

# Hadoop 生态系统安全审查 工具使用文档

## 目录

<b>1. 引言 .....</b>	<b>5</b>
1.1. 编写目的 .....	5
1.2. 技术支持 .....	5
<b>2. 工具部署.....</b>	<b>5</b>
2.1. 环境要求 .....	5
2.2. 启动说明 .....	6
<b>3. 安全审查流程 .....</b>	<b>7</b>
3.1. 工具使用基本流程.....	7
3.1.1. 检测准备.....	7
3.1.2. 外部渗透测试.....	7
3.1.3. 安全机制检查.....	8
3.1.4. 检查报告输出.....	8
3.2. 实施前准备工作.....	9
3.2.1. 运行环境调查分析.....	9
3.2.2. 弱密码知识库维护.....	9
3.2.3. 漏洞知识库维护.....	9
3.2.4. 审查策略构建与维护.....	9
3.3. 外部渗透测试流程.....	10
3.3.1. 服务发现.....	10
3.3.2. 弱密码渗透.....	10
3.3.3. 漏洞检测.....	11
3.4. 安全机制审查流程.....	11
3.4.1. 安全元数据查看.....	11
3.4.2. 安全合规性评估.....	11

3.4.3. 安全冲突检测.....	12
<b>4. 服务发现.....</b>	<b>14</b>
4.1. 待扫描 IP 段和端口段设置 .....	14
4.2. 服务发现结果查看 .....	15
<b>5. 弱密码渗透.....</b>	<b>16</b>
5.1. 选择弱密码渗透 IP 地址 .....	17
5.2. 选择弱用户名及密码字典 .....	17
5.3. 选择弱密码规则.....	18
5.4. 用户信息录入.....	18
5.5. 弱密码渗透结果查看 .....	19
<b>6. 版本漏洞检测 .....</b>	<b>20</b>
6.1. 选择待测目标.....	20
6.2. 组件版本信息查看 .....	21
6.3. 可能存在的漏洞结果查看 .....	22
<b>7. 安全元数据查看 .....</b>	<b>23</b>
7.1. 选择待测目标.....	23
7.2. Hadoop 集群基本元数据信息查看.....	24
7.3. Hadoop 集群运行状态信息查看.....	25
7.4. Hadoop 集群服务级授权信息查看.....	26
7.5. Hadoop 集群日志信息查看 .....	27

7.6.	Hadoop 集群配置信息查看 .....	28
<b>8.</b>	<b>安全评估.....</b>	<b>29</b>
8.1.	安全合规性评估.....	30
8.2.	节点间配置一致性审查 .....	32
8.3.	组件间授权一致性审查 .....	34
<b>9.</b>	<b>知识库使用与管理.....</b>	<b>34</b>
9.1.	知识库组成 .....	35
9.2.	服务组件知识库.....	35
9.3.	安全配置知识库.....	35
9.4.	密码字典知识库.....	37
9.5.	弱密码规则知识库.....	39
9.6.	漏洞补丁知识库.....	41
9.7.	审查策略知识库.....	41

# 1. 引言

## 1.1. 编写目的

占位符

## 1.2. 技术支持

占位符

# 2. 工具部署

## 2.1. 环境要求

工具需要的环境是Python 3.5以上。

工具需要的Python模块如下：

### **Django:**

安装方法： `pip install django==2.0.3`

### **Paramiko:**

安装方法： `pip install paramiko`

### **Pexpect:**

安装方法： `pip install pexpect`

### **Reportlab:**

安装方法： `pip install reportlab`

### **Nmap:**

安装方法： `pip install nmap`

### **Netaddr:**

安装方法： `pip install netaddr`

## 2.2.启动说明

在工具所在的Django工程根目录（包含manage.py文件的目录）下，启动命令行工具（Windows系统）或终端（Mac OS或Linux系统），输入并执行指令python manage.py runserver。

audit	2018/06/11 13:45	文件夹	
BigDataAudit	2018/06/11 13:45	文件夹	
knowledge	2018/06/11 13:45	文件夹	
.DS_Store	2018/05/21 21:17	DS_STORE 文件	15 KB
cve_db.py	2018/05/21 19:27	Python File	3 KB
db.py	2018/05/02 17:08	Python File	1 KB
db.sql	2018/03/25 22:12	SQL 文件	12 KB
db.sqlite3	2018/06/14 16:29	SQLITE3 文件	416 KB
dic_db.py	2018/05/17 16:02	Python File	1 KB
hadoop.csv	2018/04/03 21:40	Microsoft Excel ...	44 KB
hadoop_cve.csv	2018/05/21 19:30	Microsoft Excel ...	15 KB
hbase_cve.csv	2018/05/21 19:05	Microsoft Excel ...	2 KB
hive_cve.csv	2018/05/21 19:26	Microsoft Excel ...	7 KB
import.py	2018/04/07 20:35	Python File	1 KB
manage.py	2018/03/25 21:01	Python File	1 KB

图2.1 Django工程根目录

启动浏览器，输入IP地址127.0.0.1:8000，打开工具主界面。



图2.2 工具主界面

## 3. 安全审查流程

### 3.1. 工具使用基本流程

本工具对Hadoop生态系统的安全特性检查提供了系统而全面的支持，包括了从检查前的检测预备，到外部渗透测试、安全机制检查，以及最后检查报告输出等各个步骤。

#### 3.1.1. 检测准备

在对Hadoop集群进行自动化检查之前，测试人员应尽可能的了解被测系统的相关信息。本工具针对这方面需求，提供了运行环境调查分析、用户基本信息维护等辅助功能，使得安全评估人员可以更好地在Hadoop集群的运行环境具体配置、用户信息情况等方面与测试系统的管理员进行交互。因此在使用本工具和检测目标系统之前，为保证安全审查有效实施，安全测试人员需要根据被测系统的实际情况，对其运行环境进行调查研究，并对工具的基础知识库进行相应的维护，例如维护安全特性知识库中的服务组件、安全配置、审查策略、潜在的用户弱密码及弱密码规则、漏洞补丁等。

#### 3.1.2. 外部渗透测试

在对目标对象检查前，首先要使用相关的工具对集群运行环境进行扫描，以发现Hadoop生态系统及相关组件。Hadoop相关组件一般会开放服务端口来响应某些功能需求。因此服务发现可通过IP地址段和端口探测Hadoop相关组件。当获取了Hadoop集群的IP地址以后，测试工具可以与远程数据库进行通信，在没有

合法用户名和密码的情况下，对集群进行渗透性探测。在渗透性测试过程中，本工具提供了对弱密码用户进行暴力破解的登录尝试。因此在运行本测试之前，建议用户对知识库中常见用户名及其密码库进行维护，以保证渗透测试的有效性。此外，本工具建立了Hadoop相关的CVE知识库，能够对Hadoop集群中各组件的版本进行检测并提醒用户相关漏洞可能存在及解决方案。

### 3.1.3. 安全机制检查

安全机制检查主要分为两部分的内容：安全元数据查看和安全评估。安全元数据查看是展示集群相关的安全元数据信息。安全评估是对集群急用的安全机制进行分析并给出安全建议。通过工具可以查看的集群的安全元数据信息有：集群基本元数据信息，集群运行状态信息，集群服务级授权信息，集群日志名和日志路径信息以及集群安全配置信息。安全评估分为两部分，安全合规性评估主要检验集群的安全配置是否与推荐配置相符合，展示不符合的配置以及修改意见；安全冲突检测主要检查的是节点间配置是否一致以及不同组件对用户的授权是否一致。

