功能测试就是对产品的各功能进行php?name=%D1%E9%D6%A4">验证，根据功能**[测试用例](http://www.ltesting.net/html/94/category-catid-94.html" \t "_blank)**，逐项测试，检查产品是否达到用户要求的功能。针对web系统的常用**[测试方法](http://www.ltesting.net/html/news.html" \t "_blank)**如下：      
  
1. 页面链接检查：每一个链接是否都有对应的页面，并且页面之间切换正确。可以使用一些工具，如LinkBotPro、File-AIDCS、HTML Link Validater、Xenu等工具。LinkBotPro不支持中文，中文字符显示为乱码；HTML Link Validater只能测试以Html或者htm结尾的网页链接；Xenu无需安装，支持asp、do、jsp等结尾的网页，xenu测试链接包括内部链接和外部链接，在使用的时候应该注意，同时能够生成html格式的测试报告。如果系统用**[QTP](http://www.ltesting.net/html/13/category-catid-113.html" \t "_blank)**进行自动化测试，也可以使用QTP的页面检查点检查链接。  
  
2. 相关性检查：功能相关性：删除/增加一项会不会对其他项产生影响，如果产生影响，这些影响是否都正确，常见的情况是，增加某个数据记录以后，如果该数据记录某个字段内容较长，可能会在查询的时候让数据列表变形。  
数据相关性：下来列表默认值检查，下来列表值检查，如果某个列表的数据项依赖于其他模块中的数据，同样需要检查，比如，某个数据如果被禁用了，可能在引用该数据项的列表中不可见。  
  
3. 检查按钮的功能是否正确：如新建、编辑、删除、关闭、返回、保存、导入，上一页，下一页，页面跳转，重置等功能是否正确。常见的错误会出现在重置按钮上，表现为功能失效。  
  
4. 字符串长度检查: 输入超出**[需求](http://www.ltesting.net/html/62/category-catid-162.html" \t "_blank)**所说明的字符串长度的内容, 看系统是否检查字符串长度。还要检查需求规定的字符串长度是否是正确的，有时候会出现，需求规定的字符串长度太短而无法输入业务数据。  
  
5. 字符类型检查: 在应该输入指定类型的内容的地方输入其他类型的内容(如在应该输入整型的地方输入其他字符类型),看系统是否检查字符类型。  
  
6. 标点符号检查: 输入内容包括各种标点符号,特别是空格,各种引号,回车键。看系统处理是否正确。常见的错误是系统对空格的处理，可能添加的时候，将空格当作一个字符，而在查询的时候空格被屏蔽，导致无法查询到添加的内容。  
  
7．特殊字符检查：输入特殊符号，如@、#、$、%、!等，看系统处理是否正确。常见的错误是出现在% ‘ " 这几个特殊字符  
  
8. 中文字符处理: 在可以输入中、英文的系统输入中文,看会否出现乱码或出错。  
  
9. 检查信息的完整性: 在查看信息和更新信息时,查看所填写的信息是不是全部更新,更新信息和添加信息是否一致。要注意检查的时候每个字段都应该检查，有时候，会出现部分字段更新了而个别字段没有更新的情况。  
  
10. 信息重复: 在一些需要命名,且名字应该唯一的信息输入重复的名字或ID,看系统有没有处理,会否报错,重名包括是否区分大小写,以及在输入内容的前后输入空格,系统是否作出正确处理。  
  
11. 检查删除功能:在一些可以一次删除多个信息的地方,不选择任何信息,按“delete”,看系统如何处理,会否出错;然后选择一个和多个信息,进行删除, 看是否正确处理。如果有多页，翻页选，看系统是否都正确删除，并且要注意，删除的时候是否有提示，让用户能够更正错误，不误删除。  
  
12. 检查添加和修改是否一致: 检查添加和修改信息的要求是否一致,例如添加要求必填的项,修改也应该必填;添加规定为整型的项,修改也必须为整型.  
  
13. 检查修改重名:修改时把不能重名的项改为已存在的内容,看会否处理,报错.同时,也要注意,会不会报和自己重名的错.  
  
