓ O:/新建文件夹 (2)/网马全/新建文件夹/array_map_1.php		详情	
☑ O:/新建文件夹 (2)/网马全/新建文件夹/array_map_2(1).php		详情	•
已启用网马引擎: 🐲	上报(話任区 隔离区	日志

图 6.1.11 网马扫描进度

◆ 一键处理:扫描完成后系统默认选中所有扫描结果,点击一键处理按钮,对所有风险文件进行隔离、清理。

◆ 暂不处理: 放弃对本次扫描结果处理, 返回网马扫描主界面。

◆ 添加信任:在扫描结果列表选择需要被添加信任的文件,点击添加信任,该文件将 不再被网马扫描引擎判断为风险文件。

◆ 详情:点击扫描结果后面的详情,查看该风险文件的相关信息。

6.1.7 网马扫描功能设置

网马扫描功能设置包含扫描文件类型、扫描文件大小、扫描项目、自动扫描与清理、隔 离区设置与云安全计划等。如下图 6.1.12 所示。

❷ 设置		×
 ② 系统常规设置 ② 网马扫描设置 ③ 漏洞防护设置 □ 文件防护设置 □ IT黑白名单设置 □ 防护日志设置 	・	-
恢复出厂设置	◎ 日初归油升清理厄極又件	↓ 7

图 6.1.12 网马扫描功能设置

◆ 详情请参见 6.8.4.2 网马扫描设置。

6.2 网站防护

网站防护功能包含漏洞防护、文件防护以及行为防护在内的三大功能模块。通过开启/ 关闭功能开关或对相应的功能进行规制设置,可以实现更加高效、可靠的安全防护。

● 返回		≡ - ×
网站防护	保护网站安全	
	والمعالية ومراجع والمتعارية والمتعارية والمتعارية والمتعارية والمتعارية والمتعارية والمتعارية والمتعارية والمتع	
漏洞防护 阻止并记录 🔅	文件防护 阻止并记录 📦	行为防护 阻止并记录 💿
http安全检测 已开启 上传防护 已开启	浏览防护 日开启 短文件名防护 日开启 目录漏洞防护 日开启 禁止浏览畸形文件 日开启	危险组件防护 日开启 敏感函数防护 日天房 禁止IIS执行程序 日开启 一句话后门防护 日开启 TCP/UDP发包 日关词
一键关闭	一键关闭	一键开启
官方防护规则版本:2016-06-16		

图 6.2.1 网站防护

◆ 只记录:网站遇到攻击时,系统记录攻击该攻击行为的详细内容,并在防护日志界 面显示,但不进行拦截。

✤ 阻止并记录:网站遇到攻击时,系统记录攻击该攻击行为的详细内容,并在防护日 志界面显示,同时对该攻击行为进行有效拦截。

◆ 建议用户按照自身运营实际,选择合适的防护方式。

e 返回		≡ − ×
网站防护 参 主动拦截各类针对网站攻击,	保护网站安全	
漏洞防护 只记录 🔯	文件防护 阻止并记录 💿	行为防护 阻止并记录 🕸
http安全检测 已开启 上传防护 已开启	浏览防护 已开启 短文件名防护 已开启 目录漏洞防护 已开启 禁止浏览畸形文件 已开启	危险组件防护 已开启 敏感函数防护 日关闭 禁止IIS执行程序 日开启 一句话后门防护 日开启 TCP/UDP发包 日关闭
一键关闭	一键关闭	一键开启
官方防护规则版本:2016-06-16		

图 6.2.2 防护模式

6.2.1 漏洞防护

6.2.1.1 HTTP 安全检测

根据攻击特征库,对用户输入进行过滤,用于检测实时的 SQL 注入,主动防护引擎,并 及时屏蔽恶意攻击,从而达到防护网站的目的。

						<u></u>	×
	漏洞防护规则-HTTP安全检测						~
://1	HTTP检测规则	类型	来源	检测项目	状态		^
ー ー ー ー ー ー ー ー ー ー ー ー ー ー ー ー ー ー ー	URL地址全检测				已关闭		ш
	☐ 检测GET、POST之外的请求				已开启		
\frown	URL长度上限				已开启	\$	
	──防止复杂的and or 方式注入规则二	SQL注入拦截	官方	URL	已开启	a	
上传防御	☐ 防止简单的and or 方式注入	SQL注入拦截	官方	URL	已开启	- \$	
	防止基于时间的注入判断	SQL注入拦截	官方	URL	已开启	b	
	防止SQL联合查询	SQL注入拦截	官方	URL	已开启	= Ø	
	防止特殊关键字查询	SQL注入拦截	官方	URL	已开启	- 0	
	☐ 防止MySQL特征恶意利用	SQL注入拦截	官方		已开启	a	
	防止创建或者删除函数	SQL注入拦截	官方	URL	已开启	= 🕸	
	☐ 防止创建或者删除Mysql用户	SQL注入拦截	官方	URL	已开启	- ¢	
	防止对数据库进行创建、删除、备份操作	SQL注入拦截	官方	URL COOKIE POST内容	已开启	a	
		COLVE / 144+P		·····		- ~	-
	□ 全选 删除			更新防护规则 添	加规则	白名单	

图 6.2.3HTTP 安全检测

防护规则支持两种形式的更新:

(1)在线更新防护规则:安全狗云中心会收集海量注入语句,进行统计、分析并验证, 提取出大量有效的防护规则,自动更新至网站安全狗客户端,使得其能够对各种变形的注入 进行防护,如下图 6.2.4 所示。

6 返回	漏洞防护规则-HTTP安全检测					<u></u>)	×
://1	HTTP检测规则	类型	来源检测	则项目	状态		^
HTTP安全检测	 □ URL地址全检测 ● 信息提示 ■ 检J 				R¥)		Ш
					8	ŵ	
	[] 防止	0			9	a	
上传防御	防止		更新成	功	8	- ¢	
	[] 防」	e				a	
	[] 防山				9	∃ Ø	
	防止					- \$	
	<u>□</u> 防」				确定]	∃ Ø	
	防止创建或者删除函数	SQL注入拦截	官方 URI	L	已开启	a	
	防止创建或者删除Mysql用户	SQL注入拦截	官方URI	L	已开启	a	
	□ 防止对数据库进行创建、删除、备份操作	SQL注入拦截	官方 URI	L COOKIE POST内容	已开启	b	
		r a : 5± 1 ±±+P	T	· · · · · · · · · · · · · · · · · · ·			-
	全选删除			更新防护规则	添加规则	白名单	

图 6.2.4 检测规则更新

(2) 用户自定义防护规则: 自定义设置 SQL 注入防护规则。如下图 6.2.5 所示。

💩 添加нтте	安全检测防护规则	I		×
正则表达式: 规则描述: 检测项目:	□ 检测URL □ 检测HTTP头	□ 检测COOKIE 更多	检测P	OST
			确定	取消

图 6.2.5 自定义防护规则

◆ 提供检测 Ur1 长度或者 Ur1 地址全检测的功能。

◆ 提供设置Sq1注入白名单:白名单列表中的网络路径不受SQ1注入防护设置的限制。
如下图 6.2.6 所示。

⑤ 返回	漏洞防护规则-HTTP检测白名单	- ×
	路径白名单。	路径类型
HTTP安全检测		
	 ◆ 添加物理路径白名单 ※ 路径类型: 网络路径 ● 自定义路径: www.safedog.cn/root/index.php! 请输入网络路径,如: www.safedog.cn/root/index.php 确定 取消 	
	□ 全选	添加白名单

图 6.2.6 添加网络路径白名单

6.2.1.2 上传防护

通过设置禁止上传的文件名后缀,禁止上传特定类型的文件到网站,主动拦截上传网页 木马,防护网站不受网络木马的攻击。

6 返回			<u></u> 1	×
-	漏洞防护规则-上传防御			
://]	禁止上传的文件类型	启用状态	É	Â
UTTD立今校制	asa	已开启	Ξ	
	asax	已开启	Ξ	
	ascx	已开启	\Box	
	ashx	已开启	=	
上传防御	asmx	已开启	-	=
	asp	已开启		
	aspx	已开启	Ξ	
	cdx	已开启	_	
	cer	已开启	Ξ	
	□ cgi	已开启	Ξ	
	🗌 dll	已开启		
	exe	已开启	Ξ	
		-		-
	□ 全选 删除		添加规则	

图 6.2.7 上传防护

◆ 上传防护规则:通过添加文件后缀名,禁止该类型的所有文件上传,如下图 6.2.8

所示。

,如: asp, asa	_
	确定取

图 6.2.8 添加上传防护规则

6.2.2 文件防护

6.2.2.1 浏览防护

通过设置需要防护的资源类型,若有指定类型文件被扫描出带有木马,则限制该文件在 用户浏览器中显示。设置防护资源类型,如下图 6.2.9 所示。

⑤ 返回	文件防护规则-浏览防护	- ×
	防护的文件类型	启用状态
浏览防护		已开启
	asax asax	已开启
	asox	已开启
	ashx	已开启
	asmx	已开启
	asp	已开启
	aspx	已开启
	edx	已开启
	cer	已开启
	cgi	已开启
	jsp	已开启
	рыр	已开启
	□ 全选 删除	添加规则 白名单

图 6.2.9 浏览防护

◆ 通过添加文件后缀名,禁止浏览该类型的所有文件,如下图 6.2.10 所示。

● 添加文件防护规则		×
添加需要禁止浏览的文件类型,输入文件 支持同时输入多个,中间以","(半角)	⊧后缀名(不带"."),如)隔开,如: asp, asa]: asp
	确定	町省
	如72	取泪

图 6.2.10 添加浏览防护规则

6.2.2.2 短文件名防护

黑客可以通过 * [~] 组合用于猜测目录名和文件名,使用 windows 短文件名可以直接访问文件。如果黑客用这个方法智能的 Brute force,然后攻击一些备份了敏感数据,如(.sql)的 WEB 程序,那么就可能严重威胁网站的安全。通过启用短文件名防护功能,有效拦截Windows 短文件名漏洞利用。

e 返回		≡ - ×
网站防护 参 主动拦截各关针对网站攻击,	保护网站安全	
漏洞防护 只记录 💿	文件防护 阻止并记录 🔞	行为防护 阻止并记录 🔯
http安全检测 已开启	浏览防护 日开启	危险组件防护 已开启
	是文件石的护 已 开启	禁止IIS执行程序 已开启
	禁止浏览畸形文件 已开启	一句话后门防护 已开启
		TCP/UDP发包
一键关闭	一键关闭	一键开启
官方防护规则版本:2016-06-16		

