

中华人民共和国国家标准

GB/T 43741—2024

网络安全技术 网络安全众测服务要求

Cybersecurity technology—
Requirements for crowdsourcing security test services

2024-04-25发布

2024-11-01 实施

国家市场监督管理总局
国家标准化管理委员会

发布

目次

前言 I

引言 II

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 通则 2

 4.1 角色及职责 2

 4.2 服务流程 3

 4.3 安全风险 4

5 服务要求 4

 5.1 准备阶段服务要求 4

 5.2 实施阶段服务要求 5

 5.3 后处理阶段服务要求 7

附录 A（资料性）网络安全众测服务平台功能 8

附录 B（规范性）授权测试方行为准则 11

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。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：国家计算机网络应急技术处理协调中心、中国电子技术标准化研究院、国家信息技术安全研究中心、阿里云计算有限公司、奇安信网神信息技术(北京)股份有限公司、中国移动通信集团有限公司、中国科学院软件研究所、上海斗象信息科技有限公司、北京天融信网络安全技术有限公司、中通服咨询设计研究院有限公司、上海文颯信息科技有限公司、蚂蚁科技集团股份有限公司、杭州安恒信息技术股份有限公司、北京市政务安全保障中心(北京信息安全测评中心)、北京东方通网信科技有限公司、北京众安天下科技有限公司、北京奇虎科技有限公司、中国工业互联网研究院、启明星辰信息技术集团股份有限公司、北京数字观星科技有限公司、中国电子科技网络信息安全有限公司。

本文件主要起草人：云晓春、王文磊、耿冬梅、刘贤刚、张大江、舒敏、孙彦、杨晨、高继明、王宏、严寒冰、何能强、董航、王惠莅、邓萍萍、俞斌、崔婷婷、李媛、胡鸣、王俊杰、郭亮、闫宏石、王奠、邱勤、左敏、胡晓娜、查奇文、张奇、杨蔚、李旭楠、严定宇、伍俊毓。

引 言

《中华人民共和国网络安全法》第二十七条规定“任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具……”。本文件在遵守国家相应的法律法规和技术标准要求的基础上，紧密围绕国内网络安全众测服务的发展实践和需求，提出了网络安全众测服务要求。

网络安全技术 网络安全众测服务要求

1 范围

本文件描述了网络安全众测服务的角色及其职责，服务流程，以及安全风险，规定了服务要求。
本文件适用于网络安全众测服务活动。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 25069—2022 信息安全技术 术语
GB/T 28458—2020 信息安全技术 网络安全漏洞标识与描述规范
GB/T 30276—2020 信息安全技术 网络安全漏洞管理规范
GB/T 35273 信息安全技术 个人信息安全规范

