上海络安信息技术有限公司
TECHNOLOGY SHANGHAI LUOAN INFORMATION&TECHNOLOGY CO.,LTD

蓬莱路第二小学
安全检测报告

上海络安信息技术有限公司

二零一七年九月

■ 文档信息

文档名称	蓬莱路第二小学网站安全检测报告		
文档编号	2017092639	**文档属性**	
版本编号	V 3.0	**日　　期**	2017 年 09 月 26 日

■ 适用性声明

本文档是上海络安信息技术有限公司为蓬莱路第二小学网站提交的安全检测报告，供蓬莱路第二小学网站的项目相关人员阅读。

报告目录

1 安全检测概述 - 1 -
2 检测结果综述 - 1 -
2.1 目标信息收集 - 1 -
2.2 威胁等级划分 - 2 -
2.3 漏洞分布情况 - 2 -
2.3.1 风险等级分布 - 2 -
2.3.2 漏洞比例分布 - 3 -
2.3.3 漏洞计数分布 - 3 -
2.4 漏洞摘要统计 - 3 -
2.4.1 高危漏洞 - 3 -
2.4.2 中危漏洞 - 3 -
2.4.3 低危漏洞 - 4 -
2.4.4 信息提示 - 4 -
2.5 受影响 URL 统计排行 - 4 -
2.5.1 威胁级别排名 - 4 -
2.5.2 漏洞数量排名 - 4 -
3 漏洞详细信息 - 4 -
3.1 高危漏洞详细信息 - 4 -
3.2 中危漏洞详细信息 - 4 -
3.3 低危漏洞详细信息 - 4 -
3.3.1 启用了不安全的 HTTP 方法 - 4 -
3.4 提示信息详细信息 - 5 -

1 安全检测概述

网站安全检测的工作内容主要涵盖检测目标、检测范围、检测参考规范、检测原则、风险规避、检测流程、信息收集、检测实施和报告输出。

检测项目主要包含以下几方面：

1)SQL 注入。检测 Web 网站是否存在 SQL 注入漏洞，如果存在该漏洞，攻击者对注入点进行注入攻击，可轻易获得网站的后台管理权限，甚至网站服务器的管理权限。

2) XSS 跨站脚本。检测 Web 网站是否存在 XSS 跨站脚本漏洞，如果存在该漏洞，网站可能遭受 Cookie 欺骗、网页挂马等攻击。

3)网页挂马。检测 Web 网站是否被黑客或恶意攻击者非法植入了木马程序。

4)缓冲区溢出。检测 Web 网站服务器和服务器软件，是否存在缓冲区溢出漏洞，如里存在，攻击者可通过此漏洞，获得网站或服务器的管理权限。

5)上传漏洞。检测 Web 网站的上传功能是否存在上传漏洞，如果存在此漏洞，攻击者可直接利用该漏洞上传木马获得 WebShell。

6)源代码泄露。检测 Web 网络是否存在源代码泄露漏洞，如果存在此漏洞，攻击者可直接下载网站的源代码。

7)隐藏目录泄露。检测 Web 网站的某些隐藏目录是否存在泄露漏洞，如果存在此漏洞，攻击者可了解网站的全部结构。

8)数据库泄露。检测 Web 网站是否在数据库泄露的漏洞，如果存在此漏洞，攻击者通过暴库等方式，可以非法下载网站数据库。

9)弱口令。检测 Web 网站的后台管理用户，以及前台用户，是否存在使用弱口令的情况。

10)管理地址泄露。检测 Web 网站是否存在管理地址泄露功能，如果存在此漏洞，攻击者可轻易获得网站的后台管理地址。

2 检测结果综述

2.1 目标信息收集

检测对象信息

检测对象名称	蓬莱路第二小学网站
检测对象域名	penglai.hpe.cn
检测对象 IP	210.22.116.94;

