铱迅漏洞扫描系统
安全评估报告

报表名称	单域名报表 http://39.105.86.118/
报表编号	NVS-20191012-001H
生成时间	2019-10-12 13:51:33
任务名称	http://39.105.86.118/

目录

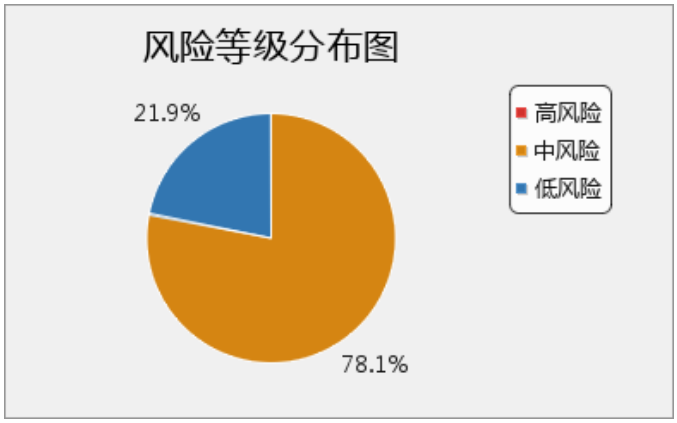
1 综述

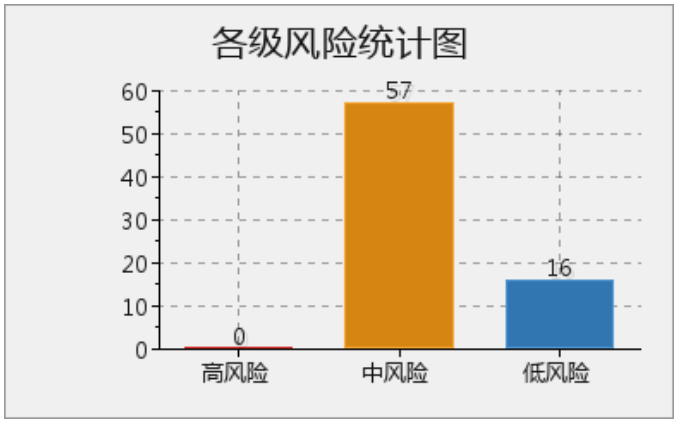
域名 http://39.105.86.118/ 共存在风险 73 个，信息安全风险总评级为 中风险 。

