|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | |  |  |  |  |  | |  |  |  |  |  | |  | **渗透测试报告** |  |  | |  |  |  |  | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|  | |  | | | | | | | |  |  |  |  |  |  |  | | | |  |  |  |  | | | |  | |  |  |  |  | | | |  | | | |
|  | | **第1章 概述** | | | | | | | | | | | | | |  | | | |  |  |  |  | | | |  | |  |  |  |  | | | |  | | | |
|  | |  | | | | | | | |  |  |  |  |  |  |  | | | |  |  |  |  | | | |  | |  |  |  |  | | | |  | | | |
|  | |  | | | | | | | |  |  | **1.1测试目的** | | | | | | | |  |  |  |  | | | |  | |  |  |  |  | | | |  | | | |
|  | |  | | | | | | | |  |  |  | **采用黑盒的方式，模拟黑客的入侵行为，对指定的网站应用系统进行安全漏洞扫描和利用测试。评估是否存在可以被攻击者真实利用的漏洞以及由此引起的风险大小，为制定相应的安全措施与解决方案提供实际的依据。** | | | | | | | | | | | | | | | | | | | | | | |  | | | |
|  | |  | | | | | | | |  |  |  |  |  |  |  | | | |  |  |  |  | | | |  | |  |  |  |  | | | |  | | | |
|  | |  | | | | | | | |  |  | **1.2测试范围** | | | | | | | |  |  |  |  | | | |  | |  |  |  |  | | | |  | | | |
|  | |  | | | | | | | |  |  |  |  |  |  |  | | | |  |  |  |  | | | |  | |  |  |  |  | | | |  | | | |
|  | |  | | | | | | | |  |  |  |  |  |  |  | | | |  |  |  |  | | | |  | |  |  |  |  | | | |  | | | |
|  | |  | | | | | | | |  |  |  |  |  |  | | | |  |  |  | | | |  | |  |  |  | | | |  | | | |
|  | |  | | | | | | | |  |  |  |  | **应用系统名称** | | | | |  |  |  | | | |  | |  |  |  | | | |  | | | |
|  | |  | | | | | | | |  |  |  |  |  |  |  | | | | **应用系统IP/URL** | |  |  |  | | | |  | | | |
|  | |  | | | | | | | |  |  |  |  |  |  |  | | | |  | |  |  |  | | | |  | | | |
|  | |  | | | | | | | |  |  |  |  |  |  | | | |  |  |  | | | |  | |  |  |  | | | |  | | | |
|  | |  | | | | | | | |  |  |  |  |  |  | | | |  |  |  | | | |  | |  |  |  | | | |  | | | |
|  | |  | | | | | | | |  |  |  |  |  |  | | | |  |  | **www.gomeb2b.gome.com.** | | | | | | |  |  | | | |  | | | |
|  | |  | | | | | | | | **ECP应用系统（外网）** | | | | | | | | | |  |  |  | | | |  | | | |
|  | |  | | | | | | | |  |  | | | |  | |  |  |  | | | |  | | | |
|  | |  | | | | | | | |  |  |  |  |  |  | | | |  |  |  | | | |  | |  |  |  | | | |  | | | |
|  | |  | | | | | | | |  | | | | | | | | | | | | | | | | | | | | |  |  | | | |  | | | |
|  | |  | | | | | | | |  |  |  |  |  |  |  | | | |  |  |  |  | | | |  | |  |  |  |  | | | |  | | | |
|  | |  | | | | | | | |  |  | **1.3参考标准** | | | | | | | |  |  |  |  | | | |  | |  |  |  |  | | | |  | | | |
|  | |  | | | | | | | |  |  |  |  |  |  |  | | | |  |  |  |  | | | |  | |  |  |  |  | | | |  | | | |
|  | |  | | | | | | | |  |  |  |  | **《OWASP Testing Guide》** | | | | | | | | | | | | | | | | | |  | | | |  | | | |
|  |  | |  | | |  | | |  | |  |  | | | | | | | | | | | |  | |  |  | | | | | |  |  |  | | |  | |
|  |  | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |  | |
|  |  | |  | | |  | | |  | |  |  | | | | | | | | | | | |  | |  |  | | | | | |  |  |  | | |  | |
|  |  | | **第2章 测试综述** | | | | | | | | | | | | | | | | | | | | | | | |  | | | | | |  |  |  | | |  | |
|  |  | |  | | |  | | |  | |  | **2.1安全漏洞分布情况** | | | | | | | | | | | | | |  |  | | | | | |  |  |  | | |  | |
|  |  | |  | | |  | | |  | |  |  | | | | | | | | | | | |  | |  |  | | | | | |  |  |  | | |  | |
|  |  | |  | | | **本次应用系统渗透测试对1个应用系统进行了测试，发现的安全漏洞共计22个，其中高风险的有22个，中风险的有0个，低风险的有0个。  通过统计分析，目前安全漏洞详细分布情况如下图所示：** | | | | | | | | | | | | | | | | | | | | | | | | | | | | |  | | |  | |
|  |  | |  | | |  | | | | | | | | | | | | | | | | | | | | | | | | | | | |  |  | | |  | |
|  |  | |  | | |  | | |  | |  |  | | | | | | | | | | | |  | |  |  | | | | | |  |  |  | | |  | |
|  |  | |  | | |  | | | **2.2安全漏洞风险描述** | | | | | | | | | | | | | | |  | |  |  | | | | | |  |  |  | | |  | |
|  |  | |  | | |  | | |  | |  |  | | | | | | | | | | | |  | |  |  | | | | | |  |  |  | | |  | |
|  |  | |  | | |  | | |  | |  | | | | | | | | | | | | | | | | | | | | | |  |  |  | | |  | |
