



云翼-安全一体机系统 用户手册

北京瑞和云图科技有限公司

www.rivercloud.com.cn

2020 年

目录

1. 软件入门	6
1.1. 使用说明	6
1.2. 系统使用	6
2. 操作入门	7
2.1. 用户登录	7
3. 管理界面	8
3.1. 预警提示	8
3.2. 用户信息	8
4. 菜单	9
4.1. 首页菜单	10
4.2. 资产管理菜单	11
4.2.1. 资产分组管理	11
4.2.2. 资产管理	12
4.2.3. 网站管理	12
4.2.4. 认证信息	13
4.3. 任务管理菜单	14
4.3.1. 资产梳理	15
4.3.2. 主机漏洞扫描	16
4.3.3. 基线配置核查	18
4.3.4. 网站漏洞监控	21
4.3.5. 网站可用性监测	25

4.3.6.	网站篡改监测	26
4.3.7.	数据库扫描	27
4.3.8.	弱口令猜解	29
4.4.	等保合规菜单	31
4.5.	报表管理菜单	32
4.5.1.	主机漏洞扫描报告	33
4.5.2.	基线配置核查报告	34
4.5.3.	网站漏洞监控报告	35
4.5.4.	网站篡改监测报告	36
4.5.5.	网站可用性监测报告	37
4.5.6.	数据库漏洞扫描报告	38
4.5.7.	弱口令猜解报告	39
4.5.8.	等保合规报告	40
4.5.9.	历史报告列表	40
4.6.	模板管理菜单	41
4.6.1.	主机扫描策略	42
4.6.2.	基线核查策略	44
4.6.3.	网站扫描策略	45
4.6.4.	数据库扫描策略	46
4.6.5.	敏感关键字模板	46
4.6.6.	网站代理服务器	47
4.6.7.	密码字典模板	47

4.7.	日志管理菜单	48
4.7.1.	操作日志	48
4.7.2.	系统日志	49
4.7.3.	告警日志	49
4.8.	系统管理菜单	50
4.8.1.	用户管理	50
4.8.2.	角色管理	52
4.8.3.	系统设置	53
4.8.4.	引擎管理	54
4.8.5.	数据备份	55
4.8.6.	诊断工具	55
4.8.7.	升级管理	56
4.8.8.	服务器管理	57

版权申明

本文档包含了机密的技术和商业信息，提供给客户或合作伙伴使用。接受本文档表示同意对其内容保密并且未经书面认可，不得复制、泄露或散布本文档的全部或部分内容。

本文档及其描述的产品受有关法律的版权保护，对本文档内容的任何形式的非法复制，泄露或散布，将导致相应的法律责任。

保留在不另行通知的情况下修改本文档的权利，并保留对本文档内容的解释权。

1. 软件入门

1.1. 使用说明

如果您的访问业务较大，或者需要支持更多资产的扫描，可以联系开发厂商使用分布式部署方式。

1.2. 系统使用

将该系统接入网络后，打开浏览器（建议使用 chrome、firefox 或 ie10 及以上版本），输入地址：<https://ip> 即可访问综合扫描系统。

第一次进入系统会提示缺少许可文件，根据操作界面(下图)，复制授权号，把授权号发送给软件开发商，软件开发商会根据约定生成 license.dat，最后通过界面把 license.dat 文件导入系统即可。license.dat 许可文件只适用于指定的机器运行才有效，即授权号与 license.dat 是一一对一关系。



提示：

许可文件未找到：

请将“授权号”文本或“二维码授权号图片”发给开发商制作许可文件 (license.dat) 后再导入该系统！

1、授权号：

a76a6cbfb93cbb6daa4c4836544564fb777a0803|RHYT-0001-01|1593327000083

2、二维码授权号：

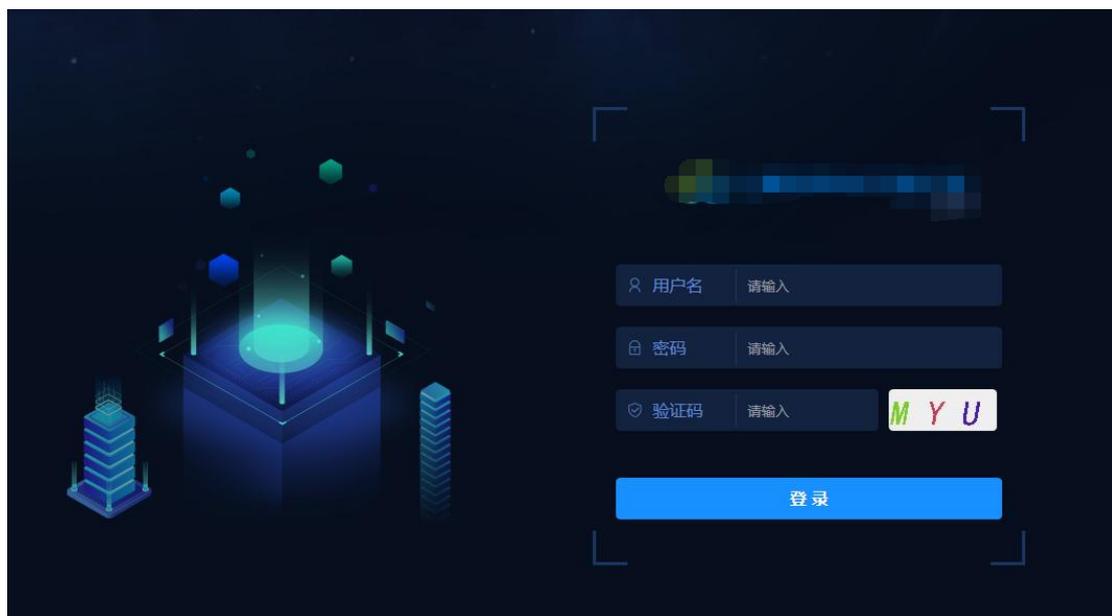


导入许可

2.操作入门

2.1. 用户登录

输入正确的用户名、密码、验证码后点击登录按钮，即可成功登录到系统。



- 首次登录系统会有 4 个默认的用户。（用户名分别为：admin、audit、secret、scan，密码均为：用户名 123456）输入正确的验证码后即可登录，且该用户不能被删除和锁定。
- 创建的用户密码输入错误 5 次会被锁定 300 秒，可通过系统管理菜单里的用户管理进行解锁。（可在用户管理中对密码输入的错误次数和锁定时间进行设置）