### 3.1.4. 检查报告输出

在进行完以上所有工作后，可以把目标系统的安全特性检测结果用统计图表、文档等形式输出并可供评估人员下载。



## 3.2. 实施前准备工作

为了保证Hadoop安全审查的有效顺利进行，需要在使用工具进行审查之前，根据被测系统的具体情况，进行必要的准备工作，包括运行环境调查分析，工具安全知识库基本信息维护等工作：

### 3.2.1. 运行环境调查分析

在对Hadoop生态系统本身进行安全审查之前，首先需要对运行环境进行调查分析，作为目标Hadoop系统风险评估的基本参考信息。

### 3.2.2. 弱密码知识库维护

需要对用户个人信息与密码习惯进行调查，根据调查结果，通过本工具的知识库管理模块可以对弱密码字典与弱密码生成规则进行管理与维护，以保证弱密码渗透的有效性。

### 3.2.3. 漏洞知识库维护

每隔一段时间需要对工具的CVE知识库进行更新与补充，通过本工具的知识库管理模块可以对漏洞知识库进行管理与维护，以保证漏洞检测的时效性。

### 3.2.4. 审查策略构建与维护

需要有针对性地建立或维护相关检查策略。比如HIPAA——健康保险隐私及责任法案，主要是针对健康信息的存储数据库的

安全设定的一系列相关标准，FISMA——联邦信息安全管理法案，主要是针对政府管理信息的存储数据库的安全设定的一系列相关标准等。

### 3.3.外部渗透测试流程

#### 3.3.1. 服务发现

服务发现流程图如下。

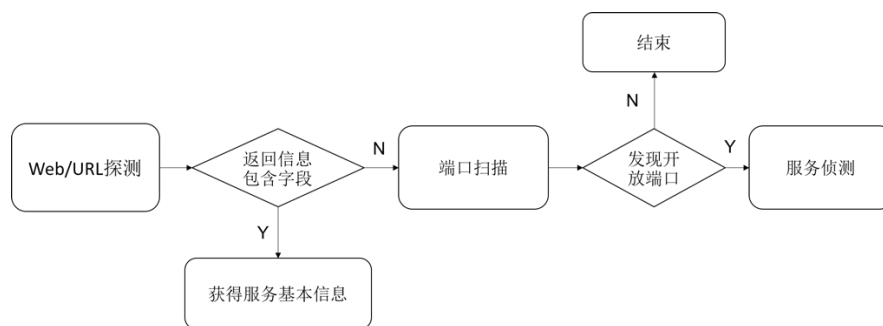


图 3.1 服务发现流程图

#### 3.3.2. 弱密码渗透

弱密码渗透流程图如下。

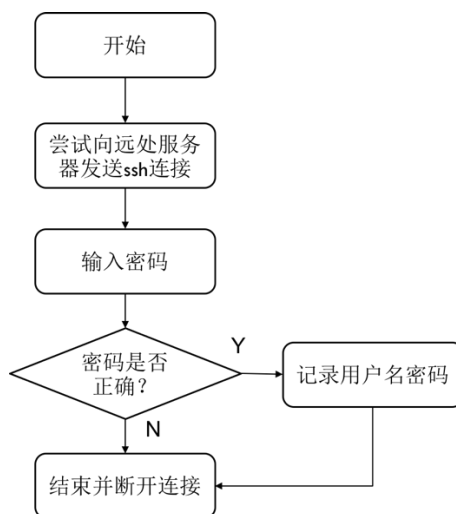


图 3.2 弱密码渗透流程

### 3.3.3. 漏洞检测

漏洞检测是根据对当前集群组件进行版本发现，于CVE知识库中进行比对从而实现。版本发现流程图如下。

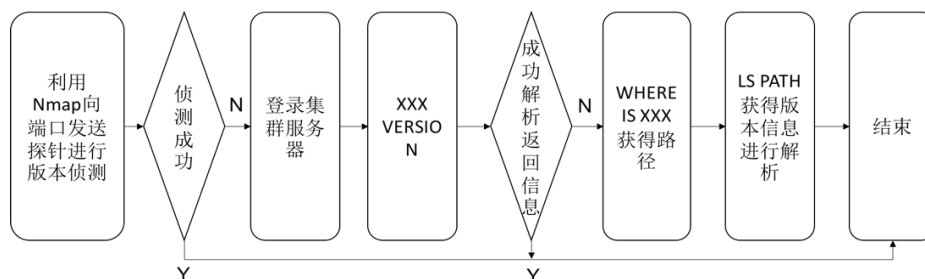


图 3.3 版本发现流程图

## 3.4. 安全机制审查流程

### 3.4.1. 安全元数据查看

安全元数据查看主要是从集群中采集得到安全元数据信息并展示。这部分流程较为简易直观，流程图略去。

### 3.4.2. 安全合规性评估

安全合规性评估流程图如下。

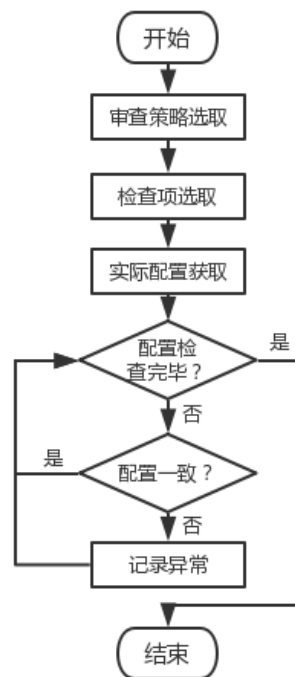


图3.4 安全合规性评估流程图

### 3.4.3. 安全冲突检测

节点间配置一致性审查流程图如下。

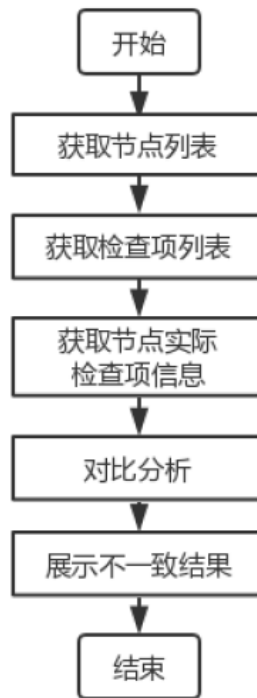


图3.5 节点配置一致性审查流程图

组件间授权一致性审查流程图如下。

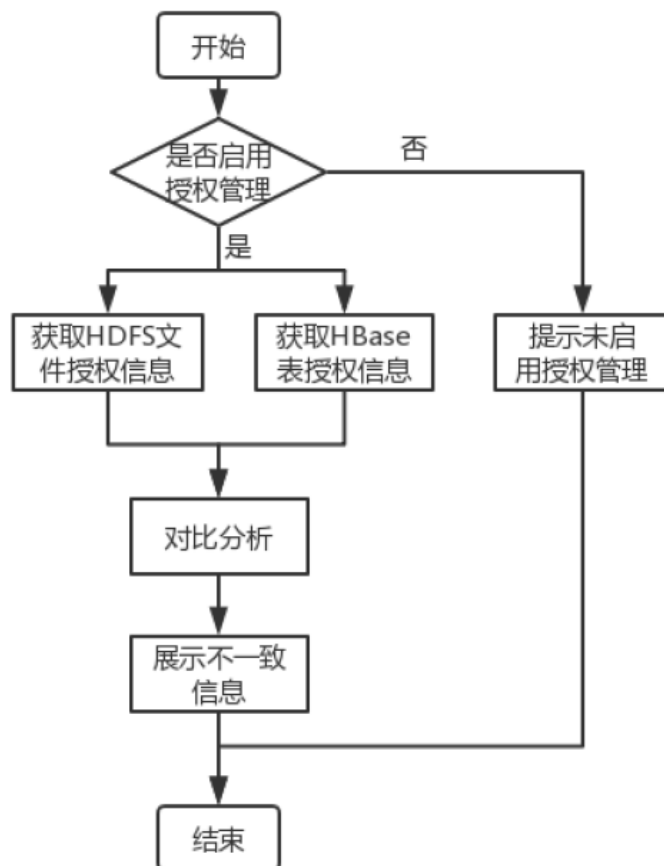


图3.6 组件授权一致性审查流程图

## 4. 服务发现

在对目标Hadoop生态系统进行安全特性审查之前有两种方法指定被测生态系统：一是审查人员通过手工方式输入Hadoop集群IP地址；另一种方式是让审查人员使用工具提供的Hadoop服务发现功能，在网段中自动查找运行的Hadoop生态系统。

服务发现主要是对远程Hadoop集群的端口和服务进行扫描，以便发现Hadoop集群所在IP位置以及Hadoop相关组件所在端口。

### 4.1. 待扫描 IP 段和端口段设置

在开始服务发现之前，审查人员需要在审查工具的服务发现流程主界面（如图4.1所示）中键入待扫描IP段或是独立IP，并自动汇总到待扫描IP列表，以及待扫描端口段或是独立端口，并自动汇总到待扫描端口列表。



该界面是服务发现的配置主界面，顶部有面包屑导航：主页 > 审查项目 > 服务发现。右侧有“帮助”链接。界面顶部是一个流程进度条，包含8个步骤：1. 服务发现（当前步骤）、2. 运行环境安全审查、3. 弱密码检测、4. 版本漏洞检测、5. 漏洞攻击检测、6. 安全元数据查看、7. 安全评估、8. 生成报表。

