奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

https://www.qianxin.com

2021

中国网站安全报告

THE REPORT

发布机构：

奇安信行业安全研究中心
奇安信态势感知第一事业部
网络空间测绘系统（全球鹰）
补天漏洞响应平台
网站卫士
奇安信技术研究院

主要观点

- ✧ 由于建设不足或管理不当引发的各类网站安全隐患普遍存在：
- ✧ 国内存在高危协议端口暴露问题的网站约有 6644.6 万个；
- ✧ 11.5 万个网站被报告安全漏洞 14.6 万个；
- ✧ 信息泄露、SQL 注入和弱口令等问题最为普遍；
- ✧ IT 信息技术与互联网通信、制造业和教育培训类网站的安全漏洞问题最为突出；
- ✧ 平均每天有 2604.9 万次网站攻击被拦截。

摘　要

- 2021 年全年，奇安信全球鹰系统共监测到国内网站资产 18.3 亿个，覆盖 Web 独立 IP 0.6 亿个，其中存在高危协议（例如：SSH、SMB、MySQL 等）端口暴露问题的网站约有 6644.6 万个，占被监测网站总数的 3.6%。
- 2021 年全年，补天漏洞响应平台共收录全国各类网站安全漏洞 146293 个，共涉及网站 115243 个。其中，信息泄露漏洞占比最高，达 36.0%，其次是 SQL 注入漏洞，占比 18.4%，弱口令占比 12.9%。从行业分布来看， IT 信息技术与互联网通信类最多，占比 35.5%，其次是制造业占比 4.3%，教育培训类占比 3.5%排名第三。
- 2021 年全年，奇安信网站卫士共为全国 40.3 万个网站拦截各类网站攻击 95.1 亿次，平均每天拦截攻击 2604.9 万次。其中，异常协议请求占比最高，达 58.1%；其次是扫描器扫描，占 5.3%；SQL 注入攻击占 5.0%。拦截量排名 Top10 的攻击类型，占拦截攻击总量的 84.7%。
- 2021 年全年，奇安信技术研究院累计监测到全国 28.7 万个 IP 遭到 84.2 万次 DDoS 攻击。从攻击类型来看 NTP 最多，占到国内全年 DDoS 攻击总次数的 80.4%；其次是 Jenkins 占 7.7%，Memcached 占 6.2%，SSDP 占 5.4%。
- 2021 年，全国范围内活跃的僵尸网络感染节点 IP 地址共有约 53.0 万个。其中，漏洞攻击源约有 7.2 万个，弱口令暴破源 38.8 万个。

关键词：网站安全、高危端口暴露、安全漏洞、攻击拦截、DDOS 攻击、僵尸网络

目　　录

研究背景

2021 年是我国“十四五”开局之年，也是“两个一百年”奋斗目标的交汇与转化之年。国家信息化、数字化发展进入新的战略阶段，网络安全建设也进入了新的历史时期。以“内生安全框架”为代表新型网络安全建设思想，已经成为国内大中型政企机构新时期网络安全建设与发展的有力思想武器。

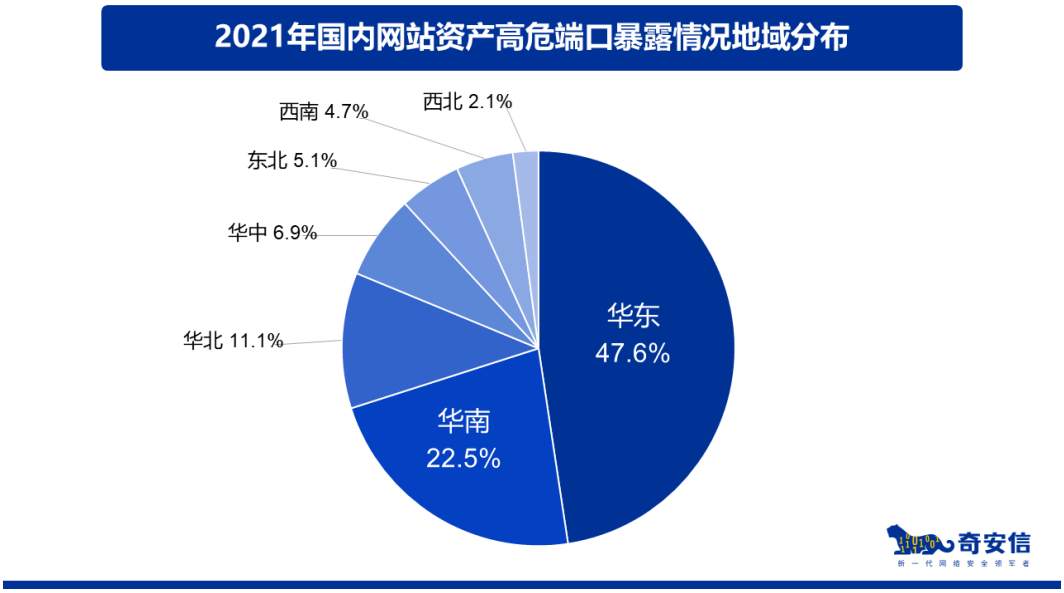
网站是政府和企业重要的信息化平台。网站安全也是政企机构最为关注的网络安全问题之一。近年来，国内大中型政企机构的网站安全建设已然取得了巨大的进步，但安全隐患仍然普遍存在。本文将主要从高危端口暴露、第三方漏洞报告、漏洞攻击、DDoS 攻击、僵尸网络等几个方面，来分析 2021 年国内网站安全的整体状况。