3. 管理界面

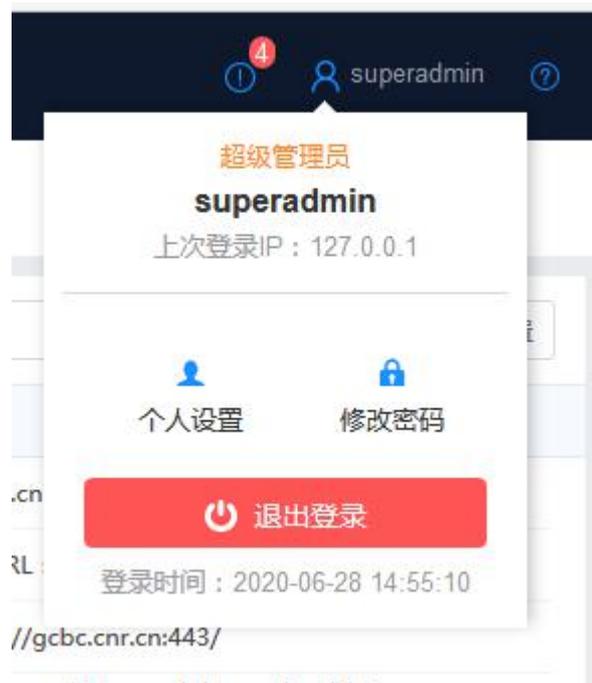
3.1. 预警提示

页面右上角：预警提示，显示弱点总条数，可点击查看预警详情（风险类型、名称和预警时间）。



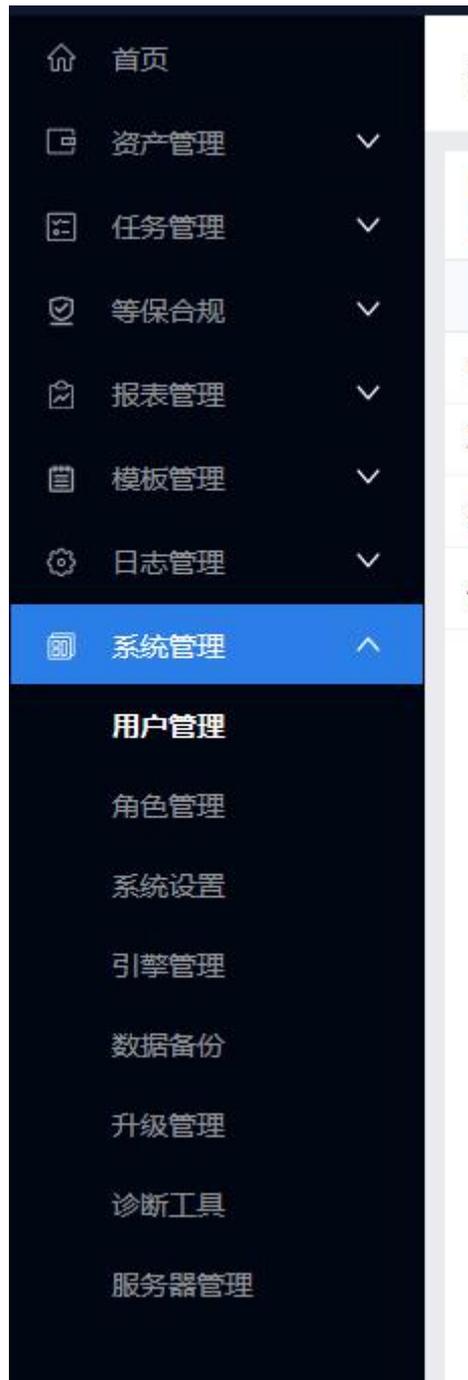
3.2. 用户信息

页面右上角：用户信息，显示当前用户，可以查看用户名、角色、登录时间、上次登录 IP，还可以修改当前用户密码和切换用户。



4. 菜单

不同的用户登录可能看见的菜单不同，系统只会显示当前登录用户有权限的菜单。



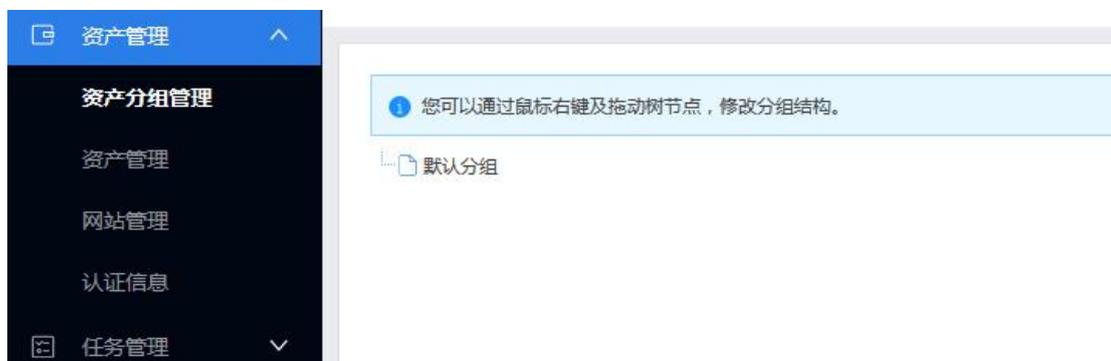
4.1. 首页菜单

该页面主要用于显示系统使用状态以及风险状态。



4.2. 资产管理菜单

资产管理菜单包括资产分组管理、资产管理、网站管理和认证信息。



4.2.1. 资产分组管理

该模块主要用于管理平台的所有资产组，便于对资产做管理以树的形式显示资产组，支持无限极管理资产组。资产组位于资产管理左侧。

资产管理 > 资产分组管理



4.2.2. 资产管理

该模块主要用于管理平台所有资产，便于在添加任务的时候选择资产。以列表的方式显示资产名称、资产类型、所属区域、描述等信息。资产管理主要分为“资产组”和“资产列表”，创建资产时需先选择资产。

资产管理 > 资产管理



4.2.3. 网站管理

该模块主要用于管理平台所有网站资产，便于在添加网站任务的时候选择资产。以列表的方式显示资产名称、资产类型、所属区域、描述等信息。资产管理主要分为“资产组”和“资产列表”，创建资产时需先选择资产。

资产管理 > 网站管理



4.2.4. 认证信息

该模块主要用于管理资产的认证信息,个别扫描功能在对资产进行安全评估时需要使用用户名及密码等信息登录目标资产,这里主要用于管理资产对应的登录方式。

资产管理 > 认证信息

系统认证 添加认证 ×

连接认证 资产类型 ▾

① 如果需要对系统、中间件、网络设备等进行基线配置核查需要填写该页用户名和密码等认证信息。

名称: * 请输入名称

IP地址: *

协议: ▾

端口: 不填写将使用默认端口, ssh:22,telnet:23,smb:445,WinRM:

用户名: 建议使用管理员用户, 非管理员用户可能扫描不完整。

密码: 🔒 扫描需要登录的密码

管理员密码: 🔒 如果是以普通用户扫描且没有sudo权限则无法扫描, 或者su

4.3. 任务管理菜单

任务管理菜单包括资产梳理、主机漏洞扫描、基线配置核查、网站漏洞监控、网站篡改监测、网站可用性监测、数据库漏洞扫描、弱口令猜解等。



4.3.1. 资产梳理

根据探测目标、探测端口范围等参数信息自动发现目标网络中的资产。



4.3.2. 主机漏洞扫描

4.3.2.1. 任务管理

该模块主要用于管理平台所建的主机漏洞扫描任务。以列表的方式显示任务名称、扫描周期、预警方式、预警周期、当前状态等信息。



- 点击  按钮，输入信息，即可添加扫描任务；

任务管理 > 主机漏洞扫描

主机扫描任务 添加扫描任务 ×

基本信息 授权认证

任务名: * 任务名, 中文、字母、

目标引擎: 自动 ▼ 任务被下发到的目标引擎

描述:

资产IP: * 支持格式:
ipv4/6
192.168.0.100,101,102
192.168.0.*
192.168.0/24
192.168.0.1-100
192.168.0.1-192.168.0.100
多个ip使用换行分隔。

🔍 从资产管理选择

排除IP: 不进行扫描的ip, 格式

扫描顺序: 顺序 ▼

主机扫描模板: ▼ * "完全扫描" 模板扫描

扫描类型: 手动扫描
 周期扫描

详细

- 点击  按钮, 即可查看任务详情;

任务管理 > 主机漏洞扫描



4.3.3. 基线配置核查

该模块主要用于管理平台所建的基线扫描任务。以列表的方式显示任务名称、扫描类型、预警方式、告警类型、任务状态等信息。

任务管理 > 基线配置核查



- 点击  按钮，输入信息，即可添加扫描任务；

任务管理 > 基线配置核查

基线配置核查任务 添加核查任务 ×

基本信息 授权认证 (*)

① 如果需要数据库、中间件、网络设备或者想进行更详细的基线配置核查，需要添加认证信息。该选项需要事先到“资产管理”——>“认证”

