

|  |
| --- |
| **XXXX云原生平台渗透测试报告** |

* **文档说明**

|  |  |  |  |
| --- | --- | --- | --- |
| **文档名称** | XXXX云原生平台渗透测试报告 | | |
| **文档编号** | / | **保密级别** | 商密 |
| **编制人员** | 光头强 | **编制日期** | 2025年08月01日 |
| **审核人员** | 超人强 | **审核日期** | 2025年08月01日 |
| **扩散范围** | 限“安恒信息”和“XXXX”内部传阅 | | |

* **适用性声明**

本报告仅适用于杭州安恒信息技术股份有限公司（以下简称“安恒信息”）在XXXXX有限责任公司（以下简称“XXXX”）开展渗透测试时的状况。渗透测试结束之后，因内部环境或不可预知的国内国际政治、经济、法律等社会环境的变化，可能会影响评估结论的有效性，当被测试对象变更时，本报告不再适用。再者，任何控制系统都存在固有的局限性，错误、违反内部控制的情况仍然有可能发生及不被发现。在任何情况下，若需引用本报告中的结果或数据都应保持其本来的意义，不得擅自增加、修改、伪造或掩盖事实。

* **版权声明**

本文中的所有信息均为XXXX内部信息，务请妥善保管，未经XXXX和安恒信息明确作出的书面许可，不得为任何目的、以任何形式或手段（包括电子、机械、复印、录音或其他形式）对本文档的任何部分进行复制、存储、引入检索系统或者传播。

* **适用范围**

本文档是经XXXX授权，由安恒信息对XXXX管辖内提供的信息系统进行安全渗透测试，根据渗透测试结果所提交的报告，用于对XXXX提供的信息系统安全状况阐述。

目 录

[1 项目目标 2](#_Toc1298166537)

[2 测试依据 3](#_Toc1998617486)

[3 测试结论 4](#_Toc1972364475)

[4 测试计划 5](#_Toc972156233)

[4.1 测试对象 5](#_Toc974221655)

[4.2 测试人员 5](#_Toc1328030857)

[5 渗透测试结果 6](#_Toc1417070328)

[6 安全建议 7](#_Toc1635225937)

[7 服务商介绍 9](#_Toc1894092500)

[8 附录 10](#_Toc1862548019)

[8.1 附录一（渗透测试实施流程） 10](#_Toc2122916661)

[8.2 附录二（漏洞定级依据） 11](#_Toc1567010169)

[8.3 附录三（风险定级依据） 11](#_Toc463575)

# 项目目标

根据XXXX公司提供的信息系统的安全性需求，授权安恒信息对其进行安全渗透测试；并根据本次渗透测试过程中所发现的系统脆弱性提供改进方案，以指导XXXX公司开展安全整改、完善安全策略，降低安全风险，使XXXX公司提供的信息系统的安全保障能力符合国家的相关政策法规和自身业务的安全需求。

# 测试依据

项目所依据及参考的标准：

* 《中华人民共和国网络安全法》
* 《中华人民共和国数据安全法》
* 《中华人民共和国个人信息保护法》
* 《关键信息基础设施安全保护条例》（国务院令 第745令）
* 《关于加强信息安全保障工作的意见》（中办发【2003】27号）
* 《信息安全等级保护管理办法》（公通字【2007】43号）
* 《信息安全技术 信息安全风险评估规范》(GB/T 20984-2007)
* 《信息安全技术 信息安全风险评估方法》（GB/T 20984-2022）
* 《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）
* 《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）
* 《信息安全技术 网络安全等级保护实施指南》（GB/T 25058-2019）
* 《信息系统安全保障评估框架》(GB/T 20274-2006)
* 《信息安全技术 网络安全等级保护安全设计技术要求》（GB/T 25070-2019）
* 《信息安全技术 个人信息安全规范》（GB/T 35273-2020）
* 《信息安全技术 网络安全漏洞管理规范》（GB/T 30276-2020）
* 《信息技术 安全技术 信息技术安全性评估准则》（GB/T 18336-2015）
* 《证券期货业移动互联网应用程序安全检测规范》(JR/T0240-2021)
* 《信息技术 IT安全管理指导方针》（ISO/IEC TR 13335）
* 《信息技术 安全性评估通用准则》（ISO15408 CC）
* 《开源安全测试方法手册(OSSTMM)3》(2010)
* 《OWASP测试指南V4.0》