第一章　高危端口暴露

2021 年全年，奇安信全球鹰系统共监测到国内网站资产 18.3 亿个，覆盖 Web 独立 IP 0.6 亿个，平均每个 Web 独立 IP 地址对应 30.5 个网站。其中，具备 ICP 备案的网站约 1.7 亿个，网站备案率约为 9.3%，平均每 10.8 个资产中有一个资产具备 ICP 备案。

在本文中，网站资产与 Web 资产含义相同，是指可以通过互联网直接访问的 Web 类信息资产，包括但不限于：网站、App、微信小程序等等。为叙述方便，后文中将网站资产统一简称为网站。

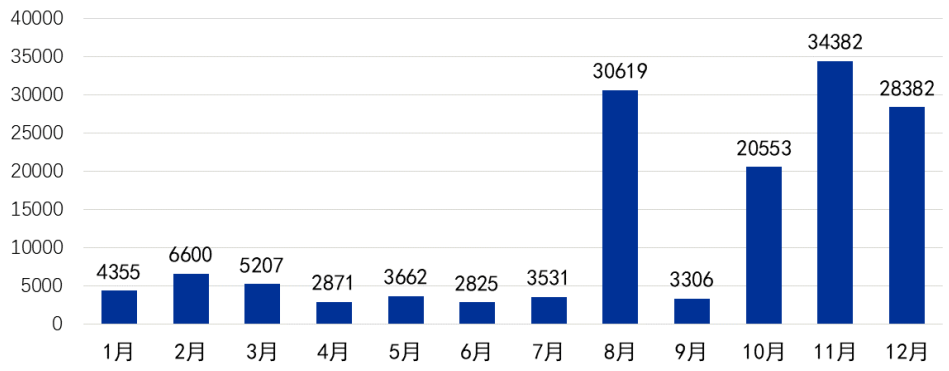
监测显示，在所有被监测的网站中，存在高危协议（例如：SSH、SMB、MySQL 等）端口暴露（简称：高危端口暴露）问题的网站约有 6644.6 万个，占被监测网站总数的 3.6%。从地域分布来看，华东地区存在高危端口暴露的网站最多，在全国占比 47.6%；其次为华南地区，占比 22.5%；华北排名第三，占比 11.1%。具体分布如下图所示：



第二章　第三方漏洞报告

第三方漏洞报告，是网站安全漏洞收集与收录的重要渠道。2021 年全年，补天漏洞响应平台共收录全国各类网站安全漏洞 146293 个，共涉及网站 115243 个。其中，11 月份收录的网站漏洞数量最多，为 34382 个。