任务名: * 请输入任务名

目标引擎: 自动 任务被下发到的目标引擎，自动表示系统自动选择一个性能较优的。

描述:

资产IP: * 格式如：
ipv4/6
192.168.0.100,101,102
192.168.0.*
192.168.0/24
192.168.0.1-100
192.168.0.1-192.168.10.100
多个ip使用换行分隔。

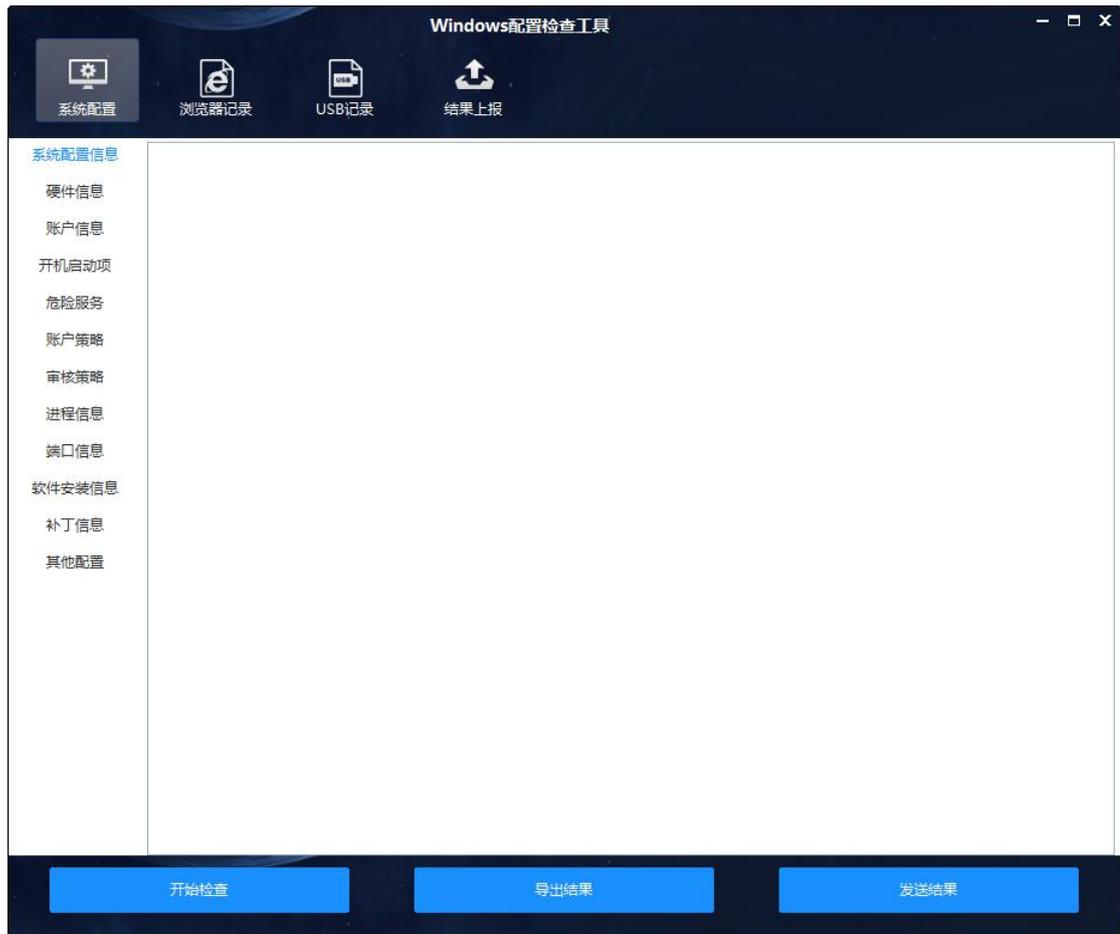
基线策略模板: *

扫描类型: 手动扫描
 周期扫描

预警方式: 系统提示
 邮件预警 (未设置预警邮件服务器地址)
 短信预警 (未设置短信平台地址)

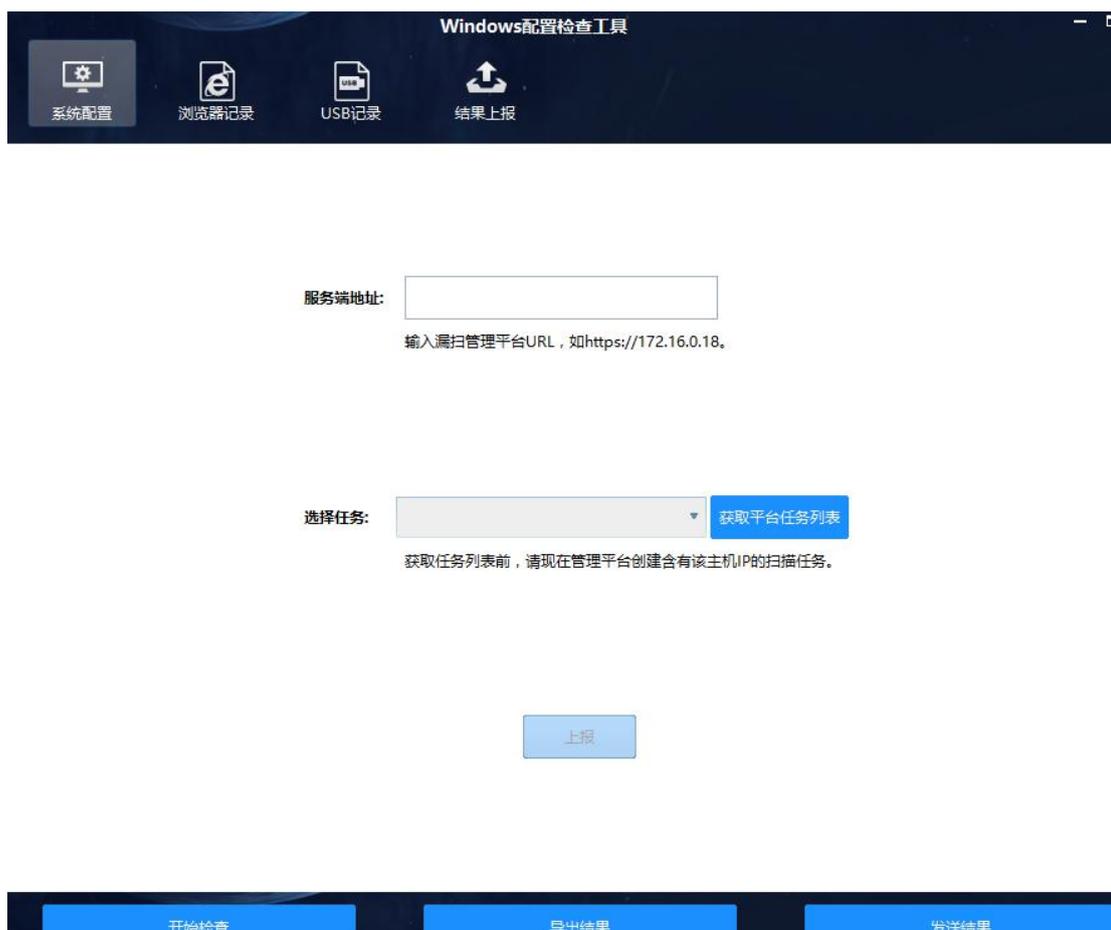
■ 点击  按钮，选择文件，即可上报离线扫描结果；

■ 点击  按钮，即可下载 Windows 离线检查工具
(Windows 离线检查工具即检查本机的配置核查)



