**XXX集团漏洞扫描分析报告**

|  |  |  |  |
| --- | --- | --- | --- |
| **版本编号** | V1.0 | **密级** | 商业保密 |
| **制作人** | DX-Tools | **日期** | 2023年03月27日 |

|  |  |  |  |
| --- | --- | --- | --- |
| **版本变更记录** | | | |
| **时间** | **版本** | **说明** | **修改人** |
| 2023年03月27日 | V1.0 | 由DX-Tools导出初版渗透测试报告 | DX-Tools |
|  |  |  |  |



**2023年03月27日**

|  |
| --- |
| 目录 |
| [一. 漏洞扫描介绍 1](#_Toc36126144)  [1.1 漏洞扫描的概念 1](#_Toc36126145)  [1.2 漏洞扫描的必要性 1](#_Toc36126146)  [1.3 漏洞扫描客户收益 1](#_Toc36126147)  [1.4 漏洞扫描的依据 2](#_Toc36126148)  [1.5 漏洞扫描的原则 3](#_Toc36126149)  [1.6 漏洞扫描的范围 4](#_Toc36126150)  [1.7 漏洞扫描的流程 4](#_Toc36126151)  [1.8 漏洞扫描风险控制 5](#_Toc36126152)  [二. 漏洞扫描工具介绍 7](#_Toc36126153)  [2.1 漏扫工具简介 7](#_Toc36126154)  [2.2 漏扫工具截图 7](#_Toc36126155)  [三. 测试目标说明 8](#_Toc36126156)  [3.1 测试对象 8](#_Toc36126157)  [3.2 时间 11](#_Toc36126158)  [3.3 参与测试人员 11](#_Toc36126159)  [3.4 测试环境 11](#_Toc36126160)  [四. 扫描过程 12](#_Toc36126161)  [4.1 漏洞介绍 12](#_Toc36126162)  [4.2 漏洞扫描结果简介 12](#_Toc36126163)  [4.3 漏洞分析 13](#_Toc36126164)  [4.3.1 高风险项 13](#_Toc36126165)  [4.3.2 中风险项 27](#_Toc36126166)  [4.3.3 低风险项 34](#_Toc36126167)  [五. 总结 40](#_Toc36126168)  [5.1 风险项统计 40](#_Toc36126169)  [5.2 风险扇形图 42](#_Toc36126170)  [六. 测试结论 43](#_Toc36126171)  [七. 感谢 44](#_Toc36126172) | |

1. 漏洞扫描介绍
   1. 漏洞扫描的概念

漏洞扫描技术是一类重要的网络安全技术。它和防火墙、入侵检测系统互相配合，能够有效提高网络的安全性。通过对网络的扫描，网络管理员能了解网络的安全设置和运行的应用服务，及时发现安全漏洞，客观评估网络风险等级。网络管理员能根据扫描的结果更正网络安全漏洞和系统中的错误设置，在黑客攻击前进行防范。如果说防火墙和网络监视系统是被动的防御手段，那么安全扫描就是一种主动的防范措施，能有效避免黑客攻击行为，做到防患于未然。

* 1. 漏洞扫描的必要性

漏洞扫描工作往往作为风险评估的一个重要环节，为风险评估提供重要的原始参考数据。

随着计算机技术、网络技术的飞速发展和普及应用，网络安全已日渐成为人们关注的焦点问题之一。近几年来，安全技术和安全产品已经有了长足的进步，部分技术与产品已日趋成熟。但是，单个安全技术或者安全产品的功能和性能都有其局限性，只能满足系统与网络特定的安全需求。因此，为了有效利用现有的安全技术和安全产品来保障系统与网络的安全，更加需要定期进行漏洞扫描。

配备漏洞扫描系统，网络管理人员可以定期的进行网络安全检测服务，安全检测可帮助客户最大可能的消除安全隐患，尽可能早地发现安全漏洞并进行修补，有效的利用已有系统，优化资源，提高网络的运行效率。