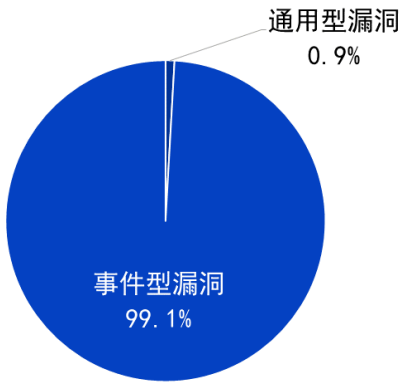
2021年补天平台每月收录网站安全漏洞个数



从漏洞成因分布来看，2021 年全年补天平台收录所有漏洞中，事件型漏洞占比 99.1%，通用型漏洞占比 0.9%。

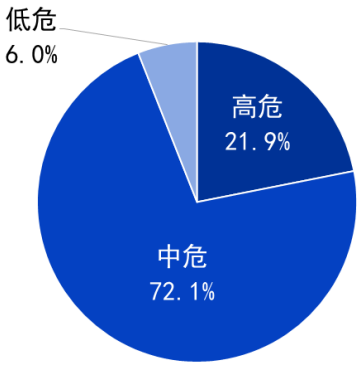
所谓通用型漏洞，通常是指由网站开发平台、开发工具或开发语言等原因引发的同类网站或网站的同类功能模块中普遍存在的安全漏洞。而事件型漏洞，通常是指由于网站自身开发、建设、运维管理等原因引发的，相对孤立存在的安全漏洞。通用型安全漏洞通常可以借助一些自动化工具进行检测，而事件型安全漏洞则通常需要由白帽子来进行人工挖掘。

2021年补天平台收录网站安全漏洞属性分析



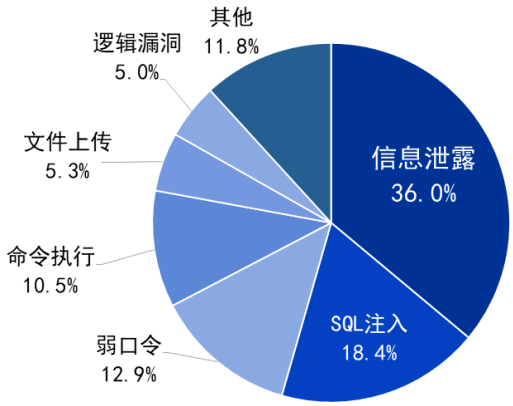
从漏洞的危险程度来看，2021 年全年，在补天平台收录的网站安全漏洞中，高危漏洞占比 21.9%，中危漏洞占比 72.1%，低危漏洞占比 6.0%。中低危漏洞总占比近八成。

2021年补天平台收录网站安全漏洞风险等级分布

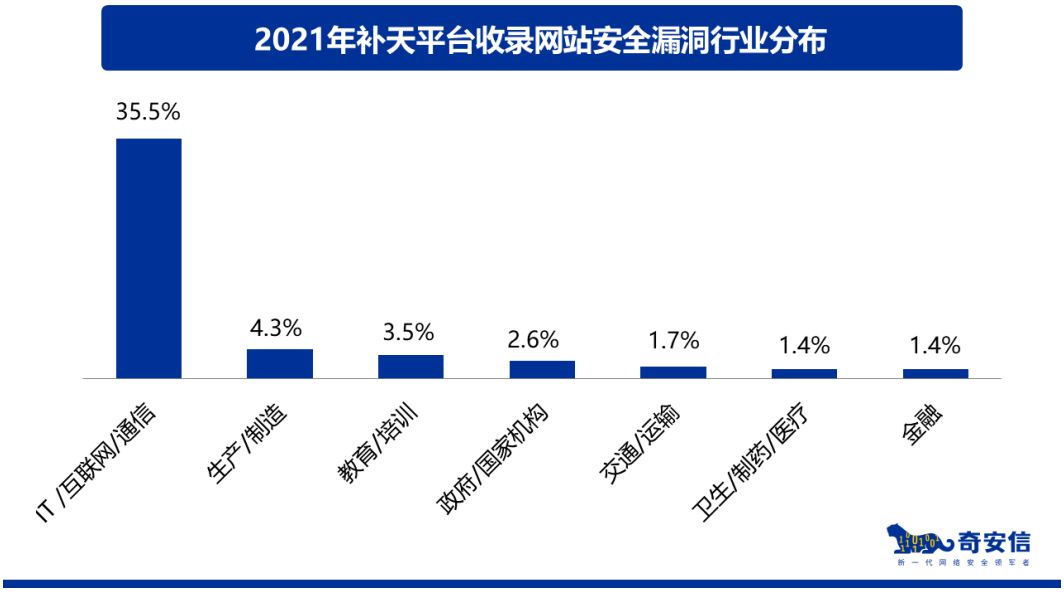


从漏洞的技术类型来看，2021 年全年，在补天平台收录的网站安全漏洞中，信息泄露漏洞占比最高，达 36.0%，其次是 SQL 注入漏洞，占比 18.4%，弱口令占比 12.9%。具体漏洞类型分布见下图：

