安全性测试用例

# 1、WEB系统安全性

|  |  |
| --- | --- |
| 说明：执行每一步Steps时，请参照对应编号的Expected Results，得出测试结论 | |
| Test Case001：客户端验证，服务器端验证(禁用脚本调试，禁用Cookies) | |
| Summary：检验系统权限设置的有效性 | |
| Steps：  1、输入很大的数（如4,294,967,269），输入很小的数(负数)。  2、输入超长字符,如对输入文字长度有限制,则尝试超过限制,刚好到达限制字数时有何反应。  3、输入特殊字符如:~!@#$%^&\*()\_+<>:”{}|  4、输入中英文空格，输入字符串中间含空格，输入首尾空格  5、输入特殊字符串NULL,null，0x0d 0x0a  6、输入正常字符串  7、输入与要求不同类型的字符，如: 要求输入数字则检查正值,负值,零值（正零，负零）,小数,字母,空值; 要求输入字母则检查输入数字  8、输入html和javascript代码  9、某些需登录后或特殊用户才能进入的页面,是否可以通过直接输入网址的方式进入；  10、对于带参数的网址,恶意修改其参数,(若为数字,则输入字母,或很大的数字,或输入特殊字符等)后打开网址是否出错,是否可以非法进入某些页面； | Expected Results：   1. 输入的验证码错误。 2. 输入的验证码过长。 3. 输入的验证码错误。 4. 输入的验证码错误。 5. 输入的验证码错误。 6. 输入的验证码正确，成功登陆系统。 7. 输入的验证码错误。 8. 输入的验证码错误。   9、系统权限设置是有效的。 |
| 场景法 | |
| Pass/Fail： | Test Notes： |
| Author： | |
| 说明：执行每一步Steps时，请参照对应编号的Expected Results，得出测试结论 | |
| Test Case002：关于URL | |
| Summary：检验系统防范非法入侵的能力 | |
| Steps：  1、某些需登录后或特殊用户才能进入的页面,是否可以通过直接输入网址的方式进入；  2、对于带参数的网址,恶意修改其参数,(若为数字,则输入字母,或很大的数字,或输入特殊字符等)后打开网址是否出错,是否可以非法进入页面；  3、搜索页面等url中含有关键字的,输入html代码或JavaScript看是否在页面中显示或执行。  4、输入善意字符。 | Expected Results：   1. 不可以直接通过直接输入网址的方式进入。 2. 对于带参数的网址,恶意修改其参数,(若为数字,则输入字母,或很大的数字,或输入特殊字符等)后打开网址出错，不可以非法进入页面。 3. 输入html代码或JavaScript看是不会在页面中显示或执行。 4. 正常进入页面。 5. 系统防范非法入侵的能力强。 |
| 场景法 | |
| Pass/Fail： | Test Notes： |
| Author： | |
| 说明：执行每一步Steps时，请参照对应编号的Expected Results，得出测试结论 | |
| Test Case003：日志记录的完整性 | |
| Summary：检验系统运行的时候是否会记录完整的日志 | |
| Steps：   1. 进行详单查询，检测系统是否会记录相应的操作员。 2. 进行详单查询，检测系统是否会记录相应的操作时间。 3. 进行详单查询，检测系统是否会记录相应的系统的状态。 4. 进行详单查询，检测系统是否会记录相应的操作事项。 5. 进行详单查询，检测系统是否会记录相应的IP地址等。 | Expected Results：   1. 系统会记录相应的操作员。 2. 系统会记录相应的操作时间。 3. 系统会记录相应的系统的状态。 4. 系统会记录相应的操作事项。 5. 系统会记录相应的IP地址。 6. 系统运行的时候会记录完整的日志 |
| 场景法 | |
| Pass/Fail： | Test Notes： |
| Author： | |
| 说明：执行每一步Steps时，请参照对应编号的Expected Results，得出测试结论 | |
| Test Case004：软件安全性测试涉及的方面 | |
| Summary：检验系统的数据备份 | |
| Steps：   1. 是否设置密码最小长度 2. 用户名和密码是否可以有空格和回车？ 3. 是否允许密码和用户名一致 4. 防恶意注册：可含用自动填表工具自动注册用户？ 5. 遗忘密码处理 6. 有无缺省的超级用户？ 7. 有无超级密码？ 8. 密码错误有无限制？ 9. 密码复杂性（如规定字符应混有大、小写字母、数字和特殊字符） | Expected Results：   1. 是。 2. 不可以 3. 否 4. 不可以 5. 是 6. 无 7. 无 8. 有 9. 有 |
| 场景法 | |
| Pass/Fail： | Test Notes： |
| Author： | |
| 说明：执行每一步Steps时，请参照对应编号的Expected Results，得出测试结论 | |
| Test Case005：没有被验证的输入 | |
| Summary：检验输入验证 | |