由于漏洞和安全隐患的形式多种多样，安装新软件和启动新服务都有可能使原来隐藏的漏洞暴露出来，因此进行这些操作之后应该重新扫描系统，才能使安全得到保障。

网络承担重要任务前应该多采取主动防止出现事故的安全措施，从技术上和管理上加强对网络安全和信息安全的重视，形成立体防护，由被动修补变成主动的防范，最终把出现事故的概率降到最低。配备网络漏洞扫描/网络评估系统可以让您很方便的进行安全性测试。

* 1. 漏洞扫描客户收益

对于客户而言，漏洞扫描可以带来以下收益：

* 明确安全隐患点

漏洞扫描是一个对网络系统中已知漏洞全面排查的过程，很多人工难以实现或者极其复杂的漏洞，都可以通过漏洞扫描来排查，让我门清除的了解漏洞的大致范围，以及网络系统的脆弱级别，以此明确整体系统中的安全隐患点。

* 提高安全意识

如上所述，任何的隐患在漏洞扫描服务中都可能造成“千里之堤溃于蚁穴”的效果，因此漏洞扫描服务可有效督促管理人员杜绝任何一处小的缺陷，从而降低整体风险。

* 提高安全技能

在测试人员与用户的交互过程中，可提升用户的技能。另外，通过专业的漏洞扫描报告，也能为用户提供当前流行安全问题的参考。

* 1. 漏洞扫描的依据

Potato漏洞扫描服务将参考下列国内、国际与漏洞扫描有关的标准结合Potato在漏洞扫描方面的规范和经验进行工作。

* 国内可参考的标准、指南或规范
* ISO/IEC 27001:2005信息技术-安全技术-信息系统规范与使用指南
* ISO/IEC 13335-1: 2004 信息技术-安全技术-信息技术安全管理指南
* ISO/IEC TR 15443-1: 2005 信息技术安全保障框架
* ISO/IEC PDTR 19791: 2004 信息技术 安全技术 运行系统安全评估
* GB/T 20984-2007信息安全技术 信息安全风险评估规范
* GB/T 19715.1-2005 信息技术-信息技术安全管理指南
* GB/T 19716-2005 信息技术-信息安全管理实用规则
* GB/T 18336-2001 信息技术-安全技术-信息技术安全性评估准则
* GB/T17859-1999 计算机信息系统安全保护等级划分准则
* GB/T 20984-2007信息安全技术 信息安全风险评估规范
* GB/T 20988-2007信息系统灾难恢复规范
* GB/Z 20986-2007信息安全事件分类分级指南
* Potato渗透测试最佳实践
* Potato安全服务工作规范、渗透测试实施规范
* ……
* 国际可参考的标准、指南或规范
* 信息系统审计标准（ISACA）G3 利用计算机辅助审计技术
* 信息系统审计标准（ISACA）G7 应有的职业谨慎
* 信息系统审计标准（ISACA）G9 不正当行为的审计考虑
* 信息系统审计标准（ISACA）G18 信息系统管理
* 信息系统审计标准（ISACA）G19 不正当及非法行为
* 信息系统审计标准（ISACA）G33 对网络使用的总体考虑
* CESG (CHECK) IT Health Check方法
* OWASP OWASP\_Testing\_Guide\_v3
* OWASP OWASP\_Development\_Guide\_2005
* OWASP OWASP\_Top\_10\_2010\_Chinese\_V1.0
* OSSTMM OSSTMM\_Web\_App\_Alpha
* Web应用安全委员会（WASC）WASC Threat Classification v2
* ……
  1. 漏洞扫描的原则

Potato在提供漏洞扫描服务中，将遵循下列原则。

* 保密性原则

保密性原则是漏洞扫描服务中最重要的原则，它是鼓励客户实施漏洞扫描服务的心理基础，同时也是对客户隐私权的最大尊重。漏洞扫描的保密范围，包括实施过程的保密性和输出成果的保密性。对服务过程中获知的任何客户系统信息均属秘密信息，不得泄露给第三方单位或个人，不得利用这些信息进行任何侵害客户的行为；对服务的报告提交不得扩散给未经授权的第三方单位或个人。

