绿盟网站安全评估服务

——漏洞扫描报告

提交日期：2019-05-21　密级：内部资料

■ 注意事项

适用性：此报告是监测和诊断的评估结果，不保证适用于提交后的时期。
数据有效期：此报告中涉及的数据和文件，绿盟科技将在提交后存档3个月备查。
保密声明：由于此报告包含有关安全细节，请小心处理，避免遗失。
商标信息：绿盟科技、NSFOCUS、绿盟云，是绿盟科技的商标。

■ 联系我们

感谢您选择绿盟科技云安全服务，如您对本次内容有任何意见或建议，请及时反馈给绿盟安全专家团队，具体联系方式如下：
绿盟安全专家团队
北京运营中心地址：北京市海淀区车道沟一号院青东商务区A座10层(邮编：100089)
成都运营中心地址：成都市高新区科园二路10号航利中心2栋2单元14楼(邮编：610041)
安全专家团队7*24小时客户支持热线：400-818-6868转2
邮箱：rs@nsfocus.com
网址：http://cloud.nsfocus.com

一. 扫描概况

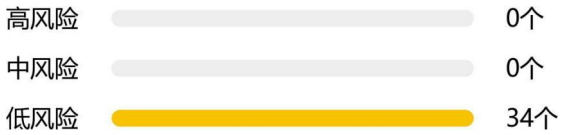
1.1 站点概况

扫描站点	扫描页面数
https://www.baibaoyun.com	393个

整体安全得分

您的网站整体状况非常安全， 建议您继续保持关注。

发现漏洞数 总数：34个

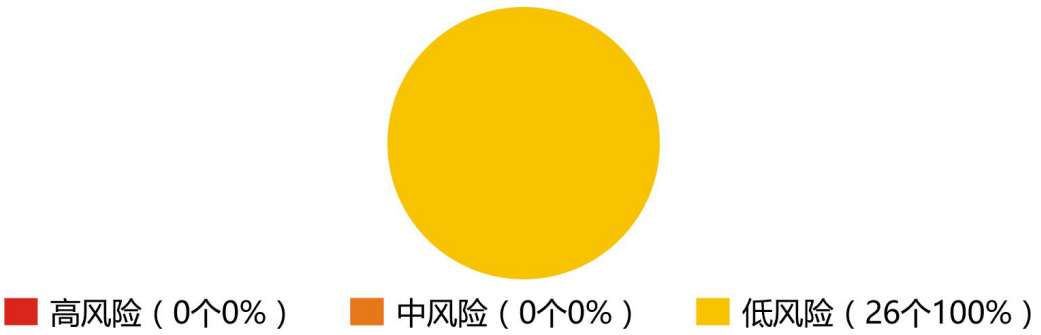


安全专家点评

您的网站整体状况非常安全，请继续保持。

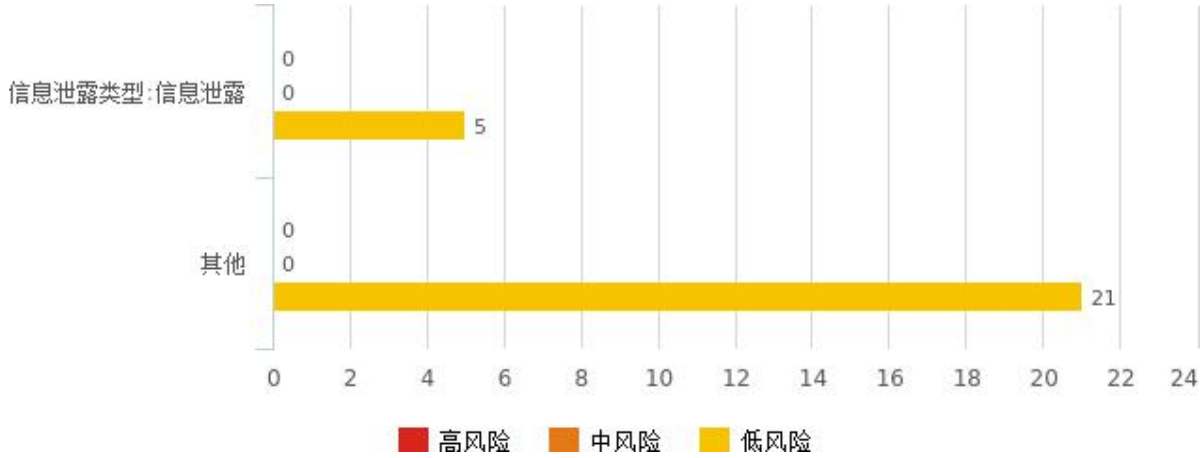
1.2 站点Web漏洞概况

1.2.1 按漏洞危险级别统计



风险等级	漏洞个数	比例
高风险	0	0.0%
中风险	0	0.0%
低风险	26	100.0%

1.2.2 按漏洞类型统计

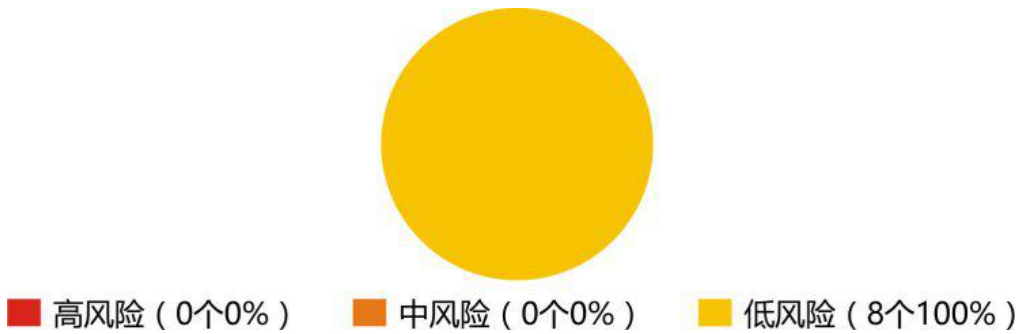


漏洞类型	高风险	中风险	低风险	总计	比例
信息泄露类型:信息泄露	0	0	5	5	19.23%
其他	0	0	21	21	80.77%

1.2.3 高风险漏洞数TOP10页面URL

1.3 站点系统漏洞概况

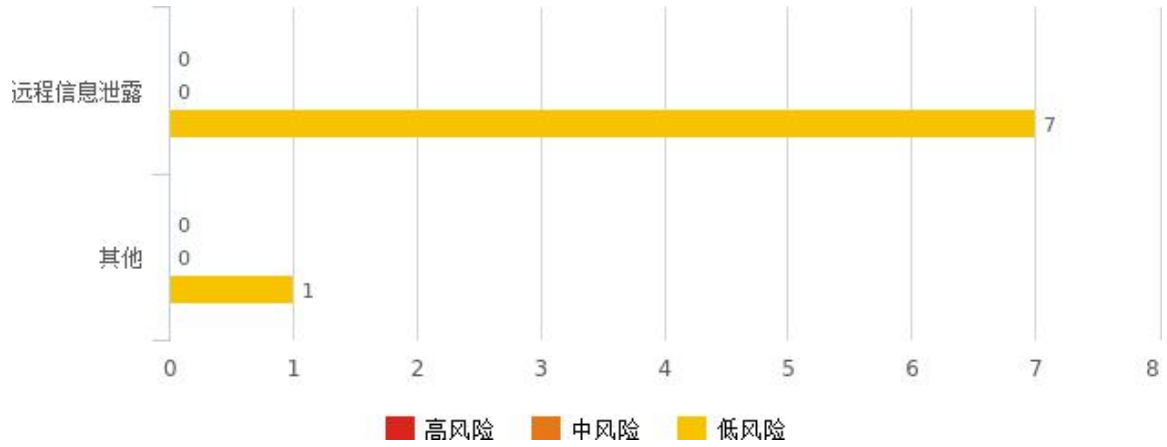
1.3.1 按漏洞危险级别统计



风险等级	漏洞个数	比例
高风险	0	0.0%
中风险	0	0.0%

低风险	8	100.0%

1.3.2 按漏洞类型统计



漏洞类型	高风险	中风险	低风险	总计	比例
远程信息泄露	0	0	7	7	87.5%
其他	0	0	1	1	12.5%

二. Web漏洞详情

2.1 高风险漏洞

2.2 中风险漏洞

2.3 低风险漏洞

■ 检测到目标服务器存在应用程序错误（低风险）