点击“开始扫描”即可扫描本机的配置，扫描完成后可“自动上报”也可“导出结果”。

自动上报：输入服务端地址和选择任务即可上报。



4.3.4. 网站漏洞监控

该模块主要用于管理平台所建的网站监控任务。网站安全监控主要对目标网站的可用性、安全漏洞、篡改、网马、暗链等进行7*24小时监控，也可对安全漏洞进行单次评估扫描。全面支持OWASP TOP 10 2013漏洞检测，如SQL注入、跨站脚本、文件包含、命令执行、信息泄漏等全部漏洞；覆盖了论坛、内容管理系统（CMS）和电子商务应用系统等平台。

4.3.4.1. 单次扫描

对目标网站进行单次扫描，可扫描网站的漏洞。

任务管理 > 网站漏洞监控

网站漏洞任务 添加扫描任务 ×

任务信息 | 预警配置 | 基本配置 | 爬行参数 | 代理设置

任务名: * 请输入任务名

目标引擎: 自动 ▼ 任务被下发到的目标引擎, 自动表示系统自动选

描述:

URL: 手动输入URL: * 多个url使用换行分隔, 至少填写或从网站库选

从网站库选择: ▼

扫描类型: 手动扫描 周期扫描

扫描内容: 安全漏洞 网马和可疑的暗链 钓鱼检测 敏感关键字扫描 * 暗链白名单为正则表达式, 多个表达式使用换行

敏感关键字扫描参数

识别图片 识别身份证和银行卡信息

关键字模板: 快速扫描 ▼

4.3.4.2. 周期扫描

对目标网站进行周期性监控, 包括安全漏洞、网马和暗链、敏感内容等。

▼

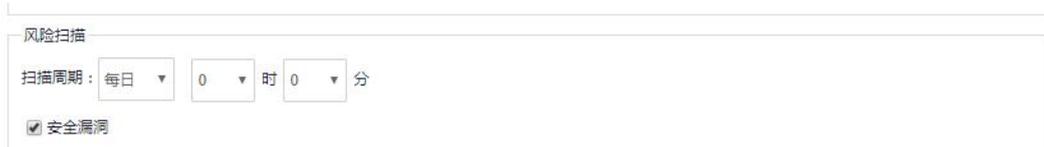
扫描类型: 手动扫描 周期扫描

按日 ▼ 每 1 ▲▼ 日 0 ▲▼ 时 0 ▲▼ 分

扫描内容: 安全漏洞 网马和可疑的暗链 钓鱼检测 敏感关键字扫描 * 暗链白名单为正则表达式

4.3.4.2.1. 安全漏洞

安全漏洞包括 SQL 注入漏洞、SQL 盲注漏洞、XPath 注入漏洞、XSS 跨站脚本漏洞、目录遍历漏洞、源代码泄露漏洞等。



4.3.4.2.2. 网马和暗链

网页挂马是攻击者通过在正常的页面中（通常是网站的主页）插入一段代码。浏览者在打开该页面的时候，这段代码被执行，然后下载并运行某木马的服务器端程序，进而控制浏览者的主机。通俗点说就是将网页木马这样的攻击程序放在网页上，浏览这个网页的人，不需要任何点击动作就会中毒。

常见的网页挂马实现方式：

- 1) iframe 框架嵌入式挂马
- 2) JS 文件调用挂马
- 3) JS 文件加密变形
- 4) JavaScript 脚本挂马
- 5) Body 挂马等。

“暗链”就是看不见的网站链接，“暗链”在网站中的链接做得非常隐蔽，短时间内不易被搜索引擎察觉。它和友情链接有相似之处，可以有效地提高 PR 值。但要注意一点 PR 值是对单独页面，而不是整个网站。

如果网站被挂马或被写入暗链，对于网站的运营来说是非常不利的，他会影响搜索引擎的排名、被降权，同时网站的数据也有可能被泄露。同时，还会篡改网站标题、网站内容，

添加大量垃圾链接，导致网站面目全非。因此，解决网站被挂马问题、暗链问题是必要的。



4.3.4.2.3. 敏感内容

网站如果被篡改，在网站页面添加了一些带有敏感政治倾向（或反执政党倾向）、暴力倾向、不健康色彩的词或不文明语、博彩等的敏感内容，将影响企业的品牌形象，严重的可能照成经济损失。



4.3.4.3. 扫描参数

4.3.4.3.1. 基本配置

任务信息	预警配置	基本配置	爬行参数	代理设置
扫描策略模板：	系统默认	▼	* 请选择扫描策略模板	
扫描子域名：	否	▼	仅扫描此目录中或目录下的链接,其他链接会被过滤	
最长扫描时间：	0	▲▼	* 该任务最长扫描时间(小时),超过时间后将结束扫描	
HTTP响应超时时间：	30	▲▼	* 连接服务器成功后,接收HTTP响应内容的超时时间(秒)	
SQL注入超时时间：	10	▲▼	* SQL注入策略执行超时时间(秒),可选值:1-20	
策略超时时间：	10	▲▼	* 策略执行超时时间(秒),可选值:1-20	
User-Agent：	Firefox	▼		
	<pre>Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; LCJB; rv:11.0) like Gecko</pre>			
同一漏洞最大检查个数：	124	▲▼	* 设置同一个漏洞的最大检查个数,可选值:1-999	
		▲▼	* 设置策略执行超时时间(秒),可选值:1-20	

4.3.5. 网站可用性监测

该模块主要用于管理平台所建的网站可用性监测任务。网站可用性监测主要对目标网站的可用性进行 7*24 小时监控。

任务管理 > 网站篡改监测

网站篡改监测任务 添加扫描任务 ×

任务信息 **预警配置** 爬行参数 代理设置 预处理规则

任务名： * 请输入任务名

目标引擎：**自动** 任务被下发的目标引擎，自动表示系统自动选择一个性能较优

描述：

URL：手动输入URL： * 多个url使用换行分隔，至少填写或从网站库选择一个网站。

从网站库选择：

扫描类型： 手动扫描
 周期扫描

扫描内容： 内容篡改 * 请至少选择一项。
 图片篡改
 新增URL
 删除URL

4.3.6. 网站篡改监测

该模块主要用于管理平台所建的网站篡改监测任务。网站篡改监测主要对目标网站的篡改性进行 7*24 小时监控，包括：内容篡改、图片篡改、新增 URL、删除 URL。

任务管理 > 网站篡改监测

网站篡改监测任务 添加扫描任务 ×

任务信息 **预警配置** 爬行参数 代理设置 预处理规则

任务名： * 请输入任务名

目标引擎：**自动** 任务被下发的目标引擎，自动表示系统自动选择一个性能较优

描述：

URL：手动输入URL： * 多个url使用换行分隔，至少填写或从网站库选择一个网站。

从网站库选择：

扫描类型： 手动扫描
 周期扫描

扫描内容： 内容篡改 图片篡改 新增URL 删除URL * 请至少选择一项。

4.3.7. 数据库扫描

该模块主要用于管理平台所建的数据库扫描任务。以列表的方式显示任务名称、扫描类型、告警方式、告警类型、当前状态以及对任务的描述等信息。



- 点击 **+ 添加** 按钮，输入信息，即可添加扫描任务；

任务管理 > 数据库漏洞扫描

数据库扫描任务 添加数据库扫描任务 ×

基本信息 系统认证(*)

! 对数据库扫描必须添加认证信息。该选项需要事先到“资产管理”——>“认证信息”，添加相应的数据库认证信息。

任务名： * 请输入任务名

描述：

资产IP： * 格式如：
 192.168.0.123
 192.168.0.100,101,102
 192.168.0.*
 192.168.0.0/24
 192.168.0.1-100
 192.168.0.1-192.168.10.100
 多个ip使用换行分隔。

最大并发数： * 同时扫描的最大线程数

数据库策略模板：

扫描类型： 手动扫描
 周期扫描

预警方式： 系统提示
 邮件预警 (未设置预警邮件服务器地址)
 短信预警 (未设置短信平台地址)

