绿盟科技"远程安全评估系统"安全评估报告

报表生成时间 2021-05-27 16:38:14

目录

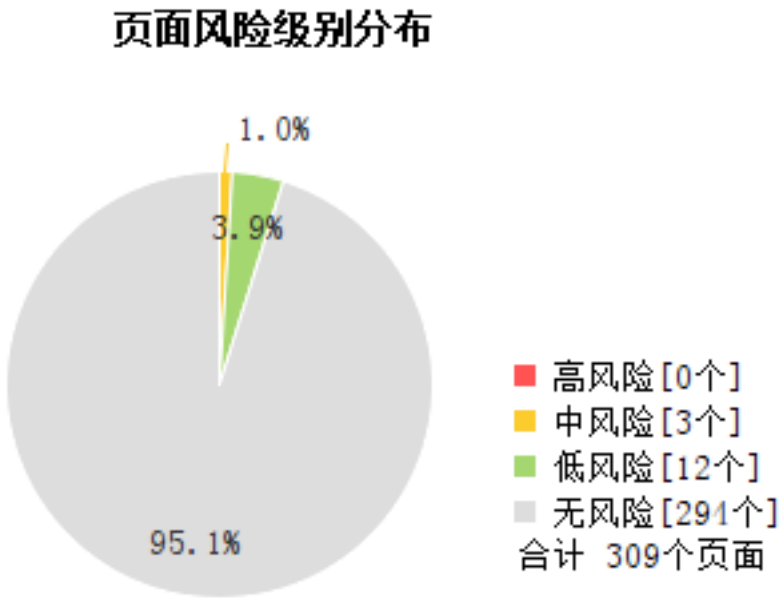
1 综述信息

1.1 任务信息

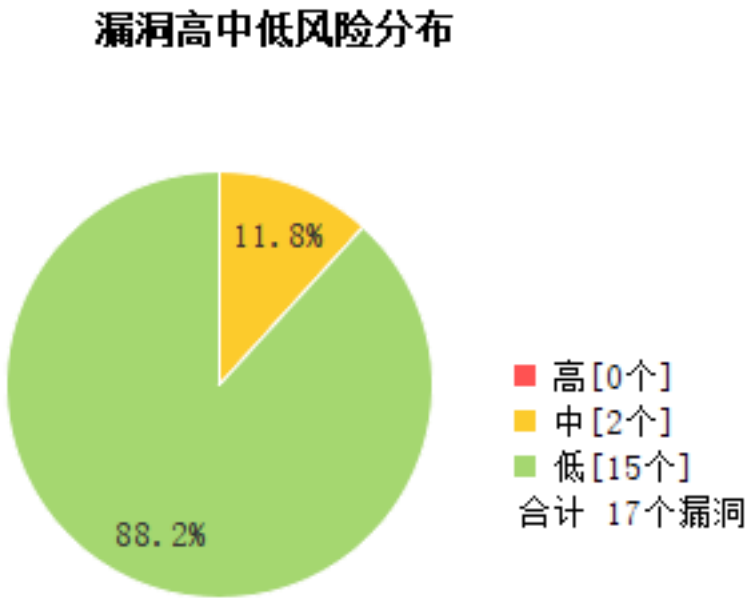
任务名称	《中国医药》杂志
扫描目标	http://www.chinamedicinej.com
任务类型	WEB应用扫描
任务状态	扫描完成
网络风险	风险值：5.3
漏洞扫描模板	自动匹配扫描
域名统计	已扫描域名数：1 非常危险域名：0
信息统计	已爬取文件数：309 有漏洞文件数：15 已扫描链接数：109 已爬取链接数：388
时间统计	开始：2021-05-25 17:40:05 结束：2021-05-25 19:58:35 耗时：2小时18分30秒
下达任务的用户	admin
任务数据来源	本地扫描
任务说明	
版本信息	系统版本：V6.0R04F00SP03 Web插件版本：V6.0R02F00.2003

