传美服务
Inherit Beauty Service

2020 山西药科职业学院 网站监测报告

监测报告

山西传美科技股份有限公司

1. 概要信息

1.1 扫描概要

本报告由传美科技 saas 云监测平台制作，采用 web 安全检查后得出的扫描报告，属于机密资料，请进行妥善管理。

本报告共扫描 1 个网站，发现 web 安全漏洞 5 个，其中 0 个紧急，0 个高危，0 个中危，5 个低危。

1.2 扫描对象

网站名称	山西药科职业学院
网站 URL	http://sso.sxphc.cn/
域名	sso.sxphc.cn
域名注册有效期	2012-08-28 - 2022-08-28
主办单位名称	山西药科职业学院
主办单位性质	事业单位
ICP 备案号	晋 ICP 备 05007286 号-1

1.3 网站风险分布

您的网站较安全，暂未发现安全问题，请持续关注！

安 全

各漏洞风险等级个数

紧急	高危	中危	低危
0	0	0	5

漏洞列表

漏洞等级	漏洞类型	涉及页面数
低危	开启 options 方法	1
低危	启用了不安全的 HTTP 方法	1
低危	X-Frame-Options Header 未配置	1
低危	基于 HTTP 连接的登录请求	1
低危	Web 应用程序错误	1

2. 网站漏洞详情

2.1. 开启 options 方法 【低危】

漏洞等级： 低危/无危害

漏洞 URL：

http://sso.sxphc.cn/

漏洞 POC：

method_unsafe:GET,HEAD,POST,PUT,DELETE,OPTIONS

漏洞取证：

无取证图片

2.2. 启用了不安全的 HTTP 方法 【低危】

漏洞等级： 低危/无危害

漏洞 URL：

http://sso.sxphc.cn/

漏洞 POC：

method_unsafe:PUT,DELETE

漏洞取证：

无取证图片

2.3. X-Frame-Options Header 未配置 【低危】

漏洞等级： 低危/无危害

漏洞 URL：

http://sso.sxphc.cn/

漏洞 POC：

http://sso.sxphc.cn/

漏洞取证：

无取证图片

无取证图片

2.4.Web 应用程序错误 【低危】

漏洞等级：低危/无危害

漏洞 URL：

http://sso.sxphc.cn/sso-server/login?null

漏洞 POC：

HTTP CODE : 500

漏洞取证：

无取证图片

3.漏洞修复建议

漏洞类型	漏洞描述	修复建议
HttpMethodOptionsEnabled	弱点描述：Web 服务器配置为允许使用危险的 HTTP 方法，如 PUT、MOVE、COPY、DELETE、PROPFIND、SEARCH、MKCOL、LOCK、UNLOCK、PROPPATCH，该配置可能允许未授权的用户对 Web 服务器进行敏感操作。	一般性的建议：[1]如果服务器不需要支持 WebDAV 请禁用 WebDAV，或禁用掉不安全的 HTTP 方法，IIS 在 IIS 服务中的"Web 服务扩展"中关闭 WebDav。
UnsafeHttpMethod	弱点描述：Web 服务器配置为允许使用危险的 HTTP 方法，如 PUT、MOVE、COPY、DELETE、PROPFIND、SEARCH、MKCOL、LOCK、UNLOCK、PROPPATCH，该配置可能允许未授权的用户对 Web 服务器进行敏感操作。	一般性的建议：如果服务器不需要支持 WebDAV 请禁用 WebDAV，或禁用掉不安全的 HTTP 方法，IIS 在 IIS 服务中的"Web 服务扩展"中关闭 WebDav。
XFrameOptions	弱点描述：X-Frame-Options HTTP 响应头可以指示浏览器是否允许当前网页在“frame”或	一般性的建议：给您的网站添加 X-Frame-Options 响应头，赋值有如下三种，1、DENY：无论如何不在框架中显示；2、SAMEORIGIN：仅在同源域名下的框架中显示；3、

	“iframe”标签中显示,以此使网站内容不被其他站点引用和免于点击劫持攻击。	ALLOW-FROM uri：仅在指定域名下的框架中显示。如 Apache 修改配置文件添加“Header always append X-Frame-Options SAMEORIGIN”；Nginx 修改配置文件“add_header X-Frame-Options SAMEORIGIN;”。
LoginWithHttp	弱点描述:在应用程序测试过程中,检测到基于不安全的 http 连接的登录请求。由于采用未加密的 http 请求发送敏感的登录请求,有可能被同一个局域网内的攻击者嗅探到用户输入的登录数据,如账号和密码。	一般性的建议:[1]采用 https 协议。
WebApplicationError	弱点描述：Web 应用程序在处理访问者的请求时，如果符合 Web 应用程序的逻辑或者 Web 应用程序本身没有异常,那么将结果直接反馈给访问者。如果提交不符合 Web 应用程序逻辑的数据，Web 应用程序在处理这些请求的时候未做相应的处理，直接把 Web 服务器的错误反馈给访问者。	一般性的建议：过滤客户端提交的危险字符，客户端提交方式包含 GET、POST、COOKIE、User-Agent、Referer、Accept-Language 等，其中危险字符如下：[1] |[2] &[3] ;[4] $[5] %[6] @[7] '[8] "[9] [10] ()[11] +[12] CR[13] LF[14] ,[15] .开发语言的建议:[1] 检查入局请求，以了解所有预期的参数和值是否存在。 当参数缺失时，发出适当的错误消息，或使用缺省值。[2] 应用程序应验证其输入是否由有效字符组成（解码后）。 例如，应拒绝包含空字节（编码为 %00）、单引号、引号等的输入值。[3] 确保值符合预期范围和类型。 如果应用程序预期特定参数具有特定集合中的值，那么该应用程序应确保其接收的值确实属于该集合。 例如，如果应用程序预期值在 10..99 范围内，那么就该确保该值确实是数字，且在 10..99 范围内。[4] 验证数据属于提供给客户端的集合。[5] 请勿在生产环境中输出调试错误消息和异常。

智慧教育整体解决方案服务商

数字化校园●超算平台●私有云平台●信息安全●教学实训●运维服务

地址：太原市高新区创业街5号航天科研综合楼7层
电话：0351-5685774
网址：http：//www.cloud-3.cn

山西药科职业学院
安全风险隐患排查报告

山西护网信息科技有限公司

2020 年 6 月 23 日

目 录

为贯彻落实《教育部办公厅关于开展网络安全检查的通知》，全面加强山西药科职业学院网络与信息安全工作，我公司于 6 月 23 日-24 日对该校网络、信息系统和门户网站的安全问题组织了自查，现将自查情况总结如下：

一、概述

本次检查主要包含网络与信息系统安全的组织管理、日常维护、技术防护、应急管理 4 个方面，共涉及信息系统主要有教务系统、学工系统、资产管理系统及门户网站等系统。

从检查情况看，该校网络与信息安全总体情况良好。该校一贯重视信息安全工作，始终把信息安全作为信息化工作的重点内容。网络信息安全工作机构健全、责任明确，日常管理维护工作比较规范，技术防护措施得当，信息安全风险得到有效降低；此外，该校比较重视网络安全，拥有应急处置技术队伍，基本保证了校园网信息系统持续安全稳定运行。但在网络安全管理、技术防护设施、信息系统等级保护工作等方面，还需要进一步加强和完善。