配置区域包含以下输入项：

- 独立IP**：输入框显示“xxx.xxx.xxx.xxx”，右侧有“添加IP”按钮。
- IP段**：包含“起始”和“结束”两个输入框，分别显示“xxx.xxx.xxx”和“xxx.xxx.xxx.xxx”，右侧有“添加IP段”按钮。
- IP列表**：一个大的文本输入框，右侧有“双击删除”按钮。
- 独立端口**：输入框显示“xxx”，右侧有“添加端口”按钮。
- 端口段**：包含“起始”和“结束”两个输入框，分别显示“xxx”和“xxx”，右侧有“添加端口段”按钮。
- 端口列表**：一个大的文本输入框，右侧有“双击删除”按钮。

底部有三个按钮：“开始”、“重置”和“下一步”。

图 4.1 待扫描 IP 及端口段输入界面

## 4.2.服务发现结果查看

开始服务发现后可能需要一段时间等待，如图4.2所示。

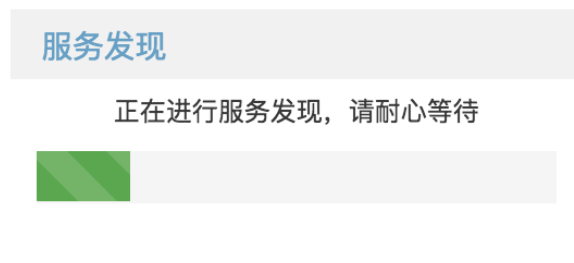


图 4.2 服务发现等待界面

如果发现了具体的 Hadoop 服务地址，审查工具会在界面左侧的已有主机导航栏中显示，如图 4.3 所示。

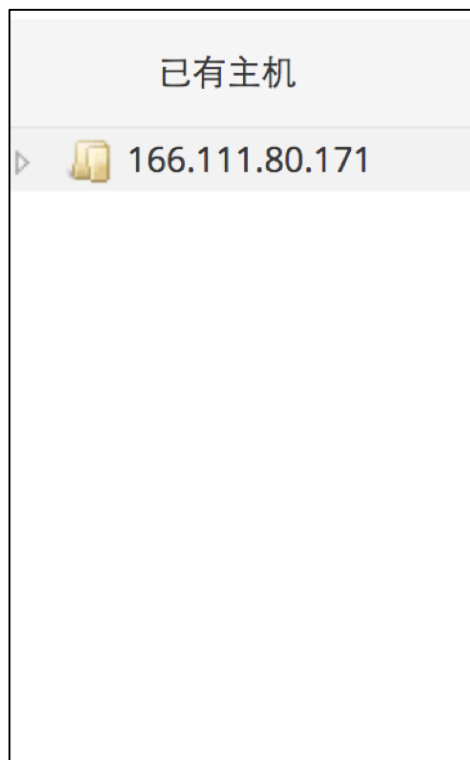


图 4.3 已有主机列表界面

具体的服务发现结果在完成后会自动显示在对话框中。如图 4.4 所示，以表格形式展示了从某个 IP 地址的某个端口发现的具体服务。

服务发现结果			服务发现结果		
IP地址	端口	组件			
166.111.80.171	8088	hadoop	166.111.80.171	50070	avro
166.111.80.171	2181	zookeeper	166.111.80.171	50070	mapreduce
166.111.80.172	2181	zookeeper	166.111.80.171	50070	zookeeper
166.111.80.174	2181	zookeeper	166.111.80.171	50070	dfs
166.111.80.171	50070	hadoop	166.111.80.171	8088	hadoop
166.111.80.171	50070	yarn	166.111.80.171	8088	yarn
166.111.80.171	50070	httpfs	166.111.80.171	8088	httpfs
			166.111.80.171	8088	avro

服务发现结果			服务发现结果		
IP地址	端口	组件			
166.111.80.171	8088	mapreduce	166.111.80.172	8040	hadoop
166.111.80.171	8088	zookeeper	166.111.80.172	50075	hadoop
166.111.80.171	8032	hadoop	166.111.80.172	13562	mapreduce
166.111.80.171	8033	hadoop	166.111.80.172	45221	hadoop
166.111.80.171	9000	hadoop	166.111.80.174	50075	hadoop
166.111.80.171	8983	solr	166.111.80.174	50020	hadoop
166.111.80.171	8030	hadoop	166.111.80.174	39899	hadoop
166.111.80.171	8031	hadoop	166.111.80.172	13562	hadoop

图 4.4 服务发现结果界面

## 5. 弱密码渗透

弱密码渗透主要是对指定IP或服务发现到的Hadoop生态系统所在集群IP进行弱用户名/密码登陆尝试。审查人员通过弱密码渗透可以暴露出Hadoop集群所在IP的密码安全威胁。