# 测试结论

安恒信息资深安全服务工程师于2025年08月01日至2025年08月08日采用科学的渗透测试手段，对XXXX公司提供的信息系统开展全面的渗透测试（流程见附录一），共发现安全漏洞3个，其中高危1个、中危1个、低危1个。存在的安全隐患主要包括Robots.txt泄露敏感信息等安全漏洞，可能将导致页面被篡改，木马传播，数据损坏等安全风险。经过科学的漏洞和风险等级划分（依据见附录二和附录三），可以判断XXXX公司提供的信息系统正面临的安全风险等级为：高危。

测试结果综述：

|  |  |  |
| --- | --- | --- |
| **序号** | **系统名称** | **漏洞名称** |
| 1 | 云原生平台 | Robots.txt泄露敏感信息 |
| 2 | 云原生平台 | 报错页面敏感信息泄漏 |
| 3 | 云原生平台 | 入侵痕迹残留 |

# 测试计划

## 测试对象

渗透测试限定于以下对象：

测试对象

|  |  |  |
| --- | --- | --- |
| 编号 | 系统名称 | URL |
| 1 | 云原生平台 | http://127.0.0.1:8000/#/ |

## 测试人员

安恒信息组成渗透测试小组，由安恒信息资深安全服务工程师主要参与，XXXX工作人员配合。

项目组成人员如下：

项目成员

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 项目角色 | 姓名 | 联系方式 |
| 1 | 渗透测试工程师 | 光头强 | 18888888 |

# 渗透测试结果

## **云原生平台**

### 【低危】Robots.txt泄露敏感信息

**漏洞描述:**

搜索引擎可以通过robots文件可以获知哪些页面可以爬取，哪些页面不可以爬取。Robots协议是网站国际互联网界通行的道德规范，其目的是保护网站数据和敏感信息、确保用户个人信息和隐私不被侵犯，如果robots.txt文件编辑的太过详细，反而会泄露网站的敏感目录或者文件，比如网站后台路径，从而得知其使用的系统类型，从而有针对性地进行利用。  
攻击者可通过发现robots.txt文件，收集网站的敏感目录或文件，从而有针对性的进行利用。

**漏洞证明:**

* URL: http://127.0.0.1:8000/#/
* 漏洞分析：

步骤：  
1、检测形式多样，工具爬虫扫描得到敏感文件的路径，从而找到robots文件  
2、手工挖掘，直接在域名后输入/robots.txt进行查看。  
结论  
若发现robots.txt中存在allow和disallow的具体内容泄露敏感目录信息，则存在robots.txt泄露敏感信息漏洞。

**加固建议:**

可根据实际情况，进行如下对应的修复：   
1、User-agent: \* 这里的\*代表的所有的搜索引擎种类，\*是一个通配符   
2、Disallow: / 这里定义是禁止爬寻站点所有的内容   
3、Disallow: /admin/ 这里定义是禁止爬寻admin目录下面的目录   
4、Disallow: /ABC/ 这里定义是禁止爬寻ABC目录下面的目录   
5、Disallow: /cgi-bin/\*.htm 禁止访问/cgi-bin/目录下的所有以".htm"为后缀的  
URL(包含子目录)。   
6、Disallow: /\*?\* 禁止访问网站中所有包含问号 (?) 的网址   
7、Disallow: /.jpg$ 禁止抓取网页所有的.jpg格式的图片   
8、Disallow:/ab/adc.html 禁止爬取ab文件夹下面的adc.html文件。   
9、Allow: /cgi-bin/ 这里定义是允许爬寻cgi-bin目录下面的目录   
10、Allow: /tmp 这里定义是允许爬寻tmp的整个目录   
11、Allow: .htm$ 仅允许访问以".htm"为后缀的URL。   
12、Allow: .gif$ 允许抓取网页和gif格式图片   
13、Sitemap: 网站地图 告诉爬虫这个页面是网站地图。

### 【中危】报错页面敏感信息泄漏

**漏洞描述:**

错误页面由服务器产生403、404、500等错误时，返回详细错误信息。报错信息中可能会包含服务器代码信息、数据库连接信息、SQL语句或者敏感文件的路径，为攻击者收集信息提供了方便。  
攻击者可通过上述几种方式触发Web应用程序报错，提取报错信息泄露的敏感信息，如Web中间件的版本信息、数据库连接信息。

**漏洞证明:**

* URL: http://127.0.0.1:8000/#/
* 漏洞分析：

步骤：  
1、通过目录扫描或手工输入不存在的文件或路径，触发服务器产生404错误并返回404页面；  
2、通过目录扫描或手工输入一个无权限查看的文件或路径，触发服务器产生403错误并返回403页面；  
3、手工输入不存在的参数或特殊构造的字符串，如单引号，尖括号等，触发服务器产生500错误并返回500页面或异常信息。  
  