14. 重复提交表单：一条已经成功提交的纪录，返回后再提交，看看系统是否做了处理。对于Web系统来说，可以通过浏览器返回键或者系统提供的返回功能。  
  
15. 检查多次使用返回键的情况: 在有返回键的地方,返回到原来页面,重复多次，看会否出错。  
  
16. 搜索检查: 有搜索功能的地方输入系统存在和不存在的内容,看搜索结果是否正确.如果可以输入多个搜索条件,可以同时添加合理和不合理的条件,看系统处理是否正确，搜索的时候同样要注意特殊字符，某些系统会在输入特殊字符的时候，将系统中所有的信息都搜索到。  
  
17. 输入信息位置: 注意在光标停留的地方输入信息时,光标和所输入的信息会否跳到别的地方。  
  
18. 上传下载文件检查：上传下载文件的功能是否实现，上传文件是否能打开。对上传文件的格式有何规定，系统是否有解释信息，并检查系统是否能够做到。下载文件能否打开或者保存，下载的文件是否有格式要求，如需要特殊工具才可以打开等。上传文件测试同时应该测试，如果将不能上传的文件后缀名修改为可以上传文件的后缀名，看是否能够上传成功，并且，上传文件后，重新修改，看上传的文件是否存在。  
  
19. 必填项检查：应该填写的项没有填写时系统是否都做了处理，对必填项是否有提示信息，如在必填项前加“\*”；对必填项提示返回后，焦点是否会自动定位到必填项。  
  
20. 快捷键检查：是否支持常用快捷键，如Ctrl+C、 Ctrl+V、 Backspace等，对一些不允许输入信息的字段，如选人，选日期对快捷方式是否也做了限制。  
  
21. 回车键检查: 在输入结束后直接按回车键,看系统处理如何,会否报错。这个地方很有可能会出现错误。  
  
22．刷新键检查：在Web系统中，使用浏览器的刷新键，看系统处理如何，会否报错。  
  
23．回退键检查：在Web系统中，使用浏览器的回退键，看系统处理如何，会否报错。对于需要用户验证的系统，在退出登录后，使用回退键，看系统处理如何；多次使用回退键，多次使用前进键，看系统如何处理。  
  
24．直接URL链接检查：在Web系统中，直接输入各功能页面的URL地址，看系统如何处理，对于需要用户验证的系统更为重要。如果系统**[安全](http://www.ltesting.net/html/04/category-catid-104.html" \t "_blank)**性设计的不好，直接输入各功能页面的URL地址，很有可能会正常打开页面。  
  
25．空格检查：在输入信息项中，输入一个或连串空格，查看系统如何处理。如对于要求输入整型、符点型变量的项中，输入空格，既不是空值，又不是标准输入。  
  
26．输入法半角全角检查：在输入信息项中，输入半角或全角的信息，查看系统如何处理。如对于要求输入符点型数据的项中，输入全角的小数点（“。”或“．”，如４．５）；输入全角的空格等。  
  
27．密码检查：一些系统的加密方法采用对字符Ascii码移位的方式，处理密码加密相对较为简单，且安全性较高，对于局域网系统来说，此种方式完全可以起到加密的作用，但同时，会造成一些问题，即大于128的Ascii对应的字符在解密时无法解析，尝试使用“uvwxyz”等一些码值较大的字符作为密码，同时，密码尽可能的长，如17位密码等，造成加密后的密码出现无法解析的字符。  
  
28．用户检查：任何一个系统，都有各类不同的用户，同样具有一个或多个管理员用户，检查各个管理员之间是否可以相互管理，编辑、删除管理员用户。同时，对于一般用户，尝试删除，并重建同名的用户，检查该用户**其它**信息是否重现。同样，提供注销功能的系统，此用户再次注册时，是否作为一个新的用户。而且还要检查该用户的有效日期，过了有效日期的用户是不能登录系统的。容易出现错误的情况是，可能有用户管理权限的非超级管理员，能够修改超级管理员的权限。  
  
29．系统数据检查：这是功能测试最重要的，如果系统数据计算不正确，那么功能测试肯定是通不过的。数据检查根据不同的系统，方法不同对于业务管理平台，数据随业务过程、状态的变化保持正确，不能因为某个过程出现垃圾数据，也不能因为某个过程而丢失数据。  
  
30．系统可恢复性检查：以各种方式把系统搞瘫，测试系统是否可正常迅速恢复。  
  
31．确认提示检查：系统中的更新、删除操作，是否提示用户确认更新或删除，操作是否可以回退（即是否可以选择取消操作），提示信息是否准确。事前或事后提示，对于Update或Delete操作，要求进行事前提示。  
  