审查工具的攻击所用到弱密码是基于用户信息和规则生成的。实际使用环境中，用户密码的构成通常和用户个人信息息息相关，单纯地采用正则表达式定义密码破解规则难以有效地猜测用户的弱口令。因此需要将用户相关的信息(即所谓密码特征)嵌入到密码规则中。显然，如果能够将用户个人信息引入都密码规则中，在密码的生成的时候加入这些个人信息，无疑会增大破解的可能性。出于这样的考虑，本工具定义了一个用户信息表结构，这样在使用工具之前，测试人员就可以维护用户信息，例如添加如数据库用户的生日、手机号、邮箱等与密码相关的辅助信息，也可以通过数据库应用软件自动的从数据库系统中导出这些数据。这些用户个人信息



将作为密码规则定义的部分数据来源。目前生成字符串的方法主要是基于正则表达式，如{Account,Field,Count,^} 语法允许从用户信息表中取出某个用户的某项信息 作为密码的一部分，{\$} 表示用户所选择的常用弱密码字典中的所有密码。举几个简单的例子，{Tom,birthday,4,^} 表示用户 Tom 生日信息取四位并反转，[A-E] 表示 A-E 间的字母，({Tom,Name,30},2) 表示重复用户 Tom 的名字两次。

## 5.1.选择弱密码渗透 IP 地址

在进行弱密码渗透前，首先需要选择弱密码渗透的目标IP地址。如图5.1所示。



图 5.1 选择 IP

## 5.2.选择弱用户名及密码字典

其次，选择内置用户名或自定义用户名并添加到列表，选择弱密码字典并添加到列表。如图5.2和图5.3所示。

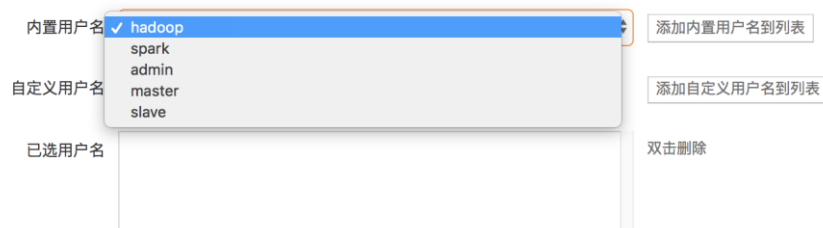


图 5.2 选择弱用户名

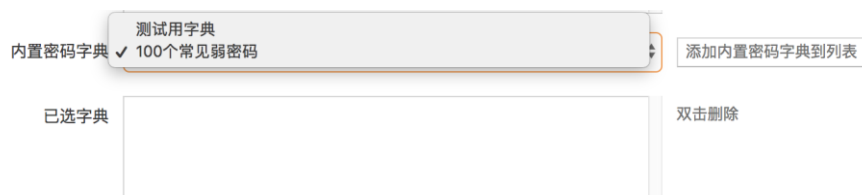


图 5.3 选择弱密码字典

### 5.3.选择弱密码规则

然后，选择内置弱密码规则或自定义弱密码规则并添加到列表。  
如图5.4所示。

内置密码规则

✓ 弱密码倒序  
3位小写字母

添加内置密码规则到列表

自定义密码规则

自定义密码规则

添加自定义密码规则到列表

已选规则

双击删除

开始 重置 上一步 下一步 录入用户信息

图 5.4 选择弱密码规则

### 5.4.用户信息录入

如果有需要，比如弱密码规则中有使用到相应的用户字段，审查人员可以单击图5.4右下按钮录入用户信息。信息录入界面如图5.5所示，包含了账户名，工号，姓名，邮件地址，手机号码，生日日期，部门等等多个字段。



The image shows a 'User Information Entry' dialog box. It contains a series of input fields for the following fields: Account Name, Employee Number, Name, Email Address, Mobile Number, Date of Birth, ID Number, Marriage Date, Spouse Name, Spouse Date of Birth, Department, and Department Number. The 'Account Name' field is highlighted with an orange border.

图 5.5 用户信息录入界面

## 5.5.弱密码渗透结果查看

开始弱密码渗透之后可能需要一段时间等待，如图5.6所示。

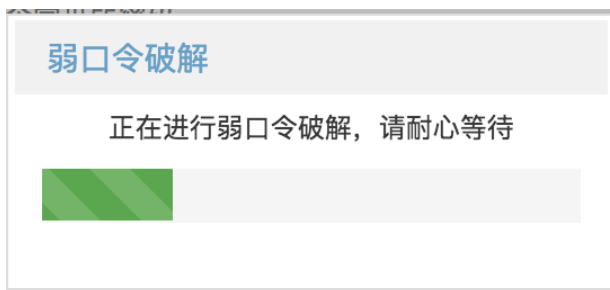


图 5.6 弱密码渗透等待界面

完成弱密码渗透之后，具体结果以表格的形式显示在对话框中。包括渗透的 IP 地址，最终破解的用户名和密码组，以及所使用的弱密码字典和生成规则。如图 5.7 所示。



图 5.7 弱密码渗透结果界面

## 6. 版本漏洞检测

版本漏洞检测是从Hadoop集群检测其各个组件的版本，将其展示给审查人员，并对照CVE知识库中的漏洞CPE发现可能存在的漏洞，从而提醒审查人员Hadoop生态系统中可能存在的隐患并给出解决方案。

### 6.1. 选择待测目标

在开始安全元数据查看前，审查人员需要选择待测节点。



图 6.1 漏洞检测 IP 选择界面



图6.2 未登录集群状态



图6.3 已登录集群状态

图6.2显示的是工具处于未登录集群的状态，图6.3显示的是工具处于已登录集群的状态。当工具处于未登录集群状态下，审查人员无法进行正常的版本检测操作。因此需要点击图6.3中的登录来出现图6.4所示界面。

该图显示了一个名为“登录集群”的对话框。对话框顶部有一个标题栏，上面写着“登录集群”并带有一个红色的关闭按钮。对话框主体包含三个输入框，分别标注为“IP:”、“用户名:”和“密码:”。在对话框底部右侧有两个按钮，分别是“登录”和“取消”。

图6.4 集群信息输入界面

图6.4是登录集群界面，审查人员需在对话框中输入待测节点的IP信息，用户名信息和密码信息后，点击登录按钮。若输入的信息正确，则工具进入如图6.3所示的状态，即可进行后续审查工作。

## 6.2.组件版本信息查看

版本信息以表格形式显示在对话框中，如图6.5所示。

版本漏洞检测结果	
组件名	版本号
Hadoop自身	2.7.5
Spark	2.2.1
Hive	1.2.2
HBase	1.2.6

图 6.5 版本信息结果界面

## 6.3.可能存在的漏洞结果查看

漏洞结果以表格形式显示在对话框中，包括IP，组件名，CVE编号，详情及解决方案，如图6.6所示。点击详情按钮后可以跳转到详情界面包括CVE分值等的一些具体信息，如图6.7所示。