结论  
攻击者可通过上述几种方式触发Web应用程序报错，提取报错信息泄露的敏感信息，如Web中间件的版本信息、数据库连接信息，则存在漏洞。

**加固建议:**

1、编码时增加异常处理模块，对错误页面做统一的自定义返回界面，隐藏服务器版本信息。   
2、不对外输出程序运行时产生的异常错误信息详情。

### 【高危】入侵痕迹残留

**漏洞描述:**

在渗透过程中发现应用中存在曾经的入侵痕迹，如存在的webshell文件。  
残留的入侵痕迹可被其他攻击者用于二次攻击，对网站造成一定的影响。

**漏洞证明:**

* URL: http://127.0.0.1:8000/#/
* 漏洞分析：

步骤：  
1、通常使用Web应用安全漏洞扫描工具或目录扫描工具发现入侵痕迹。  
  
结论  
若发现入侵痕迹，则存在漏洞。

**加固建议:**

1、可借助工具全盘清理入侵痕迹，如D盾可以扫描Windows系统中的 webshell。

# 安全建议

安恒信息作为一家致力于应用安全的专业产品和服务提供商，建议进行以下安全建设，以长期保证所提供的信息系统的安全。

1、针对渗透测试结果协调开发团队或厂商进行有效的安全整改和修复，部署漏洞管理平台，加强对漏洞的闭环管理处置。

2、定期开展对系统、应用以及网络层面的安全评估、渗透测试以及代码审计工作，主动发现目前系统、应用存在的安全隐患。

3、加强日常安全巡检制度，定期对系统配置、网络设备配合、安全日志以及安全策略落实情况进行检查，常态化信息安全工作。

4、完善安全管理制度体系，对信息系统的日常维护和使用进行规范。加大网络安全管理，建立健全内部管理操作流程，明确安全职责、强化责任落实，确保网络安全管理有章可循。

5、建立一套完整的安全运营体系。规范运营流程，持续开展安全风险评估，优化安全管理能力，有效管控安全风险，提升安全能力。

6、建立一套完善有效的应急响应预案和流程，并定期进行应急演练，一旦发现发生任何异常状况可及时进行处理和恢复，有效避免系统业务中断带来损失。

7、定期对相关管理人员和技术人员进行安全培训，提高安全技术能力和实际操作能力。

8、加强安全服务建设，通过引入外部专业服务资源为企业提供更高级别的安全服务能力，完善自身安全建设的同时，协助企业提高安全管理能力。

9、配置资产探测产品，对互联网资产、单位内部资产进行探测，摸清家底，加强对WEB应用资产的管理。

10、配备WEB应用安全防护产品（如：WEB应用防火墙、WEB应用扫描器、数据库防火墙、网页防纂改、抗DDOS等），应对常见的WEB攻击，如XSS、SQL注入、CSRF等漏洞

11、配置WEB应用监测产品，对网站进行7X24小时安全监控。

12、配置日志存储产品，对WEB应用系统、中间件等日志进行存储和分析，满足网络安全法要求及提升应对网络安全突发事件应急处置能力。

13、配置数据库审计产品，实现用户对数据库的增、删、改、查等行为进行审计。

14、加强访问控制ACL策略，细化策略粒度，严格限制各网络区域及服务器之间的访问。

15、对于0day等未被发现的问题，可采用APT攻击分析平台、大数据安全分析系统、网络安全保险等控制措施；对于不可预知的变化，可采取持续性态势感知监测技术、动态风险评估以及安全可信众测等措施加以防范。

# 服务商介绍

杭州安恒信息技术股份有限公司（简称：安恒信息）成立于2007年，于2019年11月5日正式登陆上交所科创板股票上市，股票代码：688023。自成立以来一直专注于网络信息安全领域，公司秉承“助力安全中国、助推数字经济”的企业使命，以“诚信正直、成就客户，责任至上，开放创新，以人为本，共同成长”作为企业的价值观，不断提高核心技术创新能力，致力于成为一家具有优秀企业文化和社会责任感的新时代网络信息安全产品和服务提供商。公司主营业务为网络信息安全产品的研发、生产及销售，并为客户提供专业的网络信息安全服务。

公司始终坚持持续创新的发展战略，并将每年营收的20%作为研发投入，采用研发中心和研究院双线创新机制，产品与服务涉及应用安全、大数据安全、云安全、物联网安全、工业控制安全及工业互联网安全等领域，围绕事前、事中、事后几个维度已形成覆盖网络信息安全生命全周期的产品体系，能够为客户从安全规划、安全设计、安全建设到安全运营的一站式专业安全服务与可信众测服务。专业安全服务主要包括安全评估服务、安全咨询服务、安全运维服务、红队行动服务、安全培训服务、创新安全服务六大方面。SaaS云安全服务加上城市安全大脑、全天候“三位一体”的态势感知、国家级网络安保团队组成了智慧城市安全运营中心服务的核心能力，网络空间学院，提供人才培养、攻防竞赛、认证培训三项服务。

