广州市网络与信息安全通报中心
网络安全整改通知书

广东省珠宝玉石及贵金属检测中心：

经查，你单位网站（http://gtc-china.cn）存在网络安全隐患，请立即组织专业力量全面排查并消除网络安全隐患，11月5日前整改完毕，并填写《网络安全隐患处置结果反馈表》盖章后回复我单位。

广州市网络与信息安全通报中心

2018年10月30日

（联系人：钟祖顺；联系电话：83117113）

1．综述

本报告共检查了1个网站， 共访问了107个URL，完成了87468次测试。

1.1．测试策略集

制定系统默认策略

1.2．网站统计列表

本报告包含1个web站点，通过对其进行web安全检测。具体列表如下：

网站名称	服务器类型	安全值	漏洞个数	紧急漏洞个数	备注
gtc-china.cn	Microsoft-IIS/8.5;Win32;ThinkPHP	82	7	0	网络不稳定

注：网络因素问题，可能会影响被扫描网站扫描结果的准确性;

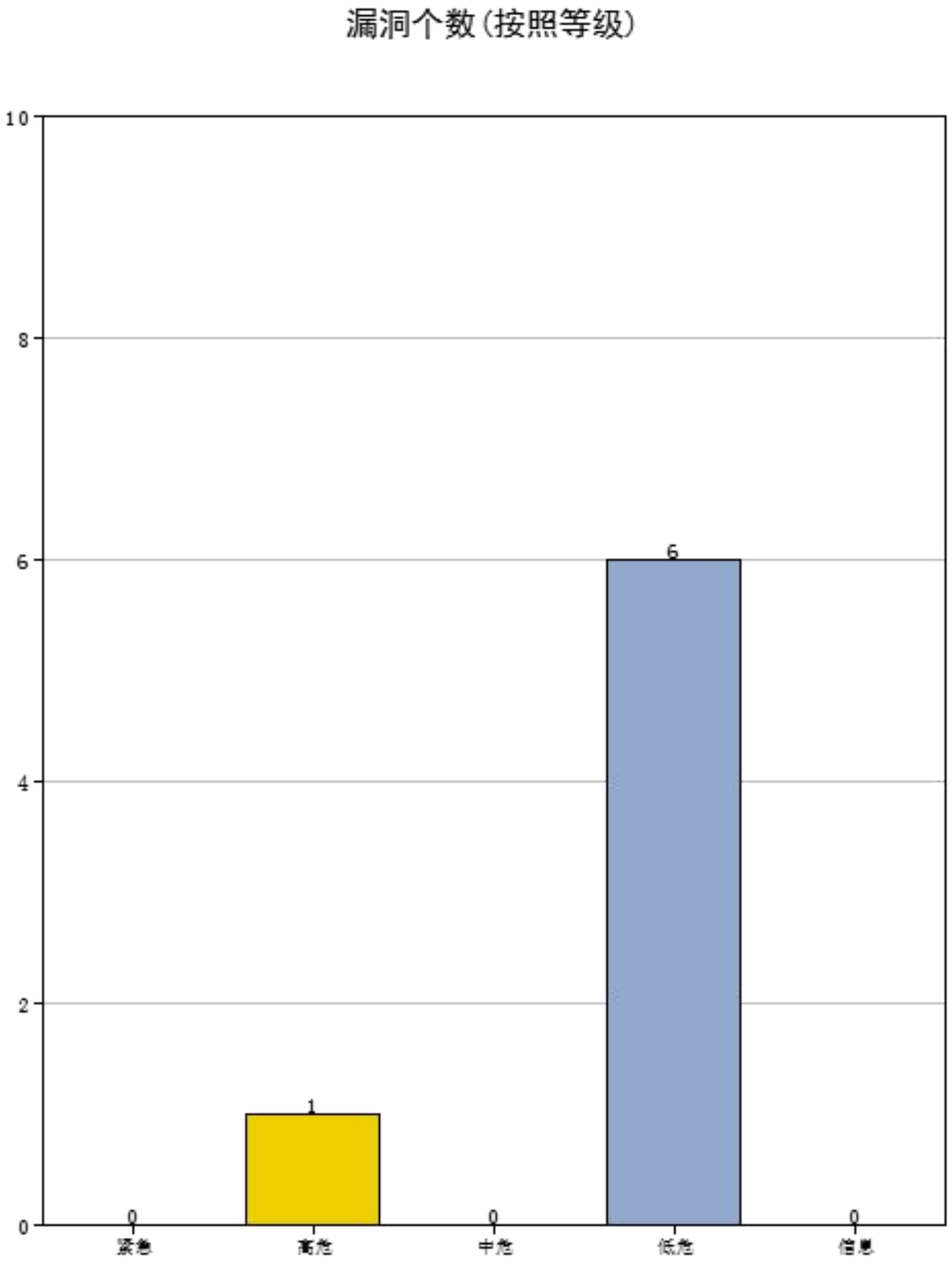
2．网站漏洞详细报告

2.1 . gtc-china.cn:80详细报告

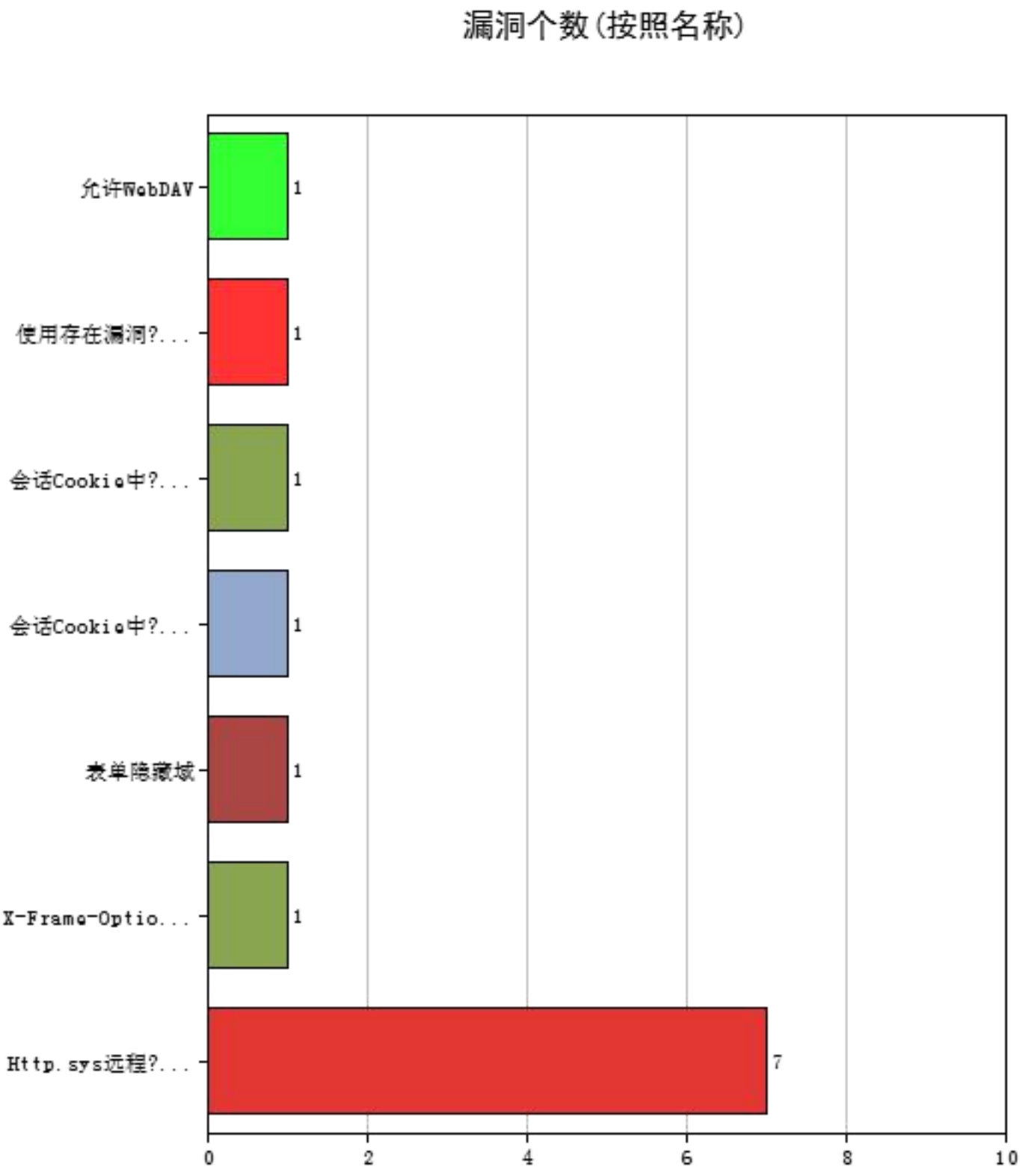
2.1.1．扫描信息列表

名称	内容
扫描对象	gtc-china.cn
主机端口	80
扫描用时(时:分:秒)	1:40:41
服务器信息	Microsoft-IIS/8.5;Win32;ThinkPHP
协　议	http
域　名	gtc-china.cn
已访问URL	107
URL总数	107
网站安全值	82
漏洞个数	7

2.1.2．按照等级统计