二、网络信息安全现状分析

1．网络信息安全组织管理

按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，学院设有网络与信息安全工作领导组，主要领导担任组长，下设领导

组办公室。领导组全面负责该校网络信息安全工作。电教中心作为信息化运维部门，承担信息系统安全技术防护与技术保障工作。

信息系统日常安全管理

学院建有《山西药科职业学院校园网安全管理办法》、“山西药科职业学院网络和信息安全突发事件应急处置办法”、“山西药科职业学院教育移动应用管理办法（试行）”等规章制度。学院网站内容有严格的审核制度，制定了《山西药科职业学院校园网络新闻管理办法》、《山西药科职业学院网络舆情管理与处置实施办法》等，系统使用部门基本能按要求，责任落实人，较好地履行网站信息上传、审批制度、门户网站数据保密与防篡改等规定。日常维护操作比较规范，能够根据要求定期修改登录密码，杜绝弱口令问题。能够定期备份数据，定期查看安全日志等，随时掌握系统状态，保证正常运行。

2．信息系统技术防护

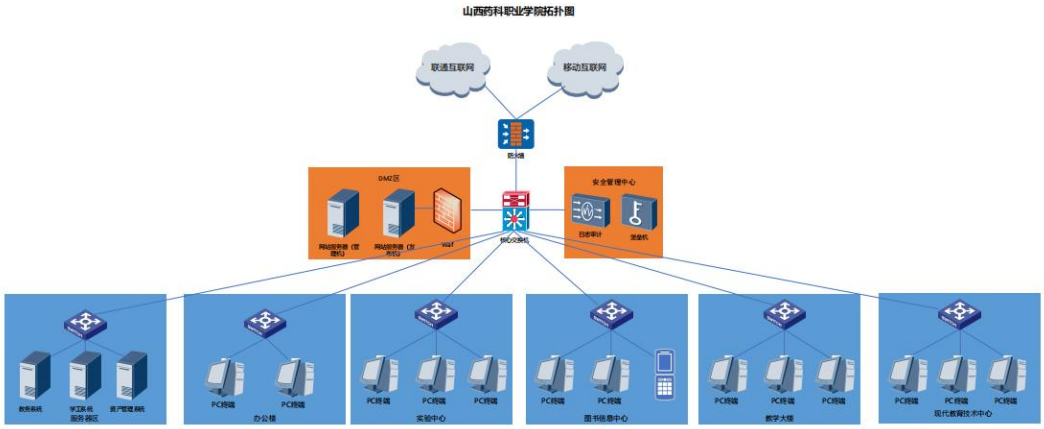
校园网机房建有一定规模的综合安全防护措施：

一是网络出口部署有防火墙，且在 DMZ 区部署 web 应用防火墙对网站系统进行保护，定期检测并更新规则库。

二是对服务器、网络设备、安全设备等定期进行安全漏洞检查，及时更新操作系统和补丁，配置口令策略保证更新频度。

三是全面实行实名认证制度，具备上网行为回溯追踪能力。

四是对重要系统和数据设置备份计划，进行定期备份，并配有独立的备份服务器。



山西药科职业学院校园网拓扑图

三、网络信息安全自查情况

1．网络安全防护措施情况

学院安排专人负责不定时对网站进行检查，未发现网站出现过有害信息、不良信息及其他违反国家法律法规的信息。

2．网络边界防护情况

学院互联网出口接入联通、移动线路，信息技术产品达到网络安全产品国产化。

在互联网出口处部署网康科技防火墙，配置相应的策略，关闭了不必要的服务和端口。

在核心交换机处旁路部署盛邦安全运维管理系统和盛邦安全日志审计系统，通过运维管理系统实现对机房网络/安全设备及服务器的安全运维，通过登录日志审计系统，了解网络/安全设备的运行情

况，发现异常情况能够对其进行分析并及时解决问题,且日志保存 6 个月以上。

此外，在 DMZ 区部署了网康 web 应用防火墙，实现对 HTTP 的请求进行异常检测，拒绝不符合 HTTP 标准的请求。并且，它也可以只允许 HTTP 协议的部分选项通过，从而减少攻击的影响范围。

3．服务器安全防护措施

系统管理员及时对服务器操作系统的安全补丁进行更新，防止因漏洞导致服务器出现任何故障。服务器操作系统不存在弱口令，且不存在管理员共用管理口令。

四、检查发现的主要问题

通过对山西药科职业学院网络、信息系统和门户网站的安全检查，发现该校在信息安全工作上还存在一定的问题：

● 安全管理方面：该校部分信息工作人员保密意识有所欠缺，未能深入理解网络信息安全的重要性。

● 技术防护方面：该校网络安全技术防护设施不足，缺少数据中心安全防御系统和数据审计系统，欠缺安全检测设备，无法对服务器、信息系统进行隐患检查。

● 信息系统等级保护测评工作尚未全面开展。

● 漏洞方面：我公司对该校教务系统、学工系统、资产管理系统及门户网站进行漏洞扫描，其中，教务系统中危漏洞 1 个；学工系统

低危漏洞 3 个，信息漏洞 2 个；资产管理系统低危漏洞 4 个；门户网站低危漏洞 1 个，暂未发现高危漏洞。门户网站具体漏洞扫描结果详见附件。

五、整改建议

针对存在的问题，我公司建议该校对目前发现的问题进行如下整改：

● 进一步加强信息技术人员技术培训，提高安全意识和技术能力。

● 继续完善网络信息安全技术防护措施，配备必要的安全防御和检测设备，实行信息系统安全检测准入制度，从根本上降低安全风险。

● 全面开展信息系统等级保护工作，按照新颁布的《教育行政部门及高等院校信息系统安全等级保护定级指南》，完成所有在线系统的定级、备案工作。积极创造条件开展后续定级测评、整改等工作。