3 术语和定义

GB/T 25069—2022 和 GB/T 28458—2020 界定的以及下列术语和定义适用于本文件。

3.1

网络安全众测服务 crowdsourcing security test service

以众包和自愿的方式组织非特定的自然人或组织，对网络产品和系统等开展漏洞发现等安全测试的过程。

注1:网络安全众测服务符合国家漏洞有关管理规定。

注2:关键信息基础设施的网络安全众测服务在网络安全主管部门和保护工作部门的指导下进行。

3.2

众测需求方 crowdsourcing test demand-side

需要网络安全众测服务(3.1)的组织。

注:众测需求方拥有对测试对象的所有权，与众测组织方(3.3)签订授权测试协议，并授权众测组织方组织授权测试方(3.4)开展网络安全众测服务(3.1)。

3.3

众测组织方 crowdsourcing test provider

在众测需求方(3.2)授权下，组织符合众测需求方要求的授权测试方(3.4)开展网络安全众测服务(3.1)的组织。

3.4

授权测试方 authorized test entity

获得众测组织方(3.3)授权对测试对象进行安全测试的自然人或组织。

3.5

众测审计方 crowdsourcing test auditing entity

网络安全众测服务(3.1)过程中进行审计及监督的组织。

3.6

第三方审计 third-party auditing

独立于众测需求方(3.2)和众测组织方(3.3)的有公信力的众测审计方(3.5)提供的审计。

3.7

网络安全众测服务平台 crowdsourcing security test service platform

由众测组织方(3.3)运营并通过在线方式提供网络安全众测服务(3.1)的平台。

4 通则

4.1 角色及职责

4.1.1 角色及其交互关系

网络安全众测服务涉及的角色包括众测需求方、众测组织方、授权测试方、众测审计方。各角色的交互关系如图1所示。

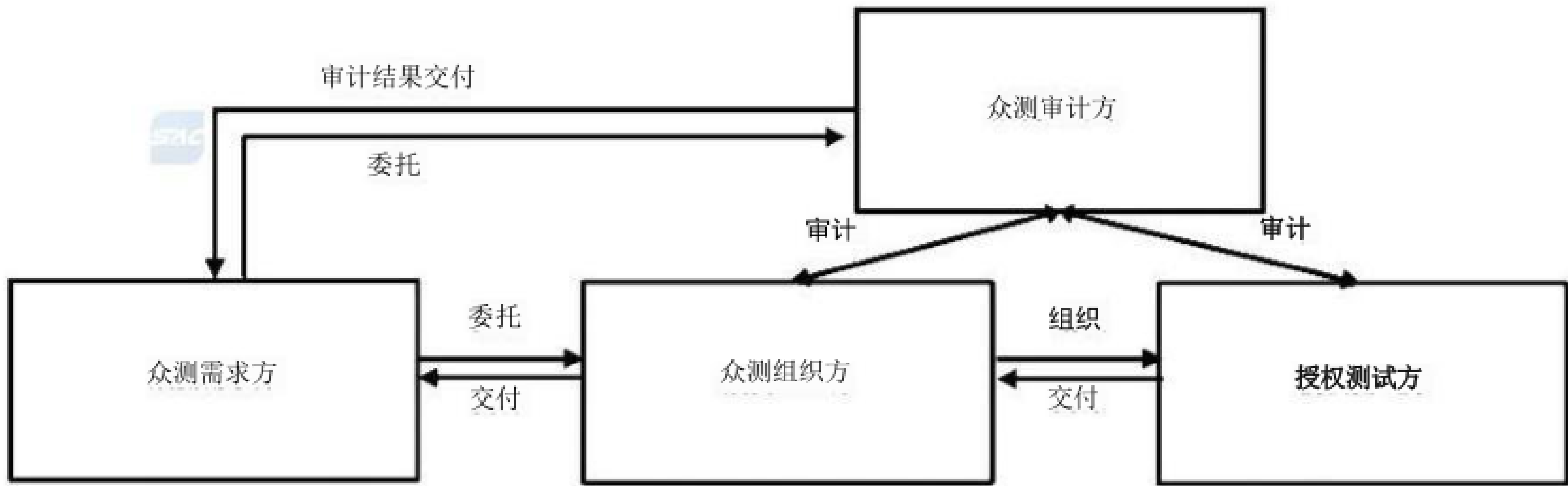


图 1 网络安全众测服务角色及其交互关系

在网络安全众测服务过程中，众测需求方与众测组织方之间通过授权委托建立众测服务关系，众测组织方组织具备测试条件和能力的授权测试方实施众测，并由众测审计方对众测过程进行审计。众测审计方一般应由具备众测审计条件和能力的第三方承担，对授权测试方的审计可由众测组织方承担。各角色的职责详见4.1.2~4.1.5。

4.1.2 众测需求方

众测需求方的职责为：委托众测组织方提供安全众测服务，提供相应证明，明确众测授权和服务要求，制定应急预案。

4.1.3 众测组织方

众测组织方的职责包括：

- a) 验证众测需求方的测试需求；
- b) 选择满足众测需求方要求的授权测试方，并给予测试授权；
- c) 管理授权测试方，包括制定并发布授权测试方行为准则等相关要求，对授权测试方进行身份核验等；
- d) 向众测需求方交付众测结果；
- e) 众测实施环境的运营和管理；

f) 接受并配合众测审计方的审计。

4.1.4 授权测试方

授权测试方的职责包括：

- a) 在众测需求方指定的测试范围及测试时间内进行测试；
- b) 在测试结束后交付测试中发现的安全漏洞及安全众测报告；
- c) 接受并配合众测审计方的审计。