图 6.2.11 短文件名防护

6.2.2.3 目录漏洞防护

在网站路径下建立文件夹名字为.asp、.asa 的文件夹,其目录内的任何扩展名的文件都会被 IIS 当作 asp 文件来解析并执行,黑客利用 IIS 目录解析漏洞,实现上传、执行恶意文件的目的。通过启用目录漏洞防护功能,有效拦截 IIS 目录漏洞利用。

● 返回		≡ - ×
网站防护	保护网站安全	
漏洞防护只记录 🔯	文件防护 阻止并记录 🔞	行为防护 阻止并记录 🕸
http安全检测 已开启 上传防护 已开启	浏览防护 日开启 短文件名防护 日开启	危险组件防护 日开启 敏感函数防护 日关闭
	目录漏洞防护 已开启 禁止浏览畸形文件 已开启	禁止IIS执行程序 已开启 一句话后门防护 已开启
		TCP/UDP发包 已关闭
一键关闭	一键关闭	一键开启
官方防护规则版本:2016-06-16		

图 6.2.12 目录漏洞防护

6.2.2.4 禁止浏览畸形文件

黑客通过构造类似 x. asp; jpg 之类的畸形文件的后缀名,上传到服务器上再结合 iis 的解析特性即可成功执行代码,获取必要的网站配置等信息。通过启用禁止浏览畸形文件防护功能,有效拦截对畸形文件的请求执行。

 返回 		≡ − ×
网站防护 ④ 主动拦截各类针对网站攻击	,保护网站安全	
漏洞防护员记录 💿	文件防护 阻止并记录 🕸	行为防护 阻止并记录 🕸
http安全检测 已开启 上传防护 已开启	浏览防护 已开启 短文件名防护 已开启 目录漏洞防护 已开启 禁止浏览畸形文件 已开启	危险组件防护 已开启 敏感函数防护 已 关闭 禁止IIS执行程序 日开启 一句话后门防护 日开启 TCP/UDP发包 已关闭
一键关闭	一键关闭	一键开启
官方防护规则版本:2016-06-16		

图 6.2.13 禁止浏览畸形文件

6.2.3 行为防护

6.2.3.1 危险组件防护

拦截恶意代码对组件的调用权限,从而保护网站安全。

€ 返回 {}	行为防护-危险组件防护			- ×
	防护的组件名称	规则描述	状态	
敏感函数保护	Shell.Application.1	执行相关组件	已开启	¢۵
2 March	WinNTNamespace	账号或不安全的组件	已开启	¢۵
	WBEMComLocator	WMI相关组件	已开启	ŵ
危险组件防护	Shell.User.1	账号或不安全的组件	已开启	¢۵
	Shell.Users.1	账号或不安全的组件	已开启	ŵ
	WScript.Shell	执行相关组件	已开启	¢3
禁止IIS执行程序	WbemScripting.SWbemLocator.1	WMI相关组件	已开启	ŵ
····	WinNT	账号或不安全的组件	已开启	ŵ
\otimes	WMINet_Utils.WmiSecurityHelper.1	WMI相关组件	已开启	¢۵
一句话后门防护	UBScript.Encode	脚本加密的组件	已美闭	¢3
TCP				
TCP/UDP发包	□ 全选 删除		添加规则 白谷	当単

图 6.2.14 危险组件防护

◆ 根据实际需要,对防护组件进行新增、修改、删除。如下图 6.2.15 所示。

😑 添加规贝	Ŋ		>
组件名称:	VBScript.encode		
组件 ID:	{B54F3743-5B07-11CF-A4BC)-00AA004A55E8}	
规则描述:	脚本加密的组件		
		确定	取消

图 6.2.15 添加危险组件防护规则

注意:

◆ 危险组件防护功能,在64位系统上,只支持32位应用程序池。

◆ 提供设置应用程序池白名单:白名单中的应用程序池不受组件防护的限制。如下图

6.2	2.16	所示。
-----	------	-----

返回	行为防护白名单-危险组件防护		- ×
{}	应用程序池名称	域名	
敏感函数保护	DefaultAppPool	192. 168. 147. 128	
危险组件防护			
一句话后门防护			
	□ 全选 删除		添加白名单

图 6.2.16 危险组件防护白名单规则

6.2.3.2 敏感函数防护

⑤ 返回	行为防护-物感函数促护			- ×
{}		代文		
「「」」	معتند المركمين عمد المركمين الم	已开启	Ξ	愈
	ADsGetObject	已开启	Ξ	ŝ
\bigcirc	ADsOpenObject	已开启		礅
危险组件防护	▷ 🔄 advapi32.dll	已开启		\$
	kernel32.dll	已开启	Ξ	\$ \$
				ų» ش
禁止IIS执行程序				~
一句话后门防护				
TCP UDP				
TCP/UDP发包	□ 全选	添加规则	É	日名单

用户通过设置 dl1 敏感函数禁止执行,防护网站安全。

图 6.2.17 敏感函数防护

(1) 设置需要进行敏感防护的 dl1 文件。如下图 6.2.18 所示。

×
添加
移除

图 6.2.18 添加需要防护的 DLL 文件

(2) 设置 d11 文件中需要进行敏感防护的函数名称,支持禁止调用和允许调用。如下 图 6.2.19 所示。

💩 编辑规	Ņ		×
DLL文件名:	activeds. dll		
函数名称:			添加
	ADsOpenObject	已开启	移除
	ADsGetObject	已开启	
	☑ 全选	确定	取消

图 6.2.19 设置需要禁用的函数名称

◆ 提供设置应用程序池白名单:白名单中的应用程序池不受敏感函数防护的限制。如下图 6.2.20 所示。

€ 返回	行为防护白名单-敏感函数保护		- ×
[]	应用程序池名称	域名	
敏感函数保护	DefaultAppPool	192. 168. 147. 128	
危险组件防护			
一句话后门防护			
	□ 全选 删除		添加白名单

图 6.2.20 敏感函数防护白名单规则

◆ 敏感函数防护功能,在64位系统上,只支持32位应用程序池。

6.2.3.3 禁止 IIS 执行程序

全面拦截 IIS 执行恶意程序,保护网站安全。如下图 6.2.21 所示。

● 返回	行为防护-禁止IIS执行程序			- ×
	禁止IIS执行程序规则	规则描述	状态	
敏感函数保护 	限制命令行最大长度	长度上限500字节	日关闭	ĝ
/> 禁止IIS执行程序				
TCP UDP				
TCP/UDP发包			白名	单
图 6.2.21 禁止 IIS 执行程序

◆ 支持限制命令行最大长度,长度范围默认推荐: 300-800,系统默认设置为 500。
 如下图 6.2.22 所示。

● 返回 {…}	行为防护-禁止IIS执行程序			- ×
	禁止IIS执行程序规则	规则描述	状态	
敏感函数保护	限制命令行最大长度	长度上限500字节	已关闭	¢
禁止IIS执行程序				
TCP/UDP发包			白名	单

图 6.2.22 禁止 IIS 执行程序

◆ 提供设置应用程序白名单:白名单中的应用程序不受禁止 IIS 执行程序的限制。如
 下图 6.2.23 所示。

● 返回	行为防护白名单-禁止IIS执行程序	- ×	
$\{\}_{1}^{1}$	应用程序白名单 应用程序池白名单		
敏感函数保护	☐ %windows%Microsoft.NET/Framework/v1.1.4322/aspnet_wp.exe	Ξ	-
	3windows%Microsoft.NET/Framework/v1.1.4322/csc.exe		
	%windows%Microsoft.NET/Framework/v1.1.4322/vbc.exe	Ξ	
危险组件防护	\%windows%Microsoft.NET/Framework/v2.0.50727/aspnet_wp.exe	\square	
	%windows%Microsoft.NET/Framework/v2.0.50727/csc.exe		
	%windows%Microsoft.NET/Framework/v2.0.50727/vbc.exe	Ξ	
些山瓜 一	3%windows%Microsoft.NET/Framework/v4.0.30319/aspnet_wp.exe	Ξ.	
	3windows%Microsoft.NET/Framework/v4.0.30319/csc.exe	E	
- Tuesdetu Te riegu	%windows%Microsoft.NET/Framework/v4.0.30319/vbc.exe	Ξ	
	%windows%Microsoft.NET/Framework64/v1.1.4322/aspnet_wp.exe		
一句话后门防护	%windows%Microsoft.NET/Framework64/v1.1.4322/csc.exe	Ξ	
	Wwindows%Microsoft.NET/Framework64/v1.1.4322/vbc.exe	Ξ	-
	□ 全选 删除	添加白名单	

图 6.2.23 应用程序白名单规则

◆ 提供设置应用程序池白名单:白名单中的应用程序池不受禁止 IIS 执行程序的限制。如下图 6.2.24 所示。

e 返回	行为防护白名单	-禁止IIS执行程序			- ×
{}	应用程序白名单	应用程序池白名单	域名		
敏感函数保护	DefaultAppPool		192. 168. 147. 12	28	
危险组件防护					
禁止IIS执行程序					
一句话后门防护					
	□ 全选 删除				添加白名单

图 6.2.24 应用程序池白名单规则

6.2.3.4 一句话后门防护

对 PHP 引擎行为进行检测,拦截存在风险的可疑一句话,避免网站服务器遭受危害。

● 返回	行为防护-一句话后门	〕防护			- ×
{}	动态加载函数执行保护	禁止变量函数	中国菜刀	启用状态	
敏感函数保护	PHP动态加载函数执行保护			已关闭	
July	move_uploaded_file			已开启	
	mysql_connect			已开启	
危险组件防护	phpinfo			已开启	
マイト 禁止IIS执行程序					
TCP/UDP发包	□ 全选 删除			添加规则 É	名单

图 6.2.25 动态加载函数执行防护

(1)动态加载函数执行防护:通过动态引擎,对 PHP 动态加载函数执行进行风险识别, 实有效拦截存在风险的函数执行;

◆ 对需要进行防护的动态函数进行新增、修改、删除。如下图 6.2.26 所示。

🖲 添加规则	U.		>
函数名称:	1		
	支持批量添加,多个函	数请用 " , " 隔开。	
		确定	取消

图 6.2.26 添加一句话后门防护函数

◆ 应用程序池白名单:白名单中的应用程序池不受函数执行防护限制。如下图 6.2.27

所示。

● 返回	行为防护白名单-一句话后门防护		- ×
1	应用程序池名称	域名	
	DefaultAppPool	192. 168. 147. 128	
禁止IIS执行程序			
	□ 全选 删除		添加白名单

图 6.2.27 一句话后门防护白名单规则

(2) 禁止变量函数:通过动态引擎,实现对变量函数扫描,有效拦截 PHP 变量对风险 函数调用。如下图 6.2.28 所示。

e 返回	行为防护-一句话后门防护	- ×
{}	动态加载函数执行保护 禁止变量函数 中国菜刀 高用利	伏态
敏感函数保护	PHP变量函数保护	美 团
Lable 1	assert ETT	
	Create_function 已开展	
危险组件防护	□ passthru 已开想	
	□ pcntl_exec 已开版	
	□ proc_open	
禁止IIS执行程序	shell_exec	
	□ system 已开作	
י ענשנ ובושניי		
TCP		
TCP/UDP发包	□ 全选 删除 添加规则	白名单

