项目安全检查规范说明

为了使项目组能够对项目的安全做到全面、细化，也为了促使项目部所有人员形成积极的质量意识，现对于各项目组的安全检查工作做以下规范说明：

1、检查项及标准说明

检查项	检查标准说明	Wiki 链接
备份机制	1. 数据库和程序文件进行异机备份（要求客户要进行异机备份）； 具体要求：异机保留 30 天备份，代码异机每天同步备份 1 次	
密码类	1.保证平台管理员账号的复杂度，不能用 whaty123、111111 等简单密码（密码要求：数字、字母大小写、最低 8 位）； 2.包括服务器登录口令（密码要求：数字、字母大小写、最低 8 位）； 3. 所有 linux 服务器必须安装 denyhost 防暴力破解软件；	
监控类	1.普通项目有项目是否正常能访问的监控（有域名监控、所有项目经理配 360 监控）；	
漏洞类	1.struts 漏洞； 2.XSS 注入漏洞； 3.SQL 注入漏洞； 4.Flash 跨域漏洞修复（新增）； 5.可上传路径 jsp 文件执行权限； 6.Whatyeditor 上传文件目录遍历； 7.Fckeditor 上传文件目录遍历；	1、http://192.168.13.241/hdwiki/index.php?doc-view-960 2、http://192.168.13.241/hdwiki/index.php?doc-view-926 3、http://192.168.13.241/hdwiki/index.php?doc-view-409 4、http://192.168.13.241/hdwiki/

		index.php?doc-view-1160 5、http://192.168.13.241/hdwiki/index.php?doc-view-1146 或者 http://192.168.13.241/hdwiki/index.php?doc-view-1145 以上两个之一，再加上下面这个 http://192.168.13.241/hdwiki/index.php?doc-view-1162 6、http://192.168.13.241/hdwiki/index.php?doc-view-1156 7、http://192.168.13.241/hdwiki/index.php?doc-view-1155
权限控制类	1.超级管理员敏感目录的访问权限控制，比如/admin; 2.除首页外所有目录的权限过滤; 3.项目要使用非 root 账号启动;	1、http://192.168.13.241/hdwiki/index.php?doc-view-1157 2、http://192.168.13.241/hdwiki/index.php?doc-view-1165
错误页面	404 或 500 等错误页面有定制页面，不能直接抛 tomcat 原生页面;	

2、检查频率

1、每季度：检查所有运行项目的 30%，项目覆盖到每个项目组，但具体项目不在检查前进行公布；

2、全年：全年的检查覆盖所有的项目，部分项目将接受全年的两次甚至多次检查；

（注：不包括 webtrn 项目、通用学历项目、北京石油、华中科技）

3、检查方式

1、检查人员：技术经理+运维团队（分工进行）；

2、检查方式：由检查人员根据项目情况制定，多方式结合，包括账号登陆检查、当面进行查看、询问式检查等；

四、结果公布

1、每项目检查后：检查人员将根据检查结果决定是否立即告知，若无问题则不需告知项目组，有问题则告知项目组在此季度截止时完成以上所有检查项的安全工作，若未完成则根据影响的严重程度评定是否设置为质量事故；

2、每季度：全部完成后，由技术经理提交本部门所有项目的检查结果至张晓霞处，由张晓霞进行全部项目检查结果的公布；

五、成绩公布

1、评分：由于各项目经理手中的项目数各不相同，如果采用累积得分的话，可能成绩会有失偏颇，故张晓霞将根据检查结果来计算检查完成率。

2、此安全检查工作：为项目组需要完成的达标任务，树立良好的质量观念。