受影响URL	3个
URL	https://www.baibaoyun.com/bbycase/11.html
请求方法	POST
URL	https://www.baibaoyun.com/bbycase/10.html
请求方法	POST
URL	https://www.baibaoyun.com/bbycase/12.html
请求方法	POST
漏洞类型	信息泄露类型:信息泄露
详细描述	如果攻击者通过伪造包含非应用程序预期的参数或参数值的请求，来探测应用程序（如以下示例所示），那么应用程序可能会进入易受攻击的未定义状态。 攻击者可以从应用程序对该请求的响应中获取有用的信息，且可利用该信息，以找出应用程序的弱点。 例如，如果参数字段应该是单引号括起来的字符串（如在 ASP 脚本或 SQL 查询中），那么注入的单引号将会提前终止字符串流，从而更改脚本的正常流程/语法。 错误消息中泄露重要信息的另一个原因，是脚本编制引擎、Web 服务器或数据库配置错误。 以下是一些不同的变体： [1] 除去参数 [2] 除去参数值 [3] 将参数值设置为空值 [4] 将参数值设置为数字溢出（+/- 99999999） [5] 将参数值设置为危险字符，如 ' " ' \")； [6] 将某字符串附加到数字参数值

解决建议	[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。

■ 检测到目标URL存在电子邮件地址模式（低风险）

受影响URL	1个
URL	https://www.baibaoyun.com/about.html
请求方法	GET
漏洞类型	信息泄露类型:信息泄露
详细描述	Spambot 搜寻因特网站点，开始查找电子邮件地址来构建发送自发电子邮件（垃圾邮件）的邮件列表。 如果检测到含有一或多个电子邮件地址的响应，可供利用以发送垃圾邮件。 而且，找到的电子邮件地址也可能是专用电子邮件地址，对于一般大众应是不可访问的。
解决建议	从 Web 站点中除去任何电子邮件地址，使恶意的用户无从利用。

■ 检测到目标网站存在无效链接（低风险）

受影响URL	7个
URL	https://www.baibaoyun.com/bbycase/3.html
请求方法	
URL	https://www.baibaoyun.com/bbycase/3.html
请求方法	
URL	https://www.baibaoyun.com/bbycase/10.html
请求方法	
URL	https://www.baibaoyun.com/bbycase/10.html
请求方法	

URL	https://www.baibaoyun.com/bbycase/8.html
请求方法	