| Steps：   1. 数据类型（字符串，整型，实数，等） 2. 允许的字符集 3. 最小和最大的长度 4. 是否允许空输入 5. 参数是否是必须的 6. 重复是否允许 7. 数值范围 8. 特定的值（枚举型） 9. 特定的模式（正则表达式） | Expected Results：  对上述输入有控制 |
| 场景法 | |
| Pass/Fail： | Test Notes： |
| Author： | |
| 说明：执行每一步Steps时，请参照对应编号的Expected Results，得出测试结论 | |
| Test Case006：访问控制 | |
| Summary：检验访问控制 | |
| Steps：  1、用于需要验证用户身份以及权限的页面，复制该页面的url地址，关闭该页面以后，查看是否可以直接进入该复制好的地址例：从一个页面链到另一个页面的间隙可以看到URL地址，直接输入该地址，可以看到自己没有权限的页面信息 | Expected Results：  1、不能进入 |
| 场景法 | |
| Pass/Fail： | Test Notes： |
| Author： | |
| 说明：执行每一步Steps时，请参照对应编号的Expected Results，得出测试结论 | |
| Test Case007：输入框验证 | |
| Summary： 验证输入框是否经验证 | |
| Steps：  对Grid、Label、Tree view类的输入框未作验证，输入的内容会按照html语法解析出来 | Expected Results：  对上述输入有控制 |
| 场景法 | |
| Pass/Fail： | Test Notes： |
| Author： | |
| 说明：执行每一步Steps时，请参照对应编号的Expected Results，得出测试结论 | |
| Test Case008：关键数据加密 | |
| Summary： 是否对关键数据进行加密 | |
| Steps：  1、登录界面密码输入框中输入密码，页面显示的是 \*\*\*\*\*，右键，查看源文件是否可以看见刚才输入的密码 | Expected Results：  1、不能看到 |
| 场景法 | |
| Pass/Fail： | Test Notes： |
| Author： | |
| 说明：执行每一步Steps时，请参照对应编号的Expected Results，得出测试结论 | |
| Test Case009：认证请求方式 | |
| Summary：检验认证请求方式 | |
| Steps：  1、认证和会话数据是否使用POST方式，而非GET方式 | Expected Results：  1、采用POST方式 |
| 场景法 | |
| Pass/Fail： | Test Notes： |
| Author： | |
| 说明：执行每一步Steps时，请参照对应编号的Expected Results，得出测试结论 | |
| Test Case010：SQL注入 | |
| Summary：检验是否存在SQL注入 | |
| Steps：  1、 | Expected Results：  1、无效 |
| 场景法 | |
| Pass/Fail： | Test Notes： |
| Author： | |
| 说明：执行每一步Steps时，请参照对应编号的Expected Results，得出测试结论 | |
| Test Case011：文件上传风险 | |
| Summary： | |
| Steps：  1、 | Expected Results：  1、无效 |
| 场景法 | |
| Pass/Fail： | Test Notes： |
| Author： | |
| 说明：执行每一步Steps时，请参照对应编号的Expected Results，得出测试结论 | |
| Test Case012：功能失效、异常带来的安全风险 | |
| Summary： | |
| Steps：  1、 | Expected Results：  1、无效 |
| 场景法 | |
| Pass/Fail： | Test Notes： |
| Author： | |
| 说明：执行每一步Steps时，请参照对应编号的Expected Results，得出测试结论 | |
| Test Case013：操作日志检查 | |
| Summary： | |
| Steps：  1、 | Expected Results：  1、无效 |
| 场景法 | |
| Pass/Fail： | Test Notes： |
| Author： | |
| 说明：执行每一步Steps时，请参照对应编号的Expected Results，得出测试结论 | |
| Test Case014：登录次数限制 | |
| Summary： | |
| Steps：  1、 | Expected Results：  1、无效 |
| 场景法 | |
| Pass/Fail： | Test Notes： |
| Author： | |
| 说明：执行每一步Steps时，请参照对应编号的Expected Results，得出测试结论 | |
| Test Case015：IE回退按钮 | |
| Summary： | |
| Steps：  1、退出系统后，点击IE回退按钮，能否重新回到系统中 | Expected Results：  1、无效 |
| 场景法 | |