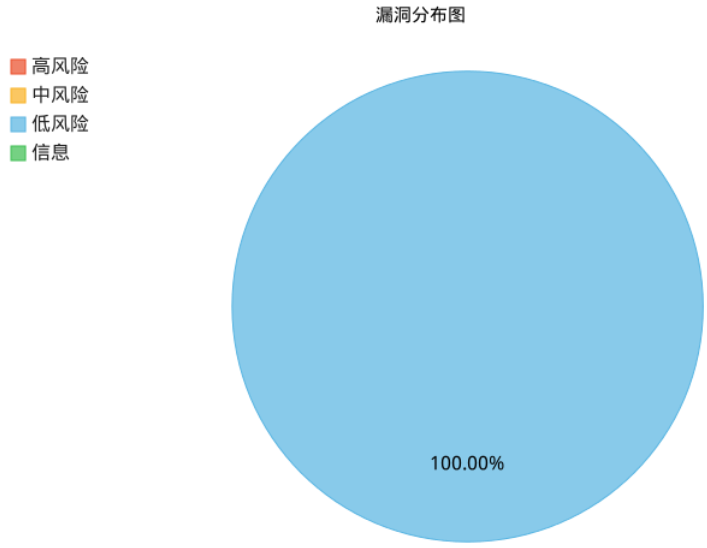
附件：漏洞扫描报告

漏洞扫描安全评估报告

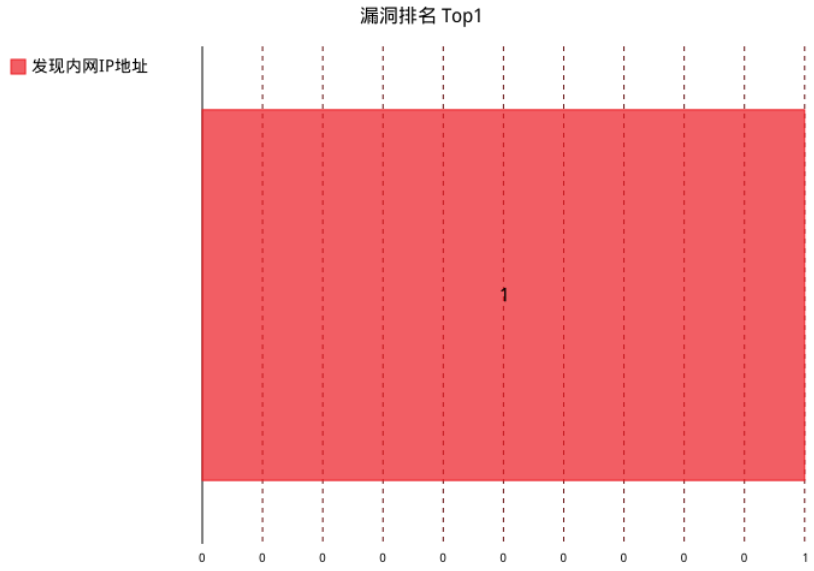
报表生成时间　　2020-06-23 21:43:18

目 录

一、资产统计分布



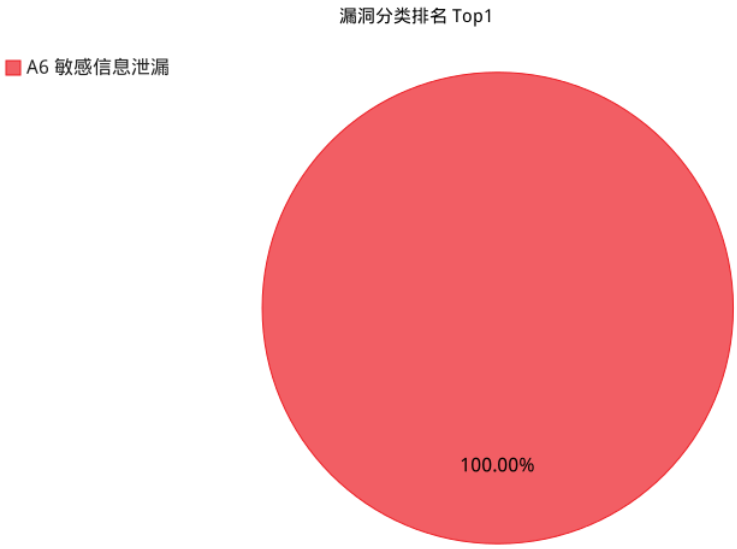
高风险	中风险	低风险	信息	总计
0	0	1	0	1



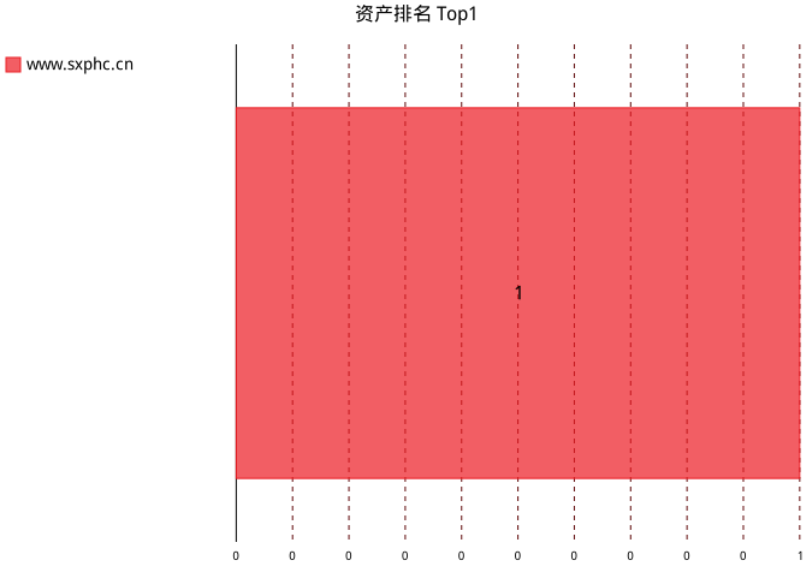
漏洞名称排名(Top10)	总计
发现内网 IP 地址	1

备注：漏洞分值在 0-2 之间为低风险资产；漏洞分值在 2-7.5 之间为中风险资产；漏洞分值在 7.5-10 之间为高风险资产。

提示：点击资产名称可跳转至该资产的详细报表。



漏洞分类统计排名(Top10)	总计
A6 敏感信息泄漏	1



资产名称统计	漏洞风险值	资产风险等级	总计
www.sxphc.cn	1.0	**低风险**	1

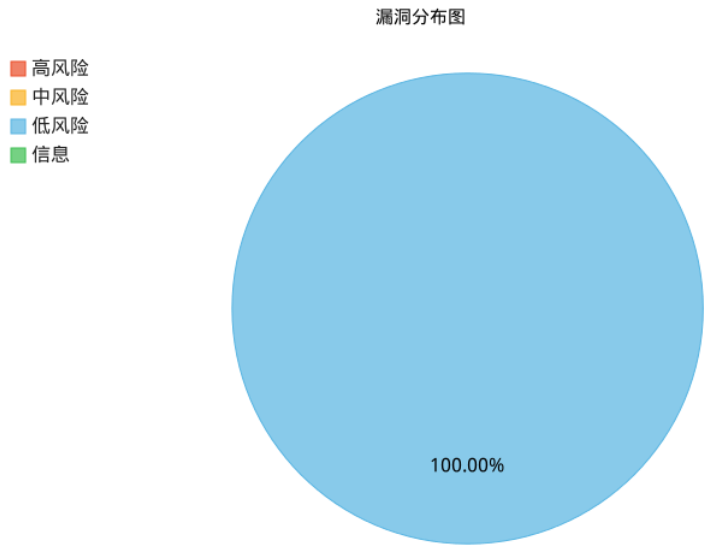
1 资产概述

1. 资产基本信息

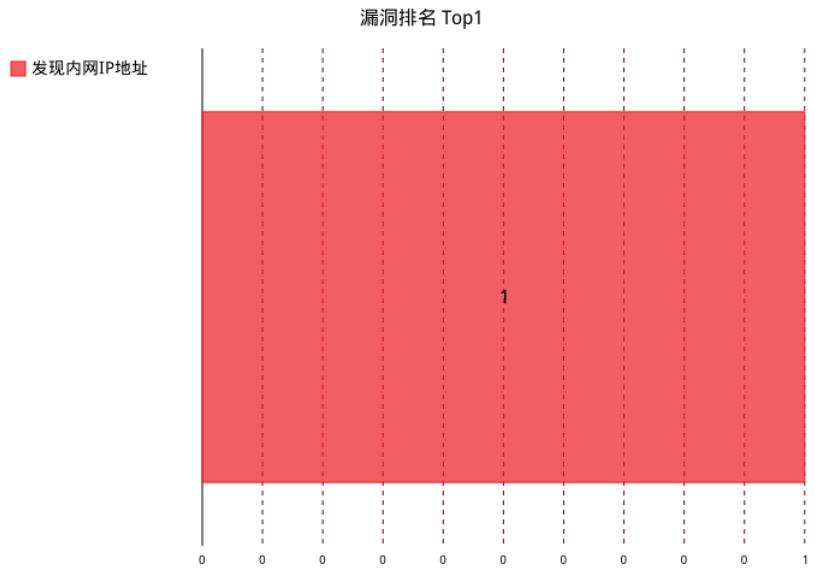
资产名称	www.sxphc.cn
IP 地址	218.26.225.130
URL 地址	http://www.sxphc.cn
网站编码	UTF-8
网站物理地址	山西省太原市-生物技术学院电教楼二楼 9 机房[218.26.225.130-218.26.225.130]
扫描时间	2021-06-23 21:32:10 - 2021-06-23 21:38:05
漏洞风险值	1.0（资产风险等级：低风险）
漏洞总计	1
漏洞状态标识	误报：0 已修复：0
漏洞分布	高风险：0 中风险：0 低风险：1 信息：0

备注：漏洞分值在 0-2 之间为低风险资产；漏洞分值在 2-7.5 之间为中风险资产；漏洞分值在 7.5-10 之间为高风险资产。

二、漏洞分布



高风险	中风险	低风险	信息	总计
0	0	1	0	1



漏洞名称统计排名(Top10)	总计
发现内网 IP 地址	1