高危及以上Web漏洞有 0 个。

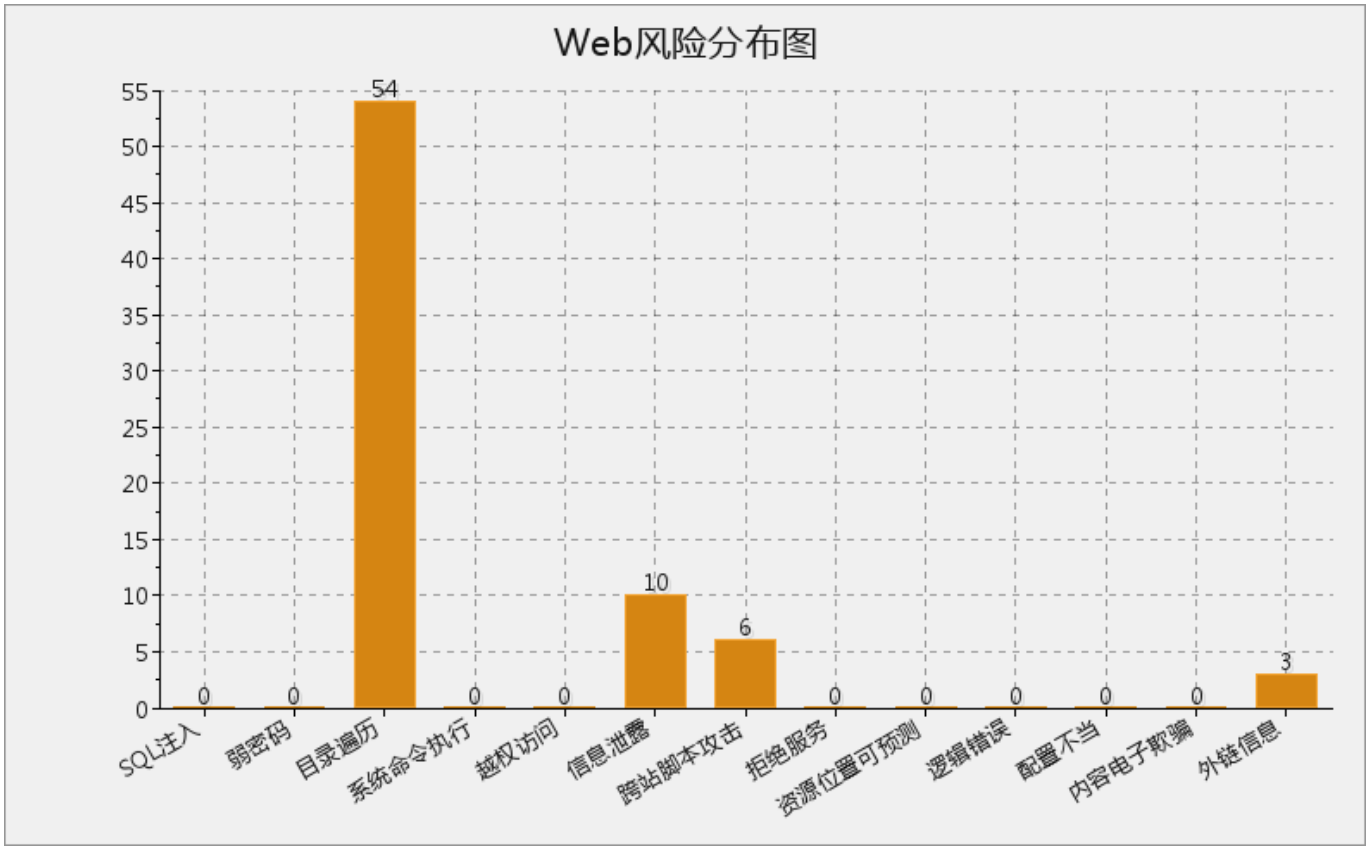
2 总体风险分析

2.1 风险等级分布





2.2 风险类型分布



3 Web漏洞列表

3.1 SQL注入

本次扫描没有发现该风险。

3.2 弱密码

本次扫描没有发现该风险。

3.3 目录遍历

本次扫描共发现该风险 1 种，共 54 个。

[中风险] 检测到遍历目录漏洞

URL列表（共54项）

URL	http://39.105.86.118/include/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/css/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/layui245/css/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/layui245/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL

漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/js/lib/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/js/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/images/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/menu/css/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/menu/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/layui230/css/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/layui230/

风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/person/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/voteinformation/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/layui245/css/modules/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/layui245/font/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/layui245/images/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/layui245/lay/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/bootstrap/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/ckeditor/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/excel/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/layer/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/phpass/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/upload/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/menu/fonts/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/menu/images/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/menu/js/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/layui230/css/modules/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/layui230/font/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/layui230/images/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/layui230/lay/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/layui245/css/modules/laydate/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/layui245/css/modules/layer/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/layui245/images/face/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/layui245/lay/modules/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/ckeditor/adapters/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/ckeditor/lang/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/ckeditor/plugins/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/ckeditor/skins/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/excel/PHPExcel/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/layer/mobile/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/layer/theme/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/phpass/c/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/upload/css/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/upload/images/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/upload/swfupload/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/menu/js/extends/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/layui230/css/modules/laydate/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/layui230/css/modules/layer/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/layui230/images/face/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/layui230/lay/modules/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/layer/theme/default/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/layui245/css/modules/laydate/default/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

URL	http://39.105.86.118/lib/layui245/css/modules/layer/default/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	目录遍历漏洞是由于Web服务器设置不当导致的，攻击者可利用此漏洞查看Web目录下的文件及其文件夹，从而找到可攻击的文件。该漏洞一般被攻击者作为辅助攻击的手段之一。