图 6.2.28 禁止变量函数

◆ 对需要进行防护的变量函数进行新增、修改、删除。如下图 6.2.29 所示。

函数名称:				
	支持批量添	加,多个函数请	猜用" ,"隔开。	

图 6.2.29 添加需要禁止的变量函数

◆ 应用程序池白名单:白名单中的应用程序池不受变量函数防护限制。如下图 6.2.30

所示。			
€ 返回	行为防护白名单-一句话后门防护		- ×
{}	应用程序池名称	域名	
敏感函数保护	DefaultAppPool	192. 168. 147. 128	
危险组件防护			
禁止IIS执行程序			
一句话后门防护			
	□ 全选 删除		添加白名单

图 6.2.30 应用程序池白名单规则

(3) "中国菜刀"一句话防护:对"中国菜刀"连接一句话木马进行识别,并拦截可疑风险行为。如下图 6.2.31 所示。

● 返回	行为防护-一句话后门	门防护				- ×
{}	动态加载函数执行保护	禁止变量函数	中国菜刀	J	启用状态	
敏感函数保护	"中国菜刀" 一句话后门防护			6	开启	
危险组件防护						
禁止IIS执行程序						
TCP UDP						
TCP/UDP发包					白谷	当单

图 6.2.31 中国菜刀

◆ 应用程序池白名单:白名单中的应用程序池不受"中国菜刀"防护限制。

e 返回	行为防护白名单-一句话后门防护		- ×
	应用程序池名称	域名	
 敏感函数保护 ● 	DefaultAppPool	192. 168. 147. 128	
一句话后门防护			
	□ 全选 删除		添加白名单

图 6.2.32 应用程序池白名单规则

6.2.3.5 TCP/UDP 发包

e 返回	行为防护-TCP/UDP发包		-	·×
{} ;	TCP/UDP发包规则	规则描述	状态	
— — 敏感函数保护	禁止对外发送UDP包		已开启	
	禁止对外发送TCP包	例外講口:1433,1521,21,3306,443,50000	已开启	Ø
危险组件防护				
TCP UDP				
TCP/UDP发包				

禁止对外放松 TCP/UDP 包, 避免宽带占用情况发生。如下图 6.2.33 所示。

图 6.2.33 TCP/UDP 发包防护

(1) 禁止对外发送 UDP 包: 基于 IIS 的网站组件模块,一般情况下通过 w3wp. exe 进程 发送 UDP 包,将会被网站安全狗阻止, UDP 数据包不会通过服务器进行对外发送,从而避免 带宽占用的情况。

(2) 禁止对外发送 TCP 包: 对外发送 TCP 包需要使用 TCP 进程端口,在 TCP 例外端口 中进行端口号添加,排除需要使用的端口号进行对外发包。如下图 6.2.34 所示。

🕑 修改端		×
规则名称:	禁止对外发送TCP包]
例外端口:	1433, 1521, 21, 3306, 443, 50000	
	(支持同时输入多个,中间以","(半角)隔开,如:1433,1521)	
	(
	确定 取消	

图 6.2.34 TCP/UDP 发包防护

✤ 设置的这些端口号对外发送 TCP 数据包时不会被网站狗拦截。比如,添加例外端口 1433(1433为数据库端口),将解除禁止该进程对外发包。

6.3 资源防护

资源防护功能包含内容防护、资源防护以及流量防护在内的三大功能模块。各个功能模块均可以通过开启/关闭功能开关或对相应规制设置进行调整,以满足用户实际运营需要。

e 返回		$\equiv - \times$
一 资源防护	重攻击,保护网站资源	
内容防护	资源防护	流量防护
网站后台防护 已开启 响应内容防护 已开启	资源防盗链 已开启 特定资源防护 已开启 环境信息隐藏 已关闭	CC攻击防护 已开启 下载控制 已开启
一键关闭	一键开启	一键关闭
官方防护规则版本:2016-06-16		

图 6.3.1 资源防护

6.3.1 内容防护

6.3.1.1 网站后台防护

网站后台防护功能通过对网站后台进行重定向,通过增加身份验证以防护网站后台路 径,并结合 IP 黑名单机制,让黑客无法对网站后台进行恶意访问,从而防护网站后台安全。

6 返回	内容保护规则-网站后台保护				<u></u>	×
	防护路径	规则名称	验证方式	启用状态		
网站后台防护	C:/inetpub/Dvbbs8.2.0_Ac/Dvbbs8.2.0_Ac/Dvbbs8.2.0_Ac/Dvbbs8.2.0_Ac/1.html	规则1	IP验证	已开启	Ξ	¢
S						
响应内容保护						
	۹					Þ
	□ 全选 删除			添加扶	则	

图 6.3.2 网站后台防护

◆ IP 验证方式:设置允许访问该后台路径的 IP,支持 IP 段。通过该 IP 或 IP 段对指定后台路径进行访问,不会被系统拦截,其余 IP 均会被当做恶意访问拦截。如下图 6.3.3 所示。

规则1	
192. 168. 147. 128:8088	浏览
2. 0_Ac\Dvbbs8. 2. 0_Ac\Dvbbs8. 2. 0_Ac\Dvbbs8. 2. 0_Ac	浏览
IP验证方式	
123. 11. 168. 1-123. 11. 168. 254	
支持IP段,如: 1.1.1.1-1.1.1.254 多IP用":"(半角)隔开,如: 1.1.1.1;1.1.1.2	
	规则1 192.168.147.128:8088 2.0_Ac\Dvbbs8.2.0_Ac\Dvbbs8.2.0_Ac\Dvbbs8.2.0_Ac IP验证方式 123.11.168.1-123.11.168.254 支持IP段,如:1.1.1.1-1.1.254 多IP用 ":"(半角)隔开,如:1.1.1.1:1.1.2

图 6.3.3 IP 验证方式规则设置

◆ 密码验证方式:设置该后台路径访问密码,访客在访问该后台路径时,需要先通过 密码方式进行身份验证,如输入错误超过系统设定则该 IP 会被添加到临时黑名单,被冻结 一定时间。如下图 6.3.4 所示。

规则描述:	规贝12		
网站域名:	192. 168. 147. 128		浏览
防护路径:	C:\inetpub\wwwroot		浏览
验证方式:	密码验证方式		-
设置密码			
输入密码:	*****		
确认密码:	*****		
验证时效			
有效时间:	30		分钟
密码验证通	过后,该IP在有效时间内可直打	接访问,无需再做验 证	Ę
密码验证通	过后,该IP在有效时间内可直打	接访问,无需再做验 证	E

图 6.3.4 密码验证方式规则设置

6.3.1.2 响应内容防护

当访问网站时,不合理的访问或者网站自身的问题,会出现各种的错误返回页面。从安 全的角度上讲,这就可以给攻击者提供判断的依据。为此,响应内容防护功能,支持禁止 400-500之间的错误类型请求返回,防护网站安全。

e 返回	内容保护规则-响应内容保护		<u></u> N	×
	HTTP请求错误类型	启用状态		
	400	已开启	-	
	403	已开启	-	
	404	已开启	-	
响应内容保护				
		添加	规则	

图 6.3.5 响应内容防护

设置需要防护的 Http 错误类型。如下图 6.3.6 所示。

输入HTTP错	詣 误请求类型,女	[]: 400, 403,	405	
I.				

图 6.3.6 添加 http 错误类型

开启响应内容防护后,防护效果如下图 6.3.7 所示。



图 6.3.7 响应内容防护效果

6.3.2 资源防护

6.3.2.1 资源防盗链

通过 Reference 技术和 Session 技术解决防盗链问题。Reference 技术通常用于图片、 mp3 等这种容易被人用 html 嵌入到其他网站资源的资源; Session 技术一般只用于论坛和社 区网站。

e 返回	资源保护-资源防盗	链				- ×
\bigcirc	防护网站	防护模式	资源类型	防护内容	启用状态	
资源防次链	192.168.147.128	引用方式	asa	信任域名:www.safedog.cn,	已开启	\$
5-10007年1日 「 存定资源保护 不境信息隐藏	192.168.147.128:8088	会适方式	asp	有效时间:30分钟		\$
	□ 全选 删除				添加	规则

图 6.3.8 网站资源防盗链

开启资源防盗链功能后,防护效果图如下图 6.3.9 所示。



图 6.3.9 网站资源防盗链效果

(1)引用方式:通过判断 referer 变量的值来判断图片或资源的引用是否合法,只有 在设定范围内的 referer,才能访问指定的资源,从而实现了防盗链的目的。支持设置信任 域名,Reference 方式能够让本域名和其他指定信任域名正常链接被防护资源。如下图 6.3.10 所示。

的护快式;		•
防护网站:	192. 168. 147. 128,	浏览
资源类型:	858	
	添加需要防护的文件类型,输入文件后缀名(不带"." 支持同时输入多个,中间以","(半角)隔开,如: asj),如: asp), asa
信任域名:	www.safedog.cn	

图 6.3.10 资源防盗链引用方式

(2) 会话方式:提供进行会话方式(对本域名及子域名信任)和有效时间的设定。如

下图 6.3.11 所示。

防护模式:	会话方式	5
防护网站:	192.168.147.128:8088,	浏览
测览器行为:	基于内存	[
资源类型:	asp	
	添加需要防护的文件类型,输入文件后缀名(不带".") 支持同时输入多个,中间以","(半角)隔开,如: asp,	,如: asp asa
1000 C	30	分钟

图 6.3.11 资源防盗链会话方式

✤ 提供自定义修改服务器提示信息的功能:可以随意设置用户所希望呈现的捕获盗链 攻击时服务器返回的提示信息。

✤ 同一网站,不提倡用户同时启用"引用方式"和"会话方式",以免使用过程中出现冲突。

6.3.2.2 特定资源防护

通过对某些特定资源的设置,来确保它们不被下载或盗用。

• 返回	资源保护-特定资源	保护		- ×	¢
\bigcirc	防护网站	防护模式	防护内容	启用状态	
资源防盗链	192.168.147.128	资源类型保护	bak,mdb,mdf,myd	已开启 日 🕸	
中 ・ 中 ・ 市 ・ 市 ・ 市 ・ 市 ・ 市 ・ 市 ・ 市 ・ 市 ・ 市 ・ 市 ・ 市 ・ 市 ・ 市 ・ 市 ・ 市 ・ 市 ・ 市 ・ 市 ・ 市 ・ 市 ・ 市 ・ 市 ・ 市 ・ 市 ・ 市 ・ 市 ・ 市 ・ 市 ・ 市 ・ 市 ・ 市 ・ 市 ・ 市 ・ 市 ・ 市 ・ 市 ・ 市 ・ 市 ・ 市 ・ 市 ・ 市 ・ ・ ・ ・ ・ ・<	192.168.147.128:8088	资源路径保护	/config/index.php		
	□ 全选 删除			添加地风川	