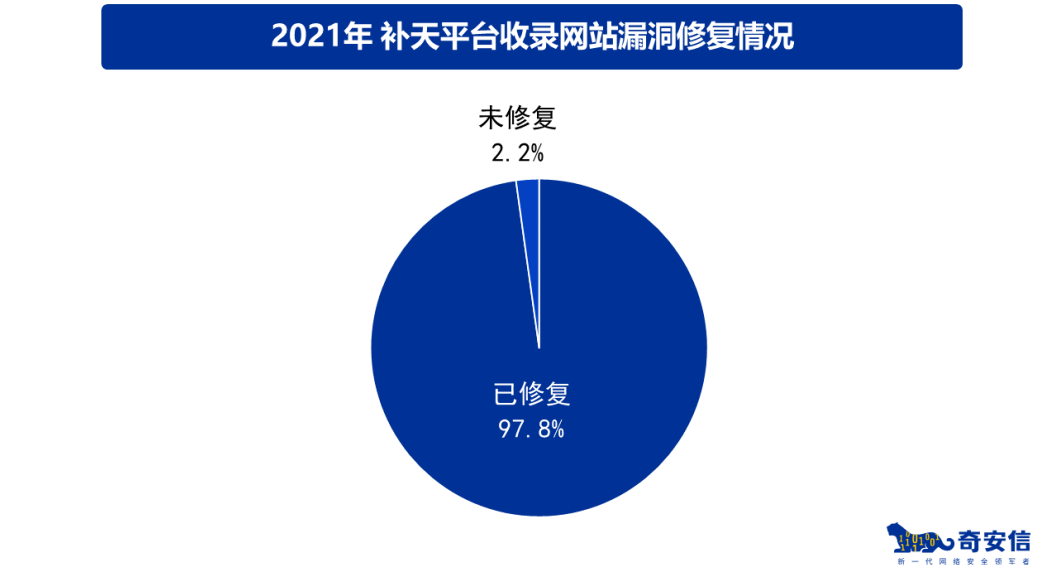
2021年补天平台收录网站安全漏洞技术类型分布



从行业分布来看，2021 年全年，在补天平台收录的网站安全漏洞中，IT 信息技术与互联网通信类最多，占全国的 35.5%，其次是制造业占比 4.3%，排名第二，教育培训类占比 3.5%排名第三。具体分布如下图所示：



抽样人工验证结果显示，2021 年全年，在补天平台收录网站安全漏洞中，97.8%的网站漏洞已经进行了修复，2.2%的网站漏洞未进行修复。网站漏洞的修复比例如此之高，与前些年网络被报漏洞也无人响应、无人管理的情况形成了鲜明的对比。这也再次说明，国内网站的安全建设水平已经有了整体性的大幅提高。

