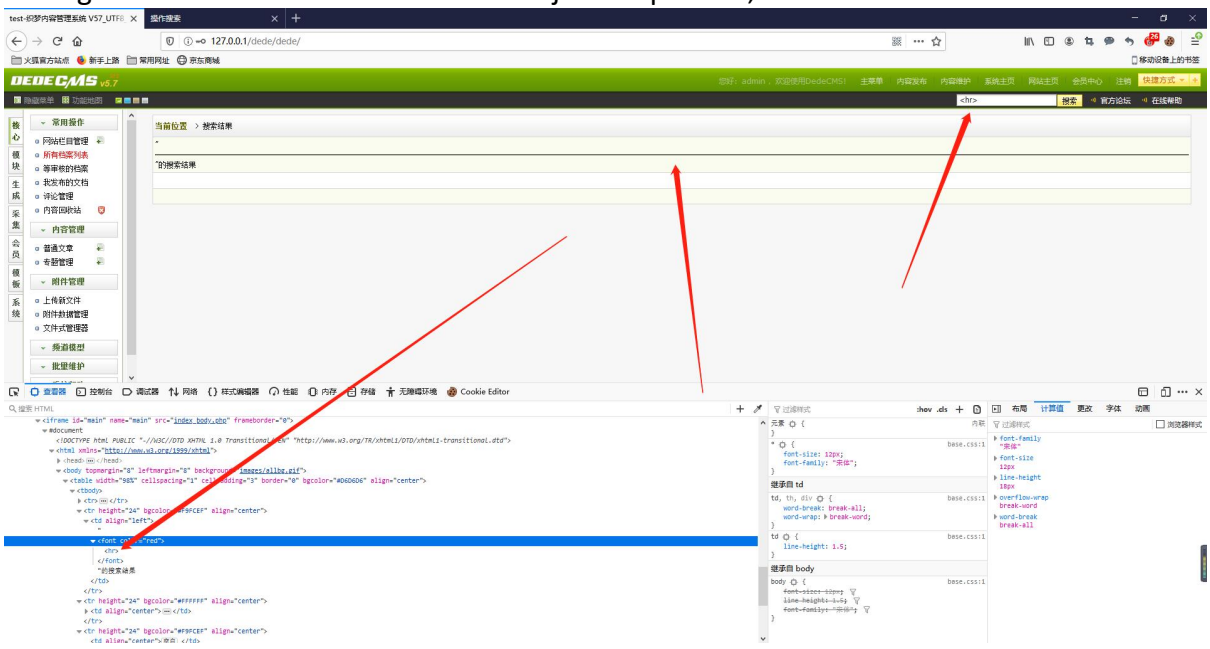
XSS and CSRF Vulnerability exists in the file of DedeCMS V5.7 SP2 version, which can be executed javascript code.

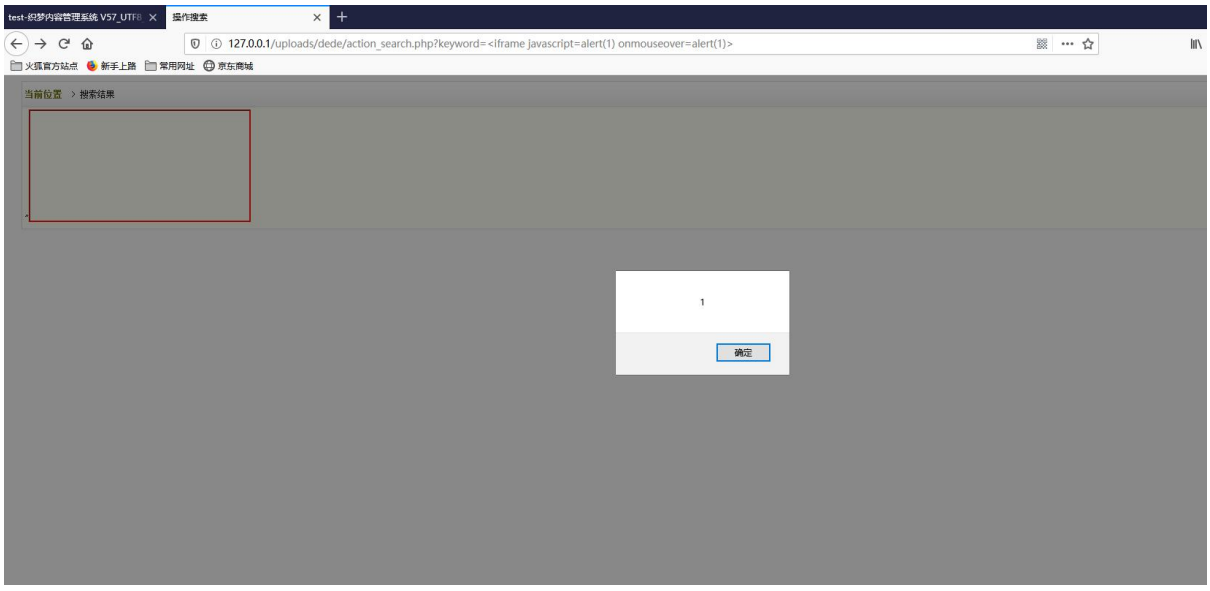
Payload:

/uploads/dede/action_search.php?keyword=%3Ciframe%20javascript=alert(1)%20onmouseover=[other javascript function] %3E

The “keyword” parameter exists vulnerability

When common user send this malicious URL to the web manager and request it, the web manager could be executed the malicious javascript code,





File:/uploads/dede/search_keywords_main.php (begin with line 67)

```
67  //获得特定的关键字列表
68  function GetKeywordList($dsql,$pageno,$pagesize,$orderby='aid')
69  {
70      global $cfg_phpurl;
71      $start = ($pageno-1) * $pagesize;
72      $printhead ="<form name='form3' action=\"search_keywords_main.php\"
            method=\"post\">
73      <input name=\"dopost\" type=\"hidden\" value=\"\">
74      <table width='98%' border='0' cellpadding='1' cellspacing='1'
            bgcolor='#cfcfcf' style='margin-bottom:3px' align='center'>
75      <tr align='center' bgcolor='#FBFCE2' height='24'>
76        <td width='5%'>选择</td>
77        <td width='6%' height='23'><a href='#'
              onclick=\"ReloadPage('aid')\"><u>ID</u></a></td>
78        <td width='20%'>关键字</td>
79        <td width='35%'>分词结果</td>
80        <td width='6%'><a href='#'
              onclick=\"ReloadPage('count')\"><u>频率</u></a></td>
81        <td width='6%'><a href='#'
              onclick=\"ReloadPage('result')\"><u>结果</u></a></td>
82        <td width='15%'><a href='#'
              onclick=\"ReloadPage('lasttime')\"><u>最后搜索时间</u></a></td>
83        <td>管理</td>
84      </tr>\r\n
```

Filter function called XSSClean defined in the file name config.php, but this function didn’t filter html tag and javascript event seriously, so you could make web manager executed javascript code by using “onmouseover” or other javascript event.

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