图 6.3.12 网站特定资源防护

(1)资源类型防护:设置需受防护资源的文件类型。如下图 6.3.13 所示。

防护模式:	资源类型防护	
防护网站:	192. 168. 147. 128:8088	浏览
资源类型:	mdb, exe	
	添加需要防护的文件类型,输入文件后缀名(不带".") 支持同时输入多个,中间以","(半角)隔开,如: mdb,	,如: mdi .exe, php

图 6.3.13 添加资源类型防护规则

(2)资源路径防护:设置需防护资源的所在路径,支持添加网络文件路径或目录路径, (网络路径:网络上的资源路径)。如下图 6.3.14 所示。

防护模式:	资源路径防护	<u> </u>
防护网站:	192. 168. 147. 128:8088	浏览
路径类型:	网络路径	<u> </u>
自定义路径:	/config/index.php	
	请输入/开头的网络文件路径或目录路径,无需再 如: /config/logic/network或/config/index.ph	输入域名, P

图 6.3.14 添加资源防护路径防护规则

6.3.2.3 环境信息隐藏

环境信息隐藏包含 Web 容器信息防护及 PHP、. Net 信息防护,用户进行相应设置后,系 统返回用户指定的,错误的 Web 容器信息或 PHP、. Net 信息,以蒙蔽黑客扫描,防护站点不 受攻击。

Θ	返回					- ×
		资源保护-环境信息隐藏				
[$\overline{\mathbb{C}}$	防护规则	防护模式	防护内容	启用状态	
运	酒防次雄	Web容器信息防护	环境信息隐藏	IIS	已开启	ŝ
		PHP、.Net信息防护	版本信息隐藏	显示为空	已开启	
Ĺ	<u> </u>					
特定	自资源保护					
(\bigcirc					
环境	ê信息隐藏					
		□ 全选 删除				

图 6.3.15 环境信息隐藏

(1) Web 容器信息防护

用户可以自行设置讲 Web 容器信息隐藏为指定版本,针对 Web 容器的信息请求,系统将返回指定值。如下图 6.3.16 所示。

防护模式: 环倍信自隐藏	
200 (9624) 21 89616 (CADOMARA	
信息隐藏为: Microsoft-IIS/6.0	_

图 6.3.16 编辑 Web 容器信息隐藏规则

(2) PHP、.Net 信息防护

开启防护功能后,针对 PHP、.Net 相关信息的请求,系统将默认返回空。如下图 6.3.17 所示。

④ 返回				- ×
	资源保护-环境信息隐藏			
$\mathbf{\hat{\mathbf{A}}}$	防护规则	防护模式	防护内容	启用状态
272 X75 R+- 272 P++	── Web容器信息防护	环境信息隐藏	IIS	已开启 🕸
资源防益链	PHP、.Net信息防护	版本信息隐藏	显示为空	已开启
P	L			
特定资源保护				
环境信息隐藏				
	□ 全选 删除			

图 6.3.17 PHP、.Net 信息防护

6.3.3 流量防护

6.3.3.1 CC 攻击防护

CC 攻击(ChallengeCollapsar)是借助代理服务器生成指向受害主机的合法请求,实现 DOS 和伪装。模拟多个用户不停的进行访问那些需要大量数据操作,大量 CPU 时间的页面, 使得页面打开速度缓慢。CC 攻击防护利用防止一个多次不断刷新而断开与该 IP 的连接,防 止服务器瘫痪,达到了防攻击目的。

e 返回	流量保护-CC攻击保护		- ×
()	CC攻击防护规则	防护内容	启用状态
	□ 单IP访问上限	100次/10秒 冻结5分钟	□开启 ◎ ◎
	□ 代理访问上限	30个IP/1秒	已开启。 命
	□ 会活验证	初级模式 放行30分钟	
下载限制			
	□ 全选 删除		白名单

图 6.3.18 CC 攻击防护

(1) 单 IP 访问上限:设置单位时间内允许通过的最大请求数目。如下图 6.3.19 所示。

规则名称:	单IP访问上限			
规则内容:	单IP 10 秒	内(1-60),允许最大请求数	100	次

图 6.3.19 编辑单 IP 防护上限规则

- 1) 规则内容:设置单位时间内单个 IP 被允许访问的最大请求数。
- 2) 冻结时间:在单位时间内被限制 IP 将无法访问本网站。

(2) 代理访问上限规则:本功能设置代理访问上限。

1) 规则内容:设置单位时间内代理 IP 的最大数和访问的时间周期。如下图 6.3.20 所示。

规则名称:	代理	访问上限	
规则内容:	1	秒内(1-60),允许最大访问IP数 30	个
	(推若	: 1秒内允许最大代理访问IP数30个,-1允许,	0棽止)
	1111		- 37.112.2

图 6.3.20 编辑代理访问上限规则

2) 会话验证规则:本功能设置会话验证级别。如下图 6.3.21 所示。

🖲 修改会词	話验证方式				
规则名称:	会话验证				
验证模式:	初级模式				-
	初级模式: 该模 (正常情况下,	[式对攻击验 推荐使用该	证判断较为宽 模式)	裙	
放行时效:	验证合法的IP	30	分钟	内访问,无言	需再做验证
				确定	取消

图 6.3.21 编辑验证方式规则

✤ 高级模式:该模式对所有的访问都会要求进行手动点击验证(网站长期处于被 攻击情况下,推荐使用该模式)。

◆ 中级模式: 该模式对所有的访问都会进行自动验证(网站处于间断性被攻击情况下,推荐使用该模式)。

◆ 初级模式: 该模式对攻击验证判断较为宽松(正常情况下推荐使用该模式)。

(3) 白名单: CC 防护功能支持网站白名单、路径白名单, 白名单中的网站或路径不受 规则防护的限制。

1)网站白名单:白名单中的网站,不受规则防护的限制。如下图 6.3.22 所示。

0	返回	流量保护白名单-CC攻击保护		- ×
(•	网站白名单 路径白名单 路径白名单	启用状态	
cc	攻击保护	192.168.147.128.8088	运行	
ŕ	\sim			
		□ 全选 删除	添加白	名单

图 6.3.22 CC 攻击防护网站白名单

● 返回	流量保护白名单-CC攻击保护	- ×
	网站白名单 路径白名单	路径类型
CC攻击保护	www.safedog.cn/root/index.php	网络路径
下载限制		
	□ 全选 删除	添加白名单

2) 路径白名单:白名单中的路径,不受规则防护的限制。如下图 6.3.23 所示。

图 6.3.23 CC 攻击防护路径白名单

6.3.3.2 下载控制

一个线程就是一个文件的下载通道,多线程也就是同时开起好几个下载通道。当服务器 提供下载服务时,使用下载者是共享带宽的,在优先级相同的情况下,总服务器会对总下载 线程进行平均分配,所以通过合理控制单用户下载的最大线程数,可以获得较高的带宽,避 免网速过慢。

e 返回	流量保护-下载限制			- ×
(\circ)	下载限制	线程数	资源类型	启用状态
CC攻击保护	● 多线程下载限制	5		已开启。 命
下载限制				
	□ 全选 删除			白名单

图 6.3.24 下载控制

(1)多线程下载控制设置:设置允许单个用户下载的最大线程数目。如下图 6.3.25 所示。

规则名称:	多线程下载限制	
最大线程数:	5	个(访问用户最大线程数,建议5-10)
资源类型:	exe	
	添加需要防护的文 古特同时输入多个	【件类型,输入文件后缀名(不带"."),如: mdt 、 由词以" " (半角) 隠开、如: mdb ava pbp

图 6.3.25 编辑下载控制规则

(2) 防护资源类型:允许用户增加、删除要防护的资源类型。

(3)网站白名单:白名单中的网站不受规则防护的限制。如下图 6.3.26 所示。

0	返回	流量保护白名单-下载限制		<u></u>	×
Č	•)	网站域名	启用状态		
× 33	攻击保护	192.168.147.128:8088	运行		
Ĺ					
		□ 全选 删除	汤	加白名单	

图 6.3.26 下载控制白名单规则

6.4 IP 黑白名单

网站安全狗 IP 黑白名单中的 IP/IP 段将不经过防护规则优先处理,即所有防护功能对 位于黑白名单列表中得 IP 地址无任何限制。通过设置一些 IP 地址为黑名单地址或者白名单 地址,可以调整指定 IP/IP 段对网站的访问权限。

e 返回					≡ - ×
	单 定IP访问权限,保护I	网站安全			
		Harris Harris			
IP白名单	ø	IP黑名单	ø	爬虫白名单	Ø
IP白名单	已开启	IP黑名单 [] 临时黑名单	2开启	爬虫白名单	已开启
一键关	闭	一键关	闭	一键关闭	0
官方防护规则版本:201	16-06-16				

图 6.4.1 IP 黑白名单

6.4.1 IP 白名单

IP 白名单设置成功后,该 IP 将不再受所选防护功能的约束。IP 白名单功能支持新增、 修改、删除、导入、导出 IP 白名单。如下图 6.4.2 所示。

🖲 返回	防护规则-IP白名单				- ×
<u></u>				导入规则	导出规则
<u>لې</u>	IP地址	规则名称	作用范围		
IP白名单规则	123.12.168.1	與武和則	HTTP检测 上传防护 GetPost之外请求 文件防护 防盗链 特定	並资源) CC防护↓ 下載限制	
	全选 删除			添	加规则

图 6.4.2 IP 白名单

支持添加单个 IP 或 IP 段,并可以指定 IP/IP 段白名单在哪些具体功能上生效,比如: HTTP 安全检测、上传防护、文件防护、资源防盗链、特定资源防护等。如用户只选择 "HTTP 安全检测"这个保护模块,那么,当该 IP 只对 HTTP 安全检测功能有效,当它触发了其他的 功能防护设置时,仍然会被拦截。如下图 6.4.3 所示。

◎ 添加IP	白名単	×
规则描述:	测试规则	
IP地址:	123. 12. 168. 1	
	1.多个IP用,分隔,如:192.168.0.100, 2.支持跨2段IP,如:1.1.1.1-1.1.2.25 3.支持通配符,如:1.1.1.*,1.1.*.*	192. 168. 0. 101 i4
作用范围:	 ✓ HTTP安全检测 ✓ 上传防护 ✓ 资源防盗链 ✓ 特定资源防护 ✓ 下载控制 ✓ Get、Post之外请3 	 ✓ 文件防护 ✓ сс攻击防护 求
		确定取消