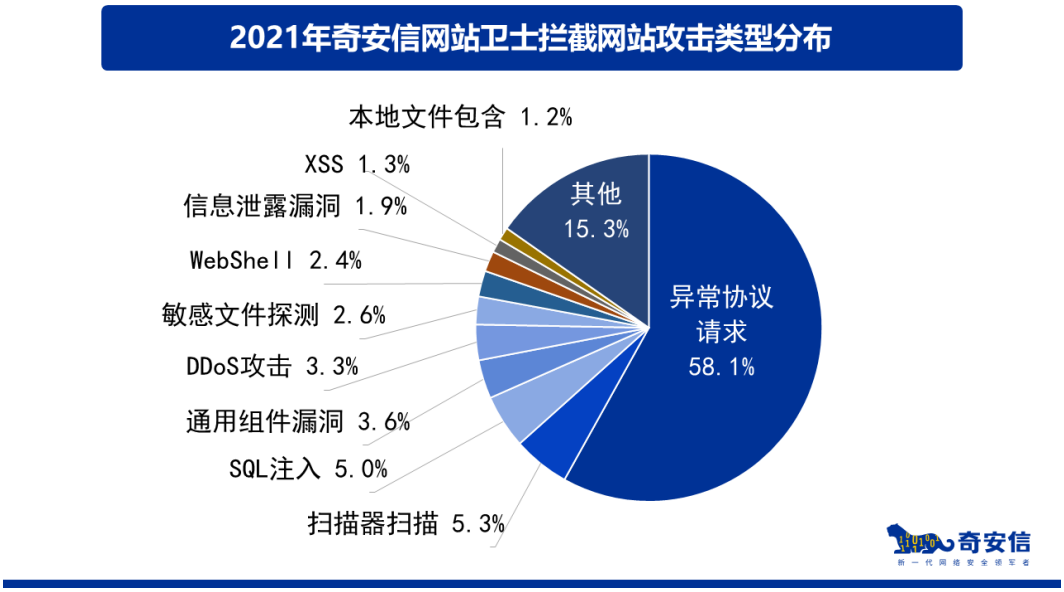


注：补天平台会不定期进行人工复核，以了解漏洞的修复情况，一般采取抽样人工验证的方式。补天平台官网上看到的漏洞修复情况，和抽样调查的结果略有不同。由于部分网站的安全负责人在修复网站漏洞后未及时在补天平台上进行登记。所以，补天平台上站长标记的修复情况会与上述统计有一定的出入。

第三章　网站攻击拦截

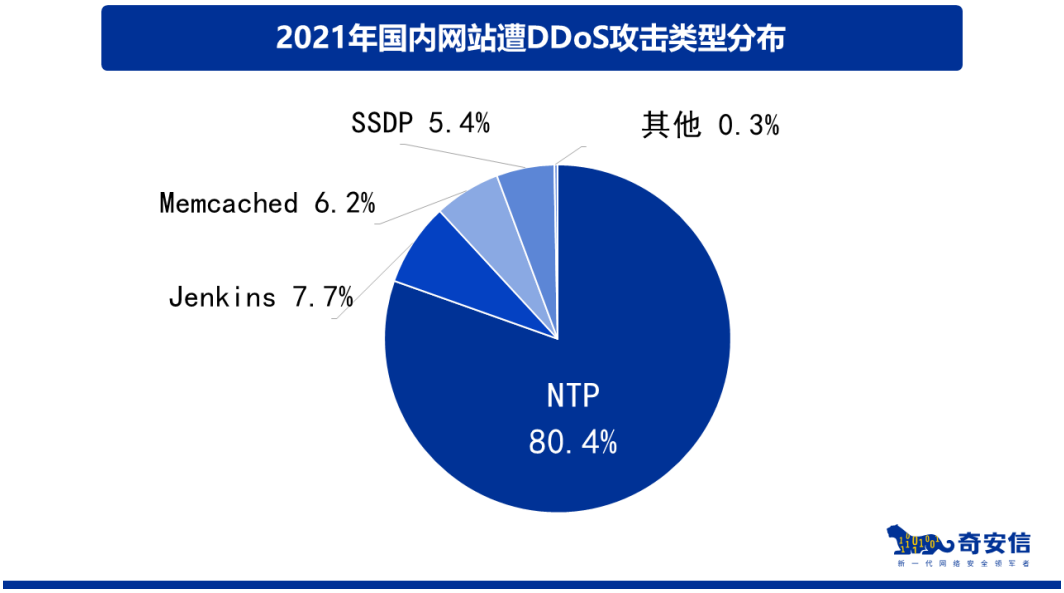
黑客会利用网站安全漏洞对网站发起攻击。而使用网站防护手段，可以对此类攻击进行检测和拦截。

2021 年全年，奇安信网站卫士共为全国 40.3 万个网站拦截各类网站攻击 95.1 亿次，平均每天拦截攻击 2604.9 万次。其中，异常协议请求占比最高，占网站卫士攻击拦截总量的 58.1%；其次是扫描器扫描，占 5.3%；SQL 注入攻击占 5.0%。拦截量排名 Top10 的攻击类型，占拦截攻击总量的 84.7%。



第四章　DDoS 攻击

2021 年全年，奇安信技术研究院累计监测到全国 28.7 万个 IP 遭到 84.2 万次 DDoS 攻击。从攻击类型来看 NTP 最多，占到国内全年 DDoS 攻击总次数的 80.4%；其次是 Jenkins 占 7.7%，Memcached 占 6.2%，SSDP 占 5.4%。