版本漏洞检测结果					
166.111.80.171	Hadoop自身	CVE-2015-7430	IBM Spectrum Scale和通用并行文件系统（GPFS）2.7.0-3之前的Hadoop连接器1.1.1，2.4，2.5和2.7.0-0允许本地用户通过未指定的向量读取或写入任意GPFS数据。	用户应该升级到2.7.0-3版本	<a href="#">详情</a>
166.111.80.171	HBase	CVE-2015-1836	在IBM InfoSphere BigInsights 3.0，3.0.0.1和3.0.0.2及其他产品中使用的Apache HBase 0.98之前0.98.12.1，1.0之前的1.0和1.1.0.1之前的1.1，使用不正确的ACL作为ZooKeeper协调状态，允许远程攻击者导致拒绝服务（守护程序中断），获取敏感信息或通过未指定的客户端流量修改数据。	HBase用户应该更新到各自的最新修补程序版本（例如0.98.12.1，1.0.1.1，1.1.0.1），确保新写入协调信息具有正确的ACL。	<a href="#">详情</a>
166.111.80.171	Hive	CVE-2018-1284	在Apache Hive 0.6.0到2.3.2中，恶意用户可以使用任何xpath UDF（xpath / xpath_string / xpath_boolean / xpath_number /	在HiveServer2和Hive中使用xpath UDF的用户建议将hive.server2.enable.doAs = false升级到2.3.3或将UDFXPathUtil.java更新到branch-2.3的头并重建hive-exec.jar: https://git1-us-west.apache.org/repos/asf?p=hive.git;a=blob;f=ql/src/java/org/apache/hadoop/hive/ql/udf/xml/UDFXPathUtil.java;hb=refs/heads/branch-2.3.	<a href="#">详情</a>

图 6.6 漏洞信息结果界面

版本漏洞检测结果	
CVE编号	CVE-2015-7430
CVSS分值	4.6
机密性影响	PARTIAL
完整性影响	PARTIAL
可用性影响	PARTIAL
攻击复杂度	LOW
攻击向量	LOCAL
身份认证	NONE
CWE描述	CWE-264权限、特权与访问控制
CPE影响版本	"cpe:/a:apache:hadoop:1.1.1 cpe:/a:apache:hadoop:2.4.0 cpe:/a:apache:hadoop:2.5.0 cpe:/a:apache:hadoop:2.7.0"

图 6.7 漏洞详情界面界面

## 7.安全元数据查看

安全元数据查看是从Hadoop 集群中获取到安全信息并且将安全信息直观地展示给审查人员。审查人员通过安全元数据查看可以对待审查的Hadoop 集群有更加深入的了解。2017 年颁布的《网络产品和服务安全审查办法》的第十二条中提到，在安全审查的过程中需要考虑到透明性的问题。安全元数据查看是使得集群安全信息透明化的重要方式。

工具定义的Hadoop 集群安全元数据分为四类。第一类是Hadoop 集群基础设施安全信息，第二类是Hadoop 集群平台安全信息，第三类是Hadoop 集群用户授权信息，第四类是Hadoop 集群安全审计与运行日志信息。

### 7.1.选择待测目标

在开始安全元数据查看前，审查人员需要选择待测节点。



图7.1 未登录集群状态



图7.2 已登录集群状态

图7.1显示的是工具处于未登录集群的状态，图7.2显示的是工具处于已登录集群的状态。当工具处于未登录集群状态下，审查人员无法进行正常的安全元数据查看操作。因此需要点击图7.1中的登录来出现图7.3所示界面。



The image shows a '登录集群' (Login Cluster) dialog box. It has a title bar with the text '登录集群' and a close button (X). The main area contains three input fields: 'IP:' with a text box, '用户名:' (Username) with a text box, and '密码:' (Password) with a text box. At the bottom right, there are two buttons: '登录' (Login) and '取消' (Cancel).

图7.3 集群信息输入界面

图7.3是登录集群界面，审查人员需在对话框中输入待测节点的IP信息，用户名信息和密码信息后，点击登录按钮。若输入的信息正确，则工具进入如图7.2所示的状态，即可进行后续审查工作。

## 7.2.Hadoop 集群基本元数据信息查看

安全元数据审查的主界面如图7.4所示，红色框内可选择安全元数据查看的类别。Hadoop集群基本元数据信息对应的是Hadoop 集群基础设施安全信息，在工具中体现为选择集群基本信息标签。



The image shows the '安全元数据查看' (View Security Metadata) interface. At the top, there is a breadcrumb navigation: '主页 > 审查项目 > 安全审查'. Below this is a progress bar with 8 steps: 1. 服务发现, 2. 运行环境安全审查, 3. 弱密码检测, 4. 版本漏洞检测, 5. 漏洞攻击检测, 6. 安全元数据查看 (highlighted), 7. 安全评估, 8. 生成报表. Below the progress bar, there is a section titled '安全元数据' (Security Metadata). Inside this section, there is a sub-section '集群基本信息' (Cluster Basic Information) which is highlighted with a red box. Below this, there is a table with two columns: '属性名' (Attribute Name) and '值' (Value). At the bottom, there are three buttons: '开始' (Start), '上一步' (Previous Step), and '下一步' (Next Step).



图7.4 集群基本元数据信息查看界面

当工具处于登录状态下时，审查人员可点击页面上的开始按钮开始安全元数据查看，等待界面如图7.5所示。

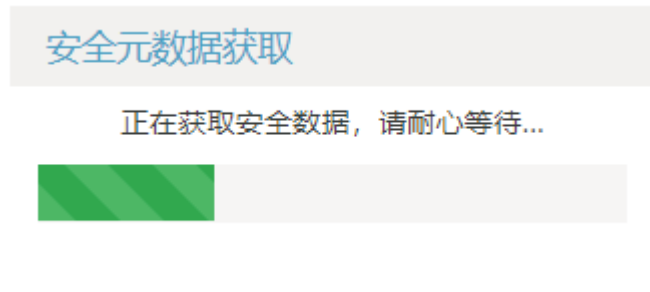


图7.5 安全元数据获取等待界面

集群基本元数据信息以表格的形式显示。

安全元数据

集群基本信息

集群状态信息

集群服务级授权信息

集群日志信息

安全配置信息

集群基本信息

属性名	值
namespaceID	662458300
clusterID	CID-19c61a02-ceed-4f91-b04e-34cf4ef60817
cTime	0
storageType	NAME_NODE
blockpoolID	BP-1309708968-166.111.80.171-1525852771689
layoutVersion	-63

图7.6 集群基本信息结果

### 7.3.Hadoop 集群运行状态信息查看

安全元数据审查的主界面如图7.7所示，红色框内可选择安全元数据查看的类别。Hadoop集群运行状态信息属于Hadoop 集群基础设施安全信息，在工具中体现为选择集群状态信息标签。