三、漏洞详情

漏洞名称	**发现内网 IP 地址**
漏洞分类	**A6 敏感信息泄漏**
漏洞类型	**WEB 漏洞**
出现次数	1
风险级别	低风险
详细描述	网页中发现内部使用的私有 IP 地址信息，可能暴露内部的网络结构。
解决办法	人工确认必要性，如无必要，请删除该 IP 地址信息。
漏洞详情	URL 地址：http://www.sxphc.cn/ 测试用例： GET / HTTP/1.1 Accept: */* Referer: http://www.sxphc.cn Host: www.sxphc.cn Connection: Keep-Alive

		User-Agent: Mozilla/5.0 compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0 Accept-Encoding: gzip,deflate	
	漏洞状态	新建	

2020年普通高校招生网站检测安全评估报告

2020 年 7 月

高校招生网站安全服务平台 https://www.sec.edu.cn/
HTTPS升级技术支持 https://ssl.cernet.com/
安全防护方案免费咨询 https://www.security.edu.cn/

客服服务中心：4008-818-5550　　电子邮件：soc@cernet.edu.cn

目录

1 概况

学校名称	山西药科职业学院
网站域名	www.sxphc.cn
URL地址	http://www.sxphc.cn/sxykzsw/
IP地址	218.26.225.130
网页编码	utf-8
漏洞数量	17
漏洞统计	高危漏洞 0 个，中危漏洞 0 个， 低危漏洞 6 个， 信息漏洞 11 个

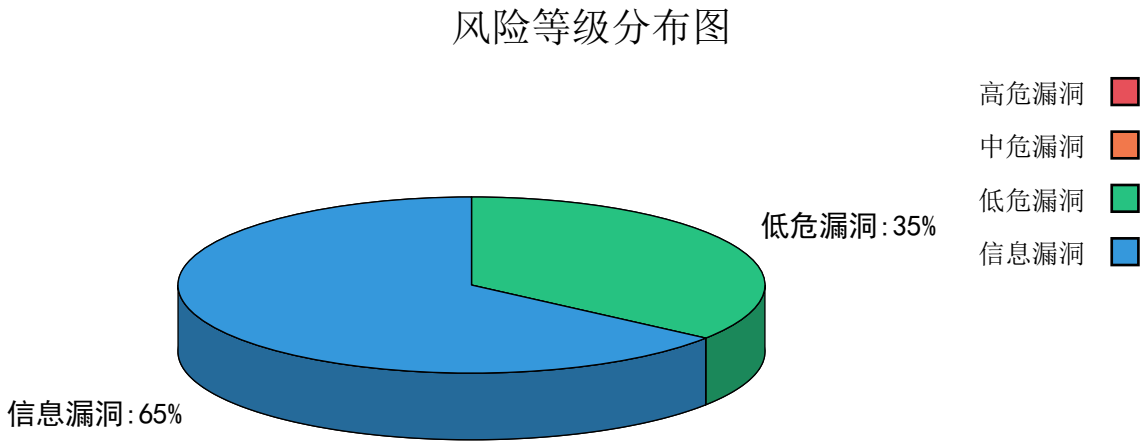
1、报告只针对本次扫描出的漏洞情况进行评价，仅作为站点安全状况评估参考。

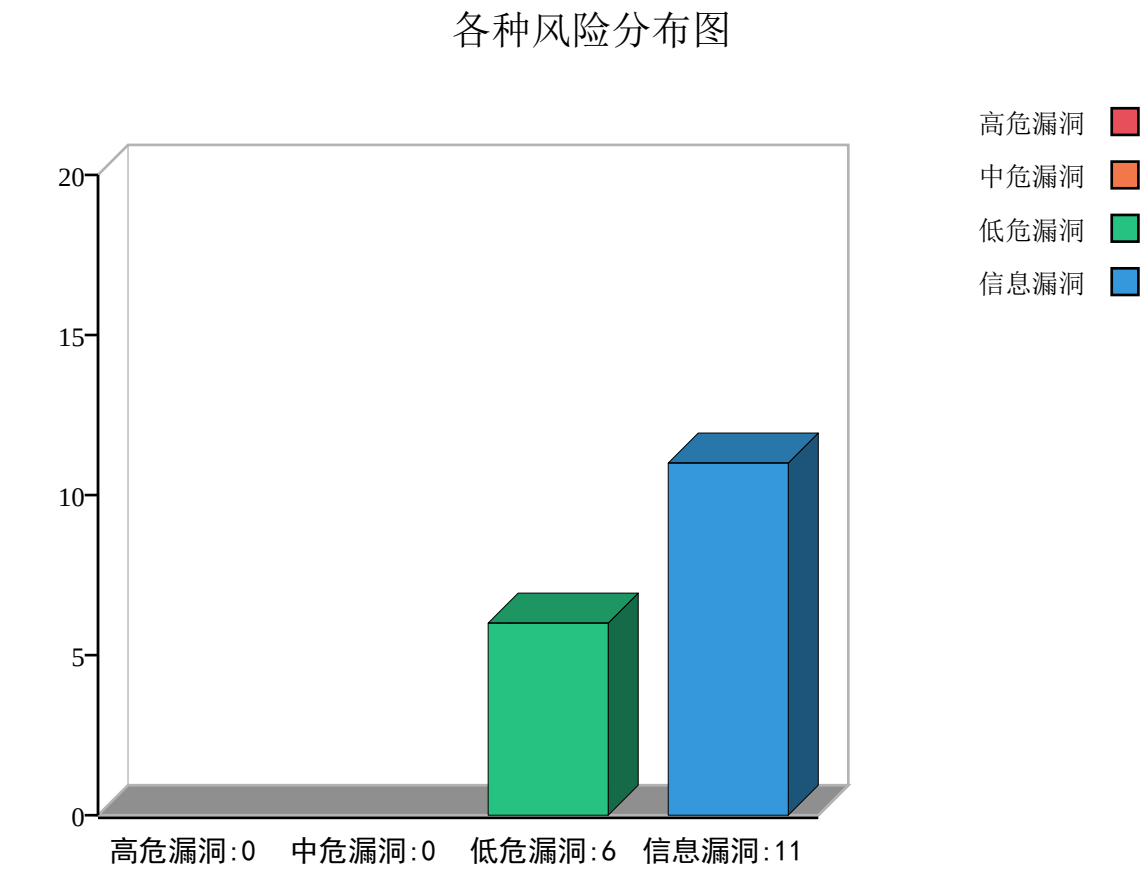
2、如果贵校网站部署了防火墙、入侵检测/防御等设备，或者网络故障、网站离线等，漏洞扫描任务可能因此失败或者中止，此时检测报告仅体现已完成扫描的结果。建议在内网环境下定期进行漏洞扫描。