4.3.8.弱口令猜解

该模块主要用于管理平台所建的弱口令扫描任务。以列表的方式显示任务名称、扫描类型、告警方式、告警类型、当前状态以及对任务的描述等信息。



- 点击  按钮，输入信息，即可添加扫描任务；

任务管理 > 弱口令猜解

弱口令猜解任务 添加扫描任务 ×

基本信息 扫描配置

用户名字典: * 请选择用户名字典

密码字典模板: * 请选择密码字典模板

最大并发数: 16 * 最大同时运行的扫描进程数

扫描协议: * 请至少指定一个协议

- SSH
- TELNET
- SMB
- RDP
- FTP
- POP3
- SMTP
- SNMP
- REDIS
- ORACLE
- MSSQL

扫描协议选择（根据目标开启的服务开选择协议）：

SSH： 目标开启了 SSH 服务，如 LINUX 系统、网络设备、安全设备等。

TELNET： 目标开启了 TELNET 服务，如 LINUX 系统、网络设备、安全设备等。

SMB/RDP： 目标为 WINDOWS 操作系统。

FTP： 目标开启了 FTP 服务。

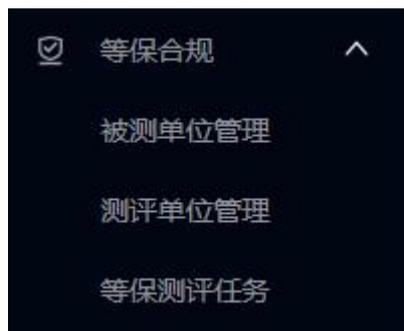
POP3/SMTP： 目标为邮件服务器。

SNMP: 目标开启了 SNMP 服务, 如服务器、网络设备、安全设备等。

REDID/ORACLE/MSSQL/MYSQL/POSTGRES/: 目标安装了对应的数据库服务。

HTTP: 目标为 WEB 服务器, 且登陆页面没有验证码。

4.4. 等保合规菜单



该模块主要用于管理平台所建的信息系统测评任务。以列表的方式显示信息系统名称、被测单位名称、系统简介、SAG 等级、资产数等信息。



- 点击  按钮, 输入信息, 即可添加信息系统测评任务;

等保合规 > 等保测评任务

测评任务 添加测评任务 ×

基本信息

被测对象名:	<input type="text"/>	*
SAG等级:	slalq1	*
等级保护对象形态:	<input checked="" type="checkbox"/> 传统IT系统 <input type="checkbox"/> 云计算 <input type="checkbox"/> 移动互联 <input type="checkbox"/> 物联网 <input type="checkbox"/> 工业控制系统 <input type="checkbox"/> 大数据 <input type="checkbox"/> 其他系统	*
备案证明编号:	<input type="text"/>	
被测对象描述:	<input type="text"/>	
被测单位:	<input type="text"/>	*
测评单位:	<input type="text"/>	*
前次测评情况:	<input type="text"/>	
业务和采用的技术:	<input type="text"/>	

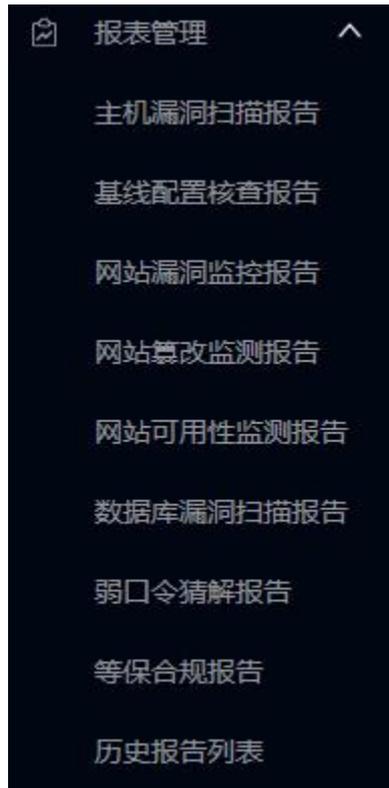
系统资产 **网络拓补图** **工具接入图**

物理机房	+ 添加	
网络设备	机房名称	物理位置
安全设备		
服务器/存储设备		
终端/现场设备		
系统管理软件/平台		
业务应用软件/平台		
关键数据类别		
安全相关人员		
安全管理文档		

确定

4.5. 报表管理菜单

报表管理菜单包括主机漏洞扫描报告、基线配置核查报告、网站漏洞监控报告、网站篡改监测报告、网站可用性监测报告、数据库漏洞扫描报告、弱口令猜解报告等。



4.5.1. 主机漏洞扫描报告

报表管理 > 主机漏洞扫描报告

主机安全评估报告

扫描任务:

报告名称:

页面设置
(仅对导出doc时有效)

页眉文本:

页眉logo:  (大小: 73px × 28px, 点击图片可更换!)

页脚链接:

不保存设置的页眉仅对本次导出有效。

选择相应的任务，可修改报告名称，点击  按钮，即可预览报告详情；

4.5.2. 基线配置核查报告

报表管理 > 基线配置核查报告

基线配置核查报告

扫描任务:

报告名称:

页面设置
(仅对导出doc时有效)

页眉文本:

页眉logo:  (大小: 73px × 28px, 点击图片可更换!)

页脚链接:

不保存设置的页眉仅对本次导出有效。



选择相应的任务，可修改报告名称，点击  按钮，即可预览报告详情；

4.5.3. 网站漏洞监控报告

报表管理 > 网站漏洞监控报告

网站漏洞监控报告

扫描任务：

报告名称：

页面设置
(仅对导出doc时有效)

页眉文本：

页眉logo： (大小：73px × 28px，点击图片可更换！)

页脚链接：

不保存设置的页眉仅对本次导出有效。

选择相应的任务，可修改报告名称，点击  按钮，即可预览报告详情；

4.5.4. 网站篡改监测报告

报表管理 > 网站篡改监测报告

网站篡改监测报告

扫描任务:

报告名称:

页面设置
(仅对导出doc时有效)

页眉文本:

页眉logo:  (大小: 73px x 28px, 点击图片可更换!)

页脚链接:

不保存设置的页眉仅对本次导出有效。

选择相应的任务，可修改报告名称，点击  按钮，即可预览报告详情；

4.5.5. 网站可用性监测报告

报表管理 > 网站可用性监测报告

网站可用性监测报告

扫描任务:

报告名称:

页面设置
(仅对导出doc时有效)

页眉文本:

页眉logo:  (大小: 73px × 28px, 点击图片可更换!)

页脚链接:

不保存设置的页眉仅对本次导出有效。

选择相应的任务，可修改报告名称，点击  按钮，即可预览报告详情；

4.5.6. 数据库漏洞扫描报告

报表管理 > 数据库漏洞扫描报告

数据库安全评估报告

扫描任务:

报告名称:

页面设置
(仅对导出doc时有效)

页眉文本:

页眉logo:  (大小: 73px x 28px, 点击图片可更换!)

页脚链接:

不保存设置的页眉仅对本次导出有效。

选择相应的任务, 可修改报告名称, 点击  按钮, 即可预览报告详情;

4.5.7.弱口令猜解报告

报表管理 > 弱口令猜解报告

弱口令安全评估报告

扫描任务:

报告名称:

页面设置
(仅对导出doc时有效)

页眉文本:

页眉logo:  (大小: 73px × 28px, 点击图片可更换!)