32．数据注入检查：数据注入主要是对**[数据库](http://www.ltesting.net/html/61/category-catid-161.html" \t "_blank)**的注入，通过输入一些特殊的字符，如“’”，“/”，“-”等或字符组合，完成对**[SQL](http://www.ltesting.net/html/18/category-catid-418.html" \t "_blank)**语句的破坏，造成系统查询、插入、删除操作的SQL因为这些字符而改变原来的意图。如select \* from table where id = ‘　’ and name = ‘ ’，通过在id输入框中输入“12’-”，会造成查询语句把name条件注释掉，而只查询id=12的记录。同样，对于update和delete的操作，可能会造成误删除数据。当然还有其它一些SQL注入方法，具体可以参考《SQL应用高级SQL注入.doc》，很多程序都是基于页面对输入字符进行控制的，可以尝试跳过界面直接向数据库中插入数据，比如用Jmeter，来完成数据注入检查。  
  
33．刷新检查：web系统中的WebForm. 控件实时刷新功能，在系统应用中有利有弊，给系统的**[性能](http://www.ltesting.net/html/95/category-catid-95.html" \t "_blank)**带来较大的影响。**[测试过程](http://www.ltesting.net/html/97/category-catid-97.html" \t "_blank)**中检测刷新功能对系统或应用造成的影响（白屏），检查控件是否回归默认初始值，检查是否对系统的性能产生较大影响（如每次刷新都连接数据库查询等）。  
  
34．事务检查：对于事务性操作，断开**[网络](http://www.ltesting.net/html/77/category-catid-377.html" \t "_blank)**或关闭程序来中断操作，事务是否回滚。  
  
35．时间日期检查：时间、日期验证是每个系统都必须的，如2006-2-29、2006-6-31等错误日期，同时，对于管理、财务类系统，每年的1月与前一年的12月（同理，每年的第1季度与前一年的第4季度）。另外，对于日期、时间格式的验证，如2006年2月28日、2006-2-28、20060228等。日期检查还要检查日期范围是否符合实际的业务，对于不符合时间业务的日期，系统是否会有提示或者有限制。  
  
36．多浏览器验证：越来越多的各类浏览器的出现，用户访问Web程序不再单单依赖于Microsoft Internet Explorer，而是有了更多的选择：Maxthon、Firefox、Tencent Traveler等，考虑使用多种浏览器访问系统，验证效果。  
  
37．安装测试：对于C/S架构的系统，安装程序的测试是一个重要方面，安装程序自动化程度、安装选项和设置（验证各种方案是否都能正常安装）、安装过程中断测试、安装顺序测试（分布式系统）、修复安装及卸载测试。  
  
38．文档测试：主要是对用户使用手册、产品手册进行测试，校验是否描述正确、完整，是否与当前系统版本对照，是否易理解，是否二义性等。  
  
39．测试数据检查：事实告诉我们，测试数据比代码更有可能是错的，因此，当测试结果显示有错误发生的时候，怀疑代码错误前要先对测试数据检查一遍。  
  
40．请让我的机器来运行：在某些项目中，出现一个病态的问题：系统没有问题呀，它在我的机器上是能够通过的。这就说明了其中存在着和环境相关的BUG。“是否所有的一切都受到了**[版本控制](http://www.ltesting.net/html/63/category-catid-163.html" \t "_blank)**工具的管理？”、“本机的**[开发](http://www.ltesting.net/html/4/category-catid-4.html" \t "_blank)**环境和**[服务器](http://www.ltesting.net/html/78/category-catid-378.html" \t "_blank)**的环境是否一样？”、“这里是否存在一个真正的BUG，只不过是在其他的机器里偶然出现？”。所有的测试必须在所有系统要求的机器上运行通过，否则的话，代码就可能存在问题。  
  
41．Ajax技术的应用：Ajax有很多优点，但也有很多缺点，如果利用优点、避免缺点，是我们对新的Web2.0应用的一个挑战。而Ajax的应用最直接的问题就是用户体验，用户体验的效果直接关系到是否使用Ajax技术。“会做，并不意味着应该做、必须做”，这就是对Ajax技术的很重要的注解。  
  
42．Ajax技术的应用：Ajax采用异步调用的机制实现页面的部分刷新功能，异步调用存在异常中断的可能，尝试各种方法异常中断异步的数据调用，查看是否出现问题。在这里遇到的一个问题就是对日期控件的操作，已经如果页面数据较多的时候的刷新。  
  
43．脚本错误：随着Ajax、IFrame等异步调用技术的发展，**[Java](http://www.ltesting.net/html/54/category-catid-154.html" \t "_blank)**scrīpt技术也越来越受到开发人员的重视，但Javascrīpt存在调试困难、各浏览器存在可能不兼容等问题，因此在Web系统中