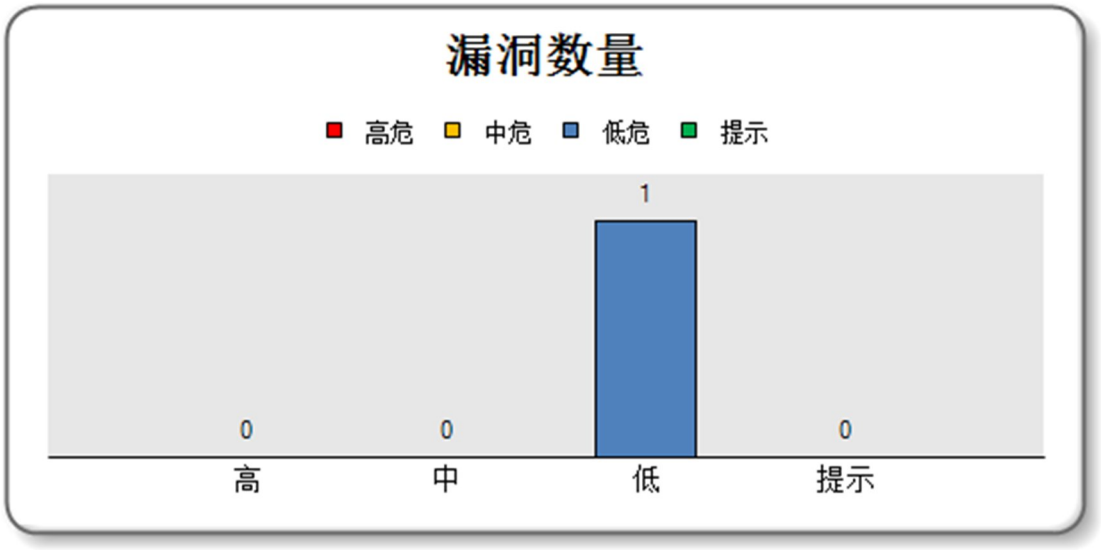
2.2 威胁等级划分

等级标识	威胁等级	等级描述
■■■■	高危	攻击者可以远程执行任意命令或代码，或进行远程拒绝服务攻击。
■■■	中危	攻击者可以远程创建、修改、删除文件或数据，或对普通服务进行拒绝服务攻击。
■■	低危	攻击者可以远程进行受限文件和数据的读取、修改和删除。
■	提示	开放了不必要或危险的服务，攻击者可远程获取系统或应用服务版本等敏感信息。