URL	https://www.baibaoyun.com/bbycase/8.html
请求方法	
URL	https://www.baibaoyun.com/bbycase/all.html?page=3
请求方法	

漏洞类型	其他
详细描述	无效链接是指存在于页面中，但其指向的资源已经不存在。 本漏洞属于Web应用安全常见漏洞。
解决建议	将无效链接从页面中删除。

■ 检测到目标URL存在电话号码泄露（低风险）

受影响URL	1个
URL	https://www.baibaoyun.com/about.html
请求方法	GET
漏洞类型	信息泄露类型:信息泄露
详细描述	web应用程序响应中含有电话号码，可能被用于社会工程学攻击。
解决建议	从 Web 站点中除去电话号码，使恶意的用户无从利用。

附录A 网站安全等级评定标准

网站安全等级	网站安全等级得分区域
非常危险	0<=网站安全等级得分<45
比较危险	45<=网站安全等级得分<61
比较安全	61<=网站安全等级得分<85
非常安全	85<=网站安全等级得分<=100

附录B Web漏洞危险等级评定标准

漏洞危险等级	漏洞危险值区域	漏洞危险等级说明
高	7 <= 漏洞危险值 <= 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 <= 漏洞危险值 < 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	1 <= 漏洞危险值 < 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）。

附录C 系统漏洞危险等级评定标准

漏洞危险等级	漏洞危险值区域	漏洞危险等级说明
高	7 <= 漏洞危险值 <= 10	攻击者可以远程执行任意命令或者代码，或进行远程拒绝服务攻击
中	4 <= 漏洞危险值 < 7	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	1 <= 漏洞危险值 < 4	攻击者可以获取某些系统、服务的信息，或读取系统文件和数据。

分值	评估标准
1	可远程获取OS、应用版本信息。
2	开放了不必要或危险的服务，可远程获取系统敏感信息。
3	可远程进行受限的文件、数据读取。
4	可远程进行重要或不受限的文件、数据读取。
5	可远程进行受限文件、数据修改。
6	可远程进行受限重要文件、数据修改。
7	远程进行不受限的重要文件、数据修改，或对普通服务进行拒绝服务攻击。
8	可远程以普通用户身份执行命令或进行系统、网络级的拒绝服务攻击。
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）。