**附录F**

1. **渗透测试情况统计**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **系统名称** | **高危风险** | **中危风险** | **低危风险** | **合计** |
| «system» | 0 | 2 | 4 | 6 |

1. **测试人员和联系方式**

|  |  |  |  |
| --- | --- | --- | --- |
| **测试人员** | | | |
| **姓名** | **«name»** | **联系方式（邮箱/电话）** | («shouji») |

1. **测试时间**

|  |  |  |  |
| --- | --- | --- | --- |
| **测试时间** | | | |
| **起始时间** | («time») | **结束时间** | («time») |

1. **漏洞统计列表**

|  |  |  |
| --- | --- | --- |
| **序号** | **漏洞名称** | **风险级别** |
| **1** | {{ AAA }} | 中危 |
| **2** | 登录错误消息凭证枚举 | 中危 |

1. **测试结果详述**
   * 1. **敏感数据明文传输（中危）**

**问题描述：**

系统使用了HTTP访问模式，程序自身没有对传输的用户名和密码等敏感信息进行加密。

**风险等级：中危**

**风险分析：**

攻击者或者其他恶意用户通过网络窃听手段监听通讯协议，可以获取正常用户登陆过程，获取用户登陆密码或认证凭据，冒充合法用户登陆。

**影响主机：**

**相关URL：**

**验证过程：**

**安全建议：**

建议在页面认证信息传输之前先对认证信息实现加密，不要使用base64/MD5/SHA1等过于简单的加密算法，建议使用AES或更高强度的算法实现加密。或者使用https

* + 1. **登录错误消息凭证枚举（中危）**

**问题描述：**

应用程序在用户名/密码验证错误时会分别输出不同的错误信息，攻击者可能利用此缺陷进行暴力猜解攻击。

**风险等级：中危**

**风险分析：**

应用程序在用户名/密码验证错误时会分别输出不同的错误信息，攻击者可能利用此缺陷进行暴力猜解攻击。

**影响主机：**

**相关URL：**

**测试过程：**

**安全建议：**

不论用户名错误还是密码错误，都输出同样的错误信息。