|  | | | |  |  |  |  |  | | |  | | | | | |  |  |  | | | | | |  | | |  | | | | | | | | |  |  | |
|  | | | | **第3章 测试结果** | | | | | | | | | | | | | | | | | | | | | | | |  | | | | | | | | |  |  | |
|  | | | |  |  |  |  |  | | | **3.1. 跨站脚本攻击** | | | | | | | | | | | | | |  | | |  | | | | | | | | |  |  | |
|  | | | |  |  |  |  |  | | |  | | | | | |  |  |  | | | | | |  | | |  | | | | | | | | |  |  | |
|  | | | |  | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |  | |
|  | | | |  |  |  |  |  | | |  | | | | | |  |  |  | | | | | |  | | |  | | | | | | | | |  |  | |
|  | | | |  | **风险分析** | | | | | | | | | | | |  |  |  | | | | | |  | | |  | | | | | | | | |  |  | |
|  | | | |  |  |  |  |  | | |  | | | | | |  |  |  | | | | | |  | | |  | | | | | | | | |  |  | |
|  | | | |  |  | **攻击者可以通过构造URL注入JavaScript、VBScript、ActiveX、HTML或者Flash的手段，利用跨站脚本漏洞欺骗用户，收集Cookie等相关数据并冒充其他用户。通过精心构造的恶意代码，可以让访问者访问非法网站或下载恶意木马，如果再结合其他攻击手段（如社会工程学、提权等），甚至可以获取系统的管理权限。** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |  |  | |
|  | | | |  |  |  |  |  | | |  | | | | | |  |  |  | | | | | |  | | |  | | | | | | | | |  |  | |
|  | | | |  |  |  |  | **高** | | | | | | | | | | |  | | | | | |  | | |  | | | | | | | | |  |  | |
|  | | | |  |  |  |  |  | | |  | | | | | |  |  |  | | | | | |  | | |  | | | | | | | | |  |  | |
|  | | | |  |  |  | **影响URL** | | | | | | | | | | |  |  | | | | | |  | | |  | | | | | | | | |  |  | |
|  | | | |  | |  | | | | | | | | | | |  | | | | | | | | | | | | | | | | | | |  | | |  |
|  | | | | 1.https://gomeb2b.gome.com.cn/trade/index.jsp?\_suppliercode=0010090000（参数\_suppliercode） 2.https://gomeb2b.gome.com.cn/bo/authority/user!clickGet.action POST提交数据包： loginName=admin&captcha\_2=（参数loginName） 3.https://gomeb2b.gome.com.cn/aps/question/sell-question-post!supplierQuestionSelect.action POST提交数据包： type=1&questTitle=&questTypeId=&dateStart=2016-12-01&dateEnd=2016-12-01&questStatus=&page.pageNo=1&page.totalPages=1&page.pageSize=20&page.jumpNumber=1（参数dateStart、dateEnd） 4.https://gomeb2b.gome.com.cn/aps/portal/portal-setting!saveOrUpdateCustomLayout.action POST提交数据包： layout={'column1':[{id:'bulletin',url:'/aps/board/queryOtherBoardList.action',title:'公告通知 <svg/onload=alert(document.domain)>',height:'175',embedType:'1'},{id:'factoring',url:'/aps/portlet/portlet!factoring.action',title:'供应链融资 ',height:'130',embedType:'1'},{id:'picture',url:'/aps/flow.jsp',title:'流程 ',height:'150',embedType:'1'},{id:'olcenter',url:'/aps/statistics/portal-statistics!vendorQuestStatistics.action',title:'在线咨询 ',height:'200',embedType:'1'},{id:'knowledgecollection',url:'/aps/knowledgecollection/queryKnowledgeCollectionByUserId.action',title:'我的收藏 ',height:'200',embedType:'1'},{id:'org',url:'/aps/statistics/portal-statistics!orgStatistics.action',title:'企业资料完整性 ',height:'180',embedType:'1'}],'column2':[{id:'stationmsg',url:'/aps/stationMsg/station-msg!list.action',title:'站内消息 ',height:'180',embedType:'1'},{id:'order',url:'/aps/portlet/portlet!order.action',title:'订单 ',height:'155',embedType:'1'},{id:'logistics',url:'/aps/portlet/portlet!logistics.action',title:'物流 ',height:'155',embedType:'1'},{id:'balance',url:'/aps/portlet/portlet!balance.action',title:'结算 ',height:'115',embedType:'1'},{id:'kpi',url:'/aps/portlet/portlet!kpi.action',title:'KPI指标 ',height:'135',embedType:'1'},{id:'knowledge',url:'/aps/knowledgeportal/queryKnowledgePortal.action',title:'培训学院 ',height:'220',embedType:'1'}]}&layoutMode=2\_right（参数title） | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |  |
|  | | | |  | |  | | | | | | | | | | |  | | | | | | | | | | | | | | | | | | |  | | |  |
|  | | | |  | | **解决方法** | | | | | | | | | | |  | | | | | | | | | | | | | | | | | | |  | | |  |
|  | | | |  | |  | | | | | | | | | | |  | | | | | | | | | | | | | | | | | | |  | | |  |
|  | | | |  | | **对用户输入的数据进行全面安全检查或过滤，尤其注意检查是否包含HTML特殊字符。这些检查或过滤必须在服务器端完成。** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |  | | |  |