4.1.5 众测审计方

众测审计方的职责包括：

- a) 对众测组织方及由众测组织方组织开展的众测服务活动进行审计及监督；
- b) 客观、公正出具众测审计报告。

4.2 服务流程

网络安全众测服务流程可分为准备阶段、实施阶段、后处理阶段三个阶段。网络安全众测服务流程如图2所示。

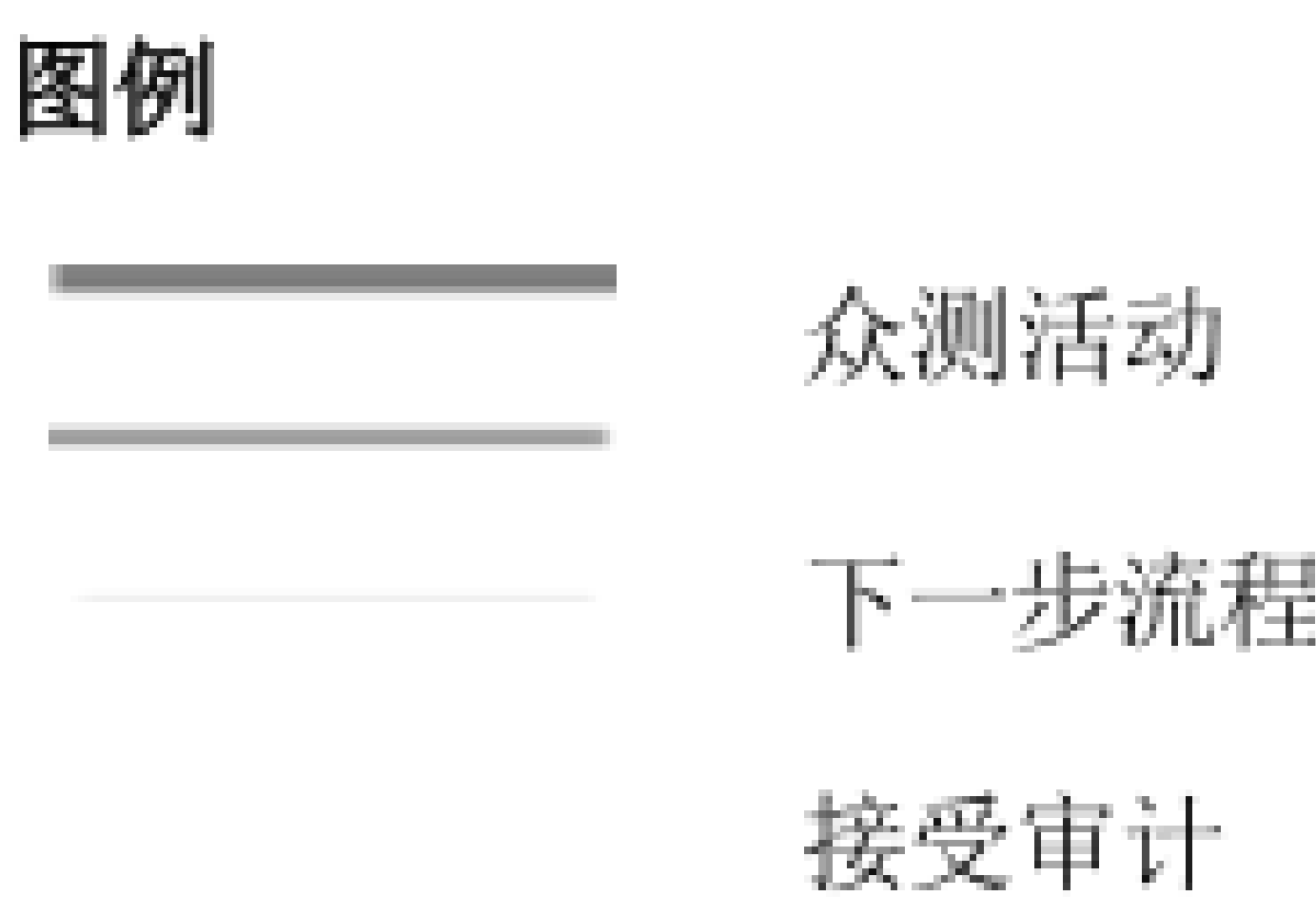
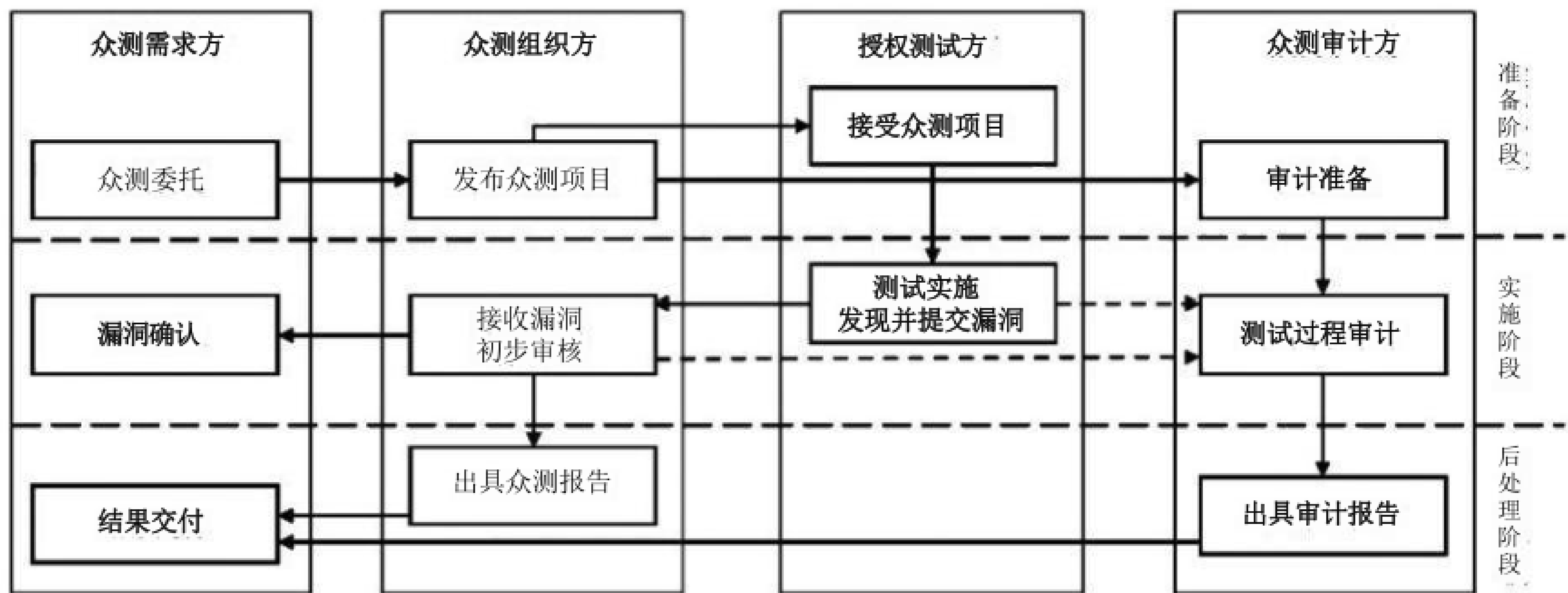