风险描述

可以查看和下载特定Web应用程序虚拟目录下的内容，其中可能包含访问被限制的文件。

原因：开启了目录浏览功能。

Web 服务器通常配置成不允许目录浏览。不过，如果Web服务器配置不当，便有可能发送对于特定目录（而不是文件）的请求来获取目录列表。名称为“some_dir”的目录，其目录的列出请求示例如下：http://www.xxxx.com/some_dir/

利用Web服务器和Web应用程序中会强迫Web服务器返回目录列表的特定问题，例如“URL 诡计”攻击，或形态异常的HTTP请求，是另一个获取目录列表的可能方式。可以从应用程序或服务器供应商下载补丁，以解决这些安全漏洞。
在某些运行于Win32操作系统的Web服务器中，使用短文件名（8.3 DOS 格式）可以略过访问控制。
例如，Web服务器会拒绝浏览/longdirname/目录，但它的DOS 8.3对等名称/LONGDI~1/却开放浏览。
注意：攻击者使用目录列表来查找Web目录中，通常不通过Web站点上的链接显现出来的文件。配置文件及可能含有敏感信息的Web应用程序其他组件，都可以利用这个方式来查看。

解决方案

1. 将 Web 服务器配置成拒绝列出目录。
2. 根据 Web 服务器或 Web
应用程序上现有的问题来下载特定安全补丁。部分已知的目录列表问题列在这个咨询的“引用”字段中。
3. 利用“CERT”咨询中的变通方法（在这项咨询的“引用”字段中）来修订短文件名（8.3 DOS 格式）问题：
----a. 想要完全由Web服务器来保护的文件仅用 8.3 标准短文件名。在FAT文件系统（16
位）上，您可以启用“Win31FileSystem”注册表键（设为
1，注册表路径：HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem\）来强制这一点。
----b. 在 NTFS（32 位）上，您可以启用“NtfsDisable8dot3NameCreation”注册表键（设为
1，注册表路径：HKEY_LOCAL_MACHINE\System\ CurrentControlSet\Control\FileSystem\）来禁用创建长文件名文件的8.3 标准短文件名。不过，这个步骤可能会引起与16 位应用程序的兼容性问题。
----c. 使用基于NTFS的ACL（目录或文件级别的访问控制表）来扩增或替换基于Web服务器的安全。

3.4 系统命令执行

本次扫描没有发现该风险。

3.5 越权访问

本次扫描没有发现该风险。

3.6 信息泄露

本次扫描共发现该风险 1 种，共 10 个。

[低风险] 发现电子邮件地址模式

URL列表（共10项）

URL	http://39.105.86.118/
风险评级	低风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	检测到邮件信息，可能导致信息泄露。

URL	http://39.105.86.118/?usertype=1&usertype=2
风险评级	低风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	检测到邮件信息，可能导致信息泄露。

URL	http://39.105.86.118/lib/JSEncrypt.js
风险评级	低风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	检测到邮件信息，可能导致信息泄露。

URL	http://39.105.86.118/icons/blank.gif
风险评级	低风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	检测到邮件信息，可能导致信息泄露。

URL	http://39.105.86.118/icons/back.gif
风险评级	低风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	检测到邮件信息，可能导致信息泄露。

URL	http://39.105.86.118/icons/unknown.gif
风险评级	低风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	检测到邮件信息，可能导致信息泄露。

URL	http://39.105.86.118/index.php
风险评级	低风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	检测到邮件信息，可能导致信息泄露。

URL	http://39.105.86.118/icons/text.gif

风险评级	低风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	检测到邮件信息，可能导致信息泄露。

URL	http://39.105.86.118/icons/folder.gif
风险评级	低风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	检测到邮件信息，可能导致信息泄露。

URL	http://39.105.86.118/js/lib/base64.js
风险评级	低风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	检测到邮件信息，可能导致信息泄露。