页脚链接:

不保存设置的页眉仅对本次导出有效。

选择相应的任务，可修改报告名称，点击  按钮，即可预览报告详情；

4.5.8. 等保合规报告

报表管理 > 等保合规报告

等保合规报告

测评任务：

报告名称：

页面设置
(仅对导出doc时有效)

页眉文本：

页眉logo： (大小：73px × 28px，点击图片可更换！)

页脚链接：

不保存设置的页眉仅对本次导出有效。

选择相应的任务，可修改报告名称，点击  按钮，即可预览报告详情；

4.5.9..历史报告列表

该模块主要用于管理以前所有已经导出的报告，方便用户追踪查看历史监控情况。已列表的方式显示报告名称、生成时间、报告类型等内容。可批量导出报告。

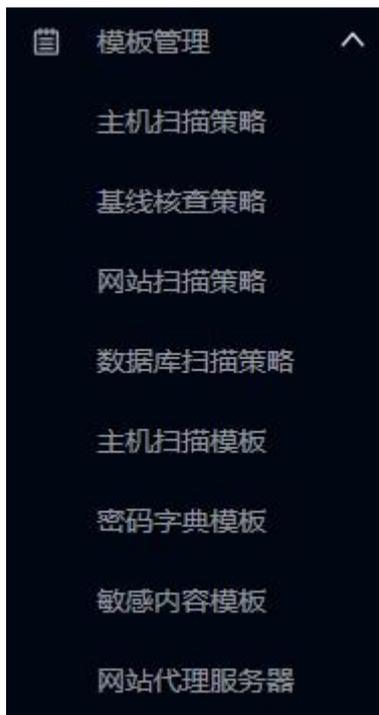
报表管理 > 历史报告列表

<input type="checkbox"/>	报告名称	创建者	报告类型	生成时间
<input type="checkbox"/>	(test)网站漏洞监控报告_2020年06月22日19时42分.zip	superadmin	网站监控报告	2020-06-22 19:54:01
<input type="checkbox"/>	(test)网站漏洞监控报告_2020年06月22日19时41分.zip	superadmin	网站监控报告	2020-06-22 19:41:50
<input type="checkbox"/>	(test)网站漏洞监控报告_2020年06月22日19时41分.zip	superadmin	网站监控报告	2020-06-22 19:41:25
<input type="checkbox"/>	(test)网站漏洞监控报告_2020年06月22日19时40分.zip	superadmin	网站监控报告	2020-06-22 19:40:30
<input type="checkbox"/>	(test)网站漏洞监控报告_2020年06月22日19时39分.zip	superadmin	网站监控报告	2020-06-22 19:39:25
<input type="checkbox"/>	(test)网站漏洞监控报告_2020年06月22日19时38分.zip	superadmin	网站监控报告	2020-06-22 19:38:56
<input type="checkbox"/>	(test)网站漏洞监控报告_2020年06月22日19时38分.zip	superadmin	网站监控报告	2020-06-22 19:38:44
<input type="checkbox"/>	(test)网站漏洞监控报告_2020年06月22日19时36分.zip	superadmin	网站监控报告	2020-06-22 19:36:20
<input type="checkbox"/>	(test)网站漏洞监控报告_2020年06月22日19时35分.zip	superadmin	网站监控报告	2020-06-22 19:35:26
<input type="checkbox"/>	(test)网站漏洞监控报告_2020年06月22日19时29分.zip	superadmin	网站监控报告	2020-06-22 19:30:06
<input type="checkbox"/>	(test)网站漏洞监控报告_2020年06月22日19时28分.zip	superadmin	网站监控报告	2020-06-22 19:29:40
<input type="checkbox"/>	(test)网站漏洞监控报告_2020年06月22日19时28分.zip	superadmin	网站监控报告	2020-06-22 19:28:50
<input type="checkbox"/>	(test)网站漏洞监控报告_2020年06月22日19时21分.zip	superadmin	网站监控报告	2020-06-22 19:22:28
<input type="checkbox"/>	(test)网站漏洞监控报告_2020年06月22日19时18分.zip	superadmin	网站监控报告	2020-06-22 19:19:52
<input type="checkbox"/>	(test)网站漏洞监控报告_2020年06月22日19时15分.zip	superadmin	网站监控报告	2020-06-22 19:17:22

- 勾选需要导出的报告，点击工具栏中的  按钮，即可批量下载报告；

4.6. 模板管理菜单

模板管理菜单包括主机扫描策略、基线核查策略、网站扫描策略等。



4.6.1. 主机扫描策略

该模块的主要功能为将常用的主机扫描策略保存起来,方便直接应用到各个不同的主机扫描任务中,以列表的方式显示模板名称和配置内容等信息。(默认的策略模板不可修改、删除)

模板管理 > 主机扫描策略

模板名	高危数	中危数	低危数	信息数	总数	详细	删除
1 所有策略	30495	24717	2507	2406	60125		
2 Windows策略	7951	6704	747	2314	17716		
3 Amazon Linux策略	5640	6149	695	2088	14572		
4 Centos策略	7084	7072	736	2099	16991		
5 Debian策略	7969	7694	875	2099	18637		
6 Fedora策略	12431	11394	1200	2099	27124		
7 FreeBSD策略	6305	6808	790	2099	16002		
8 Oracle Linux策略	6249	6793	755	2099	15896		
9 RedHat策略	6571	6797	744	2099	16211		
10 SuSE策略	6994	6652	701	2099	16446		
11 Ubuntu策略	7315	7309	805	2099	17528		
12 AIX策略	5377	5863	663	2099	14002		
13 HP-UX策略	4849	5345	597	2009	12800		
14 Solaris策略	5662	6286	752	2099	14000		

- 点击工具栏中的  按钮，即可添加策略模板；

直接输入模板名添加；



也可勾选系统中的策略进行添加；

模板管理 > 主机扫描策略

主机策略模板
【所有策略】详细 x

模板名:

全部策略

条件查询:
所有等级 v
不限(CVE) v
不限(CNNVD) v
不限(CNVD) v
不限(CNCVE) v
不限(CVSS) v
不限(BUGTRAQ) v
策略名

	策略名	CVE	CNNVD	CNVD	CNCVE	CVSS	BUGTRAQ	详细
高危								
1	<input type="checkbox"/> yppasswdd缓冲区溢出(原理扫描)	CVE-2001-0779	CNNVD-200110-06		CNCVE-20010779	10	2763	<input type="button" value="眼"/>
2	<input type="checkbox"/> X server访问控制漏洞	CVE-1999-0526	CNNVD-199707-00		CNCVE-19990526	10		<input type="button" value="眼"/>
3	<input type="checkbox"/> TFTP目录遍历	CVE-1999-0498, CVI	CNNVD-199109-00		CNCVE-19990498, C	10	6198, 11584, 11582	<input type="button" value="眼"/>

显示1到20,共60125记录

已选策略

条件查询:
所有等级 v
不限(CVE) v
不限(CNNVD) v
不限(CNVD) v
不限(CNCVE) v
不限(CVSS) v
不限(BUGTRAQ) v
策略名

	策略名	CVE	CNNVD	CNVD	CNCVE	CVSS	BUGTRAQ	详细
高危								
1	<input type="checkbox"/> yppasswdd缓冲区溢出(原理扫描)	CVE-2001-0779	CNNVD-200110-06		CNCVE-20010779	10	2763	<input type="button" value="眼"/>
2	<input type="checkbox"/> X server访问控制漏洞	CVE-1999-0526	CNNVD-199707-00		CNCVE-19990526	10		<input type="button" value="眼"/>
3	<input type="checkbox"/> TFTP目录遍历	CVE-1999-0498, CVI	CNNVD-199109-00		CNCVE-19990498, C	10	6198, 11584, 11582	<input type="button" value="眼"/>

显示1到20,共60125记录

4.6.2. 基线核查策略

该模块以列表的方式显示模板名称、所属分组和策略总数等信息。(基线评估模板不可添加、修改、删除)