1.2 风险分布

1.2.1 页面风险级别分布

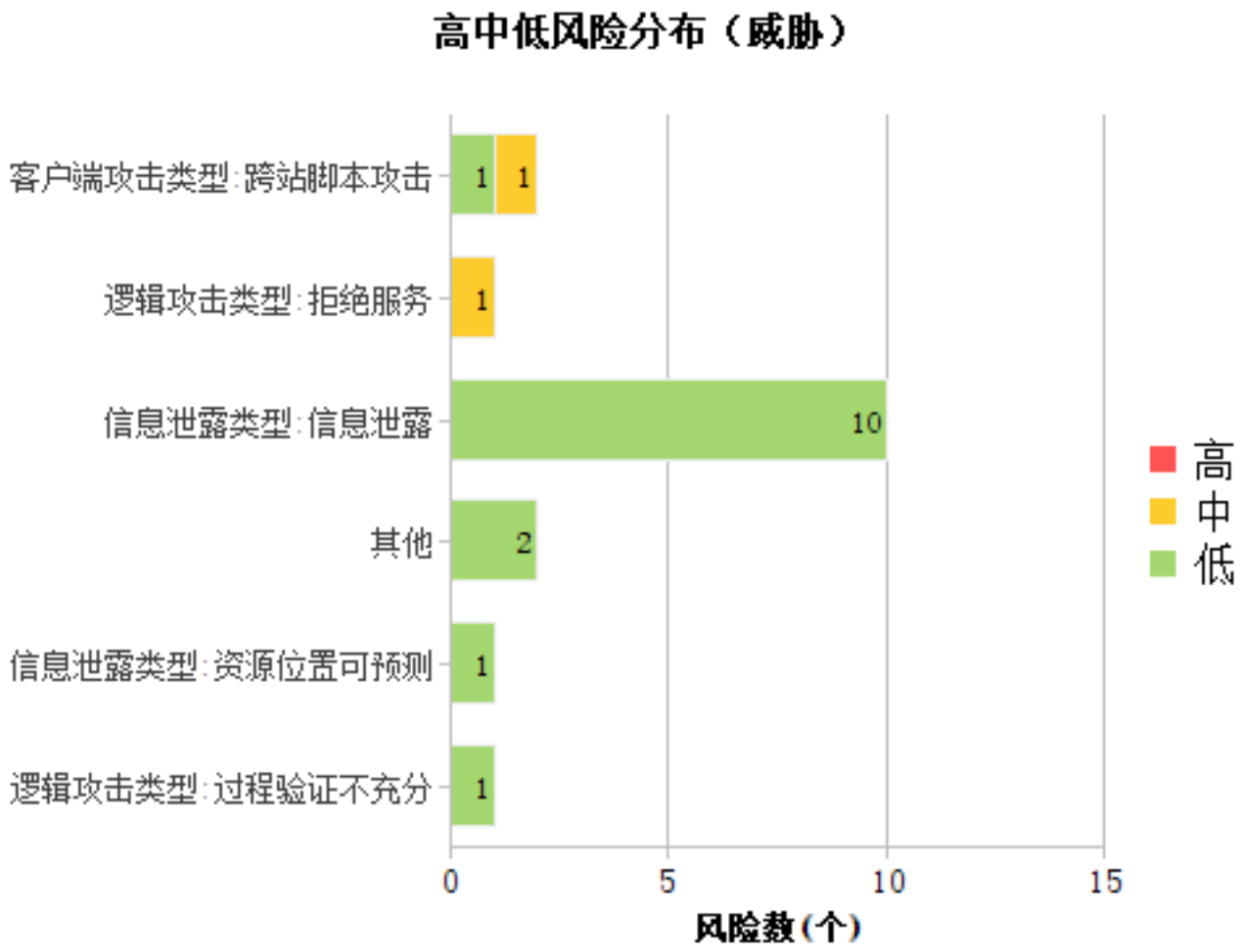


1.2.2 漏洞风险等级分布



1.3 风险分类统计

1.3.1 风险类型



威胁分类	高风险	中风险	低风险	总计
信息泄露类型:资源位置可预测	0	0	1	1
信息泄露类型:信息泄露	0	0	10	10
逻辑攻击类型:过程验证不充分	0	0	1	1
逻辑攻击类型:拒绝服务	0	1	0	1
客户端攻击类型:跨站脚本攻击	0	1	1	2
其他	0	0	2	2
合计	0	2	15	17

1.3.2 高危漏洞最多页面TOP10

2 站点列表

站点名称	已扫描链接数	扫描耗时	高风险（个）	中风险（个）	低风险（个）	已验证（个）	未验证（个）	风险值
http://www.chinamedicinej.com	109	2小时18分16秒	0	3	35	0	27	5.3

异常站点列表	
站点名称	异常原因

3 漏洞列表

3.1 漏洞分布

漏洞类别：中风险[2]低风险[15]
漏洞验证：可验证[0/27]

