ICS 35.240.01
CCS L 60

DB52

贵 州 省 地 方 标 准

DB52/T 1867—2025

大数据安全靶场软件系统建设功能要求

Functional requirements for the construction of big data security range software system

2025－03－06 发布　　2025－06－01 实施

贵州省市场监督管理局　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由贵州大学提出。

本文件由贵州省大数据发展管理局归口。

本文件起草单位：贵州大学(公共大数据国家重点实验室)、上海交通大学、贵州数安汇大数据产业发展有限公司、西安电子科技大学、贵州国卫信安科技有限公司、贵州省信息中心、南京大学、东南大学、中电科大数据研究院有限公司、武汉大学、贵州省信息中心、贵州省大数据应用推广中心、大数据安全工程研究中心（贵州）有限公司、贵州民族大学、贵阳宏图科技有限公司、贵州电子信息职业技术学院。

本文件主要起草人：陈玉玲、秦永彬、朱浩瑾、裴庆祺、贾文生、李志刚、王良民、孟岩、刘景伟、陈国兴、余楷、张旭、许封元、陈艳平、黄瑞章、宁建廷、杨义先、谭伟杰、杨秀璋、欧阳智、杨静、李嘉淳、王崎、徐计、杜逆索、吕虓、黄思齐、董森、豆慧、谭超月、吴越、龙洋洋、罗运、杨宇项、孙静、钟新洋、陈泽瑞、赵素芳、李雪松、廖芳、宋芬芳、李香冬、钱晓斌、张馨予、石睿、徐翼凌、秦曦、丁会敏、严峥晖、杨胜丰、张邦梅、吉健维、李清荷、王华、陶政坪、谢真强、王婧、黄兴、李良懿、胡滔。

大数据安全靶场软件系统建设功能要求

1 范围

本文件规定了大数据安全靶场软件系统建设的功能要求，包括总体要求，平台建设、核心资源库建设和体系建设等要求。

本文件适用于大数据安全靶场软件系统建设工作。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

GB/T 5271.8、GB/T 20984和GB/T 31722界定的以及下列术语和定义适用于本文件。

3.1

大数据安全靶场 big data security range

一种利用虚拟化技术模拟真实网络环境的设施，用于大数据网络安全的演练、测试和人才培养，以增强数据安全防护和应急响应能力，下文简称为靶场。

3.2

靶标 target

被网络攻击者选定的系统、服务或数据。

3.3

漏洞 leak

在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，攻击者能够在未授权的情况下访问或破坏系统。

3.4

信息安全风险 information security risk

特定威胁利用单个或一组资产脆弱性的可能性以及由此可能给组织带来的损害。

[来源：GB/T 31722—2015，3.2]

3.5

访问控制 access control

一种保证手段，即数据处理系统的资源只能由被授权实体按授权方式进行访问。

[来源：GB/T 5271.8，08.04.01]

3.6

探测扫描 ping sweep

向各个IP地址发送ICMP回声请求的一种攻击，旨在寻找易受攻击的主机。

3.7

渗透测试 penetration test

通过模拟恶意黑客的攻击方法，来评估计算机网络系统安全的一种评估方法。

3.8

完整性 integrity

保证信息及信息系统不会被非授权更改或破坏的特性，包括数据完整性和系统完整性。

[来源：GB/T 20984，3.10]

4 缩略语

下列缩略语适用于本文件。

XML：可扩展标记语言（Extensible Markup Language）

XSS：跨站脚本攻击（Cross Site Scripting）

5 总体要求

5.1 基本特征

大数据安全靶场软件系统应涵盖各领域、各行业典型应用的科研与试验保障环境，具有网络空间安全体系规划论证、网络安全防御技术演示验证和体系化安全性评估等能力。大数据安全靶场软件系统的基本特征主要包括行业域、任务域和应用域三个维度，见图1。