图 6.4.3 添加 IP 白名单功能

不允许添加不同 IP 段的开启 IP 和结束 IP,也就是说 IP 地址首字节不一样时,将不允许添加。如下图 6.4.4 所示。

⑤ 返回	吃油加加 ID 白夕 英	- ×
<u>تې</u>	③ 添加IP白名单 × 规则描述: 测试规则	见则 导出规则
IP白名单规则	IP地址: 123.12.168.1-123.15.168.1	
	 ● 信息提示 	×
	IP地址前两段必须一样。	
	作用范围	
	· · · · · · · · · · · · · · · · · · ·	
	□ 全选 删除	添加规则

图 6.4.4 IP 白名单添加错误提示

◆ 导入:支持导入以前设置并备份的 IP 白名单规则,只需要在网站安全狗"IP 黑白名单"功能界面右上角处点击"导入",选择以前存放的路径,然后选择需要导入的 规则,点击"打开"就可导入。如下图 6.4.5 所示。

⑤ 返回	防护规则-IP白名单		- ×
		导入规	则 导出规则
<u>ت</u>	IP地址	规则名称 作用范围	
IP白名单规则	123.12.168.1	测试规则 HTTP检测 上传防护 GetPost之外请求 文件防护 防盗链 特定资源 CC防护	下载限制 📃 🕼
	 ② 选择一个dat或 ② ③ ● ● ● ● 组织 ● 新報 组织 ● 新報 文 收藏夹 ● 下载 ● 重 風片 ● 通 ① 出雷下载 ● 音乐 	xml文件导入 · 规则导入导出测试	
	≤	1)丌() 秋間	添加规则

图 6.4.5 IP 白名单导入

◆ 导出:当 IP 白名单中设置的规则需要应用到其他地方的网站安全狗,或者想

备份时,可以通过导出的方式,将 IP 白名单功能下的规则导出到指定的路径进行保存。 用户可以选中需要导出的规则,然后点击桌面右上角的"导出"按钮,选择要保存的路径, 点击"保存"即可。如下图 6.4.6 所示。

€ 返回	防护规则-IP白名单	- ×
	导入规则	导出规则
Ē	IP地址 规则名称 作用范围	
IP白名单规则	✓ 123.12.168.1 测试规则 HTTP检测 上传防护 GetPost之外请求 文件防护 防盗链 特定资源 CC防护 下载限制	- \$
	●保存文件 ● ●● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	
	✓ 全 隐藏文件夹 保存(S) 取消	砚则

图 6.4.6 IP 白名单导出

6.4.2 IP 黑名单

IP 黑名单是相对白名单进行设置的,通过设置一些不良 IP 地址为黑名单地址,从而限制它们访问网站的权限。

④ 返回	防护规则-IP黑名单			- ×
			导入规则	导出规则
<u> </u>	IP地址	规则名称		
IP黑名单规则	123.12.168.11	测试规则		□ \$\$
IP临时黑名单规则				
	□ 全选 剛涂			添加规则

图 6.4.7 IP 黑名单

6.4.2.1 IP 黑名单

支持新增、修改、删除 IP 黑名单, IP 黑名单设置对所有功能模块都生效。如下图 6.4.8 所示。

舰则名称:	测试规则
I P 地址:	123. 12. 168. 11

图 6.4.8 添加 IP 黑名单

◆ IP 黑名单和 IP 白名单一致,同样支持导入与导出操作,详见 6.4.1。

◆ IP 黑名单和 IP 白名单一致,不允许不同 IP 段的开启 IP 和结束 IP 进行添加,也 就是说 IP 地址首字节不一样时,将不允许添加。详见 6.4.1。

6.4.2.2 IP 临时黑名单

IP 临时黑名单主要用于具体的防护功能,支持针对具体的防护功能,设置单位时间内 访问 IP 触发规则后的冻结时效。IP 临时黑名单实现了自动化的 IP 黑名单添加,在冻结时 间内,用户对网站进行的操作都会被拦截。如下图 6.4.9 所示。

● 返回	防护规则-IP临时黑名单			- ×
<u>نې کارې انځا</u>	临时黑名单规则	规则内容	冻结时间	
IP黑名单规则	HTTP安全检测功能临时黑名单	60秒内非法访问10次	5分钟 -	- ŵ
IP临时黑名单规则				
	□ 全选 删除		添加規	M

图 6.4.9 IP 临时黑名单

(1) 目前 IP 临时黑名单只针对 HTTP 安全检测、上传防护、文件防护资源防盗链、资源防下载等功能模块。

(2)作用范围:用于设置 IP 临时黑名单在哪个功能点生效。如下图 6.4.10 所示。

作用范围:	文件防	方护				-
单IP访问上限:	60	秒内非法	法访问超过	10	次	
冻结时间:	5		分钟(建	议冻结时	时长不超过3	80分钟)

图 6.4.10 添加 IP 临时黑名单规则

(3) IP 访问上限:用于设置单位时间内,单个 IP 访问上限。

(4)冻结时间:用于设置触发规则后,该 IP 冻结时效。

6.4.3 爬虫白名单

न्द्र न			-	- ×
	防护规则-爬虫白名单			
6	爬虫关键字	描述		
爬中白名单规则	360spider		- 1	ŝ
	baiduspider		- 1	\$
	fast-webcrawler			ĝi 🛛
	google		<u> </u>	ĝi
	googlebot		- 1	ĝi 🛓
	🔲 iaskspider			\$
	mediapartners		<u> </u>	\$
	msnbot		- 1	\$
	slurp		— 1	ŝ
	sogou			ŝ
	sohu			ŝ
	sosospider		- 1	\$3
	-		— ,	~ *
	全选 删除		添加规则	Ņ

可以通过新增、删除爬虫搜索引擎访问关键词(针对 Http 协议中的 UserAgent 字段) 设置允许爬虫访问的网站。

图 6.4.11 爬虫白名单

通过添加爬虫关键字,放行爬虫,官方默认提供目前主流主流爬虫白名单,用户可以根据自身需要,进行调整。如下图 6.4.12 所示。

关键字描述:	雅虎		
爬虫关键字:	yahoo		

图 6.4.12 添加爬虫白名单规则

6.5 防护日志

防护日志功能提供详细的攻击拦截信息,通过查看防护日志可以对攻击情况进行分析,

为后续运营调整提供参考依据。

e 返回							≡ - >
	进日志 性化的日志功能	٤,有效分析、如	h理各类攻击。				(〇) 设置
			日志类型: 所有类型		<u>-</u>	2016/06/23 至 2016/06/23	刷新
时间	攻击IP	攻击类型	访问地址	端口	等级	说明	
2016-06-23 16:07:09	192.168.88.105	网站漏洞防护	192.168.88.109:8000/forum.php?(%	8000	1	拦截原因:Struts2远程命令执行漏洞	(s2-2016-3
2016-06-23 16:07:06	192.168.88.105	网站漏洞防护	192.168.88.109:8000/forum.php?%2	8000	1	拦截原因:Struts2远程命令执行漏洞	(s2-2016-3
2016-06-23 16:07:03	192.168.88.105	网站漏洞防护	192.168.88.109:8000/forum.php?(%	8000	1	拦截原因:Struts2远程命令执行漏洞	(s2-2016-3
2016-06-23 16:06:58	192.168.88.105	网站漏洞防护	192.168.88.109.8000/forum.php?id	8000	1	拦截原因:防止复杂的and or 方式注	入规则二
2016-06-23 16:06:55	192.168.88.105	网站漏洞防护	192.168.88.109.8000/forum.php?%2	8000	1	拦截原因:Struts2远程命令执行漏洞	(s2-2016-3
2016-06-23 16:06:52	192.168.88.105	网站漏洞防护	192.168.88.109.8000/forum.php?%2	8000	1	拦截原因:Struts2远程命令执行漏洞	(s2-2016-3
2016-06-23 16:06:48	192.168.88.105	网站漏洞防护	192.168.88.109:8000/forum.php?%2	8000	1	拦截原因:Struts2远程命令执行漏洞	(s2-2016-3
2016-06-23 16:06:45	192.168.88.105	网站漏洞防护	192.168.88.109.8000/forum.php?ld	8000	1	拦截原因:防止SQL联合查询	
2016-06-23 16:06:40	192.168.88.105	网站漏洞防护	192.168.88.109:8000/forum.php?id	8000	1	拦截原因:防止SQL联合查询	
2016-06-23 16:06:37	192.168.88.105	网站漏洞防护	192.168.88.109:8000/forum.php?id	8000	1	拦截原因:防止注入存储过程	
官方防护规则	版本:2016-06-1	16					

图 6.8.1 防护日志

◆ 日志类型:通过日志类型筛选,可以从数量众多的记录中查看指定类型的记录,如下图 6.8.2 所示。

Θ	返回							≡ - ×
		防护日志 个性化的日志功能	, 有效分析、	处 理各类 攻击。				(〇) 设置
				日志类型:	所有类型	2016/06/24	至 2016/06/24	刷新
	时间	攻击IP	攻击类型	访问划	网站漏洞防护 非法盗辩		说明	
					CU政治 学研程下数控制 事法構成文文件 事法感謝文文件 第15 物理文件 115 分配当件利用 115 分配当件利用 115 分配当件利用			
	官方防护规	则版本:2016-06-16						

图 6.8.2 日志类型

◆ 时间:点击时间栏目,设置时间范围查看指定范围内所有防护记录,如下图 6.8.3

所示。

Θ	返回					≡ - ×
		防护日志 个性化的日志功能	,有效分析、	处理各关攻击。		() 设置
				日志类型: 所有类型	2016/06/24 至 2016/06/24	刷新
	时间	攻击IP	攻击类型	访问地址	。	最近30天
					2016/6/24 ▼	确定
	官方防护规	则版本:2016-06-1	6			

图 6.8.3 时间段

◆ 设置:点击设置按钮进入防护日志功能设置界面,用户可以选择日志保存路径、文

件上限、保存天数,同时也可以指定需要展示的日志内容,如下图 6.8.4 所示。

0	❷ 设置					×] ≡ - ×
e	 设置 设置 公司与扫描设置 公司与扫描设置 公司漏洞防护设置 文件防护设置 文件防护设置 可工黑白名单设置 III IT黑白名单设置 	日志保存设置 保存路径: 日志文件大小: 保存天数: び町间 ☑前同地址 ☑ 说明	C:/Program 50 30	Files/SafeDog/SafeDogSiteI MB 天 又 辺 攻击IP 」 第口	IS/Anelysis/ ☑ 攻击类型 ☑ 等级	× 浏览	二 一 设置
	恢复出厂设置					保存	