3、鉴于有些漏洞危害性较大，可能造成信息系统的不稳定，我们未对所有漏洞进行验证，报告存在误报的可能。

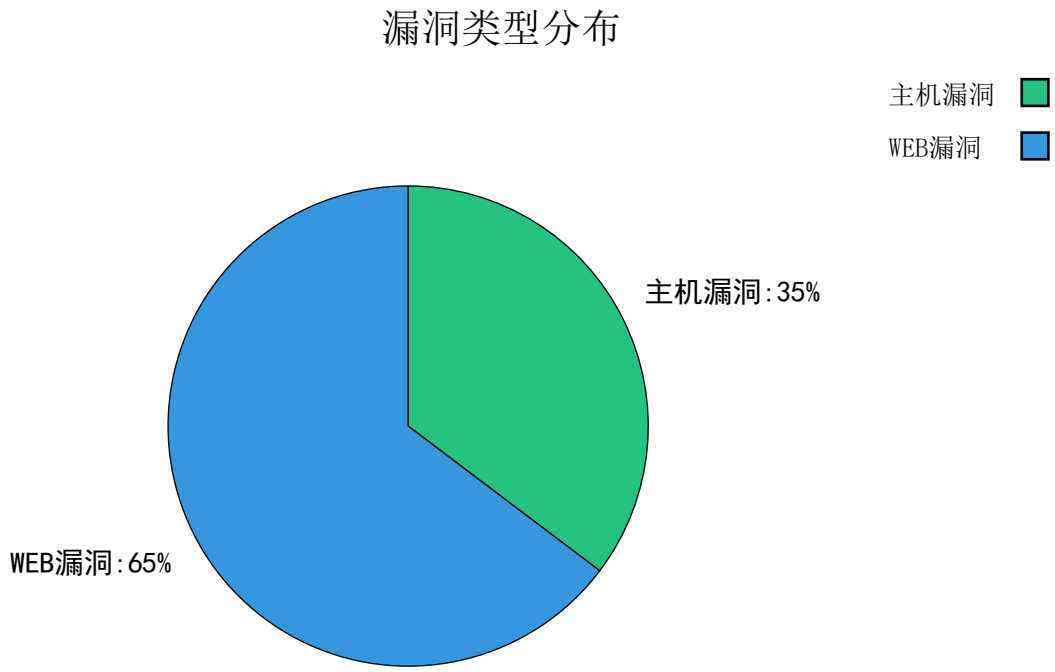
2 总体风险分布

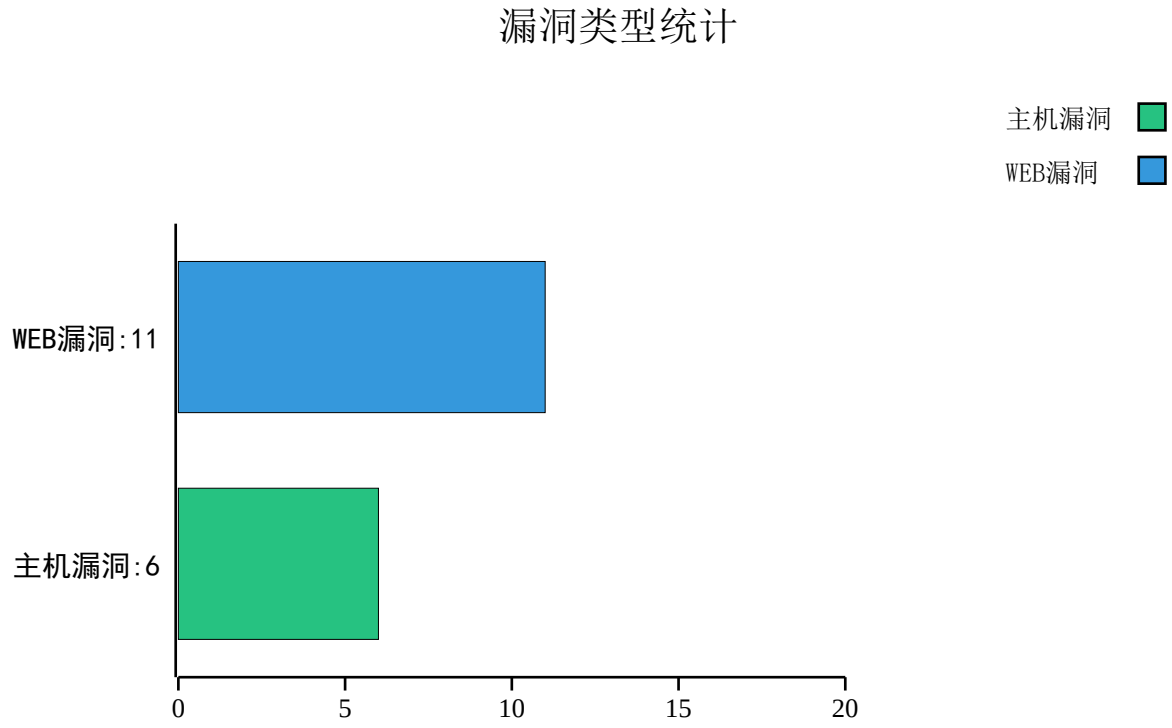
2.1 风险等级分布





2.2 风险类型分布

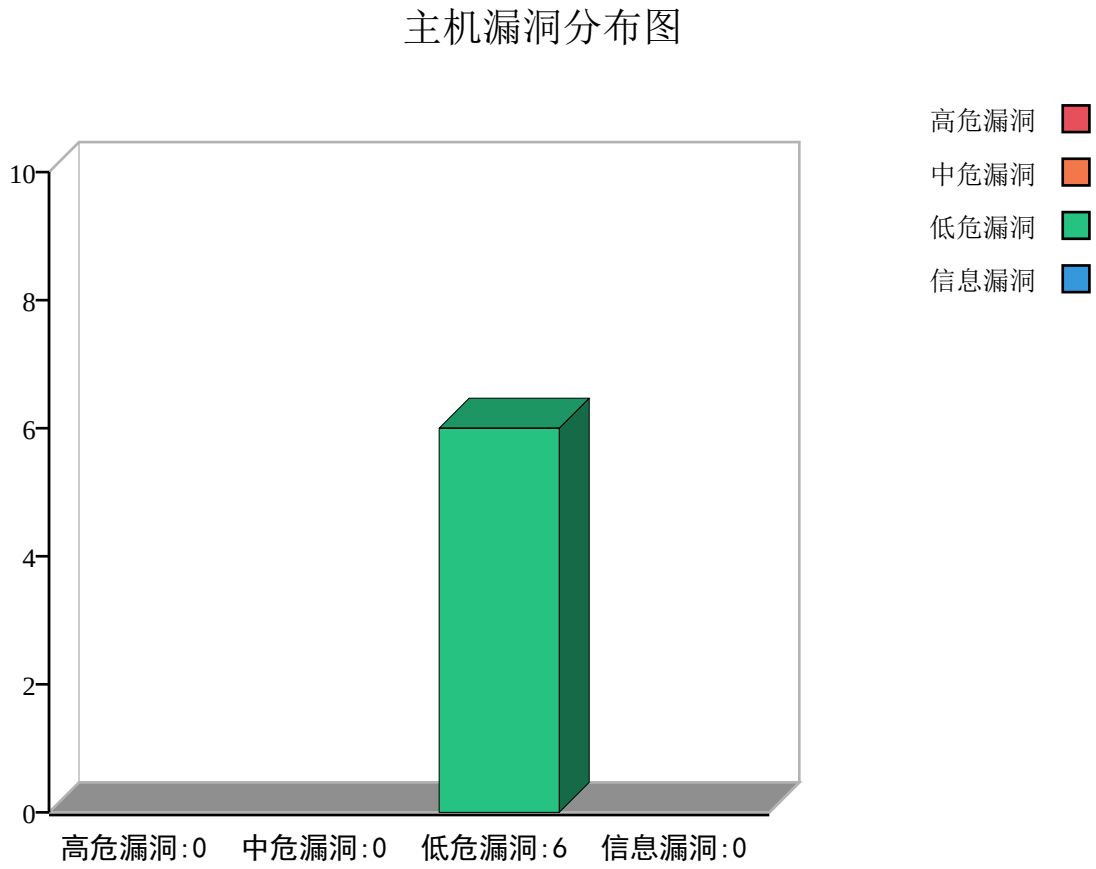

漏洞类型分布
主机漏洞
WEB漏洞
主机漏洞:35%
WEB漏洞:65%


漏洞类型统计
主机漏洞
WEB漏洞
WEB漏洞:11
主机漏洞:6
0
5
10
15
20

3 主机漏洞分析

3.1 主机漏洞统计

高危漏洞	中危漏洞	低危漏洞	信息漏洞	总计
0	0	6	0	6



3.2 主机漏洞详情

序号	1
漏洞名称	目标服务器启用了OPTIONS方法
漏洞类型	系统漏洞
主机端口	90
CVE编号	
风险级别	低危漏洞
漏洞描述	通过调用OPTIONS方法，可以确定目标服务器允许哪些HTTP方法。OPTIONS方法可能会暴露一些敏感信息，这些信息将帮助攻击者准备更进一步的攻击。
解决方法	建议WEB服务器仅启用GET、POST、HEAD方法，禁用OPTIONS、PUT、PATCH、DELETE、TRACE、CONNECT、DEBUG等方法。如果实在必要，请限定这些HTTP方法只能在指定的目录下运行，该目录不应包含重要的文件。

序号	2
漏洞名称	HTTP响应头未设置X-Frame-Options
漏洞类型	系统漏洞
主机端口	90
CVE编号	
风险级别	低危漏洞
漏洞描述	目标服务器的HTTP服务未设置X-Frame-Options响应头。 攻击者可以使用一个透明的iframe覆盖在目标网页上，可以诱使用户恰好点击iframe页面的一些功能性按钮上，导致被劫持。 X-Frame-Options HTTP 响应头是用来告知浏览器此页面是否可在 <frame>、<iframe> 或者 <object> 中展示。
解决方法	修改WEB服务器配置，在所有页面上设置X-Frame-Options响应头。其值有如下三种： （1）DENY：不能被嵌入到任何iframe或frame中。 （2）SAMEORIGIN：页面只能被本站页面嵌入到iframe或者frame中。 （3）ALLOW-FROM uri：只能被嵌入到指定域名的iframe或者frame中。

序号	3
漏洞名称	HTTP响应头未设置X-XSS-Protection
漏洞类型	系统漏洞
主机端口	80
CVE编号	
风险级别	低危漏洞