图7.7 集群运行状态信息查看页面

当工具处于登录状态下时，审查人员可点击页面上的开始按钮开始安全元数据查看，等待界面如图7.5所示。

集群运行状态信息以文字的形式显示。

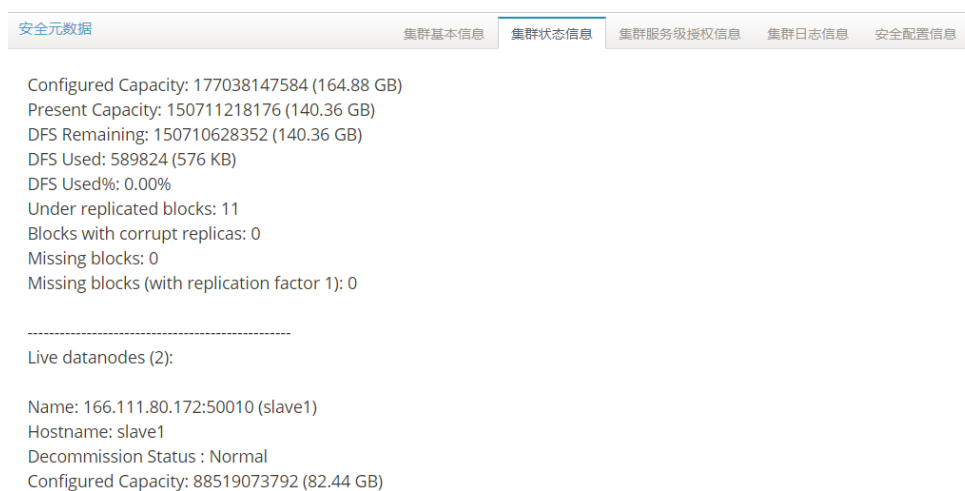


图7.8 集群运行状态信息结果

## 7.4.Hadoop 集群服务级授权信息查看

安全元数据审查的主界面如图7.7所示，红色框内可选择安全元数据查看的类别。Hadoop集群服务级授权信息属于Hadoop 集群用户授权信息，在工具中体现为选择集群服务级授权信息标签。



图7.9 集群服务级授权信息查看页面

当工具处于登录状态下时，审查人员可点击页面上的开始按钮开始安全元数据查看，等待界面如图7.5所示。

集群服务级授权信息以表格的形式显示。

## 7.5.Hadoop 集群日志信息查看

安全元数据审查的主界面如图7.7所示，红色框内可选择安全元数据查看的类别。Hadoop集群日志信息属于Hadoop 集群安全审计与运行日志信息，分为日志名称信息和日志路径信息，在工具中体现为选择集群日志信息标签。



图7.10 集群日志信息查看页面

当工具处于登录状态下时，审查人员可点击页面上的开始按钮开始安全元数据查看，等待界面如图7.5所示。

集群日志信息以表格的形式显示。

## 7.6.Hadoop 集群配置信息查看

安全元数据审查的主界面如图7.7所示，红色框内可选择安全元数据查看的类别。Hadoop集群配置信息属于Hadoop 集群平台安全信息，在工具中体现为选择安全配置信息标签。



图7.11 集群配置信息查看页面

当工具处于登录状态下时，审查人员可点击页面上的开始按钮开始安全元数据查看，等待界面如图7.12所示。



图7.12 集群配置信息获取等待页面

集群日志信息以树形结构的形式显示。



图7.13 集群安全配置信息结果图

展开树形结构可以看到对应组件的具体配置项名称，在配置项名称上（图中红色框的范围内）右键可弹出菜单，点击详情按钮可查看配置项的具体信息。

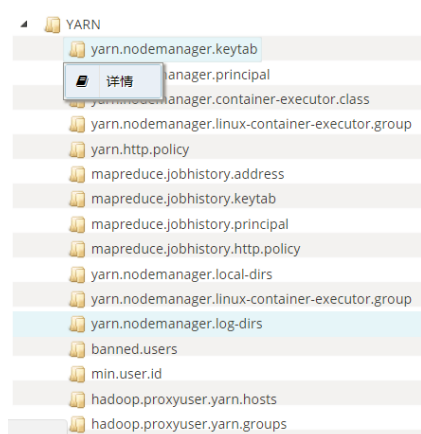


图7.14 右键弹出菜单

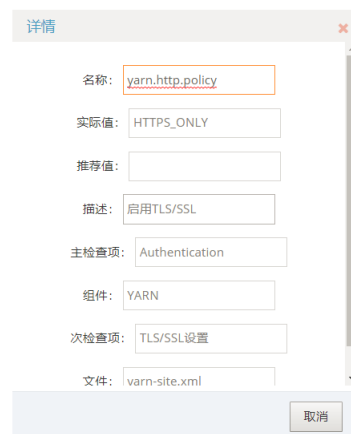


图7.15 安全配置详细信息

## 8. 安全评估

安全评估部分主要分为安全合规性评估和安全冲突检测两个部分。

安全合规性评估的主要内容是对Hadoop 集群启用的安全机制进行分析。安全合规性评估发现并展示集群中存在问题或者缺失的安全机制，并且基于Hadoop 集群安全机制的分析结果给出安全建议。

安全冲突检测概念的提出源于Hadoop 生态系统在结构上的特点。部署了Hadoop 生态系统的系统往往是分布式集群的形式，在集群的每个节点上都存在着配置文件。当管理者对集群的某项配置进行修改时，所有包含该配置所在的配置文件的集群内节点都应该修改该项配置。不同节点不一致的配置会影响到该配置项涉及的安全机制的启用，因此我们需要安全冲突检测的概念，用于审查不同节点上同一配置项的配置值是否相同。此外，对于存储结构而言，其逻辑存储和物理存储可以分别从属于不同组件，然而不同组件的用户授权情况可能存在不一致的情形。为避免授权不一致导致可能的数据泄露，我们也需要安全冲突检测的概念。因此，安全冲突检测分为节点配置一致性审查和组件授权一致性审查。

在执行安全评估前，需要先输入主机用户名密码信息。点击左上方登录后出现如下界面，输入IP、用户名和密码。



图8.1 输入用户名密码图

## 8.1.安全合规性评估

安全评估的主界面如下图所示。



图8.2 安全评估主界面

安全合规性评估涉及审查策略和组件的选取。页面中间可以选择审查策略和待检测的组件。除了工具预置的几种审查策略外，还可以点击自定义策略打开策略维护界面。关于策略维护的具体操作将在文档的第9章中具体说明。选择策略和组件后点击下方安全合规性评估按钮即可开始安全合规性评估。

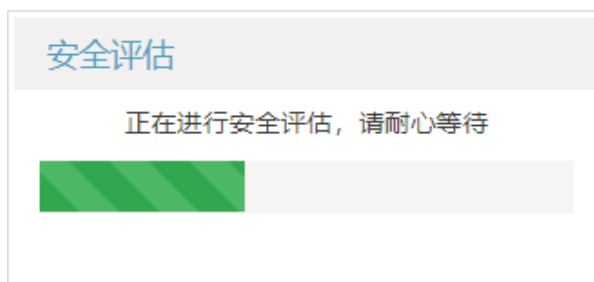


图8.3 安全评估等待界面

安全合规性评估的结果将以弹出页面的形式显示，显示为表格。单击右下角关闭按钮可关闭页面。若不存在不合规的配置，则弹出页面显示提示文字，单击右下角关闭按钮可关闭界面。

安全合规性评估结果			
组件名	配置项	配置文件	安全建议
HDFS	dfs.encrypt.data.transfer	hdfs-site.xml	没有设置启用数据传输协议加密, 建议设置值为true
HDFS	dfs.encrypt.data.transfer.cipher.key.bitlength	hdfs-site.xml	没有设置设置密钥长度, 建议设置值为256
HDFS	dfs.encrypt.data.transfer.cipher.suites	hdfs-site.xml	没有设置设置用于加密的加密套件, 建议设置值为AES/CTR/NoPadding
HDFS	dfs.http.policy	hdfs-site.xml	没有设置启用HDFS的SSL/TLS, 建议设置值为HTTPS_ONLY