图 6.8.4 防护日志设置

6.6 安全工具

包含网站加速、网站监控、、批量替换及 dede 专杀等小工具。

⑤ 返回		≡ - ×
*	→ 安全工具→ 网站狗安全实验室提供的工具	
■ 网站管理	Ē	
 図 図 図 図 図 図 第 1 1 1	度 図 強 に 空 に 空 に 空 に 空 に 空 に 空 に 空 に つ の 始 に 空 の ら に 空 の ら し つ の ら し つ の ら し つ の ら し の う の ら の う の ら の ら の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う の う つ う つ う つ う つ う つ う つ う つ う つ う つ う つ う つ う つ う つ う つ う つ う つ う つ う つ う つ う つ う つ う つ う つ う つ う つ う つ う つ う つ う つ う つ つ つ つ つ つ つ つ つ つ つ	
北星替拆 加 载	dede专系 加载	
	S 服务器安全狗 🔂	工具箱

图 6.6.1 安全工具

6.6.1 网站加速

网站加速主要是为网站图片、CSS、JS等静态资源提供全国性的访问加速服务。当网站 页面被访客访问时,该页面所包含的图片、CSS、JS等静态资源将会被部署在全国各地的智 能加速节点推送到访客面前。

网站加速		× 已开启
网站域名	加速效果	启用状态
□ 全选 删除		添加网站

图 6.6.2 网站加速

点击"开启按钮"开启网站加速服务。如果没有加入安全狗服云,就会弹出 提示"加入服云,才能开启使用网站加速功能"弹窗。如下图 6.6.3 所示。

⑤ 返回				≡ - ×
🗙 😪	全工具 均安全实验室提供的工具			
■ 网站管理	● 信息提示		×	
の 站加速 加載 ■ 实用工具		启用该功能必须先加入服云,请登陆]	
~			确定	
批量替换 已开启	dede专乐 加载			
			5 服务器安全狗	工具箱

图 6.6.3 加入服云

选择需要加速的网站,添加到加速列表,如下图 6.6.4 所示。

● 选择需要加速的网站				×
		Q L-↑	下一个	刷新
网站域名	网站路径		d	状态
■ 全选			确定	取消

图 6.6.4 添加网站加速

特别注意:

- ◆ 网站加速功能暂不支持对纯 IP 域名、带端口域名、动态资源进行加速;
- ✤ 加速的资源类型包含: gif、jpg、jpeg、png、bmp、js、css等;
- ◆ 若网页内容发生改变,只需点击"刷新缓存"即可;

6.6.2 网站监控

网站监控功能实现对 IIS 下所有网站的实时、单独流量监控,CPU 资源耗用监控,帮助 用户掌握实时的网站流量信息,快速判断、及时定位攻击。用户在"安全工具"选择"网站 监控"功能,点击加载安装即可实时查看网站和服务器的基本使用状态。
④ 返回	= - ×
×	安全工具网站狗安全实验室提供的工具
■ 网站管理	
 図 Minia ○ 用工具 	一 の 対 监 控 已 开 肩
北星替换日开启	-dcde dede专系 已开启
	S 服务器安全狗 二具箱

图 6.6.5 网站监控

6.6.2.1 流量监控

流量监控功能可以帮助用户实时监控 IIS 下各个站点的流入、流出及总流量,并且提供 全部站点实时实时的流入、流出及总流量总体信息。用户可以通过个性化的选择,来筛选需 要显示流量信息的网站,也可以通过选择不同的排序方式,重新排列网站流量信息的顺序, 方便查看。

🗾 阿站监控工具-安全狗安全实验室提供				A REAL PROPERTY.	×
流量监控CPU监控					
🔼 如果网站名称被修改,i	青重新选择网站!	显示所有网站	▼ 按总流量排序	▼ 选择站。	Ψ.
💟 🔽 自动刷新 🔂 立即刷新					
网站域名	网站名称	流进流量	流出流量	总流量	<u> </u>
全部站点	_Total	0.00B/S	0.00B/S	0.00B/S	
192. 168. 7. 60	默认网站	0.00B/S	0.00B/S	0.00B/S	
192. 168. 7. 60:100	dwlt7.1.0	0.00B/S	0.00B/S	0.00B/S	
192. 168. 7. 60: 101	mutillidae2.4.5	0.00B/S	0.00B/S	0.00B/S	
192. 168. 7. 60:102	sqlol-master	0.00B/S	0.00B/S	0.00B/S	
192. 168. 7. 60:103	exploit-wa	0.00B/S	0.00B/S	0.00B/S	
192. 168. 7. 60: 104	OWASP Hackademic	0.00B/S	0.00B/S	0.00B/S	
192. 168. 7. 60: 105	WackoPicko-master	0.00B/S	0.00B/S	0.00B/S	
102 160 7 60-12060	J:90	0.000/0	n nnø/e	0.002/6	•

图 6.6.6 流量监控

6.6.2.2 CPU 监控

CPU 监控功能根据对进程池的监控,实现对网站占用 CPU、内存的实时监测。用户可以 通过选择不同的排序方式,查看各个应用程序池的 CPU、内存占用情况,及时发现相应网站 的实时运营状态。

网站监控工具-安全狗安全实验室提供				
流里监控 CPV监控				
如果您更改了应用程序测 □ 自动刷新 ○ 立即刷新	9 与网站的关联,请点击"关联刷新"按钮。 ➤ 关联刷新		按应用程序池排序 💌	
应用程序池	域名	CPU利用率	内存大小	

图 6.6.7 CPU 监控

6.6.3 批量替换

用户在"安全工具"栏目选择"批量替换"功能,点击加载安装即可通过小工具进行文件内容批量替换。

⑤ 返回		≡ - ×
*	安全工具 网站狗安全实验室提供的工具	
■ 网站管理		
図4功0速ごますごます第二月	図站监控 已开启	
北星替换日开启	dede dede专杀 已开启	
	5 服务器安全狗	

图 6.6.8 批量替换

添加需要进行内容替换的文件路径,设置涉及替换操作的文件类型。如下图 6.6.9 所示。

批型替换工具	安全狗安全实验室提供		×
文件类型:	□ 所有类型	更多软件请登录www.safed	og. cn
*. asp *. php *. asp	x *. html *. htm *. inc *. js	*. shtml *. txt *. doc *. cpp	
要检查的目录,可直	接拖: + - 2个		
D:\Axure_RP_Pro_ D:\HttpWatchPro	6.0.0.2899_for_Windows_Ch 5\HttpWatch	inese\Axure_RP_Pro_6.0.0.2899_	for_V
4			•
		后退 下一	步

图 6.6.9 文件路径与类型设置

点击"下一步",设置替换内容,点击"下一步",执行替换操作。如下图 6.6.10 所示。

	↑記刀空ノ: ┓━━━━━━┓	🔲 是否区分大小写
普通字符串	正则表达式	
VBScript.Enco	ode	
	BN1 ++ 15 st ->-	
奋换后的内谷,	默认替换为空:	

图 6.6.10 批量替换内容设置

6.6.4 dede 专杀

用户在"安全工具"栏目选择"dede 专杀"功能,点击加载安装即可进行数据库后门 扫描。

⑤ 返回		≡ - ×
*	 ◆ 安全工具 ◆ 网站狗安全实验室提供的工具 	
■ 网站管		
 网站II 已开启 ■ 实用工		
	· dede 使 dede 专系 已开启	
	● 服务器安全狗	工具箱

冬	6.	6.	11	dede	专杀
---	----	----	----	------	----

配置数据库相关信息,点击扫描开始查杀后门。如下图 6.6.12 所示。

🙀 DedeCMS数据库后门查并	工具一安全狗安全实验	金室提供	_ ×
数据库IP: 127.	0.0.1	端口: 3306	
用户名:		密 码:	
数据库名称:		添加 批量	詩入
数据库IP	用户名	数据库名	端口号
	(注穴別主)		
	「用王列衣」		

图 6.6.12 dede 专杀设置

6.7 防护等级

按照防护严格程度,系统提供包括初级、中级、高级及自定义在内的四种安全模式。初 装网站安全狗状态下,系统默认选中初级防护模式。

● 网站安全狗(IIS版) V4.0 正式版 ④ safedog000 [体验版]	
上次发现2个危险文件,其中1个未处理 上次扫描时间:2016-06-2010:33:51 立即扫描	2天 持续保护网站 0 个
⑦ 防护等级 自定义 ④ 拦截攻击 0次	[]] [P黑白名单] [][][][][][][][][][][][][][][][][][][
「「「我的服云」	务器安全狗 一 工具箱

图 6.7.1 防护等级

用户选择对响应功能进行开启/关闭操作时,安全模式自动调整为自定义模式。如下图 6.7.2 所示。

😌 返回					×
🗐 安全防护等	级				
(初级	中级	高级	自定义)
漏	洞防护	行为防护		资源防护	
htt 上f	tp安全检测 日开启 专防护 日开启	危险组件防护 敏感函数防护 禁止IIS执行程序 一句话后门防护 TCP/UDP发包	已开启	资源防盗链 日开启 特定资源防护 日开启 环境信息隐藏 已关	E J
Ż	件防护	内容防护		流量防护	
				保存	取消

图 6.7.2 等级设置

◆ 初级:只开启最低限度的防护功能,为用户提供基础防护,安装成功后的默认配置。

- ◆ 中级:适中的防护等级,相比初级模式,增加了一句话后门防护及网站后台防护。
- ◆ 高级:最严格的防护等级,所有防护功能全部启用。
- ◆ 自定义:允许用户进行自定义设置开启/关闭指定功能。

6.8 辅助功能

6.8.1版本信息

通过鼠标停留在界面左上角的版本号,在提示窗查看主程序版本号、网马库版本号,或 通过点击提示窗上的检查更新按钮,开启版本更新检查工具。

e 网站安全狗 (IIS版) V4.0 正式版 ● safedog000 [体验版]	ữ ≡ - ×
◎ 主程序版本: V4.0.14298	
○ 阿马库版本: 2016-06-16	
这种意思,这些意思 。 一世的一些,这些意思,我们就是一些。 一世的一些,我们就是一些。 一世的一些,我们就是一些。 一世的一些,我们就是一些。 一世的一些,我们就是一些。 一世的一些。 一世的一些。 一世的一些。 一世的一些。 一世的一些。 一世的一些。 一世的一些。 一世的一些。 一世的一些。 一世的一些。 一世的一些。 一世的一些。 一世的一些。 一世的一些。 一世的一些。 一世的一些。 一世的一些。 一世的一些。 一世的一些。 一世的一些。 一世的一些。 一世的一些。 一世的一些。 一世的一些。 一世的一些。 一世的一些。 一世的一些。 一世的一些。 一世的一些。 一世的一些。 一世的一些。 一世的一些。 一世的一些。 一世的一些。 一世的一世。 一世的一世。 一世的一世。 一世的一世。 一世的一世。 一世。 一世。 一世。 一世。 一世。 一世。 一世。	
上次扫描时间:2016-06-20 10:33:51	3天
立即扫描	持续保护网站 0 个
◎防护等级自定义 ② 拦截攻击 0次 网站防护 资源防护	IP黑白名单 防护日志
ま 我的服云 いい おお 服気	各器安全狗 一一 工具箱