| Pass/Fail： | Test Notes： |
| Author： | |
| 说明：执行每一步Steps时，请参照对应编号的Expected Results，得出测试结论 | |
| Test Case016：通信保密性 | |
| Summary： | |
| Steps：  1、测试主要应用系统，查看当通信双方中的一方在一段时间内未作任何响应，另一方是否能自动结束会话；系统是否能在通信双方建立会话之前，利用密码技术进行会话初始化验证（如SSL建立加密通道前是否利用密码技术进行会话初始验证）；在通信过程中，是否对整个报文或会话过程进行加密；  2、测试主要应用系统，通过通信双方中的一方在一段时间内未作任何响应，查看另一方是否能自动结束会话，测试当通信双方中的一方在一段时间内未作任何响应，另一方是否能自动结束会话的功能是否有效；  3、测试主要应用系统，通过查看通信双方数据包的内容，查看系统在通信过程中，对整个报文或会话过程进行加密的功能是否有效。 | Expected Results：  1、 |
| 场景法 | |
| Pass/Fail： | Test Notes： |
| Author： | |
| 说明：执行每一步Steps时，请参照对应编号的Expected Results，得出测试结论 | |
| Test Case017：通信保密性 | |
| Summary： | |
| Steps：  1、a) 应限制单个用户的多重并发会话；  b) 应对应用系统的最大并发会话连接数进行限制；  c) 应对一个时间段内可能的并发会话连接数进行限制；  d) 应根据安全策略设置登录终端的操作超时锁定和鉴别失败锁定，并规定解锁或终止方式；  e) 应禁止同一用户账号在同一时间内并发登录；  f) 应对一个访问用户或一个请求进程占用的资源分配最大限额和最小限额；  g) 应根据安全属性（用户身份、访问地址、时间范围等）允许或拒绝用户建立会话连接；  h) 当系统的服务水平降低到预先规定的最小值时，应能检测和报警；  i) 应根据安全策略设定主体的服务优先级，根据优先级分配系统资源，保证优先级低的主体处理能力不会影响到优先级高的主体的处理能力。 | Expected Results：  1、 |
| 场景法 | |
| Pass/Fail： | Test Notes： |
| Author： | |
| 说明：执行每一步Steps时，请参照对应编号的Expected Results，得出测试结论 | |
| Test Case018：数据备份和恢复 | |
| Summary： | |
| Steps：  1、a) 应提供自动备份机制对重要信息进行本地和异地备份；  b) 应提供恢复重要信息的功能；  c) 应提供重要网络设备、通信线路和服务器的硬件冗余；  d) 应提供重要业务系统的本地系统级热备份。 | Expected Results：  1、 |
| 场景法 | |
| Pass/Fail： | Test Notes： |
| Author： | |

# 2、服务器安全性

|  |  |
| --- | --- |
| 说明：执行每一步Steps时，请参照对应编号的Expected Results，得出测试结论 | |
| Test Case001： | |
| Summary：操作系统账户 | |
| Steps：  1、 | Expected Results：  1、无效 |
| 场景法 | |
| Pass/Fail： | Test Notes： |
| Author： | |
| 说明：执行每一步Steps时，请参照对应编号的Expected Results，得出测试结论 | |
| Test Case002：文件分区格式 | |
| Summary： | |
| Steps：  1、 | Expected Results：  1、无效 |
| 场景法 | |
| Pass/Fail： | Test Notes： |
| Author： | |
| 说明：执行每一步Steps时，请参照对应编号的Expected Results，得出测试结论 | |
| Test Case003：中间件密码 | |
| Summary： | |
| Steps：  1、 | Expected Results：  1、无效 |
| 场景法 | |
| Pass/Fail： | Test Notes： |
| Author： | |
| 说明：执行每一步Steps时，请参照对应编号的Expected Results，得出测试结论 | |
| Test Case004：数据库用户密码 | |
| Summary： | |
| Steps：   1. 密码是否一致？ 2. 密码长度 | Expected Results：  1、 |
| 场景法 | |
| Pass/Fail： | Test Notes： |
| Author： | |
| 说明：执行每一步Steps时，请参照对应编号的Expected Results，得出测试结论 | |
| Test Case005：数据库访问限制 | |
| Summary： | |
| Steps：  1、是否应用IP过滤策略，阻止非法访问 | Expected Results：  1、 |
| 场景法 | |
| Pass/Fail： | Test Notes： |
| Author： | |