* 标准性原则

Potato漏洞扫描服务将在国家法律、法规允许的范围内进行，特别是遵照并履行《中华人民共和国人民警察法》第六条第十二款、《全国人大常委会关于维护互联网安全的决定》、《刑法》第二百八十五条、第二百八十六条等相关规定等。

遵守国内、国际与漏洞扫描有关的标准进行工作。同时在道德方面，也会严格遵守业界普遍认同的《计算机道德10个戒律》、《信息安全职业道德规范》、以及《网络道德的基本原则》。

* 规范性原则

Potato漏洞扫描服务将按照Potato安全服务工作规范、Potato漏洞扫描实施规范进行严格落实。实施必须由专业的安全服务人员依照规范的操作流程进行，对操作过程和结果要有相应的记录，提供完整的服务报告。

* 可控性原则

可控性原则就是漏洞扫描服务中对被测试系统造成的可能的各种影响要能够控制得住，既要全面测试，又不能影响生产，服务的工具、方法和过程要在双方认可的范围之内，服务的过程中，避免出现被测试系统运行不稳定，影响生产运行的情况。

* 整体性原则

整体性原则是系统思维方法的一条基本原则。整体原则认为，世界上任何一个有机整体系统，不但内部各组成要素之间是相互联系的，而且系统与外部环境之间也是有机联系的。我们在处理与解决问题时，应当从整体出发，从分析整体内部各组成部分的关系以及整体与外部环境之间的关系入手，去揭示与掌握其整体性质。在原则指导下的漏洞扫描服务，强调以综合为基础，在综合的控制与指导下，分析发现的安全问题，对分析结果进行恰当的综合。

* 最小影响原则

漏洞扫描服务工作应尽可能小的影响被测试系统和网络的正常运行，不能对现有系统、网络的运行和业务的正常运行产生显著影响。

* 1. 漏洞扫描的范围

从整体看，一个系统主要有四个主要部分组成，包括：Web应用程序、数据库、中间件和操作系统，五个次要部分，包括：安全设备、同网段服务器环境、机房物理环境、人员管理、管理制度。Potato漏洞扫描服务的范围主要包括了WEB应用程序、数据库、中间件、操作系统。

**WEB程序包括：**ASP、PHP、JSP、.NET、Perl、Python、Shell等语言编写的WEB程序。

**数据库：**Oracle、MySQL、MSSQL、Sybase、DB2、Informix等主流数据库。

**中间件：**Apache、IIS、Tomcat、Weblogic等主流WEB服务器，FTP、DNS等主流应用服务器。

**操作系统包括：**Windows、发行版Linux、AIX、Solaris、FreeBSD等主流系统。

* 1. 漏洞扫描的流程

Potato漏洞扫描服务主要分为四个阶段，包括测试前期准备阶段、测试阶段实施、复测阶段实施以及成果汇报阶段。

1. **前期准备阶段**

在实施漏洞扫描工作前，技术人员会和客户对漏洞扫描服务相关的技术细节进行详细沟通。由此确认漏洞扫描的方案，方案内容主要包括确认的漏洞扫描范围、最终对象、测试方式、测试要求的时间等内容。同时，客户签署漏洞扫描授权书。

1. **测试阶段实施**

在测试实施过程中，Potato测试人员在晚上或者非业务繁忙截断，使用自动化的漏洞扫描工具，完成资产识别和漏洞扫描等工作。然后由人工的方式对安全扫描的结果进行人工的确认和分析。结合自动化测试和人工测试两方的结果，测试人员需整理漏洞扫描服务的输出结果并编制漏洞扫描报告，最终提交客户和对报告内容进行沟通。