图 6.8.1 版本信息

6.8.2 登录

登录服云账号,即可将该服务器加入到服云中,更加方便快捷的管理服务器。 步骤1。点击主界面左上角"未登录",点击后弹出界面。如下图6.8.2 所示。



图 6.8.2 加入服云1

步骤 2. 输入服云用户名和密码,点击"登录服云"。如下图 6.8.3 所示。

🐵 网站安全狗(IIS版) V4.0 正式版 🜘 未登录		$\Im \equiv - \times$
e	登录 (8) 用户名/邮箱/手机号码 合 密码	× 3天 炉网站 0 个
	注册服云帐号 忘记密码?	
	登录服云	
		■
110人服云		5 服务器安全狗 🗗 工具箱

图 6.8.3 加入服云2

步骤3.进行账号有效性验证。如下图6.8.4 所示。

⊖ 网站安全狗(IIS版) V4.0 正式版 ④ 未登录		$\Im \equiv - \times$
e		× 3天 炉网站 0 个
	正在验证服云帐号	
	取消	
♥防护等级 自定义		单 前护日志
15 加入服云		S 服务器安全狗 二具箱

图 6.8.4 加入服云 3

步骤 4. 登录成功后,用户可以点击"体验服云"前往服云 Web 端进行相关管理操作。 如下图 6.8.5 所示。

◎ 网站安全狗(IIS版) V4.0 正式版 ⑦ 未登录		☎ = ->	<
e *a,	您的服务器已经成功添加到云安全中心 打开服云,随时随地管理服务器安全!	× 3天 炉网站0个	
	体验服云		
⑤ 防护等级 自定义	查看特权	¥ 防护日志	
10入服云		S 服务器安全狗 — 工具箱	

步骤 5. 登录成功后,用户可以点击"查看特权",了解当前账号所能享受的服云各项服务详情,或点击主界面左下角的"我的服云"进行了解。如下图 6.8.6、图 6.8.7 所示。

图 6.8.5 加入服云4

😑 网站安全狗 (IIS版) V4.0 正式版 🜘) safedog000	$\Im \equiv - \times$
e	服云用户: safedog000 云监控 随时掌握服务器各方面安全运行数据 ② 登录监控 ③ 资源监控	3天 ^{炉网站} 0 个
	安全官理 批重安全策略管理,确保硕出快速时应对和防护调整 ⑧ 服务器安全策略 ⑧ 网站安全策略 ⑩ IDDOS云防护 『 全网高危IP黑名单	
◎ 防护等级 自定义	●	● 防护日志
15 我的服云	S 服务器安全狗	
 A Padadi (Philippe) a constration 	图 6.8.6 查看服云特权 1	
	▶ safedog000 [排驗版] 次发现2个危险文件,其中1个未处理 次扫描时间:2016-06-20 10:33:51 立即扫描	☆ = - × 3天 ^{沪网站} 0个
登录享持权: ▲ 风险管理 風 威胁分析 ④ 安全策略 ④ 云端管理 ● 云游控	0次 网站防护 资源防护 IP黑白名 5	单 防护日志
我的服云	5 服务器安全狗	

图 6.8.7 查看服云特权 2

步骤 6. 登录成功后,主界面左上角的登录状态显示账号及该账号对应的服云套餐等级,用户可以点击账户名或套餐等级,前往服云 Web 端进行相应的账号权限升级。如下图 6.8.8 所示。

 ● 网站安全狗(IIS版) V4.0 正式版 ● safedog000 (俳磁版) 上次发现2个危险文件,其中1个未处理 上次扫描时间: 2016-06-20 10:33:51 立即扫描 	☆ = - × 3天 持续保护网站 0 个
◎ 防护等级 自定义 ② 拦截攻击 0次	IP黑白名单
ま 我的服云 S 服	资器安全狗 工具箱

图 6.8.8 登录状态

6.8.3 皮肤

网站安全狗支持两种皮肤设置, "天空蓝"和"无皮肤"。

● 网站安全狗 (IIS版) V4.0 正式版	 ★ 三 - × ✓ 天空蓝 无皮肤
还未对本机进行扫描,无法确保网站安全 建议立即扫描 立即扫描	1天 持续保护网站 0 个
● 防护等级 自定义 ② 拦截攻击 0次	IP黑白名单 防护日志
	B労器安全狗

图 6.8.9 皮肤设置

6.8.4 系统设置

6.8.4.1 系统常规设置

(1) 开机启动设置:设置是否开机自启动网站安全狗。如下图 6.8.10 所示。

😌 设置		×
 系统常规设置 网马扫描设置 漏洞防护设置 文件防护设置 文件防护设置 IP黑白名单设置 防护日志设置 	开机府动设置 ● 开机时自动运行网站安全狗(IIS版) 关闭程序设置 ● 程序关闭时进行提醒 ● 检测到可用更新时,自动升级到最新版本(推荐) ● 检测到可用更新时,提曜升级(不自动升级) 自防护设置 验证方式 ● 使用版云账号验证(推荐) ● 使用本地密码验证 通勤新客码	-
恢复出厂设置	保有	Ŧ

图 6.8.10 开机启动设置

(2)关闭程序设置:可选择是否关闭程序时,弹出提示框。如下图 6.8.11 所示。

● 设置		×
 ◎ 系统常规设置 ② 网马扫描设置 ③ 漏洞防护设置 □ 文件防护设置 	开机启动设置 ✓ 开机时自动运行网站安全狗(IIS版) 关闭程序设置 ✓ 程序关闭时进行提醒 攻击提醒设置	-
 ■ IP黑白名单设置 ■ 防护日志设置 	 ✓ 开启攻击拦截提醒 升级设置 ● 检测到可用更新时,自动升级到最新版本(推荐) ● 检测到可用更新时,提醒升级(不自动升级) 自防计设置 	
	 验证方式 使用服云账号验证(推荐) 使用本地密码验证 じ置新密码 新密码: 	
恢复出厂设置	保存	

图 6.8.11 关闭程序设置

(3) 攻击提醒设置:托盘进行攻击提醒。如下图 6.8.12 所示。

😌 设置		×
◎ 系统常规设置	开机启动设置	-
 ⑦ 网马扫描设置 ◎ 漏洞防护设置 □ 文件防护设置 □ IF黑白名单设置 副 防护日志设置 	 ✓ 开机时自动运行网站安全狗(IIS版) 关闭程序设置 ✓ 程序关闭时进行提醒 攻击提醒设置 ✓ 开启攻击拦截提醒 升级设置 ● 检测到可用更新时,自动升级到最新版本(推荐) ● 检测到可用更新时,提醒升级(不自动升级) 	
	 目防护设置 验证方式 ② 使用服云账号验证(推荐) ③ 使用本地密码验证 □ 设置新密码 新密码: 新密码 	•
恢复出厂设置	保護	字

图 6.8.12 攻击提示设置

- (4)升级设置:可选择自动或提醒两种升级方式。
 - ◆ 自动升级模式:检测有新版本时,直接升级(官方推荐该方式)。
 - ◆ 提醒升级模式:检测有新版本时,提醒用户是否升级,根据用户的选择决定是否升

级。

❷ 设置		×
◎ 系统常规设置	开机启动设置	-
 ⑦ 网马扫描设置 ⑦ 漏洞防护设置 ① 文件防护设置 1 文件防护设置 1 IT黑白名单设置 圖 防护日志设置 	 ✓ 开机时自动运行网站安全狗(IIS版) 关闭程序设置 ✓ 程序关闭时进行提醒 攻击提醒设置 ✓ 开启攻击拦截提醒 升级设置 ● 检测到可用更新时,自动升级到最新版本(推荐) 	
	 检测到可用更新时,提醒升级(不自动升级) 自防护设置 验证方式 ④ 使用服云账号验证(推荐) ④ 使用本地密码验证 □ 设置新密码 新密码: 	_
恢复出厂设置	保在	Ŧ

图 6.8.13 升级设置

(5) 自防护设置: 对界面或功能进行操作时, 需要进行身份验证。

1) 验证方式

◆ 使用服云账号验证:登录服云账号,设置后,当用户操作所选功能时,需输入服云
登录密码,该方式更加安全,官方推荐采用该验证方式。

◆ 使用本地密码验证:通过设置本地密码进行身份验证,设置后,当用户操作所选功 能时,需输入已设置好的本地密码。

2) 有效时间

置输入密码后,界面无操作的最大时间间隔。当需要设置为每次操作都需要输入密码。则值可定义为 0。

3) 防护项目

选择需要进行防护的界面操作或功能设置,允许多选。

❷ 设置		×
◎ 系统常规设置	◎ 检测到可用更新时,提醒升级(不自动升级)	-
🕤 网马扫描设置	自防护设置	
③ 漏洞防护设置	验证方式	
🗀 文件防护设置	◎ 使用服云账号验证(推荐)	
🗐 IP黑白名单设置	◎ 使用本地密码验证 □ 设置新変码	
圖 防护日志设置	新密码: 新密码	
	确认密码: 确认新密码	
	有效时间	
	每次密码验证成功后 5 分钟内,无需重新验证	
	(如要求每次都需要密码验证,请输入0)	
	保护项目	
	□ 退出程序 □ 卸载程序 □ 卸载插件 □ 切换防护总开关	
	 □ 重启Web服务 □ 网马查杀 □ 网站防护 □ 资源保护 	
	□ IP黑白名单 □ 打开自防护设置页面	Ŧ
恢复出厂设置	保	存

图 6.8.14 自防护设置

6.8.4.2 网马扫描设置

(1)选择扫描文件类型。如下图 6.8.15 所示。

系统常规设置	扫描文件类型	
》网马扫描设置	◎ 扫描所有文件	
》 漏洞防护设置	● 扫描目定义文件类型	
] 文件防护设置	□.asa 添加扩展名	
IP黑白名单设罟	□.asp 移除	
防护日志设置	.aspx	
	cdx	
	.cer	
	扫描文件大小	
	扫描项目	
	☑ 扫描网页木马	
	✓ 扫描网页挂马/黑链(文件清理后无法恢复,建议做好文件备份)	