漏洞描述	目标服务器的HTTP服务未设置X-XSS-Protection响应头。大部分现代浏览器内置了跨站脚本（XSS）过滤器，默认情况下，此功能是启用的。如果用户禁用了这个功能，此响应头可以使得浏览器针对这个网站页面重新启用此过滤器，避免XSS攻击。
解决方法	修改WEB服务器配置，在所有页面上设置HTTP响应头：X-XSS-Protection：1;mode=block

序号	4
漏洞名称	HTTP响应头未设置X-XSS-Protection
漏洞类型	系统漏洞
主机端口	90
CVE编号	
风险级别	低危漏洞
漏洞描述	目标服务器的HTTP服务未设置X-XSS-Protection响应头。大部分现代浏览器内置了跨站脚本（XSS）过滤器，默认情况下，此功能是启用的。如果用户禁用了这个功能，此响应头可以使得浏览器针对这个网站页面重新启用此过滤器，避免XSS攻击。
解决方法	修改WEB服务器配置，在所有页面上设置HTTP响应头：X-XSS-Protection：1;mode=block

序号	5
漏洞名称	HTTP响应头未设置X-Content-Type-Options
漏洞类型	系统漏洞
主机端口	80
CVE编号	
风险级别	低危漏洞
漏洞描述	目标服务器的HTTP服务未设置X-Content-Type-Options响应头，或者配置错误。互联网上的资源有各种类型，通常浏览器会根据响应头的Content-Type字段来分辨它们的类型。有些资源的Content-Type是错的或者未定义，这时某些浏览器会启用MIME-sniffing来猜测该资源的类型，解析内容并执行。利用浏览器的这个特性，攻击者甚至可以让原本应该解析为图片的请求被解析为JavaScript。启用X-Content-Type-Options响应头可以禁用浏览器的类型猜测行为。
解决方法	修改WEB服务器配置，在所有页面上设置HTTP响应头：X-Content-Type-Options：nosniff

序号	6
漏洞名称	HTTP响应头未设置X-Content-Type-Options
漏洞类型	系统漏洞
主机端口	90
CVE编号	
风险级别	低危漏洞
漏洞描述	目标服务器的HTTP服务未设置X-Content-Type-Options响应头，或者配置错误。互联网上的资源有各种类型，通常浏览器会根据响应头的Content-Type字段来分辨它们的类型。有些资源的Content-Type是错的或者未定义，这时某些浏览器会启用MIME-sniffing来猜测该资源的类型，解析内容并执行。利用浏览器的这个特性，攻击者甚至可以让原本应该解析为图片的请求被解析为JavaScript。启用X-Content-Type-Options响应头可以禁用浏览器的类型猜测行为。
解决方法	修改WEB服务器配置，在所有页面上设置HTTP响应头：X-Content-Type-Options：nosniff