作为国内网络信息安全领域的领导者之一，自2015年公司历年均被美国著名网络安全风险投资公司（Cybersecurity Ventures）评选为全球网络安全创新500强，参与了众多国家与行业标准的制定。根据国家发改委正式发布的“2018年度国家地方联合工程研究中心”名单，公司成为“大数据网络安全态势感知及智能防控技术国家地方联合工程研究中心”的依托单位。

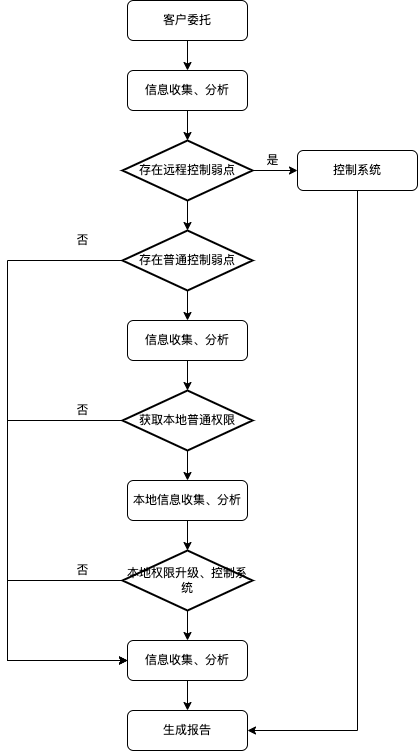
未来公司将牢牢抓住网络强国和数字中国战略背景下网络信息安全行业市场发展机遇，依托多年积累的行业经验，围绕“云、大、物、智”开发适应新场景的网络信息安全新产品，提供综合网络信息安全解决方案，具备真正的城市级感知、防护和运营能力。 通过人工服务将技术、流程和人有机结合起来，并形成标准化的流程和数据分析模型用于安全运营管理工作。

# 附录

## 附录一（渗透测试实施流程）

渗透测试服务通过远程利用目标应用系统等安全弱点，模拟真正的黑客入侵攻击方法，以人工渗透为主，以漏洞扫描工具为辅，在保证整个渗透测试过程都在可以控制和调整的范围之内尽可能的获取目标信息系统的管理权限以及敏感信息。

安恒信息渗透测试服务的主要流程如下：



渗透测试流程

1. 信息收集

信息收集是指渗透实施前尽可能多地获取目标信息系统相关信息，例如网站注册信息、共享资源、系统版本信息、已知漏洞及弱口令等等。通过对以上信息的收集，发现可利用的安全漏洞，为进一步对目标信息系统进行渗透入侵提供基础。

1. 弱点分析

对收集到的目标信息系统可能存在的可利用安全漏洞或弱点进行分析，并确定渗透方式和步骤实施渗透测试。

1. 获取权限

对目标信息系统渗透成功，获取目标信息系统普通权限。

1. 权限提升

当获取目标信息系统普通管理权限后，利用已知提权类漏洞或特殊渗透方式进行本地提权，获取目标系统远程控制权限。

## 附录二（漏洞定级依据）

漏洞定级依据

| 序号 | 漏洞等级 | 描述 |
| --- | --- | --- |
| 1 | 紧急 | 可以直接被利用的漏洞，且利用难度较低。被攻击之后可能对网站或服务器的正常运行造成严重影响，或对用户财产及个人信息造成重大损失。 |
| 2 | 高危 | 被利用之后，造成的影响较大，但直接利用难度较高的漏洞。或本身无法直接攻击，但能为进一步攻击造成极大便利的漏洞。 |
| 3 | 中危 | 利用难度极高，或满足严格条件才能实现攻击的漏洞。或漏洞本身无法被直接攻击，但能为进一步攻击起较大帮助作用的漏洞。 |
| 4 | 低危 | 无法直接实现攻击，但提供的信息可能让攻击者更容易找到其他安全漏洞。 |

## 附录三（风险定级依据）

风险等级

|  |  |  |
| --- | --- | --- |
| 编号 | 风险等级 | 风险描述 |
| 1 | 高风险 | 可对目标网站造成重大损失，如信息篡改、数据损坏以及远程控制。 |
| 2 | 中风险 | 可获取目标网站敏感信息，并结合其他安全漏洞可能影响目标网站的正常运营。 |
| 3 | 低风险 | 可获取目标网站少量敏感信息，一般不会导致严重的安全事件。 |