1. **成果汇报阶段**

根据一次自动化的漏洞扫描测试和人工确认分析，在于客户进一步沟通完成之后，整理漏洞扫描服务输出成果，最后汇报项目领导。

* 1. 漏洞扫描风险控制

为保障客户系统在漏洞扫描过程中稳定、安全的运转，我们将提供以下多种方式来进行风险规避。

* 时间控制

从时间安排上，测试人员将将尽量避免在数据高峰时进行测试，以此来减小测试工作对被测试系统带来的压力。另外，测试人员在每次测试前也将通过电话、邮件等方式告知相关人员，以防止测试过程中出现意外情况。

* 工具使用

在使用工具测试的过程中，测试人员会通过设置线程、插件数量等参数来减少其对系统的压力，同时还会去除任何可能对目标系统带来危害的插件，如：远程溢出攻击类插件、拒绝服务攻击类插件等等。

* 技术手段

Potato的漏洞扫描人员都具有丰富的经验和技能，在每一步测试前都会预估可能带来的后果，对于可能产生影响的测试（如：溢出攻击）将被记录并跳过，并在随后与客户协商决定是否进行测试及测试方法。

* 监控措施

针对每一系统进行测试前，测试人员都会告知被测试系统管理员，并且在测试过程中会随时关注目标系统的负荷等信息，一旦出现任何异常，将会停止测试。

* 对象选择

为更大程度的避免风险的产生，漏洞扫描还经常选择对备份系统进行测试。因为备份系统与在线系统所安装的应用和承载的数据差异较小，而其稳定性要求又比在线系统低，因此，选择对备份系统进行测试也是规避风险的一种常见方式。

* 操作记录

测试人员会在测试过程中形成操作记录文档，以便出现意外后进行追溯。

* 沟通配合

测试过程中，确定测试人员和客户方配合人员的联系方式，便于及时沟通并解决工程中的难点。

1. 漏洞扫描工具介绍
   1. 漏扫工具简介

DX漏洞扫描系统严格按照计算机信息系统安全的国家标准、相关行业标准设计、编写、制造。

* 1. 漏扫工具截图

DX漏洞扫描系统可以对单个目标或者多个目标同时进行扫描，同时可以选择web扫描或者是主机扫描，支持自动生成报告和报告的导出。如图2.2.1：

图2.2.1

1. 测试目标说明
   1. 测试对象

|  |  |  |  |
| --- | --- | --- | --- |
| 单位名称 | 涉及系统 | 系统IP | 资产数目 |
| XXX集团 | 192.168.100.3 | TRUENAS,TRUENAS | 1 |
| 统计 | | |  |

* 1. 时间

|  |  |  |  |
| --- | --- | --- | --- |
| **测试工作的时间段** | | | |
| **起始时间** | 2023-03-27 15:16:17 | **结束时间** | 2023-03-27 15:16:17 |

本份测试报告分析的各种安全风险，仅限定于在上述时间段内测试反馈信息的整理，不包括非上述时间段内的因系统调整、维护更新后出现的其他变化情况。

* 1. 参与测试人员

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **参测人员名单** | | | | | |
| **姓名** |  | **所属部门** | Potato漏扫小组 | **联系方式** |  |
| **姓名** |  | **所属部门** | Potato漏扫小组 | **联系方式** |  |

测试人员名单

* 1. 测试环境

本次漏洞扫描过程中，Potato测试小组使用以下IP地址开展的分析工作，在此通知XXX集团相关人员在对受测试的目标站点服务器、相应的网络入侵检测系统进行安全监控和日志分析时，排除以下IP地址产生的任何违规信息，以保证分析结果的准确有效。

|  |  |  |  |
| --- | --- | --- | --- |
| **IP地址** | **IP地址** | **IP地址** | **IP地址** |
| —— | —— | —— | —— |