图 2 网络安全众测服务流程

网络安全众测服务流程包括以下几个阶段。

- a) 准备阶段：众测需求方和众测组织方相互协商，明确双方权利义务；众测需求方向众测组织方明确授权并委托众测组织方组织符合要求的授权测试方实施众测；众测组织方按照众测需求方的要求发布众测项目，在获得众测需求方授权的前提下组织授权测试方；授权测试方做好测试准备；众测审计方做好审计准备。
- b) 实施阶段：授权测试方通过获得授权的安全接入方式执行测试，按要求提交漏洞；众测组织方对漏洞进行初步审核后交付给众测需求方；众测需求方对漏洞进行审核确认；众测审计方对众测过程进行审计和监督。

- c) 后处理阶段：在约定的测试时间结束后，众测组织方向众测需求方提供众测服务报告；众测审计方提交众测审计报告。

4.3 安全风险

网络安全众测服务过程中主要面临以下安全风险。

- a) 授权测试方行为不可控的风险：网络安全众测服务的授权测试方来自各种非特定的自然人或组织，若无法对众测过程进行有效管理、监督与审计，授权测试方在众测过程中可能会进行违规操作。
- b) 系统正常运行受到影响的的风险：在安全众测时，需要模拟黑客对设备和系统进行一定的攻击测试工作，可能对系统的运行造成影响，甚至可能会影响业务连续性。
- c) 信息泄露的风险：授权测试方可能会获取到被测系统的业务数据或状态信息，如用户身份信息、用户账号信息、网络拓扑、互联网协议地址、业务流程、安全机制、安全漏洞信息等，存在信息泄露风险。

为降低以上安全风险，在符合国家有关管理规定的前提下，应规范网络安全众测服务各角色在众测服务全流程的活动，网络安全众测服务要求见第5章。

5 服务要求

5.1 准备阶段服务要求

5.1.1 众测需求方

众测需求方要求如下：

- a) 应确定众测服务需求，包括但不限于测试对象、测试时间、测试人员要求、测试人员行为准则、是否第三方审计等众测项目实施参数；
- b) 当针对生产环境下系统、网络开展网络安全众测服务时，应建立测试过程中突发事件应急预案，协调人员做好测试期间的安全监控和应急响应；
- c) 应提供对测试对象拥有所有权的证明；
- d) 应对测试对象进行测试授权；
- e) 宜根据众测服务需求挑选符合条件的授权测试方，也可委托众测组织方挑选。