2.1.3 . 按照名称统计



2.1.4 . 漏洞详细信息列表

2.1.4.1 . 高危漏洞

2.1.4.1.1 . Http.sys远程代码执行

URL	http://gtc-china.cn/Public/Js/jquery.min.js
弱点	Http.sys Remote Code Execution
等级	高危
漏洞截图	

2.1.4.1.1.1 . 漏洞描述：

漏洞类型：代码执行
弱点描述：
在微软4月14日补丁日发布的补丁中，有一个针对IIS服务器的远程代码执行漏洞危害非常大，安恒信息提醒广大用户注意。
漏洞信息
远程执行代码漏洞存在于 HTTP 协议堆栈 (HTTP.sys) 中，当 HTTP.sys 未正确分析经特殊设计的 HTTP 请求时会导致此漏洞。 成功利用此漏洞的攻击者可以在系统帐户的上下文中执行任意代码。
若要利用此漏洞，攻击者必须将经特殊设计的 HTTP 请求发送到受影响的系统。 通过修改 Windows HTTP 堆栈处理请求的方式，安装更新可以修复此漏洞。
Microsoft 通过协同的漏洞披露渠道了解到此漏洞的信息。 在最初发布此安全公告时，Microsoft 未收到任何表明此漏洞已公开用于攻击用户的信息。

2.1.4.1.1.2 . 修复和改进建议：

一般性的建议：

目前微软官方已经给出修复补丁（3042553），用户安装修复补丁即可。
参考：
https://technet.microsoft.com/zh-CN/library/security/ms15-034.aspx
https://support.microsoft.com/zh-cn/kb/3042553