1. 扫描过程
   1. 漏洞介绍

所谓漏洞就是指程序设计方面在安全性上存在缺失，留下了隐患，而网络黑客可以从这些漏洞对远程计算机进行攻击，窃取数据，破坏远程用户电脑等等，危害很大。尤其是机密被窃，损失不可估计，就是个人用户也非常危险，个人账号密码被入侵后可能会被窃取。

* 1. 漏洞扫描结果简介

系统安全漏洞是在系统具体实现和具体使用中产生的错误，但并不是系统中存在的错误都是安全漏洞。只有能威胁到系统安全的错误才是漏洞。许多错误在通常情况下并不会对系统安全造成危害，只有被人在某些条件下故意使用时才会影响系统安全。

　　漏洞虽然可能最初就存在于系统当中，但一个漏洞并不是自己出现的，必须要有人发现。在实际使用中，用户会发现系统中存在错误，而入侵者会有意利用其中的某些错误并使其成为威胁系统安全的工具，这时人们会认识到这个错误是一个系统安全漏洞。系统供应商会尽快发布针对这个漏洞的补丁程序，纠正这个错误。这就是系统安全漏洞从被发现到被纠正的一般过程。

　　系统攻击者往往是安全漏洞的发现者和使用者，要对于一个系统进行攻击，如果不能发现和使用系统中存在的安全漏洞是不可能成功的。对于安全级别较高的系统尤其如此。

系统安全漏洞与系统攻击活动之间有紧密的关系。因而不该脱离系统攻击活动来谈论安全漏洞问题。了解常见的系统攻击方法，对于有针对性的理解系统漏洞问题，以及找到相应的补救方法是十分必要的。

**通过漏洞扫描软件扫描出的漏洞如下**：

**红色上箭头**代表高级风险安全漏洞

**橙色横线**代表中级风险安全漏洞

**蓝色下箭头**代表低级风险安全漏洞

|  |  |  |
| --- | --- | --- |
| 风险名称 | 风险标签 | 风险数量 |
| ShopXO\_download\_Arbitrary\_file\_read\_CNVD\_2021\_15822.json | ShopXO\_download\_Arbitrary\_file\_read\_CNVD\_2021\_15822.json | 2 |
| ╓┬╘╢OA A6 ╩²╛▌┐Γ├⌠╕╨╨┼╧ó╨╣┬╢.json | ╓┬╘╢OA A6 ╩²╛▌┐Γ├⌠╕╨╨┼╧ó╨╣┬╢.json | 2 |
| BSPHP\_index.php\_unauthorized\_access\_information.json | BSPHP\_index.php\_unauthorized\_access\_information.json | 1 |

* 1. 漏洞分析

在本章节，对于高风险项将进行主要分析，一一列出高风险项的漏洞详情以及修复方案，和相关漏洞所涉及的系统；对于中低风险项进行简要分析，列出漏洞详情及修复方案。

经过统计后高中低风险项主要分布如下。

* + 1. 高风险项
       1. ShopXO\_download\_Arbitrary\_file\_read\_CNVD\_2021\_15822.json

|  |  |
| --- | --- |
| 风险名称 | ShopXO\_download\_Arbitrary\_file\_read\_CNVD\_2021\_15822.json |
| 风险级别 | **高** |
| 风险描述 | https://192.168.100.3/public/index.php?s=/index/qrcode/download/url/L2V0Yy9wYXNzd2Q= |
| 请求数据 | - |
| 响应数据 | - |
| 修复建议 |  |
| 复测结果 |  |

* + - 1. ShopXO\_download\_Arbitrary\_file\_read\_CNVD\_2021\_15822.json

|  |  |
| --- | --- |
| 风险名称 | ShopXO\_download\_Arbitrary\_file\_read\_CNVD\_2021\_15822.json |
| 风险级别 | **高** |
| 风险描述 | http://192.168.100.3/public/index.php?s=/index/qrcode/download/url/L2V0Yy9wYXNzd2Q= |
| 请求数据 | - |
| 响应数据 | - |
| 修复建议 |  |
| 复测结果 |  |