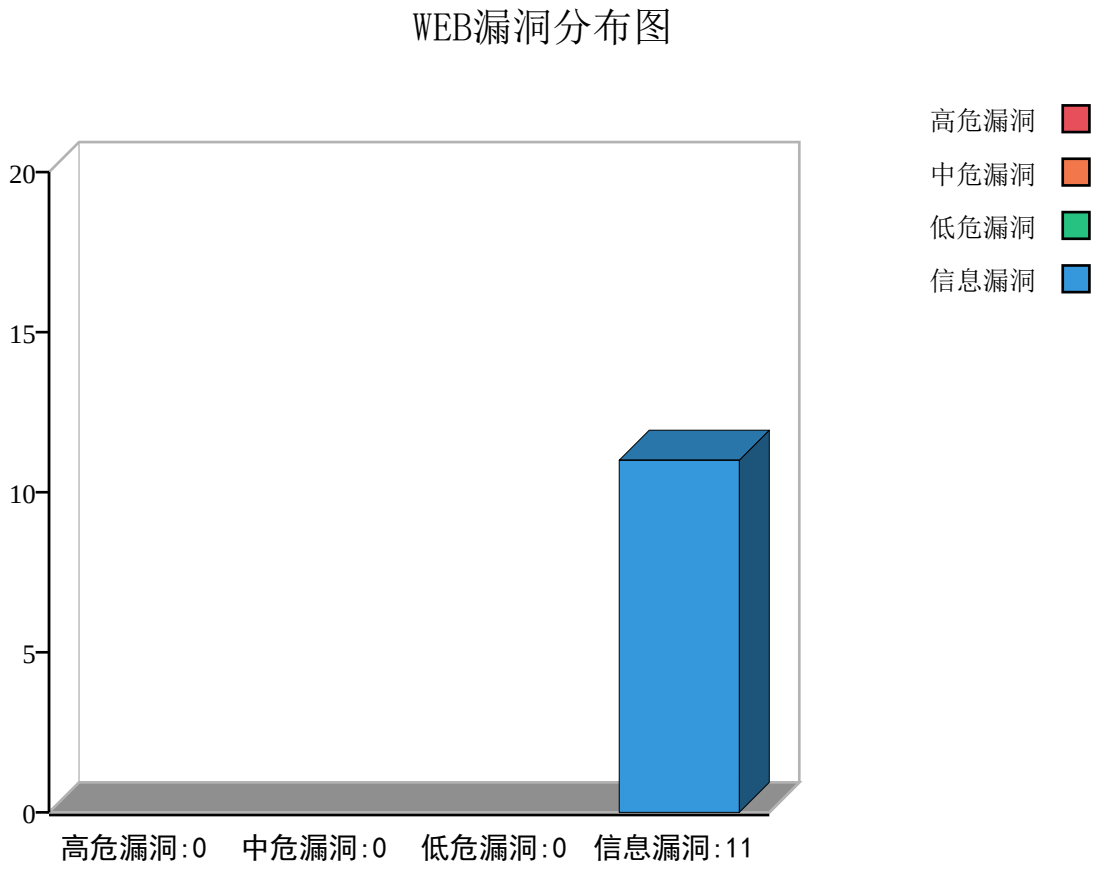
3.3 解决方案

解决方案	https://www.security.edu.cn/
咨询电话	400-650-2668

4 WEB漏洞分析

4.1 WEB漏洞统计

高危漏洞	中危漏洞	低危漏洞	信息漏洞	总计
0	0	0	11	11



4.2 WEB漏洞详情

序号	1
漏洞名称	电子邮箱信息泄露
漏洞类型	WEB漏洞
风险级别	信息漏洞
漏洞链接	http://www.sxphc.cn/sxykzsw/info/1030/1154.htm
漏洞描述	网页中发现电子邮箱信息，可能造成邮箱信息泄露。
解决方法	人工确认其必要性，如果无必要，请在页面中删除该邮箱信息。
情况说明	页面中包含邮件地址：sxykxyzjc@163.com BOsxykxyzjc@163.com
测试用例	POST /sxykzsw/info/1030/1154.htm HTTP/1.1 Accept: */* Referer: http://www.sxphc.cn/sxykzsw/info/1030/1154.htm Content-Length: 0 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 Host: www.sxphc.cn Connection: Keep-Alive User-Agent: Mozilla/5.0 compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0 Accept-Encoding: gzip,deflate Cookie: JSESSIONID=10AACC4E45262A6102FC0608ED5E0A65

序号	2
漏洞名称	电子邮箱信息泄露
漏洞类型	WEB漏洞
风险级别	信息漏洞
漏洞链接	http://www.sxphc.cn/sxykzsw/info/1005/1024.htm
漏洞描述	网页中发现电子邮箱信息，可能造成邮箱信息泄露。
解决方法	人工确认其必要性，如果无必要，请在页面中删除该邮箱信息。
情况说明	页面中包含邮件地址：sxykjijianjiancha@126.com
测试用例	POST /sxykzsw/info/1005/1024.htm HTTP/1.1 Accept: */* Referer: http://www.sxphc.cn/sxykzsw/info/1005/1024.htm Content-Length: 0 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 Host: www.sxphc.cn Connection: Keep-Alive User-Agent: Mozilla/5.0 compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0 Accept-Encoding: gzip,deflate Cookie: JSESSIONID=10AACC4E45262A6102FC0608ED5E0A65

序号	3
漏洞名称	电子邮箱信息泄露
漏洞类型	WEB漏洞
风险级别	信息漏洞
漏洞链接	http://www.sxphc.cn/sxykzsw/info/1005/1166.htm
漏洞描述	网页中发现电子邮箱信息，可能造成邮箱信息泄露。
解决方法	人工确认其必要性，如果无必要，请在页面中删除该邮箱信息。
情况说明	页面中包含邮件地址：sxykjijianjiancha@126.com
测试用例	POST /sxykzsw/info/1005/1166.htm HTTP/1.1 Accept: */* Referer: http://www.sxphc.cn/sxykzsw/info/1005/1166.htm Content-Length: 0 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 Host: www.sxphc.cn Connection: Keep-Alive User-Agent: Mozilla/5.0 compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0 Accept-Encoding: gzip,deflate Cookie: JSESSIONID=10AACC4E45262A6102FC0608ED5E0A65

序号	4
漏洞名称	电子邮箱信息泄露
漏洞类型	WEB漏洞
风险级别	信息漏洞
漏洞链接	http://www.sxphc.cn/sxykzsw/info/1030/1154.htm
漏洞描述	网页中发现电子邮箱信息，可能造成邮箱信息泄露。
解决方法	人工确认其必要性，如果无必要，请在页面中删除该邮箱信息。
情况说明	页面中包含邮件地址：sxykxyzjc@163.com BOsxykxyzjc@163.com
测试用例	GET /sxykzsw/info/1030/1154.htm HTTP/1.1 Accept: */* Referer: http://www.sxphc.cn/sxykzsw/ Host: www.sxphc.cn Connection: Keep-Alive User-Agent: Mozilla/5.0 compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0 Accept-Encoding: gzip,deflate Cookie: JSESSIONID=10AACC4E45262A6102FC0608ED5E0A65