图8.4 安全合规性评估结果界面

## 8.2. 节点间配置一致性审查

节点间配置一致性审查属于安全冲突检测的一部分。节点间配置一致性审查也需要选取审查策略以及待测的组件。节点间配置一致性审查的主界面如图8.2所示。

与安全合规性评估不同的是, 节点间配置一致性审查在选择了审查策略和待测组件后, 需要点击下方节点配置一致性审查按钮。点击后工具开始获取集群的节点列表, 等待界面如下。

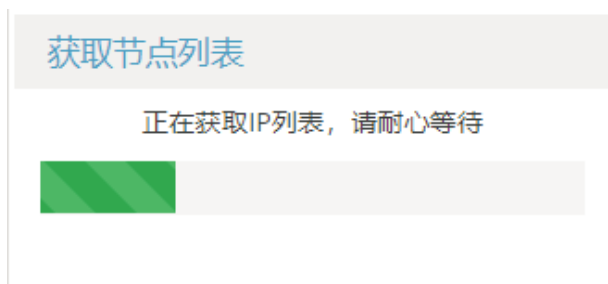


图8.5 获取节点列表等待界面

获取节点列表完毕后, 会出现包含集群节点IP信息的页面。审查人员需要输入对应节点的用户名密码信息, 输入界面如下。



输入节点用户名密码

IP名: 166.111.80.171

用户名:

密码:

IP名: 166.111.80.172

用户名:

密码:

IP名: 166.111.80.174

用户名:

确认 关闭

图8.6 输入节点用户名密码界面图

输入正确的用户名密码后，点击下方确认按钮，会出现如图8.3的等待页面。节点配置一致性审查的结果将以弹出页面的形式显示，显示为表格。单击右下角关闭按钮可关闭页面。若不存在不一致的配置，则弹出页面显示提示文字，单击右下角关闭按钮可关闭界面。

节点安全配置一致性审查结果

配置项名	配置文件	节点1 IP	值1	节点2 IP	值2
ha.zookeeper.quorum	core-site.xml	166.111.80.171	166.111.80.171,166.111.80.172,166.111.80.174	166.111.80.172	
ha.zookeeper.quorum	core-site.xml	166.111.80.171	166.111.80.171,166.111.80.172,166.111.80.174	166.111.80.174	

关闭

图8.7 节点间配置一致性审查结果页面

### 8.3. 组件间授权一致性审查

组件间授权一致性审查属于安全冲突检测的一部分。组件间授权一致性审查不需要选取审查策略以及待测的组件，默认检查Hadoop的两个存储组件HDFS和HBase。组件间授权一致性审查的主界面如图8.2所示。

尽管页面上存在策略和组件选项，这不会影响组件间授权一致性审查的结果。开始审查无需选择策略和组件，只需点击下方组件授权一致性审查按钮。此后开始获取两个组件的用户授权信息，会出现如图8.3的等待页面。组件授权一致性审查的结果将以弹出页面的形式显示，显示为表格。单击右下角关闭按钮可关闭页面。若不存在不一致的授权，则弹出页面显示提示文字，单击右下角关闭按钮可关闭界面。



