网络安全漏洞评估报告



2023年6月

# 1.目的

基于风险管理准则对滚财保网络安全漏洞进行分析和控制，保证产品综合剩余风险均处于可接受水平。

# 2.漏洞扫描基本信息

**漏洞扫描工具**

申报产品漏洞评估采用的漏洞扫描工具如下表2-1漏洞扫描工具。

表2-1漏洞扫描工具

|  |  |
| --- | --- |
| 扫描工具 | 基本功能 |
| Acunetix | 自动化的Web应用程序安全测试工具，通过检查 SQL 注入，跨站点脚本(XSS)和其他可利用漏洞等来审核 Web 应用程序。 |
|  |  |

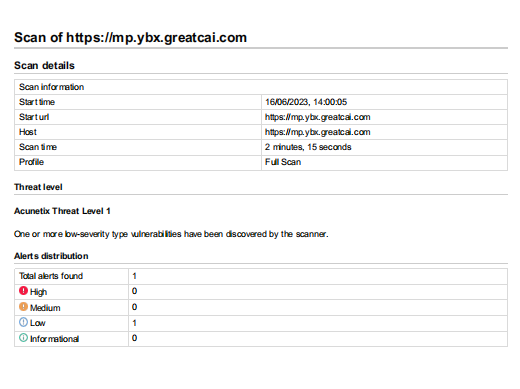
# 3.漏洞扫描过程综述

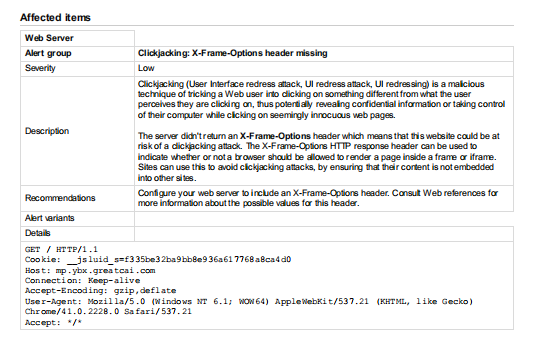
本公司基于表2-2漏洞数据库，通过漏洞扫描工具对滚财保系统的网络安全脆弱性进行检测。

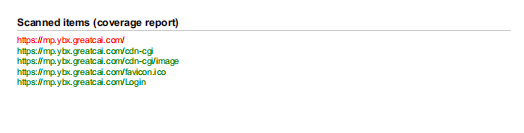
# 漏洞评估

**漏扫报告**









**高危漏洞**

|  |  |
| --- | --- |
| 漏洞编号： | 无 |
| 漏洞名称： | 无 |
| 漏洞危害： | 无 |
| 解决方案： | 无 |

**中危漏洞**

|  |  |
| --- | --- |
| 漏洞编号： | 无 |
| 漏洞名称： | 无 |
| 漏洞危害： | 无 |
| 解决方案： | 无 |

**低危漏洞**

|  |  |
| --- | --- |
| 漏洞编号： | 低危漏洞-1 |
| 漏洞名称： | Clickjacking: X-Frame-Options header missing |
| 漏洞危害： | 网站可能面临点击劫持攻击的风险 |
| 解决方案： | 将WEB服务配置为包含X-Frame-Options标头 |

针对以上漏洞，通过将WEB服务配置为包含X-Frame-Options标头纠正/预防措施进行漏洞修复，修复后再次使用漏洞扫描工具进行漏洞扫描，结果如下:

表4-2漏洞修复后漏洞扫描结果

|  |  |  |  |
| --- | --- | --- | --- |
| 漏洞编号 | 描述 | 漏洞等级 | 是否修复/解决 |
| 低危漏洞-1 | Clickjacking: X-Frame-Options header missing | 低 | 是 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 5漏洞总数及剩余漏洞统计

滚财保系统扫描漏洞总数1个(见表4-1)，采取纠正/预防措施后，剩余漏洞0个。