模板管理 > 基线核查策略

基线配置模板

	模板名	策略数	详细	删除
1	系统默认	2173	<input type="button" value="眼"/>	

- 👁
点击 按钮，即可查看模板的详情，以列表的方式显示策略名称、等级、检查点、检查项、所属策略模板、所属策略分组等信息；

模板管理 > 基线检查策略

基线配置模版
【系统默认】详细 ×

模版名：

全部策略

+ 添加到模版
+ 添加策略项
删除
条件查询：基线标准：
规则名
所有组
所有等级
所有类型

<input type="checkbox"/>	分组	类型	规则名	安全等级	详细
Linux					
<input type="checkbox"/>	1	Centos	系统	检查系统是否启用了sudo命令	高危 详情
<input type="checkbox"/>	2	Centos	系统	检查系统中是否存在密码为空的帐户	高危 详情
<input type="checkbox"/>	3	Centos	系统	检查系统中是否存在UID与root帐户相同的帐户	高危 详情

显示1到30,共2173记录

已选策略

删除
条件查询：规则名
所有组
所有等级
所有类型
查询
重置

<input type="checkbox"/>	分组	类型	规则名	安全等级	详细
Linux					
<input type="checkbox"/>	1	Centos	系统	检查系统是否启用了sudo命令	高危 详情
<input type="checkbox"/>	2	Centos	系统	检查系统中是否存在密码为空的帐户	高危 详情
<input type="checkbox"/>	3	Centos	系统	检查系统中是否存在UID与root帐户相同的帐户	高危 详情

显示1到30,共2173记录

4.6.3. 网站扫描策略

该模块的主要功能是添加、删除网站策略模版，也可查看全部的网站扫描策略，支持对策略进行检索。

模板管理 > 网站扫描策略

网站策略模版
+ 添加

模版名	高危数	中危数	低危数	信息数	总数	详细	删除
1 所有策略	496	251	59	81	887	详情	
2 系统默认	204	49	18	67	338	详情	

模板管理 > 网站扫描策略

网站策略模板
【系统默认】 详细 ×

模板名:

全部策略

+ 添加 >> 条件查询: 所有等级 策略名

<input type="checkbox"/>	策略名	CVE	详细
= 高危			
<input type="checkbox"/>	08cms 3.1 /include/paygate/alipay/pays.phf		🔍
<input type="checkbox"/>	53KF 任意文件下载漏洞		🔍
<input type="checkbox"/>	骑士cms ajax_street.php sql注入漏洞		🔍
<input type="checkbox"/>	骑士cms jobs_near-list.php文件SQL注入漏洞		🔍
<input type="checkbox"/>	骑士cms ajax_common.php文件SQL注入漏洞		🔍
<input type="checkbox"/>	骑士cms V3.4 /plus/ajax_officebuilding.php :		🔍
<input type="checkbox"/>	74cms /street-search.php SQL注入漏洞		🔍
<input type="checkbox"/>	Apache solr管理页面泄露		🔍
<input type="checkbox"/>	AspCMS 2.2.9 /AspCms_AboutEdit.asp SQL		🔍
<input type="checkbox"/>	视频监控厂商AVTECH产品多个漏洞		🔍

20 第 1 共45页 显示1到20,共887记录

已选策略

 条件查询: 所有等级 策略名

<input type="checkbox"/>	策略名	CVE	详细
= 高危			
<input type="checkbox"/>	Tomcat跨站请求伪造漏洞	CVE-2015-5351	🔍
<input type="checkbox"/>	phpMyFAQ小于2.5.4跨站脚本攻击漏洞		🔍
<input type="checkbox"/>	Wordpress DukaPress插件路径遍历漏洞	CVE-2014-8799	🔍
<input type="checkbox"/>	Struts2远程命令执行S2-015漏洞	CVE-2013-2135	🔍
<input type="checkbox"/>	宽字符集跨站脚本漏洞		🔍
<input type="checkbox"/>	Http.sys远程代码执行漏洞	CVE-2015-1635	🔍
<input type="checkbox"/>	Wordpress Persuasion Theme 2.x 任意文件下		🔍
<input type="checkbox"/>	Adobe ColdFusion管理控制台多个目录遍历漏洞	CVE-2010-2861	🔍
<input type="checkbox"/>	Joomla com_bt_media组件SQL注入漏洞		🔍
<input type="checkbox"/>	Ecmall groupbuy.app.php SQL注入漏洞		🔍

20 第 1 共17页 显示1到20,共338记录

4.6.4. 数据库扫描策略

该模块的主要功能是管理数据库策略，以列表的方式显示模板名称、紧急、高危、中危、低危、信息策略数等信息。（数据库策略模板不可添加、修改、删除）

模板管理 > 数据库扫描策略

数据库策略模板						
模板名	高危数	中危数	低危数	信息数	总数	详细
1 系统默认	597	1267	308	56	2228	🔍

4.6.5. 敏感关键字模板

该模块的主要功能是添加、删除网站安全监控中的敏感关键字。

模板管理 > 敏感内容模板

+ 添加					
模板名	模板内容	模板描述	模板文件	修改	删除
1	快速扫描		keywords2.txt		
2	系统默认		keywords.txt		

4.6.6. 网站代理服务器

该模块的主要功能的添加、删除访问的网站代理服务器。可导入和导出服务器模板。

模板管理 > 网站代理服务器

+ 添加			
模板名称	代理类型	ip地址	端口

4.6.7. 密码字典模板

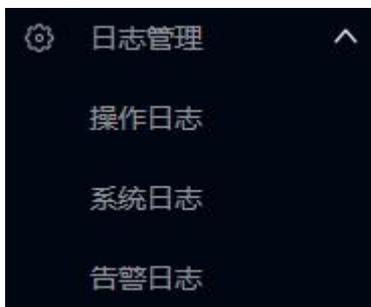
该模块的主要功能为将常用的弱口令字典保存起来,方便直接应用到各个不同的弱口令扫描任务中,以列表的方式显示字典名称、字典类型和字典内容等信息。**(系统默认的弱口令字典不可修改、删除)**

模板管理 > 密码字典模板

字典名	字典类型	内容	字典描述	字典文件	修改
1 SSH账号字典	用户名字典			sshuser.txt	
2 SSH账号字典_大字典	用户名字典			sshuserbig.txt	
3 SSH密码字典	密码字典			sshpass.txt	
4 SSH密码字典_大字典	密码字典			sshpassbig.txt	
5 snmp密码字典	密码字典			snmppass.txt	
6 SMB账号字典_大字典	用户名字典			smbuserbig.txt	
7 SMB账号字典	用户名字典			smbuser.txt	
8 SMB密码字典	密码字典			smbpass.txt	
9 SMB密码大字典	密码字典			smbpassbig.txt	
10 网络设备默认用户名字典	用户名字典			netdevdefuser.txt	
11 网络设备默认密码字典	密码字典			netdevdefpass.txt	
12 密码字典	密码字典			password.txt	
13 用户名字典	用户名字典			username.txt	

4.7. 日志管理菜单

日志管理菜单包括操作日志、系统日志、告警日志。



4.7.1. 操作日志

操作日志记录了用户对系统进行的所有操作，以列表的方式显示操作时间、操作用户、操作事件以及描述信息等。

日志管理 > 操作日志

用户名	操作时间	操作事件	IP地址	操作结果	描述
1 superadmin	2020-06-28 21:09:18	查询主机扫描配置模板	127.0.0.1	成功	
2 superadmin	2020-06-28 21:08:47	数据库策略模板查询	127.0.0.1	成功	
3 superadmin	2020-06-28 21:08:25	数据库策略模板查询	127.0.0.1	成功	
4 superadmin	2020-06-28 21:07:33	网站策略模板查询	127.0.0.1	成功	
5 superadmin	2020-06-28 21:06:56	基线配置模板查询	127.0.0.1	成功	
6 superadmin	2020-06-28 21:06:34	基线配置模板查询	127.0.0.1	成功	
7 superadmin	2020-06-28 21:04:35	主机策略模板查询	127.0.0.1	成功	
8 superadmin	2020-06-28 21:02:32	历史报告查询	127.0.0.1	成功	
9 superadmin	2020-06-28 21:02:09	历史报告查询	127.0.0.1	成功	
10 superadmin	2020-06-28 20:55:37	2.0测评任务查询	127.0.0.1	成功	
11 superadmin	2020-06-28 20:44:04	添加主机漏洞扫描任务	127.0.0.1	成功	任务名=xxx
12 superadmin	2020-06-28 20:43:35	用户登录	127.0.0.1	成功	用户名=superadmin
13 superadmin	2020-06-28 15:05:09	系统认证查询	127.0.0.1	成功	
14 superadmin	2020-06-28 15:03:35	网站查询	127.0.0.1	成功	
15 superadmin	2020-06-28 14:57:27	告警日志查询	127.0.0.1	成功	