5.1.2 众测组织方

众测组织方要求如下。

- a) 应制定众测服务项目应急预案。
- b) 应做好众测实施环境准备，网络安全众测服务宜依托网络安全众测服务平台开展，网络安全众测服务平台的功能参考附录A。
- c) 依托网络安全众测服务平台提供网络安全众测服务的，应按照网络安全等级保护等制度的要求履行安全保护义务并通过等级保护测评，收集非自身网络产品和系统安全漏洞的网络安全众测服务平台应履行网络产品安全漏洞收集平台备案。
- d) 应在众测项目正式实施前与众测需求方、众测审计方签订众测授权书及安全保密协议，安全保密协议内容包括但不限于：
 - 测试对象、测试过程、测试结果等众测项目信息；
 - 网络拓扑信息、应用代码等；
 - 众测中发现的漏洞信息等。

- e) 应对众测需求方进行认证以及对测试对象进行所有权校验，确保众测需求方测试内容合法。所有权校验宜支持网站、移动应用程序方式。
- f) 应与众测需求方明确众测服务需求，见5.1.1 a)。
- g) 应按照众测需求方的需求生成众测项目，生成项目的关键要素包括：测试时间、测试范围、测试要求、漏洞评级标准、验收标准。
- h) 应支持众测需求方按测试时间、技能、信誉、排名等多维度挑选授权测试方进行测试或对报名的授权测试方进行筛选；也可受众测需求方委托为其选择合适的授权测试方。
- i) 应根据众测需求方要求支持众测审计方完成代理账号创建、配置等工作。
- j) 应制定并公开发布授权测试方行为准则，授权测试方行为准则应满足附录B的要求。
- k) 应对授权测试方进行实名认证和背景调查。应要求授权测试方提供公民身份证号码或组织机构代码统一社会信用代码等相关信息并进行核实；为方便众测服务的开展，可要求授权测试方提供手机号或其他联系方式。
- l) 应严格管理授权测试方，管理内容包括但不限于实名认证、技能评估、任务完成情况、近三年内无违法违规纪录审核等。
- m) 针对授权测试方的个人信息处理活动应符合 GB/T 35273的要求。
- n) 应根据授权测试方的历史漏洞提交情况，分析其技能、擅长挖掘的漏洞类型、漏洞级别、漏洞报告质量等，审查授权测试方以保证获得良好的测试效果，并判定是否符合众测要求。同时应建立授权测试方的信誉体系及筛选机制，对不符合相关法律法规及不按众测需求方要求进行测试的授权测试方进行处罚及清退，确保身份可信、技能可行。
- o) 宜支持授权测试方填写多维度的属性信息，如技能列表及擅长挖掘的漏洞类型等。
- p) 应面向授权测试方定期开展培训，培训的内容宜包括项目测试范围、项目测试时间、测试行为准则、安全保密要求等。

5.1.3 授权测试方

授权测试方要求如下：

- a) 应符合众测项目的相关要求，包括项目测试范围、项目测试时间、项目测试行为准则、安全保密要求等；
- b) 应提供准确的身份信息，并配合众测组织方完成身份、技能认证；
- c) 应签订保密承诺书；
- d) 宜提供详细的技能列表及擅长挖掘的漏洞类型等信息。

5.1.4 众测审计方

众测审计方要求如下：

- a) 应成立项目实施小组和应急小组，确定项目负责人；
- b) 应完成众测审计的技术准备工作，包括系统环境搭建、稳定性测试、安全接入账号的创建与配置等。

5.2 实施阶段服务要求

5.2.1 众测需求方

众测需求方要求如下。

- a) 当针对生产环境下系统、网络开展网络安全众测服务时，应做好测试期间的系统、网络等的安全监测工作，发现重大安全攻击事件或系统服务中断等突发事件，向有关主管部门报告并启动