* + 1. 中风险项
    2. 低风险项
       1. ╓┬╘╢OA A6 ╩²╛▌┐Γ├⌠╕╨╨┼╧ó╨╣┬╢.json

|  |  |
| --- | --- |
| 风险名称 | ╓┬╘╢OA A6 ╩²╛▌┐Γ├⌠╕╨╨┼╧ó╨╣┬╢.json |
| 风险级别 | **低** |
| 风险描述 | https://192.168.100.3/yyoa/createMysql.jsp |
| 请求数据 | - |
| 响应数据 | - |
| 修复建议 |  |
| 复测结果 |  |

* + - 1. ╓┬╘╢OA A6 ╩²╛▌┐Γ├⌠╕╨╨┼╧ó╨╣┬╢.json

|  |  |
| --- | --- |
| 风险名称 | ╓┬╘╢OA A6 ╩²╛▌┐Γ├⌠╕╨╨┼╧ó╨╣┬╢.json |
| 风险级别 | **低** |
| 风险描述 | http://192.168.100.3/yyoa/createMysql.jsp |
| 请求数据 | - |
| 响应数据 | - |
| 修复建议 |  |
| 复测结果 |  |

* + - 1. BSPHP\_index.php\_unauthorized\_access\_information.json

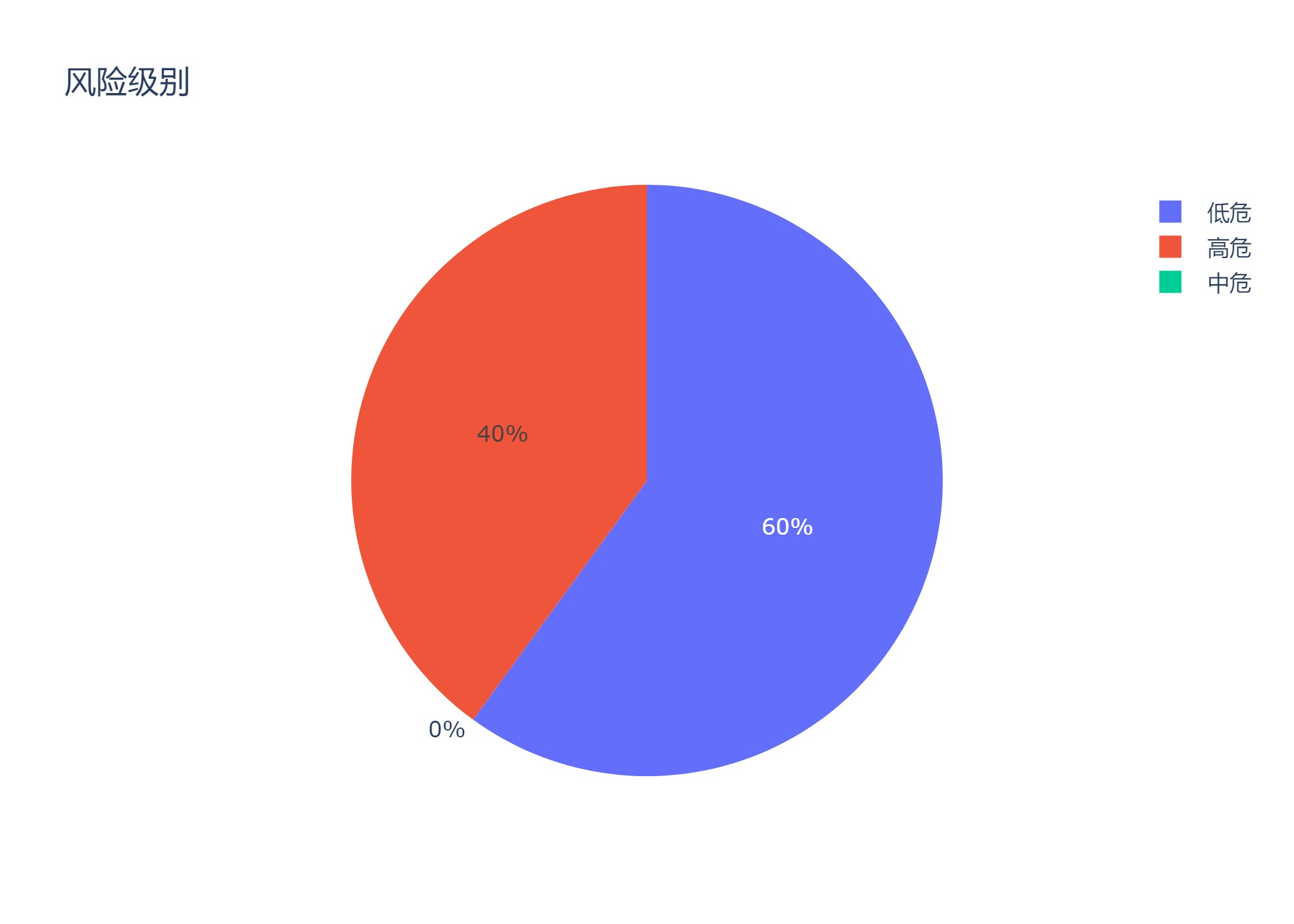
|  |  |
| --- | --- |
| 风险名称 | BSPHP\_index.php\_unauthorized\_access\_information.json |
| 风险级别 | **低** |
| 风险描述 | https://192.168.100.1/admin/index.php?m=admin&c=log&a=table\_json&json=get&soso\_ok=1&t=user\_login\_log&page=1&limit=10&bsphptime=1600407394176&soso\_id=1&soso=&DESC=0' |
| 请求数据 | - |
| 响应数据 | - |
| 修复建议 |  |
| 复测结果 |  |