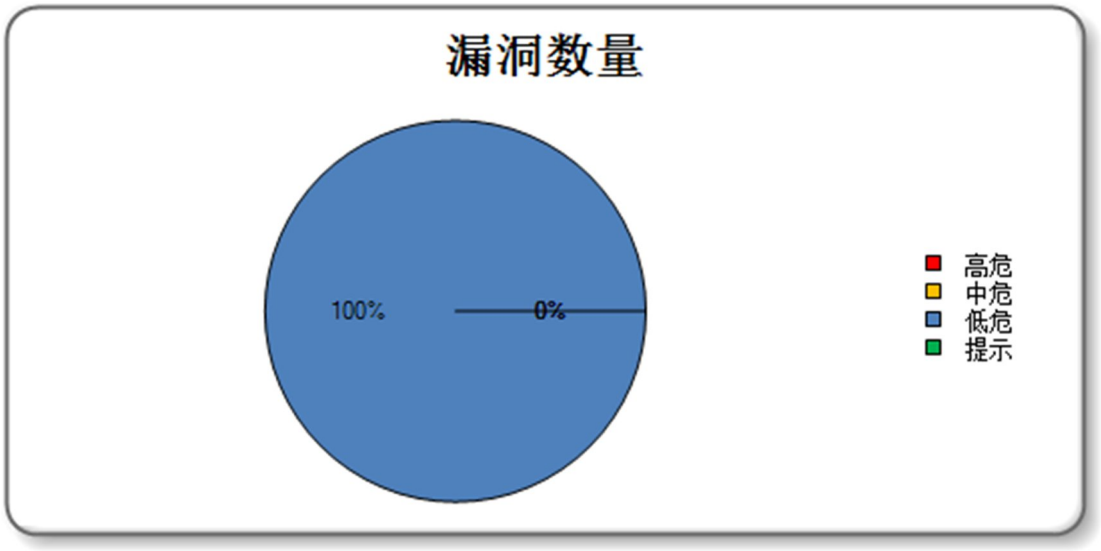
2.3 漏洞分布情况

目标网站存在部分低危漏洞，开放了不必要或危险的服务，攻击者可远程获取系统或应用服务版本等敏感信息，可能对业务造成影响，建议进行关注。

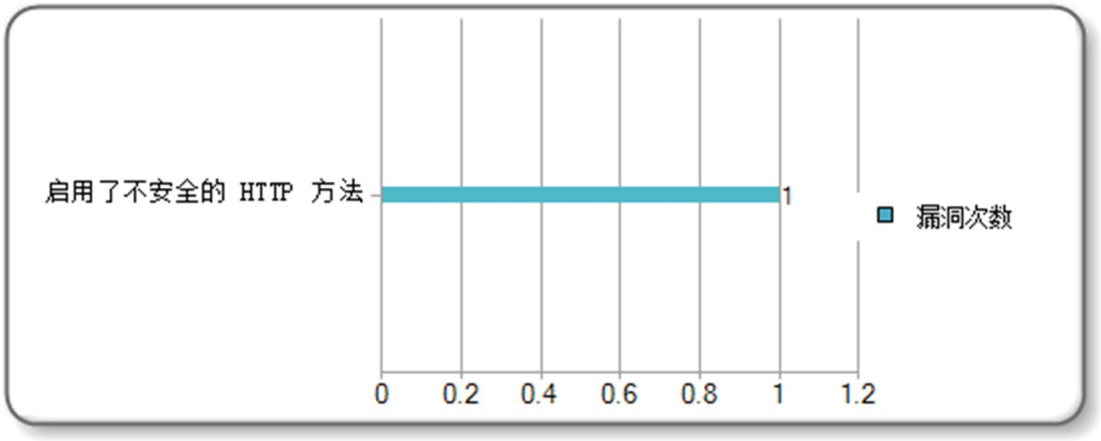
2.3.1 风险等级分布



2.3.2 漏洞比例分布



2.3.3 漏洞计数分布



2.4 漏洞摘要统计

2.4.1 高危漏洞

无

2.4.2 中危漏洞

无

2.4.3 低危漏洞

漏洞 ID	漏洞名称	出现次数
LUOAN-0303	启用了不安全的 HTTP 方法	1

2.4.4 信息提示

无

2.5 受影响 URL 统计排行

2.5.1 威胁级别排名

存在漏洞的 URL（威胁级别排名前十）	漏洞数量	最高威胁级别
http://penglai.hpe.cn:80/	1	

2.5.2 漏洞数量排名

存在漏洞的 URL（漏洞数量排名前十）	漏洞数量	最高威胁级别
http://penglai.hpe.cn:80/	1	

3 漏洞详细信息

3.1 高危漏洞详细信息

无

3.2 中危漏洞详细信息

无

3.3 低危漏洞详细信息

3.3.1 启用了不安全的 HTTP 方法

LUOAN-0303

漏洞名称	启用了不安全的 HTTP 方法		
威胁等级		CVE 编号	不适用
漏洞描述			
可能原因 Web 服务器或应用程序服务器是以不安全的方式配置的 技术描述 似乎 Web 服务器配置成允许下列其中一个（或多个）HTTP 方法（动词）： - DELETE - SEARCH - COPY - MOVE - PROPFIND - PROPPATCH - MKCOL - LOCK - UNLOCK - PUT 这些方法可能表示在服务器上启用了 WebDAV，可能允许未授权的用户对其进行利用。			
修复建议			
如果服务器不需要支持 WebDAV，请务必禁用它，或禁止不必要的 HTTP 方法（动词）。			
受影响的 URL			
http://penglai.hpe.cn:80/			

3.4 提示信息详细信息

无