课后报告六

为预防统计局网站遭到 SQL 注入攻击，可以对用户输入内容进行检查与验证。检查所输入字符串变量的内容，使用白名单，只接受所需的值，拒绝包含二进制数据、转义序列和注释字符的输入内容，限制用户输入内容的大小和数据类型，对输入内容进行强制转换等。

政务信息发布子模块、站内信息检索子模块、政务受理子模块、统计数据发布子模块、群众意见反馈子模块、业务人员权限管理子模块之间应设置独立的安全区域，做好区域边界的安全防御工作，严格限制重要区域的访问权限并关闭不必要、不安全的服务。

需要禁止重要服务器主动发起外部连接请求，对于需要向外部服务器推送共享数据的，应使用白名单的方式，在出口防火墙加入相关策略，对主动连接 IP 范围进行限制；部署高级威胁监测设备，及时发现恶意网络流量，同时可进一步加强追踪溯源能力，对安全事件发生时可提供可靠的追溯依据；在服务器上部署安全加固软件，通过限制异常登录行为、开启防爆破功能、防范漏洞利用等方式，提高系统安全基线，防范黑客入侵。

定期进行内部人员安全意识培养，禁止将敏感信息私自暴露至公网，禁止点击来源不明的邮件附件等；为 Redis 服务添加密码验证，为 Redis 服务创建单独的 user 和 home 目录，并且配置禁止登陆，低权限运行 Redis 服务；加强日常安全巡检制度，定期对系统配置、系统漏洞、安全日志以及安全策略落实情况进行检查，及时修复漏洞、安装补丁，将信息安全工作常态化；建议配置 VPN 登录的双因素认证，如增加手机短信验证码认证等，严格控制用户登录，防止账号信息被盗用。

将检测到的相关非法域名，通过安全防护设置将其加入黑名单列表，并设置安全策略为阻断访问；系统、应用相关用户杜绝使用弱口令，应使用高复杂强度的密码，加强内部人员安全意识，禁止密码重用的情况出现；增强内部人员密码管理意识，禁止将密码进行本地保存；安装防病毒软件，及时对病毒库进行更新，并且定期进行全面扫描，加强服务器上的病毒发现及清除能力；加强日常安全巡检制度，定期对系统配置、系统漏洞、安全日志以及安全策略落实情况进行检查，及时修复漏洞、安装补丁，将信息安全工作常态化。

受到不法分子的 SOL 注入攻击后，首先要分析攻击事件的类型，SQL 注入攻击进行数据库入侵攻击、数据库篡改攻击属于信息泄漏。分析完攻击事件的类型之后，要针对该事件进行排查，寻找是否存在异常情况，一般的排查流程如下：

一是文件分析排查，按照文件日期、新增文件、可疑或异常文件、最近使用文件、浏览器下载文件进行排查，排查和分析 webshell，核心应用的关联目录文件分析。重点排查分析敏感目录的文件（类/tmp 目录、命令目录/usr/bin/usr/sbin）、新增文件、特殊权限的文件、隐藏的文件（以 "."开头的具有隐藏属性的文件）。

二是进程分析，当前活动进程和远程连接，启动进程和计划任务，使用进程工具进行分析。使用 netstat 网络连接命令，分析可疑端口、可疑 IP、可疑 PID 及程序进程。需要注意如果攻击者获取到了 Root 权限，被植入内核或者系统层 Rootkit 的话，连接可能会被隐藏。

另外还要查看已经建立的网络连接，例如反弹 bash。检查可以监听端口，例如攻击者在本地开启 sock5 代理，然后使用 SSH 反弹 sock5。使用 ps 命令，分析进程。查看可疑进程打开的文件，查看文件类型，使用 ls、strings 以及 stat 查看系统命令是否被替换，查看隐藏进程。

三是系统信息分析，包括环境变量，账号信息，History，系统配置文件。查看分析 history (cat /root/.bash_history)，曾经的命令操作痕迹，以便进一步排查溯源。运气好有可能通过记录关联到用户相关分析、分析任务计划、Linux 开机启动程序、系统用户登录信息、系统路径分析、指定信息检索、查看 ssh 相关目录有无可疑的公钥存在。

四是日志分析，包括操作系统日志分析，具体体现在 Windows 系统上需要通过事件查看器（eventvwr）查看系统日志，在 Linux 系统上系统日志存放在/var/log 中。还有应用日志分析，比如 Access.log 和 Error.log。