特别说明，在上述统计中，DDoS 攻击的次数统计是以“波次”为单位进行统计的。即在一段连续时间内，对某一个 IP 进行的持续的 DDoS 攻击被认为是一个“波次”的攻击，计为 1 次。这与上一小节中，统计的 DDoS 攻击拦截次数的统计方法有所不同。可以看出，NTP、Jenkins、Memcached、SSDP 等是 DDoS 的主要攻击手法。

此外，进一步分析还显示，约有 4.3%的 DDoS 攻击事件，同时配合使用了多种其他类型攻击手法。攻击者根据目标系统的具体环境灵动组合，发动多种攻击手段，既具备了海量的流量，又利用了协议、系统的缺陷，尽其所能地展开攻势。对于被攻击目标来说，他们需要面对不同协议、不同资源的分布式攻击，分析、响应和处理的成本就会大大增加。

从攻击时长来看，在 2021 年，DDoS 攻击的平均时长为 139.5 秒，99.3%的 DDoS 攻击持续时长在 30 分钟以内，持续时间最长的 DDoS 攻击连续攻击目标长达 18.2 小时。

短时攻击的高占比说明攻击者越来越重视攻击成本和效率，倾向于在短时间内，以极大的流量导致目标服务的用户掉线、延时和抖动。同时，“僵尸网络即服务”和“DDoS 即服务”等黑产运行方式的流行也是重要原因之一，平台用户只要付款就可以即时获得一批佣兵式的攻击资源，可以在短时间内发起大规模攻击。在长周期内，多次瞬时攻击能够严重影响目标服务质量，同时攻击成本能够得到有效控制。

第五章　僵尸网络

僵尸网络是寄生在互联网机体上的毒瘤。攻击者会利用僵尸网络发起漏洞利用、弱口令暴破、恶意扫描等多种类型的攻击，并在攻击成功时下发木马文件以实现自身传播。

奇安信技术研究院对国内互联网上的僵尸网络进行了长期的安全监测。监测显示，2021年，全国范围内活跃的僵尸网络感染节点 IP 地址共有约 53.0 万个（去重统计）。其中，漏洞攻击源约有 7.2 万个，弱口令暴破源 38.8 万个。下面两个表格分别给出了全国漏洞攻击源和弱口令暴破源最多的 5 个 IP 所属 C 段。

表 1 全国漏洞攻击源最多的 5 个 IP 所属 C 段

IP C 段	独立 IP 数（个）
61.242.40.0	212
61.242.54.0	212
61.242.58.0	186
58.248.193.0	184
114.247.84.0	164

表 2 全国弱口令暴破源最多的 5 个 IP 所属 C 段

IP C 段	独立 IP 数（个）
1.202.113.0	256
1.85.218.0	256
49.113.100.0	256
123.160.233.0	256
171.34.178.0	256

附录一 作者简介

《2021 中国政企机构网络安全形势分析报告》是由奇安信集团多个专业研究团队共同编撰完成的。我们在这里向所有参与报告撰写的研究团队致以诚挚的感谢，同时也对各个团队的研究方向及主要贡献进行简要的介绍。

奇安信行业安全研究中心

奇安信行业安全研究中心（以下简称中心）是奇安信集团旗下，专注于行业网络安全研究的机构，为政府、公安、军队、保密、交通、金融、医疗卫生、教育、能源等行业客户及监管机构提供专业安全分析与研究服务。

中心以奇安信集团的安全大数据、全球威胁情报大数据为基础，结合前沿网络安全技术、国内外政策法规，以及近万起应急响应事件的处置经验，全面展开行业级、领域级、国家级网络安全研究。

中心自 2016 年成立以来，已累计发布各类专业研究报告近千篇，在数字安全建设、信息泄露、网站安全、APT、应急响应、人才培养等多个领域的研究成果受到海内外网络安全从业者的高度关注。

奇安信态势感知第一事业部

态势感知第一事业部，主要面向监管部门提供网络安全态势感知和协调指挥相关模式的解决方案，满足国家监管机构和行业监管机构对态势感知的标准要求。团队积累了丰富的监管行业解决方案案例，可为满足不同客户的差异化需求，进行快速的迭代开发。

网络空间测绘系统（全球鹰）

网络空间资产目前面临“查不清”、“摸不准”、“找不到”的难题。对于暴露在互联网上的资产数量不清楚；获取资产属性的手段单一；资产信息靠人工填报，掌握资产信息少、不准确，无法掌握资产的变化；在威胁发生、获得情报、被通报等情况下无法快速定位受影响资产。