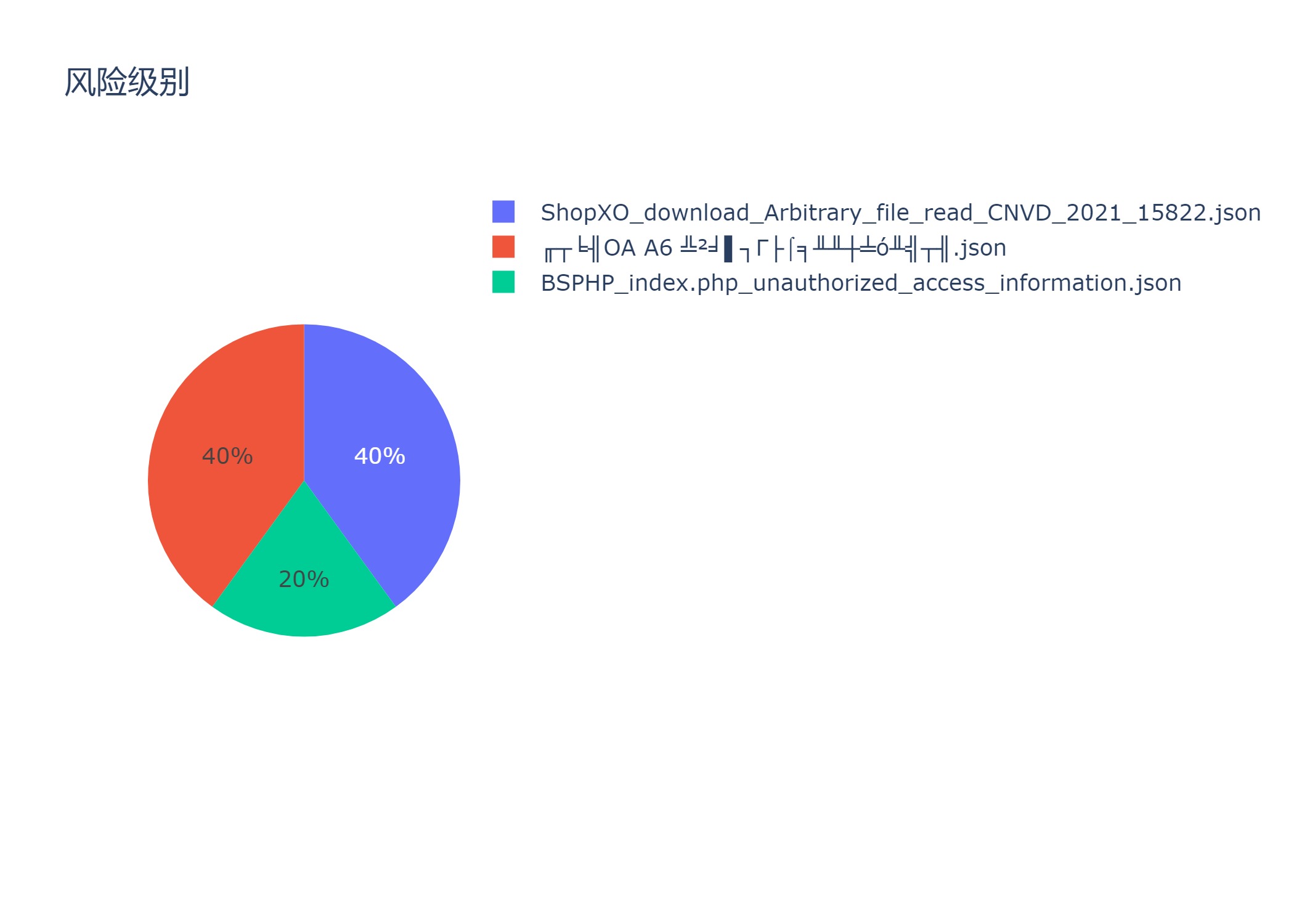
1. 总结
   1. 风险项统计

通过对1个目标进行漏洞扫描，共发现所有级别风险5个，其中高风险项2个，中风险项0个，低风险项3个，

|  |  |  |  |
| --- | --- | --- | --- |
| 单位名称 | 系统名称 | 风险级别 | 漏洞个数 |
| XXX集团 | 192.168.100.3 | 高 | 20 |
| 中 | 0 |
| 低 | 30 |

* 1. 风险扇形图





1. 测试结论

经过本次对目标的漏扫测试，我们对此次漏扫目标的整体安全评价是 **远程不安全系统。**

|  |  |
| --- | --- |
| **安全等级** | **资源内容描述** |
| 远程不安全系统  **（**符合任何一个条件**）** | 1、存在一个或一个以上严重的安全问题，可直接导致系统受到破坏；  2、与其他非安全系统连接，同时存在相互信任关系（或账号互通）的主机；   1. 发现已经被人入侵且留下远程后门的主机； 2. 存在3个以上中等安全问题的主机；   5、与其他非安全系统在一个共享网络中，同时远程维护明文传输口令；  6、完全不能抵抗小规模的拒绝服务攻击 |
| 远程一般安全系统  **（**符合任何一个条件**）** | 1. 存在一个或一个以上中等安全问题的主机； 2. 开放过多服务，同时可能被利用来进行拒绝服务的主机；   3、与其他非安全系统直接连接，但暂时不存在直接信任(或账号互通)关系；  4、远程维护通过明文的方式传递信息；  5、存在三个以上轻度安全问题的主机；  6、只能抵御最低级的拒绝服务攻击； |
| 远程安全系统  **（**符合全部条件**）** | 1. 最多存在1-2个轻度安全问题； 2. 远程维护方式安全； 3. 与不安全或一般安全系统相对独立；   4、能抵挡一定规模的拒绝服务攻击。 |

安全等级评定

1. 感谢

在本次远程漏洞扫描过程中，Potato感谢相关人员和在漏洞扫描过程中进行沟通、协调的相关部门和人员的大力配合，以使得我们的工作能够顺利完成。对于您的大力支持我们深表感谢。