白云新闻搜索
解题思路

DBAppSecurity Lab

题目描述

中国又出现了一个搜索巨头！据报道，中国网络大亨小明近日编写了一个搜索引擎，叫白云新闻搜索，具体链接在下方，该搜索链接功能欠打，界面乏力，小明出一包辣条悬赏漏洞，豪言入侵高手都去试试，你服不服？不服就去试试呗~(答案为flag{}形式，提交{}内内容即可)

步骤一

- 首先拿到一个页面，是新闻搜索页面

步骤二

- 试一下默认的搜索项，搜出了包含“内容”两个字的五条新闻.

步骤三

- 尝试注入，得到错误提示

步骤四

- 另一个注入口我们也试试，发现被限定为数字。

步骤五

- 看源码，发现是有前端校验的。那么这个地方有可能有注入点，正则分析。

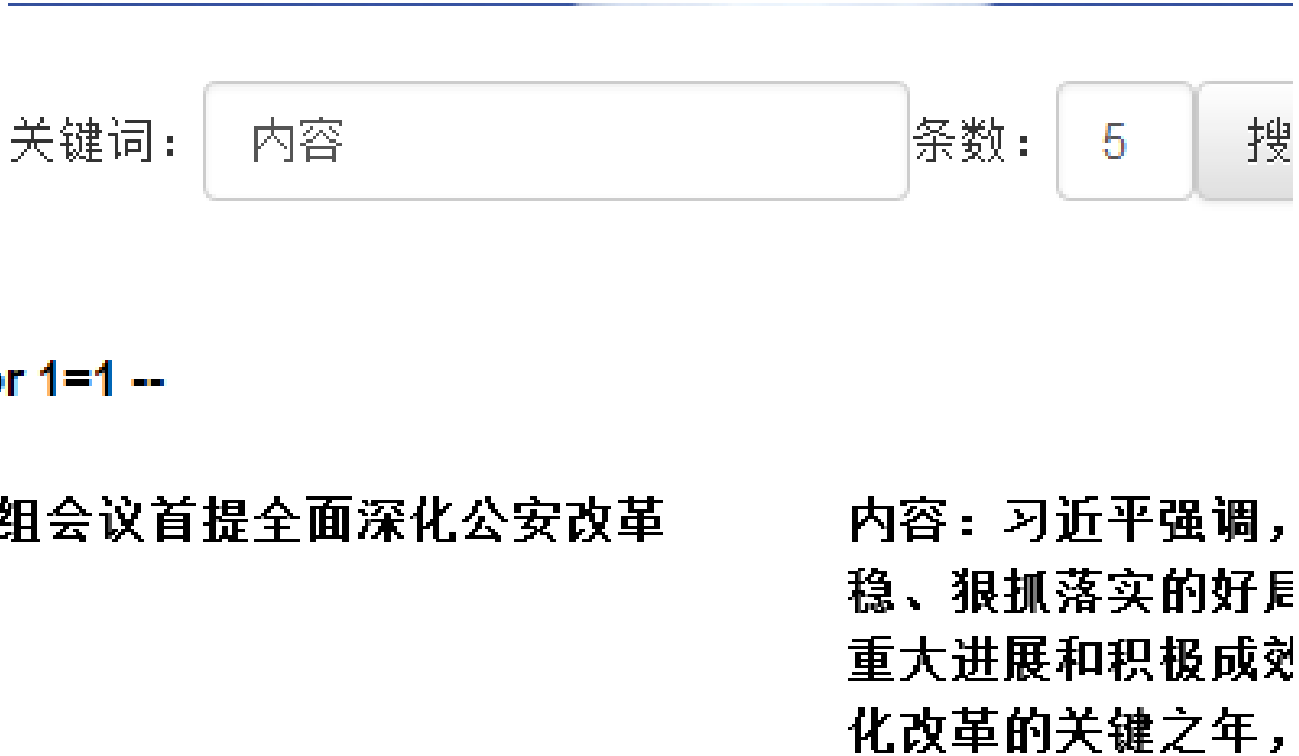
```
function myFunction()
{
    var x=document.getElementById("number").value;
var a=document.getElementById("word").value;
var b=a.replace(/[\ |\~|\`|\!|\@|\#|\$|\%|\^|\&|\*|\(|\)|\-|\_|\+|\=|\||\\|\[|\]|\{|\}|\;|\:|\"|\'|\,|\<|\.|\
if(a.length!=b.length)
{
  alert("请输入正确字符。");
  document.getElementById("number").value = '';
  document.getElementById("word").value = '';
}
else if(isNaN(x))
{
  alert("请输入数字。");
  document.getElementById("number").value = '';
}

}


<script>
```

步骤六

- 在火狐浏览器中禁用javascript，回到原来的页面刷新，可以输入各类字符了，看来是前端校验。

步骤七

- 通过简单判断发现存在搜索型注入。



步骤八

- 通过注入从数据库中获得flag。