风险描述

发现页面上存在电子邮箱地址，可能存在敏感信息泄露。

解决方案

删除页面上不必要存在的电子邮箱地址。

3.7 跨站脚本攻击

本次扫描共发现该风险 3 种，共 6 个。

[中风险] 表单CSRF攻击

URL列表（共3项）

URL	http://39.105.86.118/
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	该页面表单容易受到CSRF攻击，请检查该页面所有表单。

URL	http://39.105.86.118/index.php
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	该页面表单容易受到CSRF攻击，请检查该页面所有表单。

URL	http://39.105.86.118/person/update_dept_user.php
风险评级	中风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	该页面表单容易受到CSRF攻击，请检查该页面所有表单。

风险描述

所谓的CSRF(跨站请求伪造)攻击，就是攻击者盗用了被攻击者的身份，以被攻击者的名义发送恶意请求。CSRF漏洞可能会危及最终用户的数据和操作，如果被攻击对象是管理员，可能会危及整个Web应用程序。

解决方案

详细检查该页面表单是否需要CSRF防护。
如果需要，解决方法如下：
1.使用token，增加一隐藏表单项，服务器校验该token合法性。

[低风险] 客户端（ JavaScript ） Cookie引用

URL列表（ 共2项 ）

URL	http://39.105.86.118/lib/jquery.cookie.js
风险评级	低风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	Cookie 是在客户端创建的。代码用于操纵站点的 cookie。可以将实施 cookie 逻辑的功能移至客户端（ 浏览器 ）。这样一来，攻击者就能发送其本无权发送的 cookie。

URL	http://39.105.86.118/lib/ckeditor/ckeditor.js
风险评级	低风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	Cookie 是在客户端创建的。代码用于操纵站点的 cookie。可以将实施 cookie 逻辑的功能移至客户端（ 浏览器 ）。这样一来，攻击者就能发送其本无权发送的 cookie。

风险描述

Cookie 是在客户端创建的。代码用于操纵站点的 cookie。可以将实施 cookie
逻辑的功能移至客户端（ 浏览器 ）。这样一来，攻击者就能发送其本无权发送的 cookie。

解决方案

Cookie 是在客户端创建的，可能会被恶意用户篡改，所以建议利用Session进行控制。

[低风险] 点击劫持

URL列表（ 共1项 ）

URL	http://39.105.86.118/
风险评级	低风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	服务器未设置X-Frame-Options响应头，易受到点击劫持攻击

风险描述

点击劫持是一种视觉上的欺骗手段。攻击者使用一个透明的、不可见的iframe，覆盖在一个网页上，然后诱使用户在该网页上进

行操作，此时用户将在不知情的情况下点击透明的iframe页面。通过调整iframe页面的位置，可以诱使用户恰好点击在iframe页面的一些功能性按钮上。

解决方案

设置X-Frame-Options响应头
它有三个可选的值：
DENY
SAMEORIGIN
ALLOW-FROM origin
当值为DENY时，浏览器会拒绝当前页面加载任何frame页面；若值为SAMEORIGIN，则frame页面的地址只能为同源域名下的页面；若值为ALLOW-FROM，则可以定义允许frame加载的页面地址。

3.8 拒绝服务

本次扫描没有发现该风险。

3.9 资源位置可预测

本次扫描没有发现该风险。

3.10 逻辑错误

本次扫描没有发现该风险。

3.11 配置不当

本次扫描没有发现该风险。

3.12 内容电子欺骗

本次扫描没有发现该风险。

3.13 外链信息

本次扫描共发现该风险 1 种，共 3 个。

[低风险] 检测出网站存在死链接

URL列表（共3项）

URL	http://39.105.86.118/lib/Login.html?r=
风险评级	低风险
相关域名	http://39.105.86.118/ 访问域名 访问URL

漏洞简述	--

URL	http://39.105.86.118/lib/PhoneBinding.html?r=
风险评级	低风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	--

URL	http://39.105.86.118/lib/Role.html?r=
风险评级	低风险
相关域名	http://39.105.86.118/ 访问域名 访问URL
漏洞简述	--

风险描述

死链就是服务器的地址已经改变了，无法找到当前地址位置。这样会影响到网站的用户体验和搜索引擎优化。

解决方案

去除死链接。