

**{{report\_center}}**

**{{report\_systemname}}**

**漏洞扫描及渗透验证报告**

**江苏正信信息安全测试有限公司**

**（年份！！！）年（月份！！！）月（日期！！！）日**

1. 验证综述
   1. 目标信息

**漏洞来源IP地址段/域名：**

|  |  |
| --- | --- |
| **目标** | **备注** |
|  |  |
|  |  |
|  |  |

* 1. 已发现漏洞类型

|  |  |
| --- | --- |
| **高危漏洞** | 1. {% if vuls|vul\_statistics(3) ==0 %}无{% endif %}{% for vuls in vuls %}{% if vuls.vul\_level==’3’ %}{{vuls.vul\_name}} 2. {% endif %}{% endfor %} |
| **中危漏洞** | 1. {% if vuls|vul\_statistics(2) ==0 %}无{% endif %}{% for vuls in vuls %}{% if vuls.vul\_level==’2’ %}{{vuls.vul\_name}} 2. {% endif %}{% endfor %} |
| **低危漏洞、信息泄露** | 1. {% if vuls|vul\_statistics(1) ==0 %}无{% endif %}{% for vuls in vuls %}{% if vuls.vul\_level==’1’ %}{{vuls.vul\_name}} 2. {% endif %}{% endfor %} |

* 1. 测试遗留问题

渗透测试过程中未遗留任何威胁信息，未在目标系统遗留任何文件（如木马、后门）。

1.4验证结果详情{% for item in vuls %}

* + 1. {{item.vul\_name}}

**漏洞评级：{% if item.vul\_level ==’3’%}高危{% elif item.vul\_level ==’2’%}中危{% else %}低危{% endif %}**

**漏洞地址：**

{{item.vul\_url}}

**漏洞详情：**

{{item.vul\_describe}}

**造成的危害：**

{{item.vul\_recurrence}}

**修复建议：**

{{item.vul\_modify\_repair}}

{% endfor %}

1. 安全控制建议
   1. 应用控制建议
2. 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。
3. 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。
   1. 主机控制建议
4. 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。
5. 由于其他原因不能及时安装补丁的系统，考虑在网络边界、路由器、防火墙上设置严格的访问控制策略，以保证网络的动态安全。