相应的应急响应流程。

- b) 漏洞处置、发布、跟踪应符合国家有关管理规定和GB/T 30276—2020的要求。
- c) 应严格按照协议对授权测试方提交的漏洞进行审核确认。

5.2.2 众测组织方

众测组织方要求如下。

- a) 应对漏洞信息进行加密存储。
- b) 发生网络安全事件时，应及时启动应急预案，对事件进行响应和处置。
- c) 应严格管理授权测试方，要求其按照项目要求，在授权的时间范围内，对授权范围内的测试对象，使用授权范围内的测试方法开展测试工作。
- d) 应严格要求授权测试方对测试中可能获取的网络拓扑信息、应用代码、漏洞等严格保密，不应用于其他用途。
- e) 应仅支持授权测试方查看自己提交的漏洞信息。
- f) 当众测需求方和授权测试方对漏洞的判定不一致时，应承担纠纷处理职责。
- g) 应建立授权测试方的信誉或积分体系，对不符合相关法律法规及不按众测需求方要求进行测试的授权测试方进行处罚及清退；对违反相关法律法规等损害众测需求方利益的行为，应协助众测需求方及执法机关，对授权测试方的非法测试行为及其造成的后果进行取证。
- h) 应协助众测审计方，在众测过程中进行审计及监督。

5.2.3 授权测试方

授权测试方要求如下。

- a) 应严格遵守授权测试方行为准则，严格按照众测项目要求开展测试。
- b) 不应私自越界访问/篡改数据信息。
- c) 不应超出项目测试范围对内部网络进行探测、攻击。
- d) 未经许可不应进行高风险操作，包括但不限于服务器提权操作等。
- e) 不应实施对业务造成稳定性、可用性受损的操作行为；发现操作造成了业务稳定性、可用性受损，应立即停止并报告。
- f) 未经许可不应下载/拖取交易数据、用户信息等敏感信息；收到对数据拖取行为的报警时应立即停止当前动作，并配合众测组织方和众测审计方等进行责任追溯。
- g) 应对测试中可能获取的少量的网络拓扑信息、应用代码、数据、漏洞等严格保密，不应使用于其他途径。
- h) 应提交真实完整且描述清晰的漏洞信息，上报的安全漏洞宜参考 GB/T28458—2020 的要求进行标识与描述。
- i) 可协助众测需求方、众测组织方完成漏洞的复测工作。

5.2.4 众测审计方

众测审计方要求如下。

- a) 应对测试授权方的行为进行审计，重点检查测试授权方是否有未授权的入侵网络、干扰网络正常功能、窃取网络数据等危害网络安全的行为或活动，并保存原始日志。
- b) 应记录并加密存储授权测试方的测试流量。
- c) 发现异常时，应及时通知众测需求方和众测组织方。
- d) 应负责测试过程中，授权测试方代理账号的管理工作，包括账号暂停、账号恢复等。
- e) 突发事件时，应协助众测需求方进行突发事件的溯源分析和应急响应工作。

5.3 后处理阶段服务要求

5.3.1 众测需求方

众测需求方应及时对测试结果进行分析总结，改进和提升安全防护能力。

5.3.2 众测组织方

众测组织方要求如下：

- a) 应及时交付安全众测报告，安全众测报告内容包括但不限于安全测试对象、测试时间、测试人员、测试对象整体安全情况分析、漏洞分布及分析、漏洞信息、漏洞修复建议、安全防护建议等；
- b) 应按约定及时删除众测需求方测试对象相关材料、漏洞等敏感信息。

5.3.3 授权测试方

授权测试方应及时删除众测实施过程中上传的木马、后门程序等工具。

5.3.4 众测审计方

众测审计方要求如下。

- a) 应对测试过程中留存的日志等记录进行分析。
- b) 审计的内容包括：
 - 应审计授权测试方是否按照要求，使用授权的测试接入途径进行安全测试；
 - 应审计整体的测试过程，量化授权测试方测试工作量、测试对象范围；
 - 应审计授权测试方使用的攻击手法；
 - 应审计授权测试方的高风险行为操作(如撞库攻击、批量账号登录、扫描器攻击，未授权下载等)，溯源攻击过程。
- c) 审计结果应以众测审计报告的形式交付给众测需求方或众测组织方，说明该次众测活动审计情况。
- d) 众测审计报告的内容应包括测试范围、测试时间、测试人员、审计内容及审计结果等。
- e) 众测审计方由众测组织方承担时，在约定时间内，应支持引入第三方审计机构进行审计和监督。
- f) 应按约定及时删除众测过程中的测试流量等敏感信息。