序号	5
漏洞名称	电子邮箱信息泄露
漏洞类型	WEB漏洞
风险级别	信息漏洞
漏洞链接	http://www.sxphc.cn/sxykzsw/ssjgy.jsp?wbtreeid=1001&searchScope;=0&currentnum;=4&newskeycode2;=
漏洞描述	网页中发现电子邮箱信息，可能造成邮箱信息泄露。
解决方法	人工确认其必要性，如果无必要，请在页面中删除该邮箱信息。
情况说明	页面中包含邮件地址：sxykxyzjc@163.com
测试用例	GET /sxykzsw/ssjgy.jsp?wbtreeid=1001&searchScope;=0&currentnum;=4&newskeycode2;= HTTP/1.1 Accept: */* Referer: http://www.sxphc.cn/sxykzsw/ssjgy.jsp?wbtreeid=1001 Host: www.sxphc.cn Connection: Keep-Alive User-Agent: Mozilla/5.0 compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0 Accept-Encoding: gzip,deflate Cookie: JSESSIONID=10AACC4E45262A6102FC0608ED5E0A65

序号	6
漏洞名称	电子邮箱信息泄露
漏洞类型	WEB漏洞
风险级别	信息漏洞
漏洞链接	http://www.sxphc.cn/sxykzsw/ssjgy.jsp?wbtreeid=1028&searchScope;=0&currentnum;=4&newskeycode2;=
漏洞描述	网页中发现电子邮箱信息，可能造成邮箱信息泄露。
解决方法	人工确认其必要性，如果无必要，请在页面中删除该邮箱信息。
情况说明	页面中包含邮件地址：sxykxyzjc@163.com
测试用例	GET /sxykzsw/ssjgy.jsp?wbtreeid=1028&searchScope;=0&currentnum;=4&newskeycode2;= HTTP/1.1 Accept: */* Referer: http://www.sxphc.cn/sxykzsw/ssjgy.jsp?wbtreeid=1028 Host: www.sxphc.cn Connection: Keep-Alive User-Agent: Mozilla/5.0 compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0 Accept-Encoding: gzip,deflate Cookie: JSESSIONID=10AACC4E45262A6102FC0608ED5E0A65

序号	7
漏洞名称	电子邮箱信息泄露
漏洞类型	WEB漏洞
风险级别	信息漏洞
漏洞链接	http://www.sxphc.cn/sxykzsw/ssjgy.jsp?wbtreeid=1030&searchScope;=0&currentnum;=4&newskeycode2;=
漏洞描述	网页中发现电子邮箱信息，可能造成邮箱信息泄露。
解决方法	人工确认其必要性，如果无必要，请在页面中删除该邮箱信息。
情况说明	页面中包含邮件地址：sxykxyzjc@163.com
测试用例	GET /sxykzsw/ssjgy.jsp?wbtreeid=1030&searchScope;=0&currentnum;=4&newskeycode2;= HTTP/1.1 Accept: */* Referer: http://www.sxphc.cn/sxykzsw/ssjgy.jsp?wbtreeid=1030 Host: www.sxphc.cn Connection: Keep-Alive User-Agent: Mozilla/5.0 compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0 Accept-Encoding: gzip,deflate Cookie: JSESSIONID=10AACC4E45262A6102FC0608ED5E0A65

序号	8
漏洞名称	电子邮箱信息泄露
漏洞类型	WEB漏洞
风险级别	信息漏洞
漏洞链接	http://www.sxphc.cn/sxykzsw/ssjgy.jsp?wbtreeid=1005&searchScope;=0&currentnum;=4&newskeycode2;=
漏洞描述	网页中发现电子邮箱信息，可能造成邮箱信息泄露。
解决方法	人工确认其必要性，如果无必要，请在页面中删除该邮箱信息。
情况说明	页面中包含邮件地址：sxykxyzjc@163.com
测试用例	GET /sxykzsw/ssjgy.jsp?wbtreeid=1005&searchScope;=0&currentnum;=4&newskeycode2;= HTTP/1.1 Accept: */* Referer: http://www.sxphc.cn/sxykzsw/ssjgy.jsp?wbtreeid=1005 Host: www.sxphc.cn Connection: Keep-Alive User-Agent: Mozilla/5.0 compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0 Accept-Encoding: gzip,deflate Cookie: JSESSIONID=10AACC4E45262A6102FC0608ED5E0A65

序号	9
漏洞名称	电子邮箱信息泄露
漏洞类型	WEB漏洞
风险级别	信息漏洞
漏洞链接	http://www.sxphc.cn/sxykzsw/ssjgy.jsp?wbtreeid=1006&searchScope;=0&currentnum;=4&newskeycode2;=
漏洞描述	网页中发现电子邮箱信息，可能造成邮箱信息泄露。
解决方法	人工确认其必要性，如果无必要，请在页面中删除该邮箱信息。
情况说明	页面中包含邮件地址：sxykxyzjc@163.com
测试用例	GET /sxykzsw/ssjgy.jsp?wbtreeid=1006&searchScope;=0&currentnum;=4&newskeycode2;= HTTP/1.1 Accept: */* Referer: http://www.sxphc.cn/sxykzsw/ssjgy.jsp?wbtreeid=1006 Host: www.sxphc.cn Connection: Keep-Alive User-Agent: Mozilla/5.0 compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0 Accept-Encoding: gzip,deflate Cookie: JSESSIONID=10AACC4E45262A6102FC0608ED5E0A65

序号	10
漏洞名称	电子邮箱信息泄露
漏洞类型	WEB漏洞
风险级别	信息漏洞
漏洞链接	http://www.sxphc.cn/sxykzsw/ssjgy.jsp?wbtreeid=1007&searchScope;=0&currentnum;=4&newskeycode2;=
漏洞描述	网页中发现电子邮箱信息，可能造成邮箱信息泄露。
解决方法	人工确认其必要性，如果无必要，请在页面中删除该邮箱信息。
情况说明	页面中包含邮件地址：sxykxyzjc@163.com
测试用例	GET /sxykzsw/ssjgy.jsp?wbtreeid=1007&searchScope;=0&currentnum;=4&newskeycode2;= HTTP/1.1 Accept: */* Referer: http://www.sxphc.cn/sxykzsw/ssjgy.jsp?wbtreeid=1007 Host: www.sxphc.cn Connection: Keep-Alive User-Agent: Mozilla/5.0 compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0 Accept-Encoding: gzip,deflate Cookie: JSESSIONID=10AACC4E45262A6102FC0608ED5E0A65

序号	11
漏洞名称	发现内网IP地址
漏洞类型	WEB漏洞
风险级别	信息漏洞
漏洞链接	http://www.sxphc.cn/
漏洞描述	网页中发现内部使用的私有IP地址信息，可能暴露内部的网络结构。
解决方法	人工确认必要性，如无必要，请删除该IP地址信息，或者仅允许已登录用户查看此信息。
情况说明	页面内容包含内网IP地址：192.168.2.47
测试用例	GET / HTTP/1.1 Accept: */* Referer: http://www.sxphc.cn/sxykzsw/ Host: www.sxphc.cn Connection: Keep-Alive User-Agent: Mozilla/5.0 compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0 Accept-Encoding: gzip,deflate Cookie: JSESSIONID=10AACC4E45262A6102FC0608ED5E0A65

4.3 解决方案

解决方案	https://www.security.edu.cn/
咨询电话	400-650-2668

5 HTTPS部署状态

是否支持HTTPS	否
颁发者	
证书有效期	

6 IPv6部署状态

是否支持IPv6	否

高校招生网站安全服务平台 https://www.sec.edu.cn/

HTTPS升级技术支持 https://ssl.cernet.com/

网页防护方案免费咨询 https://www.security.edu.cn/