网站服务器与网站业务安全评估报告

|  |  |  |  |
| --- | --- | --- | --- |
| **检测人员** | 阮晓龙 | **检测时间** | 2020年04月16日 00时40分 |
| **检测工具** | Nmap 7.70（https://nmap.org） |
| **检测对象** | **主机名** | Project-03-Task-02 | **网络** | IP：10.10.2.105NetMask：255.255.25.0GateWay：10.10.2.1DNS：10.10.3.70 |
| **操作系统** | CentOS 8.1.1911 |
| **检测目的** | 了解操作系统、网站服务、PHP扩展程序、MariaDB数据库、WordPress业务程序的运行情况，全面评估系统与业务的安全性 |
| **检测步骤** | 1、检测操作系统的安全性：验证服务器是否存在版本陈旧或危险端口开放等隐患；2、检测网站服务的安全性：验证网站服务是否存在安全漏洞、敏感目录泄露等隐患；3、检测PHP的安全性：验证PHP是否存在版本陈旧、易受攻击的目录或文件等隐患；4、检测MariaDB的安全性：验证数据库是否存在安全漏洞、空口令或用户越权等隐患；5、检测WordPress的安全性：验证应用程序是否存在版本陈旧、安全漏洞等隐患。 |
| **检测结果** | **检测内容** | **安全隐患** | **参考措施** |
| 操作系统 | SSH、Apache、MySQL服务端口业务未针对特定的网络范围或主机地址进行针对性开放 | 对SSH、Apache、MySQL服务进行针对IP范围或固定IP地址的客户端主机进行端口开放操作 |
| 可查看SSH服务版本信息，进而可根据版本查找该版本可能存在的漏洞信息 | 修改SSH配置文件/usr/sbin/sshd，隐藏其版本信息 |
| 可查看Apache版本信息，进而可根据版本查找该版本可能存在的漏洞信息 | 修改Apache配置文件/etc/httpd/conf/httpd.conf，隐藏版本信息 |
| 可查看MySQL版本信息，进而可根据版本查找该版本可能存在的漏洞信息 | 可对数据库进行编译安装，在编译包中修改或删除数据库版本信息 |
| 可查看操作系统内核版本信息，进而可根据版本查找该版本可能存在的漏洞信息 | 可删除或更改/etc/issue和/etc/issue.net文件信息，从而屏蔽操作系统内核信息 |
| 网站服务 | 存在可对网站服务下敏感目录浏览权限 | 修改Apache配置文件/etc/httpd/conf/httpd.conf，禁止网站目录浏览 |
| 存在OPTIONS网站服务执行方法。可获取服务器支持的HTTP请求方法与检测服务的性能 | 修改Apache配置文件/etc/httpd/conf/httpd.conf，删除OPTIONS方法 |
| PHP | 可查看PHP版本信息，进而可根据版本查找该版本可能存在的漏洞信息 | 修改PHP配置文件/etc/php.ini，隐藏版本信息 |
| MariaDB | 可查看数据库中存在执行权限的用户，黑客可对用户密码进行破解，进而可以对数据库进行执行操作 | 删除数据库中无用的用户权限；修改用户密码，提高密码复杂度 |
| WordPress | 存在版本较低的插件和主题 | 从WordPress网站中下载最新的插件与主题包进行安装替换 |
| **问题记录** |  |
| **评估结果** |  | **审核人员** |  |