图8.8 组件间授权一致性审查结果页面

## 9. 知识库使用与管理

审查流程的实现依赖于一个完善的知识库。工具提供了一个较为完善的默认知识库并且提供了知识库管理接口。

## 9.1.知识库组成

知识库主要有六个部分的内容组成：服务组件、安全配置、密码字典、弱密码规则、漏洞列表和审查策略。



图9.1 知识库组成图

## 9.2.服务组件知识库

占位符

## 9.3.安全配置知识库

安全配置知识库在工具中以树形结构的形式显示。审查人员可以通过点击文字前方的三角形（蓝框部分）展开或者关闭次级目录。

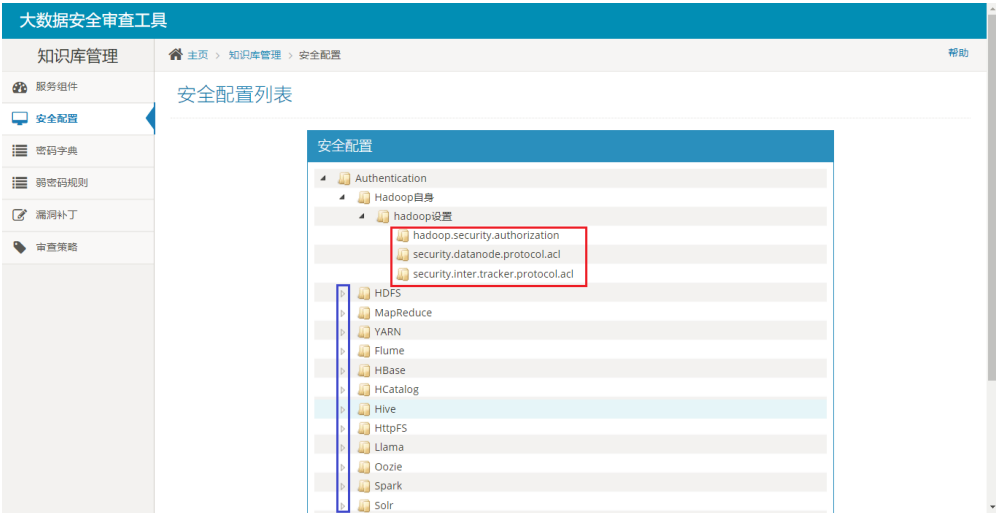


图9.2 安全配置知识库主界面

右键点击红框内部分可以打开对该项配置的操作菜单。



图9.3 操作菜单图

具体的操作界面如下，操作后点击右下角相应按钮保存操作。

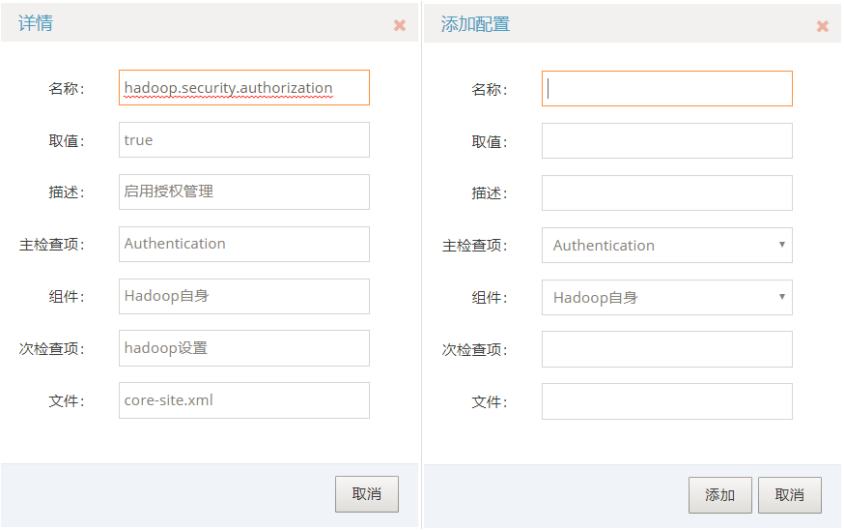


图9.4 详情界面

图9.5 添加界面

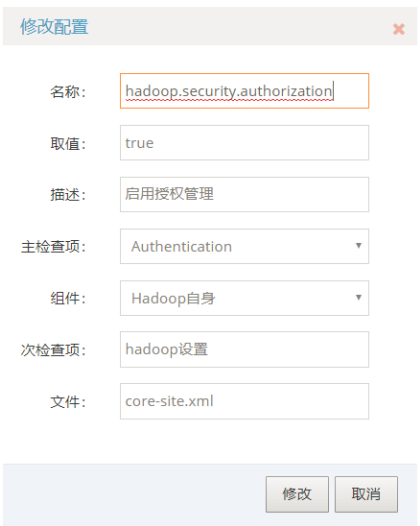


图9.6 修改界面



图9.7 删除界面

## 9.4.密码字典知识库

密码字典知识库以列表的形式显示密码字典的内容，包含了字典的名称、类型、文件名和详情描述。

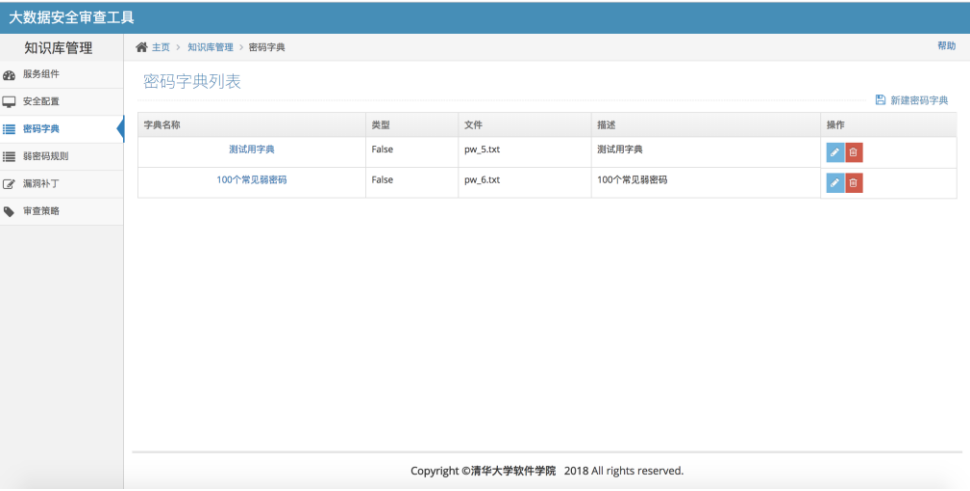


图 9.8 密码字典知识库主界面

每个字典右侧有两种颜色的按钮，蓝色按钮用于编辑字典。点击蓝色按钮可以打开字典编辑界面。审查人员可以选择文件，修改名称、类型或描述，修改完毕后点击最下方确认修改按钮保存改动。



The image shows a web interface titled "编辑字典" (Edit Dictionary) with a red close button in the top right corner. It contains four input fields: "字典名称:" (Dictionary Name) with the value "100个常见弱密码", "类型:" (Type) with a dropdown menu showing "password", "字典文件:" (Dictionary File) with a "选择文件" (Select File) button and the text "未选择任何文件" (No file selected), and "字典描述:" (Dictionary Description) with the value "100个常见弱密码". At the bottom right, there are two buttons: "修改" (Modify) and "取消" (Cancel).

图 9.9 密码字典编辑界面

点击红色按钮弹出警告对话框。点击确认删除字典。



The image shows a dialog box titled "确认删除字典?" (Confirm Delete Dictionary?) with a red close button in the top right corner. It contains a blue box with the text "字典将永远被删除，不可恢复" (Dictionary will be permanently deleted,不可恢复). Below this is a thumbs-up icon followed by the text "确认删除?". At the bottom, there are two buttons: a red button with a trash icon and the text "确认" (Confirm), and a grey button with a red 'X' icon and the text "取消" (Cancel).

图 9.10 密码字典删除界面

此外，主页面上还可以点击新建密码字典打开添加字典界面。添加字典需先输入字典名称、类型和描述并上传字典文件。

添加字典

字典名称:

类型:

username

字典描述:

字典文件:

选择文件

未选择任何文件

添加

取消

图 9.11 密码字典创建界面

## 9.5.弱密码规则知识库

弱密码规则知识库以列表的形式显示密码规则的内容，包含了规则的名称、模式和详情描述。

大数据安全审查工具

知识库管理





服务组件  
安全配置  
密码字典  
**弱密码规则**  
漏洞补丁  
审查策略

主页 > 知识库管理 > 密码字典

帮助

弱密码规则列表

新建弱密码规则

规则名称	规则模式	详细描述	操作
弱密码倒序	{8,^}	常用弱密码字典的倒序	 
3位小写字母	[a-z]{3}	3位小写字母的組合	 

Copyright ©清华大学软件学院 2018 All rights reserved.

图 9.12 弱密码规则知识库主界面

每个规则右侧有两种颜色的按钮，蓝色按钮用于编辑规则。点击蓝色按钮可以打开规则编辑界面。审查人员可以修改规则名称、模式以及描述，修改完毕后点击最下方确认修改按钮保存改动。

修改规则

规则名称：

弱密码倒序

规则模式：

{\$,^}

模式描述：

常用弱密码字典的倒序

修改

取消

图 9.13 弱密码规则编辑界面

点击红色按钮弹出警告对话框。点击确认删除字典。

确认删除规则?

规则将永远被删除，不可恢复

确认删除?

确认

取消

图 9.14 弱密码规则删除界面

此外，主页面上还可以点击新建弱密码规则打开添加规则界面。添加规则需先输入规则名称、规则模式和描述。

添加字典

规则名称：

规则模式：

模式描述：

添加

取消

图 9.15 弱密码规则添加界面



## 9.6.漏洞补丁知识库

占位符

## 9.7.审查策略知识库

审查策略知识库以列表的形式显示策略的内容，包含了策略的名称和描述。



图9.16 审查策略知识库主页面

每条策略右侧有两种颜色的按钮，蓝色按钮用于编辑策略。点击蓝色按钮可以打开策略编辑界面。上方文本框中可修改策略名和策略描述。下方以树形结构展示策略映射的检查项。可以在前方框内勾选检查项。修改完毕后点击最下方确认修改按钮保存改动。



图9.17 审查策略编辑界面

点击红色按钮弹出警告对话框。点击确认删除策略。



图9.18 删除策略对话框

此外，主页面上还可以点击新建策略打开创建策略界面。创建策略需先输入策略名和策略描述。

该界面的标题栏为浅灰色，左侧显示“添加策略”，右侧有一个红色的关闭按钮。下方有两个输入框：第一个输入框上方有“策略名称:”的标签，第二个输入框上方有“策略描述:”的标签。底部是一个浅灰色区域，包含两个按钮：灰色的“添加”按钮和灰色的“取消”按钮。

图9.19 策略名和策略描述添加界面

添加后策略将会出现在主页面的列表中，点击编辑策略按钮打开编辑界面即可选择策略对应的检查项。