附 录 A
(资料性)
网络安全众测服务平台功能

A.1 概述

网络安全众测服务平台包括众测需求模块、众测组织模块、授权测试模块、众测审计模块4个部分。

A.2 众测需求模块功能

A.2.1 概述

众测需求模块功能可包括众测需求方账户管理、众测需求管理、漏洞验收。

A.2.2 众测需求方账户管理

能够对需要服务的众测需求方账号进行管理，设置查看漏洞等数据的权限。

A.2.3 众测需求管理

众测需求管理包括如下功能。

- a) 测试项目授权：众测需求方对测试范围中涉及的服务进行授权测试，众测需求方可以通过网络安全众测服务平台进行授权约束。
- b) 测试项目管理：用于帮助众测需求方管理测试进度及测试周期，若众测需求方需要提前结束项目，需要先通知网络安全众测服务平台及授权测试方。

A.2.4 漏洞验收

支持漏洞实时查看，众测需求方可进行确认漏洞、忽略漏洞等验收操作。

A.3 众测组织模块功能

A.3.1 概述

众测组织模块的功能可包括众测项目管理、授权测试方管理、漏洞审核处理。

A.3.2 众测项目管理

众测项目管理包括如下功能。

- a) 项目生成：支持按众测需求方的需求生成众测项目，生成项目的关键要素包括测试时间、测试范围、测试要求、漏洞评级标准、验收标准等。
- b) 项目分配：支持众测需求方按测试时间、技能、信誉、排名、任务完成情况、违规情况等多维度挑选授权测试方进行测试或对报名的授权测试方进行筛选；众测需求方也可委托众测组织方为其选择最合适的授权测试方。
- c) 项目周期管理：支持按众测需求方的设置正常开始和结束项目；当有多个众测需求方发起众测时，支持多个项目并行测试，并合理分配测试人员。在众测需求方提交告知的情况下，支持提早结束或暂停测试项目。同时需对测试对象进行定期健康检查，及时发现破坏与篡改行为，保证测试对象的可用性。

A.3.3 授权测试方管理

授权测试方管理包括如下功能。

- a) 身份管理：该模块支持对测试人员的身份进行实名认证。注册申请的授权测试方需要提供自己的身份相关信息，经审核通过才能参加具体项目中来；出于就测试项目或漏洞和授权测试方沟通的目的，该模块可要求授权测试方提供手机号或其他联系方式。可设立积分、排名，对授权测试方进行管理。
- b) 技能管理：采用综合能力评定方法审查授权测试方以保证其挑选到合适的授权测试方并获得良好的测试效果，如根据历史数据判定授权测试方的测试行为和漏洞提交情况是否符合要求。
- c) 项目管理：项目开始后，能够根据测试实际情况，如测试进展缓慢、测试对象性能压力等，对测试人员进行增加、删除、修改。

A.3.4 漏洞审核处理

当授权测试方提交漏洞之后，众测需求方自行或委托众测组织方对漏洞进行审核。漏洞宜有漏洞待审核、漏洞已确认、漏洞已驳回(忽略)、漏洞已修复、漏洞已复测等状态。

- a) 漏洞待审核表示授权测试方提交漏洞后，等待众测需求方进行审核处理。
- b) 漏洞已确认表示漏洞能被复现，确认漏洞有效。需要众测需求方对漏洞进行修复。
- c) 漏洞已驳回包括漏洞经确认不真实，并不可重现；漏洞过程证明过于简单(无截图等)，众测需求方无法定位与修复漏洞；漏洞真实存在，但是影响不大，实际环境难以造成影响；漏洞属抄袭，或未经验证的提交；漏洞重复或互联网上已有细节公布。
- d) 漏洞已修复表示漏洞已经被众测需求方处理(修复)并解决。
- e) 漏洞已复测表示众测组织方在众测需求方确认漏洞修复后完成对漏洞的再次核查，再次通过技术或人工等手段，确认漏洞修复完善，漏洞不会被再次利用。

A.4 授权测试模块功能

A.4.1 概述

授权测试模块的功能可包括授权测试方账户管理、授权测试方众测项目管理、漏洞提交。

A.4.2 授权测试方账户管理

授权测试方账户管理包括如下功能。

- a) 身份/技能管理：该模块支持授权测试方进行实名认证、设置昵称、组成团队等。支持其填写技能列表及擅长挖掘的漏洞类型。
- b) 荣誉及信誉管理：授权测试方提交被确认的漏洞可获得奖励。当授权测试方在测试过程中出现违背众测需求方测试要求的行为或违反网络安全法的行为时，该模块支持对授权测试方进行相应的处罚。