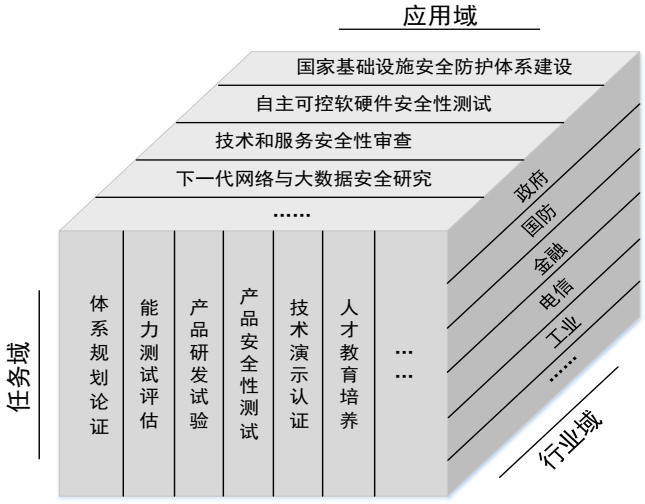

图1 大数据安全靶场软件系统基本特征

5.2 功能需求

5.2.1 行业域

应满足各行业（如政府、金融等）网络空间基础设施安全体系建设与科研试验应用需求。

5.2.2 任务域

应满足完成网络空间安全体系规划论证、能力测试评估、产品研发试验、产品安全性测试、技术演示验证和人才教育培养等任务。

5.2.3 应用域

应满足为各类用户提供一系列网络化联合应用的作用，包括支撑国家基础设施安全防护体系建设、自主可控软硬件安全性测试、技术和服务安全性审查和下一代网络与大数据安全研究等应用。

5.3 体系架构

大数据安全靶场软件系统的体系架构见图2。

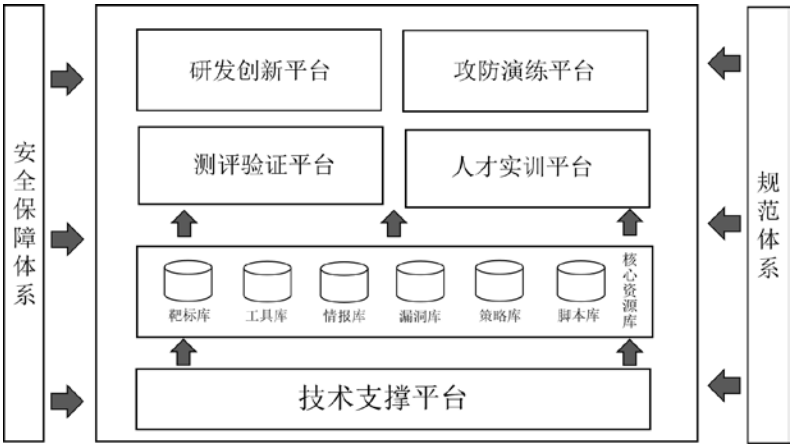

图2 大数据安全靶场软件系统体系架构

6 平台建设

6.1 技术支撑平台

技术支撑平台的建设要求包括但不限于：

a) 应支持海量数据的存储、索引和管理；
b) 应支持复杂的数据分析和处理任务；
c) 应确保测试数据的隐私和安全；
d) 应确保适应不断增长的数据量和用户需求；
e) 应具备完善的性能监控机制；
f) 应提供性能调优工具和方法；
g) 应支持自动化运维功能，如自动化部署、自动化监控、自动化故障排查等；
h) 应支持多租户架构；
i) 应能够与现有的安全工具和系统无缝集成；
j) 应具备灾难恢复计划和数据备份机制；
k) 应确保靶场的运作符合法规要求和行业标准。

6.2 研发创新平台

研发创新平台的建设要求包括但不限于：

a) 应支持研究人员对前沿技术进行深入研究，包括但不限于数据加密、隐私保护、入侵检测、威胁情报分析等；
b) 应制定统一的技术文档编写规范，确保技术文档的准确性和可读性；
c) 应支持将技术研发成果转化为实际产品或解决方案；

d) 应提供完善的实验环境和测试工具；
e) 应提供项目管理和协作工具；
f) 应建立完善的知识产权管理体系；
g) 应制定严格的权限管理制度，确保不同用户只能访问其权限范围内的资源；
h) 应建立用户反馈机制；
i) 应建立创新激励机制；
j) 应建立成果转化机制，推动技术成果向产业界转化；
k) 应建立高效的团队协作机制，包括任务分配、进度跟踪等。

6.3 攻防演练平台

6.3.1 探测扫描

探测扫描功能的建设要求包括但不限于：
a) 可对网络流量进行全面的安全检测和数据采集；
b) 可探测采集多维度安全数据；
c) 可对网络空间中的危险风险进行探测；
d) 可多层面防护措施结合，掌握目标网络安全状况和威胁风险；
e) 可对专用系统进行全面探测扫描；
f) 可深度扫描网络空间服务框架、组件、风险威胁；
g) 可基于多维度、多角度进行安全扫描；
h) 可对多方面的漏洞信息和情报数据进行扫描爬取、安全监测；
i) 可对威胁风险进行验证；
j) 可对威胁风险的影响范围提供可追溯以及可视化呈现；
k) 可智能化完成渗透测试工作；
l) 可对渗透获取信息进行解析和标签识别；
m) 可对整体网络环境进行全面呈现及分析。

6.3.2 指挥调度

指挥调度功能的建设要求包括但不限于：
a) 应保证业务操作的有序性；
b) 应保证协调合作、演练等活动的可行性；
c) 应提供数据库管理服务解决内、外部数据的存储资源；
d) 可对工单流转流程控制；
e) 可视化整体数据展示、业务操作方案。