序号	漏洞名称	影响页面个数	出现次数
1	检测到目标站点存在javascript框架库漏洞【可验证】	2	2
2	检测到目标主机可能存在缓慢的HTTP拒绝服务攻击	1	1
3	检测到目标服务器存在应用程序错误【可验证】	3	5
4	jQuery 存在 XSS 漏洞【可验证】	2	2
5	检测到会话cookie中缺少HttpOnly属性【可验证】	1	1
6	检测到目标X-XSS-Protection响应头缺失【可验证】	1	1
7	检测到目标URL存在电子邮件地址模式【可验证】	6	14
8	检测到目标web应用表单密码类型输入启用了自动完成操作	1	1
9	检测到目标服务器启用了OPTIONS方法【可验证】	1	1
10	检测到目标Referrer-Policy响应头缺失	1	1
11	检测到目标网站存在上传下载相关的目录和文件【可验证】	1	1
12	检测到目标X-Download-Options响应头缺失	1	1
13	检测到目标网站存在无效链接	2	2
14	检查出可以对表单中的隐藏字段进行操纵	2	2
15	检测到目标Strict-Transport-Security响应头缺失	1	1
16	检测到目标X-Permitted-Cross-Domain-Policies响应头缺失	1	1
17	HTTP动词篡改的认证旁路	1	1
合计		28	38

4 参考标准

4.1 单一漏洞风险等级评定标准

危险程度	危险值区域	危险程度说明
高	7 <= 漏洞风险值 <=10	攻击者可以远程操作系统文件、读写后台数据库、执行任意命令或进行远程拒绝服务攻击。
中	4 <= 漏洞风险值 < 7	攻击者可以利用Web网站攻击其他用户，读取系统文件或后台数据库。
低	0 <= 漏洞风险值 < 4	攻击者可以获取某些系统、文件的信息或冒用身份。

分值	评估标准
1	可远程获取Web服务器组件的版本信息。
2	目标Web服务器开放了不必要的服务。
3	可远程访问到某些不在目录树中的文件或读取服务器动态脚本的源码。
4	可远程因为会话管理的问题导致身份冒用。
5	可远程利用受影响的Web服务器攻击其他浏览网站的用户。
6	可远程读取系统文件或后台数据库。
7	可远程读写系统文件、操作后台数据库。
8	可远程以普通用户身份执行命令或进行拒绝服务攻击。
9	可远程以管理用户身份执行命令（受限、不太容易利用）。
10	可远程以管理用户身份执行命令（不受限、容易利用）。

4.2 页面风险级别评定标准

页面风险级别	判定标准
高风险	页面包含的漏洞最高级别为高危
中风险	页面包含的漏洞最高级别为中危
低风险	页面包含的漏洞最高级别为低危
无风险	页面不包含任何漏洞

4.3 站点风险等级评定标准

站点风险等级	站点风险值区域
非常危险	8.0 <= 站点风险值 <= 10
比较危险	5.0 <= 站点风险值 < 8.0
比较安全	1.0 <= 站点风险值 < 5.0
非常安全	0 <= 站点风险值 < 1.0

说明：

1. 按照远程安全评估系统的站点风险评估模型计算每个站点的站点风险值。根据得到的站点风险值参考"站点风险等级评定标准"标识站点风险等等级。
2. 将站点风险等级按照风险值的高低进行排序，得到非常危险、比较危险、比较安全、非常安全四种站点风险等级。

4.4 安全建议

随着越来越多的网络访问通过Web界面进行操作，Web安全已经成为互联网安全的一个热点，基于Web的攻击广为流行，SQL注入、跨站脚本等Web应用层漏洞的存在使得网站沦陷、页面篡改、网页挂马等攻击行为困扰着网站管理者并威胁着网站以及直接用户的安全。基于此，我们可从如下几个方面来消除这些风险，做到防患于未然：

- 对网站的开发人员进行安全编码方面的培训，在开发过程避免漏洞的引入能起到事半功倍的效果。
- 请专业的安全研究人员或安全公司对架构网站的程序和代码做全面的源码审计，修补所有发现的安全漏洞，这种白盒安全测试比较全面、深入，能发现绝大部分的安全问题。
- 在网站上线前，使用Web应用漏洞扫描系统进行安全评估，并修补发现的问题；在网站上线后，坚持更新并使用网站安全监测系统，对整站以及关键页面进行周期和实时监测，及时消除发现的隐患。
- 采用专业的Web安全防火墙产品，可以在不修改网站本身的情况下对大多数的Web攻击起到有效的阻断作用，绿盟科技提供了功能强大的WAF产品，可以满足用户在这方面的需求。

- 建议网络管理员、系统管理员、安全管理员关注安全信息、安全动态及最新的严重漏洞，特别是影响到Web站点所使用的系统和软件的漏洞，应该在事前设计好应对规划，一旦发现系统受漏洞影响及时采取措施。