外部网站的安全是非常重要的，必须符合一定的安全规范，比较基础的规范如

1. 系统必须保证为正常上线系统，须更新为最新。禁止采用失去技术升级的系统 （如：windows 2003 等）；禁止采用含有已知漏洞的组件、应用程序、框架（如：Struts 2.5 - Struts 2.5.10）、应用程序服务器、web 服务器、数据库服务器和平台定义，以上系统必须 执行安全配置，禁止默认安装。所有的软件应该保持及时更新。
2. 从本机关闭不需要的端口（如：关闭 windows netbios 等服务），设置本机防火墙如 iptable 对于访问的源地址进行限制，同时相关服务设置类似 host.allow,host.deny 等策略；
3. 数据库和应用系统如在同一台服务器，须采用本机回路进行访问，如前端及数据库 分为不同服务器，须设置本机防火墙访问规则，禁止非前端服务器访问数据库网络端口；
4. 使用最低权限的数据库用户作为 web 应用所需，禁止具有不必要的额外权限；
5. 保证系统服务正常与上线系统一致，无各种调试、报错信息（如：断点，printf 等 调试信息）及注释信息，系统需删除系统默认安装的各种例程、文档及管理程序；
6. 对用户输入进行严格有效过滤防止 sql 注入，xss 跨站脚本，命令执行，crsf 跨站请 求伪造等，建议采用白名单过滤策略。
7. 禁止在 HTTP 请求中以明文或可逆编码（如 base64、url 编码等）的形式传递 SQL 语句到后端程序代入执行，禁止由 Web 前端直接生成和传递 SQL 语句到数据库进行执行， 数据库查询必须采用预编译和参数结构化查询。如果程序确实需要将 SQL 语句作为内容 （非可执行代码的形式，如学生毕业设计、代码样例等）到后台，请在项目上线交付前书面 说明相应的功能代码及位置。
8. 控制上传点，对于上传文件类型进行严格控制（禁止用 js 进行控制），同时上传目 录不能有执行权限，原则上不允许有未经登陆验证的上传点。
9. 设置有效的身份认证、会话管理及访问控制机制，防止越权、平行权限及提权等 （禁止利用 js 进行控制及验证）。
10. 密码复杂度要求：系统必须有密码复杂度检查模块，设置有效的验证码或者滑动 等手段防止暴力破解，密码长度须大于 8 位，含字母（大小写）、数字及符号组合，重要系 统须采用二次认证。禁止在数据库中明文存放用户密码，需进行带 salt 的哈希之后入库。对 于多次错误登陆进行封堵。如果长期不登陆默认账号应停用处理；
11. 对于身份信息、单位职务、财务信息、健康信息、讯通信息等等敏感信息禁止在 数据库中明文存放
12. 系统中禁止暴露配置信息（如数据库连接信息），源码备份文件，.git,.svn 仓库等；
13. 须按照标准端口配置 http 或 https 服务，严禁自行设置服务端口不报告。
14. 接到系统安全评测或渗透报告后须提供详实可行的整改报告，经网络与信息中心 验证合格后方可上线。

概括为

禁止使用带有漏洞的框架

禁止使用有漏洞的操作系统

关闭有风险的服务和端口

强力建议使用Https服务 SSL连接

防止XSS攻击

防止CSRF攻击

DAF文字过滤

数据库访问binding IP

数据库用户要用最低权限的用户

数据库定期备份

避免密码的明文传输 RSA加密

密码需要加盐

身份，通讯，财务信息禁止明文储存

上传接口必须登录验证，临时文件夹无执行权限

包含有sql内容的信息（如毕业设计，代码样例等）必须标明 内容和位置

禁止多重登陆

有访问记录，会话控制