针对上述难题，奇安信全球鹰网络空间测绘系统，可对全球暴露在互联网上的服务器和设备进行资产探测、端口探活、协议解析、应用识别，刻画资产画像与主机画像。通过网络空间测绘技术，发现互联网资产暴露面、识别资产类型，实现互联网资产的可查、可定位、帮助客户解决互联网资产暴露面梳理的难题。

补天漏洞响应平台

补天漏洞响应平台（https://www.butian.net），成立于 2013 年 3 月，是国内专注于漏洞响应的第三方平台。补天平台通过充分引导民间白帽力量，实现实时的、高效的漏洞报告与响应。

面对复杂多变的网络安全态势和层出不穷的攻击手段，补天平台采用 SRC、众测等方式服务广大企业，以安全众包的形式让白帽子从模拟攻击者的角度发现问题，解决问题，帮助企业树立动态、综合的防护理念，守护企业网络安全。补天平台将多种安全服务有机的整合

起来，进一步提升企业的漏洞响应能力、积极防御能力和常态化安全运营能力。

成立 7 年来，补天平台已经成为全中国影响力最大的漏洞响应平台之一，同时也是最活跃的网络安全从业者交流平台之一。通过补天白帽大会、“补天杯”破解大赛、补天城市沙龙、补天校园行，搭建安全从业者开放、分享、成长的平台，把国内外网络安全专家、业界大咖、安全厂商、研究机构聚集到一起，结合多种形式建立网络安全从业者技术生态。同时在实战化的趋势下，人是支撑安全业务的最重要因素，补天平台也成为汇聚海量实战型网络安全人才的资源池。通过提供真实的训练环境，开放实战工具箱和资源，定制专属课程、顶级黑客进行技术教学，依托长期积累，利用独有的技术人才优势，培养出具有顶级技术的网络安全实战型人才，为行业提供强有力的人才保障，提升支撑安全业务的各项能力，应对新形势下的网络安全挑战。

网聚安全力量，为社会提供准确、详实的漏洞情报，实现漏洞的及时发现与快速响应，是补天平台始终坚持并不断履行的社会使命。通过营造实战化的学习环境、建设协同育人的导师制度、构建技能衔接的知识体系培养的实战化人才为企业网络安全贡献力量，为国家安全保驾护航。

网站卫士

网站卫士是北京奇安信科技有限公司推出的免费网站安全防护产品，是国内用户量最大的网站安全产品之一。其创新性的“隐身模式”能够保护用户网站安全，把 CC、DDoS 等攻击和入侵都通过云端防护节点进行一遍“清洗”和过滤，从而实现对用户网站的全面保护。通过详细的报表功能和实用的网站加速、网站永久在线功等能帮助网站提高运营水平，提升用户体验。

奇安信技术研究院

奇安信技术研究院，专注于网络空间安全相关技术研究，聚焦网络空间安全领域基础性或前沿性的研究课题，与清华大学、中国科学院等研究机构有深入合作，并结合国家和社会的实际需求，持续开展创新性和实践性技术研究，是国内一流的网络安全技术和学术研究机构。

附录二 95015 服务短号

2022 年 1 月 20 日，奇安信发布全国首个网络安全行业服务短号 95015 正式开通。95015 是为全国各地政府、企业、相关机构提供网络安全应急响应、合作与咨询服务的电话专线。“安全快一步，95015”。

95015 服务短号，由北京 2022 年冬奥会和冬残奥会官方网络安全服务和杀毒软件赞助商奇安信集团，在北京冬奥会开幕前夕正式推出。

在北京 2022 年冬奥会和冬残奥会期间，95015 服务短号是承载全国各地政企机构网络安全保障工作的重要支撑平台，同时也是全国各地重大网络安全事件应急响应的绿色通道，是全国冬奥网络安全保障工作中的关键一环。北京冬奥会结束后，95015 服务短号将永久保留，持续为全国各地政企机构提供网络安全应急响应、合作与咨询服务。

9 字头短号码是工信部统一管理的全国通用号码。95015 服务短号，整合了原有的 4009-727-120 应急响应专线、4009-303-120 客户服务热线和 4006-783-600 合作伙伴热线三条 400 电话专线，实现了“一号全通”。同时，更短的号码也意味着更快的响应速度，更加优质、更加便捷的平台服务，标志着网络安全行业在线服务能力与服务方式的一次重大升级。