6.3.3 攻防评估分析

攻防评估分析功能的建设要求包括但不限于：
a) 可自动评估毁伤程度；
b) 可根据毁伤程度自动中止攻防演练；
c) 可对复盘网络环境、复现毁伤过程；
d) 可实时分析演练数据；
e) 可对靶标进行评估分析；
f) 可对安全防御能力进行评估分析；

g） 可对人员技能进行评估分析；
h） 可对战术策略进行评估分析。

6.3.4 资源管理

资源管理功能的建设要求包括但不限于：
a） 可协调相关资源、推进工作进程、通信保障及应急响应等；
b） 应不对核心资源库的资源参数产生影响；
c） 应具备对其它资源自动备案存储、完整封装；
d） 应支持大数据的采集与存储；
e） 应支持情报的采集、加工、存储及调用；
f） 应具备工具配置管理；
g） 可跟踪资源全生命周期。

6.3.5 风险管控

风险管控功能的建设要求包括但不限于：
a） 应统一采取云保护措施；
b） 应对录屏信息、日志、核心数据等进行原始性、完整性保护；
c） 应提前对硬盘进行数据镜像、对工具进行刻盘备案；
d） 应固化数据环境，确保环境整体完整性；
e） 可对大数据流量进行审计；
f） 可监控演练操作、输出日志；
g） 可进行日志审计、应急处理；
h） 应确认目标系统服务的可用性；
i） 可针对外部攻击采取相应的处置和反制措施；
j） 应制定相应的应急方案；
k） 可对恶意代码进行分析；
l） 可对异常行为进行管控；
m） 可对远程攻防演练进行监控。

6.3.6 攻防可视化

攻防可视化功能的建设要求包括但不限于：
a） 可提供可视化的工具与手段；
b） 可自动采集可视化数据；
c） 可对攻防过程的相关信息进行可视化战术；
d） 可选择性地进行数据可视化；
e） 应提供多种可视化方式；
f） 应实现实时数据交互连接。

6.4 测评验证平台

6.4.1 产品测评

产品测评功能的建设要求包括但不限于：
a） 可对软件、硬件、芯片等产品进行测评；

b） 可动态收集测评信息；
c） 可收集与传递测评结果；
d） 可对测评信息、结果进行管理；
e） 可针对不同产品动态选择测评环节。

6.4.2 安全新技术验证

安全新技术验证功能的建设要求包括但不限于：
a） 应具有多种新技术验证方式；
b） 可动态收集验证信息；
c） 可收集与传递验证结果；
d） 可对验证信息、结果进行管理。

6.4.3 漏洞验证

漏洞验证功能的建设要求包括但不限于：
a） 应具有多种漏洞测评方式；
b） 可动态收集漏洞测评信息；
c） 可收集与传递漏洞测评结果；
d） 可对漏洞测评信息、结果进行管理。

6.4.4 在线安全测评

在线安全测评功能的建设要求包括但不限于：
a） 可模拟攻击行为进行非破坏性入侵测试；
b） 可发现漏洞并直观反映潜在威胁；
c） 可多方面、多角度、多检测点安全检测；
d） 可记录测评结果并对安全性进行评价；
e） 可通过安全性分析提供加固建议。

6.5 人才实训平台

人才实训平台功能的建设要求包括但不限于：
a） 应提供网络安全基础知识和技能的培训模块；
b） 应提供高级技能训练，包括但不限于渗透测试、漏洞挖掘、逆向工程等；
c） 应提供实训成果展示和评估机制；
d） 应提供在线帮助文档和视频教程；
e） 应提供个性化的学习路径和资源推荐；
f） 应支持在线学习和离线实践相结合的模式；
g） 应提供技能认证服务；
h） 应提供及时的反馈和建议。

7 核心资源库建设

7.1 靶标库

靶标库的建设要求包括但不限于：

a） 可兼容个别靶标；
b） 应能够以实际工作网络环境构建实战靶场环境；
c） 应能够同时检测各种网络攻击技术；
d） 应具备虚拟、仿真技术，高仿重要基础设施网络环境；
e） 应支持为各规模等级的攻防实战提供演练环境；
f） 可根据典型关键基础设施的网络特点构建虚实一体、以实为主的专业靶场；
g） 应能够提供真实环境支撑信息安全新技术的验证；
h） 可为常态化网络攻防对抗提供支撑；
i） 可检测现有关键基础设施网络安全底数；
j） 应具备一定的扩展性、延伸性及互补性。

