**建科网站系统漏洞扫描报告**

**一：扫描对象**

建科网站（测试服）：<http://jianke.ocean-ad.com.cn/>

**二：扫描工具**

腾讯云web漏洞扫描系统

**三：扫描环境**

Windows7系统在线扫描

**四：扫描模式**

深度扫描

**五：扫描频率**

10个HTTP请求每秒

**六：扫描结果**

高危漏洞一个，1个高危漏洞，2个提示

七：漏洞描述：

1.1：漏洞类型：Serv-U FTP服务器权限绕过漏洞 (CVE-2011-4800)，如图一所示；

1.2：漏洞描述：影响版本:Serv-U FTP Server 版本号 低于 11.1.0.5。 RhinoSoft Serv-U FTP Server实现上存在目录遍历漏洞，通过输入特定的路径串可以实现目录遍历，攻击者可以下载、上传、删除FTP根目录外的文件。

1.3：解决方案：Linux/Unix解决方案:Linux不存在该软件。Windows解决方案:升级Serv-U FTP Server到最新版本

1.4漏洞危害：RhinoSoft Serv-U FTP Server实现上存在目录遍历漏洞，通过输入特定的路径串可以实现目录遍历，攻击者可以下载、上传、删除FTP根目录外的文件。

1.5：解决情况：该漏洞是由上传源码工具（以下称为FTP）的版本所造成的，已解决



（图一）

2.1：漏洞类型：FTP Service Enable，如图二所示；

2.2漏洞描述：在该服务器上发现敏感服务端口对外开放存在风险，容易引起安全问题

2.3解决方案：关闭非必需的服务端口，如是必需开放端口，建议修改其默认端口更改为高位端口

2.4漏洞危害：在该服务器上发现敏感服务端口对外开放存在风险，容易引起安全问题

2.5：解决情况：该漏洞是因为目前是测试服，在程序编写的情况下，将所有的网站权限以及端口都对外开放，这样做是为了在编写过程中便于对网站前端后台以及数据的管理；后期上传到正式服务器以后，服务器的端口以及权限都由服务器管理人员自行设置



（图二）

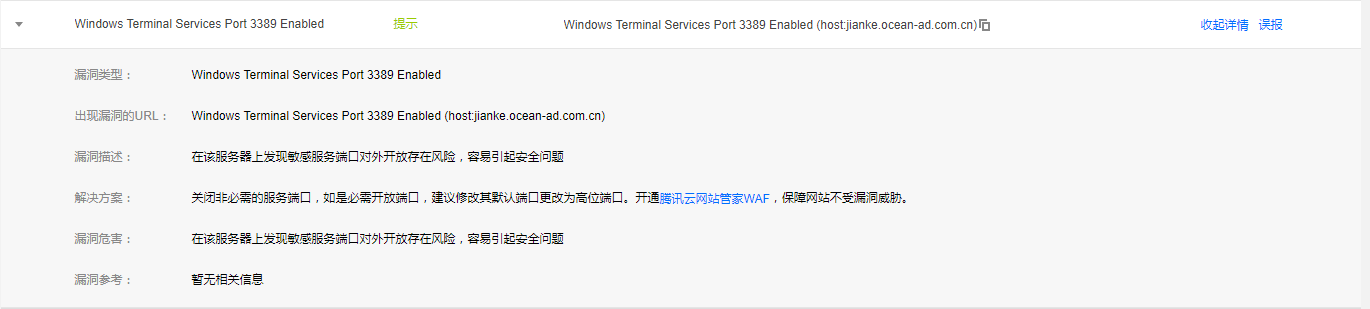
3.1：漏洞类型：Windows Terminal Services Port 3389 Enabled，如图三所示；

3.2：漏洞描述：在该服务器上发现敏感服务端口对外开放存在风险，容易引起安全问题

3.3：解决方案：关闭非必需的服务端口，如是必需开放端口，建议修改其默认端口更改为高位端口

3.4：漏洞危害：在该服务器上发现敏感服务端口对外开放存在风险，容易引起安全问题

3.5：解决情况：该漏洞是因为目前是测试服，在程序编写的情况下，将所有的网站权限以及端口都对外开放，这样做是为了在编写过程中便于对网站前端后台以及数据的管理；后期上传到正式服务器以后，服务器的端口以及权限都由服务器管理人员自行设置（与第二条提示相同）



（图三）

附件：建科网站web漏洞扫描系统报告