图 6.8.15 扫描文件类型设置

(2) 设置扫描的目标文件大小和文件类型。如下图 6.8.16 所示。

❷ 设置		×
 ● Rat ◎ 系统常规设置 ④ 网马扫描设置 ◎ 漏洞防护设置 □ 文件防护设置 □ IP黑白名单设置 □ 防护日志设置 	J描広件类型 ● 扫描所有文件 ● 扫描自定义文件类型 J描放件大小 ● 跳过大手 1024 KB文件 J描 网页木马 ● 扫描网页本马 ● 扫描网页挂马/黑鲢 (文件清理后无法恢复,建议做好文件备份) ● 扫描畸形目录/文件 ● 口动扫描与清理 ● 自动扫描 ,但不清理危险文件 ● 五田扫描 , 但不清理危险文件	-
恢复出厂设置	◎ 自动扫描并清理危险文件	↓

图 6.8.16 扫描文件大小设置

(3) 设置扫描项目。如下图 6.8.17 所示。

❷ 设置		×
 ◎ 系統常规设置 ④ 网马扫描设置 ④ 漏洞防护设置 □ 文件防护设置 □ IP黑白名单设置 □ IP黑白名单设置 □ 防护日志设置 		-
恢复出厂设置	保	存

图 6.8.17 扫描项目设置

(4) 设置自动扫描与清理。如下图 6.8.18 所示。

● 设置		×
☞ 系统常规设置	扫描项目	<u>*</u>
⑦ 网马扫描设置		
③ 漏洞防护设置		
🗀 文件防护设置	自动扫描与清理	
🗐 IP黑白名单设置	⑦ 不自动扫描	
🗐 防护日志设置	◎ 自动扫描,但不清理危险文件	
	每天 2:00 丁 开始扫描	
	◎ 自动扫描并清理危险文件	
	隔离区设置	
	□ 自动隔离一般网页木马	
	隔离区路径: ./guarantine/ 浏	览
	云安全计划	
	□ 加入"云安全计划",发现可疑文件后自动上报	-
恢复出厂设置		保存

图 6.8.18 自动扫描与清理设置

(5) 设置隔离区路径。如下图 6.8.19 所示。

❷ 设置		×
@ 系统常规设置	☑ 扫描畸形目录/文件	<u> </u>
⑦ 网马扫描设置	自动扫描与清理	
◎ 漏洞防护设置	◎ 不自动扫描	
🗅 文件防护设置	● 自动扫描,但不清理危险文件	
IP黑白名单设置	每天 2:00 ▼ 开始扫描	
圖 防护日志设置	◎ 自动扫描并清理危险文件	
	隔离区设置 自动隔离一般网页木马 隔离区路径: ./quarantine/ 浏览 	
	云安全计划 □ 加入"云安全计划",发现可疑文件后自动上报 您选择假如安全狗"云安全计划"后,我们将把扫描过程中发现得可疑文件自动上报云端作为分析样本,在此过程中,我们将严格遵守《用户协议》中关于用户隐私权的声明,绝不危害任何用户隐私。	-
恢复出厂设置	· · · · · · · · · · · · · · · · · · ·	存

图 6.8.19 隔离区设置

(6) 设置加入云安全计划。如下图 6.8.20 所示。

● 设置		×
◎ 系统常规设置	☑ 扫描畸形目录/文件	-
⑦ 网马扫描设置	自动扫描与清理	
◎ 漏洞防护设置	◎ 不自动扫描	
🗀 文件防护设置	● 自动扫描,但不清理危险文件	
🗐 IP黑白名单设置	每天 2:00 ▼ 开始扫描	
圖 防护日志设置	◎ 自动扫描并清理危险文件	
	隔离区设置	
	□ 自动隔离一般网页木马	
	隔离区路径: ./quarantine/ 浏览	
	云安全计划	
	☑ 加入"云安全计划",发现可疑文件后自动上报	
	您选择假如安全狗"云安全计划"后,我们将把扫描过程中发现得可疑文件自动上报 云端作为分析样本,在此过程中,我们将严格遵守《用户协议》中关于用户隐私权的声 明,绝不危害任何用户隐私。	
恢复出厂设置	1	↓ 保存

图 6.8.20 云安全计划设置

6.8.4.3 漏洞防护设置

支持设置漏洞防护功能的拦截提示信息。如下图 6.8.21 所示。

❷ 设置		×
 ◎ 系統常规设置 ④ 网马扫描设置 ● 漏洞防护设置 ● 文件防护设置 ● 文件防护设置 ● IP黑白名单设置 >> 防护日志设置 	 漏洞防护拦截返回页面 百方默认内容 自定义内容 HTTP头部检测功能拦截攻击提示信息 X的请求带有不合法参教,已被网站管理员设置拦截: 可能原因:您提交的内容包含危险的攻击请求 如何解决: 1)检查提交内容; 2)如闷站托管,请联系空间提供商; 3)普通网站访客,请联系网站管理员; 	A
	 上传防御拦截攻击提示信息 您请求的页面包含一些不合理的内容,已被网站管理员设置拦截: 可能原因:您请求的页面包含一些不合理的内容 如何解决: 1)检查请求的页面内容; 	-
恢复出厂设置		保存



- ◆ 官方默认内容:官方提供的拦截页面提示内容。
- ◆ 自定义内容:用户可自定义拦截页面提示内容。

6.8.4.4 文件防护设置

支持设置文件防护功能的拦截提示信息。如下图 6.8.22 所示。

● 设置		×
 ◎ 系统常规设置 ● 同与扫描设置 ● 漏洞防护设置 ● 文件防护设置 ■ IF黑白名单设置 ■ 防护日志设置 	 9 百方默认内容 ④ 百方默认内容 ④ 百定义内容 2 方能原因: 您请求的页面包含一些不合理的内容,已被网站管理员设置拦截: 可能原因: 您请求的页面包含一些不合理的内容 4 如何解决: 4 1 检查请求的页面内容; 4 2 如网站托管,请联系空间提供商; 4 3 普通网站访客,请联系网站管理员; 	
恢复出厂设置		保存

图 6.8.22 文件防护设置

- ◆ 官方默认内容:官方提供的拦截页面提示内容。
- ◆ 自定义内容:用户可自定义拦截页面提示内容。

6.8.4.5IP 黑白名单设置

支持设置文件防护功能的拦截提示信息。如下图 6.8.22 所示。

● 设置		×
 ◎ 系統常规设置 ④ 网马扫描设置 ④ 漏洞防护设置 ● 文件防护设置 ■ IF黑白名单设置 圖 防护日志设置 	 IP黑白名单拦截返回页面 會方默认內容 您的IT已被网站管理员设置成禁止访问: 可能原因:您的访问ITP被添加到网站安全狗ITP黑名单中 如何解决: 	
	◎ 自定义内容	
恢复出厂设置		保存

图 6.8.23 IP 黑白名单设置

- ◆ 官方默认内容:官方提供的拦截页面提示内容。
- ◆ 自定义内容:用户可自定义拦截页面提示内容。

6.8.4.6 防护日志设置

支持对防护日志功能的展示内容、日志文件大小、保存天数及保存路径进行设置。如下 图 6.8.22 所示。

❷ 设置					×
💿 系统常规设置	日志保存设置				
🕣 网马扫描设置	保存路径:	C:/Program Fi	les/SafeDog/SafeDogSi	teIIS/Analysis/	浏览
③ 漏洞防护设置	日志文件大小:	50	MB		
🗅 文件防护设置	保存天数:	30	F		
🔟 IP黑白名单设置	详细日志内容				
圓 防护日志设置	☑ 时间		☑ 攻击IP	☑ 攻击类型	
	☑ 访问地址		☑ 端口	☑ 等级	
	☑ 说明				
恢复出厂设置					保存

图 6.8.24 防护日志设置

- ◆ 日志保存设置:用于设置日志保存路径、日志文件大小及保存天数。
- ◆ 详细日志内容:用于设置日志界面需要展示的内容。

6.8.5 防护状态

安装成功后,主界面右上角区域将显示网站安全狗已防护网站个数及防护天数。

	ଫ ≡ - ×
び未对本机进行扫描,无法确保网站安全 建议立即扫描 立即扫描	42天 持续保护网站 2 个
● 防护等级 自定义 ② 拦截攻击 0次	[] [P黑白名单 [] [] []
影 我的服云	時器安全狗 🔂 工具箱

图 6.8.25 防护状态

6.8.6 拦截攻击

安装成功后,主界面左上角区域将显示网站安全狗已拦截的攻击数量,点击拦截攻击次数,前往服云 Web 端了解详细攻击信息或进行其他相应操作。

	镫 ≡ - ×
び未对本机进行扫描,无法确保网站安全 建议立即扫描 立即扫描	42天 持续保护网站 2 个
◎ 防护等级 自定义 ② 拦截攻击 0次	[] IP黑白名单 [] 防护日志
15. 我的服云 5. 服	务器安全狗

图 6.8.26 拦截攻击次数

6.8.7 服务器安全狗

尚未安装服务器安全狗状态下,点击主界面右下角的"服务器安全狗",系统将自动下 载并安装该产品,已安装状态下则自动启动该产品主界面。

	✿ = - ×
上次发现2个危险文件,其中1个未处理 上次扫描时间:2016-06-2010:33:51 立即扫描	3天 持续保护网站 0 个
	务器安全狗 「「二」」

图 6.8.27 服务器安全狗快捷方式

7. 关于我们

7.1 关于我们

安全狗是国内知名的互联网安全品牌,专注于(云)服务器安全。首创的云+端云安全 管理平台(SAAS模式)为用户解决公有云、私有云和混合云环境中可能遇到的安全及管理 问题,提供包含自动化系统风险识别和加固、系统级安全防护(防黑/防入侵/抗攻击)、云 监控(安全监控/性能监控/日志监控)、云管理(多公有云管理/混合云管理)以及基于大 数据架构的安全事件分析等功能。

安全狗云安全服务平台目前已经防护超过百万台的(云)服务器,日均为用户拦截超过 千万次的攻击,是国内该领域用户量最大的云安全服务平台。 同时安全狗也积极参与到国内云计算安全生态的建设,目前已经跟国内主流大型云计算 平台建立合作伙伴关系;安全狗云安全服务平台已经成功对接各大云计算平台。

安全狗归属的厦门服云信息科技有限公司在成立不到两年时间内,获得了 IDG 等国内一 线投资机构的 A、B 轮投资。作为一家年轻的云安全领域创业公司,我们致力于通过领先的 安全技术、大数据处理平台为用户提供创新性的安全服务。

7.2 联系我们

7.2.1 官方网站

http://www.safedog.cn

7.2.2 官方论坛

http://bbs.safedog.cn

7.2.3 服务与支持

- 1) 在线支持: (工作日 8:40-22:00 非工作日: 8:40-18:00)
- 2) 电话号码: 400-1000-221
- 3) 邮箱地址: tech@safedog.cn

7.2.4 市场与合作

- 1) 在线支持: (工作日 8:40-18:00)
- 2) 电话号码: 0592-3833142 0592-3775556
- 3) 邮箱地址: kangjian@safedog.cn
- 4) 联系地址: 福建省厦门市软件园二期观日路 58 号