7.2 工具库

7.2.1 信息探测工具

信息探测工具的建设要求包括但不限于：

a） 应不对目标本身造成直接伤害；
b） 可为后续攻击步骤收集有用信息；
c） 应包含多种信息探测方式；
d） 应具有多种信息探测工具。

7.2.2 漏洞扫描工具

漏洞扫描工具的建设要求包括但不限于：

a） 可对目标进行自动化检测；
b） 应提供常用的多种漏洞扫描工具；
c） 应提供第三方工具接入接口；
d） 应以兼容性的文件形式保存输出结果。

7.2.3 漏洞利用工具

漏洞利用工具的建设要求包括但不限于：

a） 应提供多种、通用的漏洞利用工具；
b） 应提供可新增漏洞利用工具的接口；
c） 应保证漏洞利用工具可被有效使用；
d） 应以兼容性的文件形式保存输出结果。

7.2.4 开源工具

开源工具的建设要求包括但不限于：

a） 应收集目前已开源的各类攻击工具；
b） 应满足工具可持续加入、迭代的需求；
c） 应提供新工具加入的接口；

d） 可多来源形式收集开源工具。

7.2.5 保密工具

保密工具的建设要求包括但不限于：

a） 应满足工具可持续加入、迭代的需求；
b） 可多来源形式收集保密工具；
c） 应包含部分保密工具；
d） 应对保密工具的保护制定相应的安全等级；
e） 可对保密工具的存储、传输及使用进行严格监控。

7.2.6 访问控制工具

访问控制工具的建设要求包括但不限于：

a） 应保证访问控制工具的有效性和实用性；
b） 应提供常用的访问控制工具；
c） 应提供第三方访问控制工具的接入接口；
d） 可输出相应的操作日志；
e） 应以兼容性的文件形式保存输出结果。

7.2.7 测试工具

测试工具的建设要求包括但不限于：

a） 应包含靶场训练、测试相关的工具；
b） 应能够满足用户基本测试要求；
c） 应包含测试所需的基本软硬件；
d） 应包含开源的测试软件和商用软件；
e） 应包含可对代码静态分析的软件代码分析能力；
f） 应包含可全方位检测各类脆弱性风险并提供分析及建议的漏洞扫描能力；
g） 应包含可自动化的渗透测试能力；
h） 应包含硬件压力测试能力；
i） 应包含健壮性测试能力；
j） 应包含应用性能测试能力；
k） 应包含工控安全测试能力等。

7.3 情报库

情报库的建设要求包括但不限于：

a） 应包含多来源漏洞信息及攻击手段等威胁情报；
b） 可从国内外安全事件中获取威胁情报；
c） 可从攻防实战中积累威胁情报；
d） 可从各种公开的恶意代码中获得漏洞信息；
e） 可多手段分析来自开源情报、传感器、合作伙伴、购买等方式获得的数据；
f） 应获得可机读情报，提供防御工具采取应对措施、决策机构制定决策的数据；
g） 可自主研发相关资源。

7.4 漏洞库

漏洞库的建设要求包括但不限于：

a） 应包含各类已知的网络安全漏洞信息；
b） 应及时收录新发现的安全漏洞；
c） 应建立明确的漏洞评估标准；
d） 应支持分类和标记；
e） 应具备严格的访问控制和数据保护机制。

7.5 策略库

策略库的建设要求包括但不限于：

a） 应包含常用的基本攻防策略；
b） 应针对特种攻防行为制定特种攻防策略；
c） 应对攻防行为制定相应的攻防等级；
d） 应对多种攻防行为具有适应性及有效性；
e） 应满足策略可持续加入、迭代的需求。

7.6 脚本库

脚本库的建设要求包括但不限于：

a） 应包含多种已满足演练要求的模板；
b） 应根据网络运行中的各种安全问题，构建不同等级的网络安全攻击和防御预案；
c） 可根据生成的战略，动态生成相关靶标、攻击策略、防御方法等；
d） 可应对突发的网络安全事件。

8 体系建设

8.1 安全保障体系

安全保障体系的建设要求包括但不限于：

a） 应确保从物理环境安全、安全基础设施、网络安全、计算环境安全、应用安全、安全管理、风险评估等多方面采用技术手段和措施；
b） 应确保靶场可靠稳定运行和试验安全可信开展；
c） 应确保靶场中同时开展的试验相互独立；
d） 应确保靶场中的敏感信息彻底销毁，无信息安全风险泄漏。

8.2 规范体系

规范体系的建设要求包括但不限于：

a） 应遵循相关法律法规，确保试验活动的合法合规性；
b） 应遵循软件开发流程和标准，确保代码质量及系统稳定性；
c） 应遵守技术标准和协议，确保软件系统与现有技术环境兼容和互操作；
d） 应遵循严格的管理制度和标准，确保所有操作符合行业最佳实践。

参 考 文 献

[1] GB/T 5271.8 信息技术词汇 第8部分：安全
[2] GB/T 20984 信息安全技术 信息安全风险评估方法
[3] GB/T 31722 信息技术 安全技术 信息安全风险管理