4.7.2.系统日志

系统日志记录了系统自动进行的一系列操作，如定时任务、预警等。

日志管理 > 系统日志

操作时间	操作事件	操作结果	描述

4.7.3.告警日志

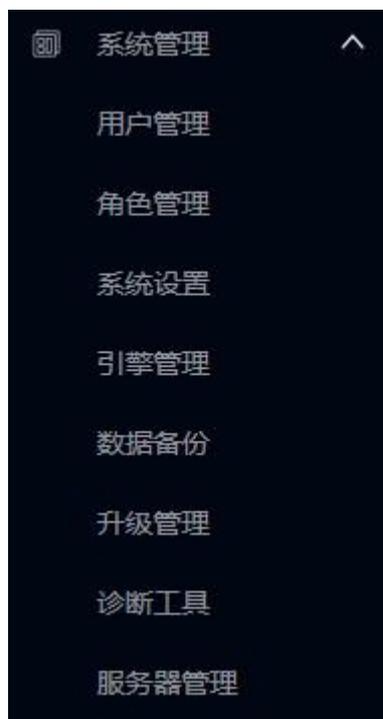
告警日志记录了系统的所有告警信息，如发现资产漏洞、系统资源使用率过高等。

日志管理 > 告警日志

<input type="checkbox"/>	标题	告警时间	类型	状态	内容
1	<input type="checkbox"/> 网站漏洞	2020-06-22 15:21:39	网站漏洞告警	未读	网站漏洞, 漏洞名: Cookie中缺少Secure属性, 安全等级: 低危, URL: https://gcbc.cnr.cn:443/
2	<input type="checkbox"/> 网站漏洞	2020-06-22 15:21:39	网站漏洞告警	未读	网站漏洞, 漏洞名: 点击劫持-X-Frame-Options Header未配置, 安全等级: 低危, URL: https://gcbc.cnr.cn:443/
3	<input type="checkbox"/> 网站漏洞	2020-06-22 15:21:39	网站漏洞告警	未读	网站漏洞, 漏洞名: 会话Cookie中缺少HttpOnly属性, 安全等级: 低危, URL: https://gcbc.cnr.cn:443/
4	<input type="checkbox"/> 网站漏洞	2020-06-22 15:23:17	网站漏洞告警	未读	网站漏洞, 漏洞名: 管理后台登录入口泄露, 安全等级: 低危, URL: https://gcbc.cnr.cn:443/quanquhuayu/html/index/dengl.html?txtemail=1&txtuserpass=1&txtemailverifycode=1&sublogin=登录

4.8. 系统管理菜单

系统管理菜单包括用户管理、角色管理、系统设置、引擎管理、诊断工具等。



4.8.1. 用户管理

以列表的方式显示用户的详细信息, 包括用户名、姓名、创建时间、所属角色、所属区域、最后登录时间、锁定状态和最后登录 IP 地址。 (系统默认管理员不可修改、删除、锁定/解锁)

系统管理 > 用户管理

用户管理							
+ 添加		设置		条件查询: 用户名 姓名 所有角色			
用户名	姓名	电话	所属角色	状态	所在地	详细	锁/解
1 admin	系统管理员		系统管理员	正常			
2 audit	安全审计员		安全审计员	正常			
3 secret	安全保密管理员		安全保密管理员	正常			
4 scan	操作员		操作员	正常			

- 点击  按钮, 输入信息, 即可添加用户;

系统管理 > 用户管理

用户管理		添加用户 x	
用户名:	<input type="text"/>	*	
密码:	<input type="password"/>	*	
确定密码:	<input type="password"/>	*	
姓名:	<input type="text"/>		
所属角色:	操作员	*	
电话号码:	<input type="text"/>		
电子邮件:	<input type="text"/>		
所在地:	请选择	请选择	请选择 *
登录IP范围:	空表示允许在所有IP登录	格式如: 192.168.0.100,101,102 192.168.0.* 192.168.0.0/24 192.168.0.1-100	

4.8.2. 角色管理

以列表的方式显示角色的详细信息，包括角色名、描述和权限。（系统默认管理员、审计员、操作员不可修改、删除）

系统管理 > 角色管理

+ 添加				
角色名	数据权限	描述	详细	修改
1 系统管理员	仅查看自己的任务数据	拥有系统管理相关权限。		
2 安全审计员	仅查看自己的任务数据	拥有日志相关权限。		
3 安全保密管理员	可查看所有任务数据	拥有安全相关以及业务操作等权限。		
4 操作员	仅查看自己的任务数据	拥有业务操作相关权限。		

- 点击  按钮，输入信息，即可添加角色；



4.8.3. 系统设置

可对系统的会话超时时间、系统时间等进行设置。

系统管理 > 系统设置

系统设置 | 时间设置

出厂设置：

会话超时时间： 单位：分

接口互动IP： 格式如：
ipv4/6
192.168.0.100,101,102
192.168.0.*
192.168.0.0/24
192.168.0.1-100
192.168.0.1-192.168.10.100
多个ip使用换行分隔。

最大并发扫描任务数： 允许值：1-10

系统管理 > 系统设置

系统设置 | 时间设置

注意：时间修改后可能导制许可过期或者当前用户登录失效！

类型： 手动设置 NTP定期同步 *

系统时间： *

NTP服务器： *

4.8.4.引擎管理

以列表方式显示所有扫描引擎，并能够查看引擎状态、接收的任务数等。

系统管理 > 引擎管理

引擎管理												
引擎名	引擎IP	引擎版本	策略版本	接收任务数	状态	CPU	内存	硬盘	重启	关机	网卡管理	
1	本机引擎	192.168.0.152	2.0.0.0	2.0.0.0	0	在线	0%	39%	15%			

4.8.5.数据备份

用于对系统进行备份、恢复操作。

系统管理 > 数据备份

备份 上传文件恢复

备份日期	备份说明	下载	恢复	删除
------	------	----	----	----

4.8.6.诊断工具

包含 ping、curl、traceroute 等常用工具，可用于系统网络诊断。

系统管理 > 诊断工具

ping traceroute tcpdump curl 调试日志

ping -c 执行

ping输出

4.8.7. 升级管理

用于对系统进行升级，包括离线升级、在线升级等。

系统管理 > 升级管理

升级记录	在线升级	离线升级
------	------	------

① 可选择系统升级包或漏洞库升级包。

上传升级包

系统管理 > 升级管理

升级记录	在线升级	离线升级
------	------	------

当前版本： V2.0 2.0.46

升级方式： 手动升级 *

代理服务器： 开启

在线升级
时可使用
代理服务器

保存

检测新版本

4.8.8. 服务器管理

系统管理 > 服务器管理

系统服务	预警邮件服务器	FTP服务器	SYSLOG服务器	WSUS联动
------	---------	--------	-----------	--------

SSH服务 : 关闭

SNMP服务 : 关闭