A.4.3 授权测试方众测项目管理

授权测试方众测项目管理功能包括：

- a) 对分配给授权测试方测试的项目，项目的测试进展、变更，项目中提交的漏洞及相关审核进展；该模块可通过短信站内信等方式通知授权测试方及时处理；
- b) 对分配给授权测试方测试的项目，该模块具备告知其测试的对象、测试范围、测试时间、测试要求、验收标准、奖励标准等功能。

A.4.4 漏洞提交

漏洞提交功能包括：

- a) 授权测试方在提交漏洞时，该模块要求提交的漏洞需包含漏洞标题、漏洞类型、漏洞危害等级、漏洞状态、漏洞简介、漏洞详情、漏洞修复建议等；
- b) 授权测试方提交漏洞后可在后台实时查看漏洞的处理进展及漏洞的状态；若提交的漏洞信息不完整，该模块支持要求授权测试方将漏洞信息补充完整，否则漏洞可能会被驳回。

A.5 众测审计模块功能

A.5.1 概述

众测审计模块的功能可包括流量接入、代理账号管理、流量镜像和数据管控。

A.5.2 流量接入

流量接入功能包括：

- a) 接入安全测试流量；
- b) 流量接入身份由众测需求方确认，流量出口范围由众测需求方确认。

A.5.3 代理账号管理

代理账号管理功能包括：

- a) 能为授权测试方创建代理账号并进行管理，为授权测试方创建针对项目的唯一代理账号，用以标记和区分测试人员的流量；
- b) 在流量存储中，按照安全众测服务平台、项目等生成授权测试方代理账号并控制账号失效时间，使其只在项目测试时段内有效；
- c) 当发现代理账号的测试行为存在风险时，可立刻对该账号进行封停操作。

A.5.4 流量镜像

能够对测试对象测试期间的流量及日志进行留存，用于后续流量分析、审计、追溯等。

A.5.5 数据管控

数据管控功能包括：

- a) 具备格式整理和切片的功能；
- b) 能够按照项目、时序、测试人员等维度将流量进行切片，并将其筛选、整理，形成行为分析模型能够读取的格式。

附 录 B
(规范性)
授权测试方行为准则

授权测试方参与网络安全众测项目应遵守的行为准则如下：

- a) 提供本人/本组织真实有效的身份信息/组织机构信息并配合众测组织方完成身份认证；
 - b) 未经测试需求方许可，不泄露任何项目相关的敏感信息；
 - c) 严格按照项目规定的测试时间，仅通过获得授权的安全接入方式，并仅针对获得明确授权的测试对象开展测试；
 - d) 经许可在众测实施过程中可实现非授权访问或用户权限越权，在完成非授权逻辑、越权逻辑验证时，不再批量获取和留存用户信息和信息系统文件信息；
 - e) 经许可在众测实施过程中可执行数据库查询条件，在获得数据库实例、库表名称等信息证明时，不再批量查询涉及个人信息、业务信息的详细数据；
 - f) 经许可在众测实施过程中可获得系统主机、设备高权限，在获得当前用户系统环境信息证明时，不再获取其他用户数据和业务数据信息；
 - g) 不利用当前主机或设备作为跳板，对测试对象以外区域进行扫描测试；
 - h) 应充分估计目标网络、系统的安全冗余，不进行有可能导致目标网络、主机、设备瘫痪的大流量、大规模扫描；
 - i) 未获得众测需求方的明确授权不执行可导致本地、远程拒绝服务危害的技术验证用例；
 - j) 不执行有可能导致整体业务逻辑扰动、有可能产生用户经济财产损失的技术验证用例；
 - k) 经许可可获得信息系统后台功能操作权限，在获得当前用户角色属性证明时，不再利用系统功能实施编辑、增删、篡改等操作；
 - l) 经许可可获得系统主机、设备、数据库高权限，在获得当前系统环境信息证明时，不再执行文件、程序、数据的编辑、增删、篡改等操作；
 - m) 经许可可在信息系统上传可解析、可执行文件，在获得解析和执行权限逻辑证明时，不驻留带有控制性目的程序、代码；
 - n) 及时提交真实完整的漏洞信息，不隐瞒，不将同一漏洞拆分提交；
 - o) 未经众测需求方许可，不将发现的漏洞信息透漏给任何组织或个人；
 - p) 众测项目完成后，及时删除所获取、留存的项目相关敏感信息。
-

www.bzxz.net

免费标准下载网