广西动环工作台(全量)渗透测试报告

2026年01月06日

1. 概述

1.1 测试概述

本次测试对 广西动环工作台 系统进行 全量 渗透测试，主要测试范围包括 全量 ， 共发现漏洞 3 个。

1.2 测试范围

系统名称	广西动环工作台
测试版本	GXEMS1.0.12.0
测试目标	http://10.1.203.120:8380/spider/web
测试环境	测试环境

1.3 测试时间

测试人员	联系方式	测试IP	测试类型	测试时间
田畅(tianchang)	13520314280	10.8.65.241	初测	2026年01月06日

1.4 规范要求

- 报告中**不体现账号密码**信息；
- 漏洞需在**测试描述**中指明**功能模块**；
- 全站漏洞复测采用**抽样验证**。

2. 测试用例（用例固定）

测试阶段	测试名称	漏洞
信息收集	web服务识别测试	组件默认信息泄露
信息收集	审查网页内容以发现信息泄露	注释中信息泄露
信息收集	web服务识别测试	系统信息泄露
信息收集	审查网页内容以发现信息泄露	JS map文件泄露
信息收集	审查网页内容以发现信息泄露	JS文件信息泄露
信息收集	web服务识别测试	组件版本信息泄露
信息收集	第三方组件检查	第三方组件漏洞
授权	授权机制绕过	水平越权
授权	授权机制绕过	垂直越权
授权	授权机制绕过	未授权访问
授权	目录遍历和文件包含测试	任意文件读取
授权	目录遍历和文件包含测试	远程包含
授权	目录遍历和文件包含测试	本地包含
授权	目录遍历和文件包含测试	目录遍历
错误处理	错误处理不当测试	报错页面信息泄露
数据保护	敏感数据安全	语音API泄露
数据保护	敏感数据安全	地图Key泄露
数据保护	敏感数据安全	敏感信息未脱敏
加密算法	传输层TLS测试	SSL版本漏洞
加密算法	传输层TLS测试	明文传输
加密算法	传输层TLS测试	心脏出血漏洞
数据验证	XPATH注入	xpath注入漏洞
数据验证	SSI注入	SSI注入漏洞
数据验证	IMAP SMTP注入	IMAP、SMTP注入漏洞

数据验证	代码注入	代码注入漏洞
数据验证	ldap注入	ldap注入漏洞
数据验证	SQL注入	SQL注入漏洞
数据验证	参数污染漏洞	参数污染漏洞
数据验证	命令注入	命令注入漏洞
数据验证	Host头注入	Host头注入漏洞
数据验证	跨站脚本攻击	存储型xss
数据验证	服务端模板注入	服务端模板注入漏洞
数据验证	服务端请求伪造	SSRF 漏洞
数据验证	反序列化	反序列化漏洞
数据验证	xml注入	xml注入漏洞
数据验证	url重定向	url重定向
数据验证	跨站脚本攻击	反射型xss
会话管理	跨站请求伪造测试	CSRF漏洞
会话管理	Cookie属性测试	HttpOnly未设置
会话管理	登出功能测试	会话未失效
会话管理	登出功能测试	密码修改会话未失效
会话管理	登出功能测试	会话未超时
会话管理	会话固定测试	会话固定
配置和部署	HTTP 请求走私测试	HTTP 走私漏洞
配置和部署	应用平台配置测试	列目录
配置和部署	应用平台配置测试	Debug模式未关闭
配置和部署	应用平台配置测试	默认文件未删除
配置和部署	备份、未链接文件测试	备份文件未删除
配置和部署	备份、未链接文件测试	元数据目录未删除
配置和部署	HTTP方法测试	XST漏洞
配置和部署	云存储测试	云存储列目录
身份鉴别管理	用户枚举与猜测(注册、登录等)	结构性账号用户枚举

身份鉴别管理	用户枚举与猜测(注册、登录等)	不同响应用户枚举
身份鉴别管理	用户枚举与猜测(注册、登录等)	错误信息用户枚举
浏览器端	DOM型跨站测试	DOM型XSS
浏览器端	点击劫持测试	点击劫持漏洞
浏览器端	Flash跨站测试	Flash跨站漏洞
浏览器端	CORS测试	CORS漏洞
逻辑漏洞	业务逻辑数据验证测试	1分钱漏洞
逻辑漏洞	业务逻辑数据验证测试	提示当前接口缺失参数
逻辑漏洞	业务逻辑数据验证测试	正负值对冲
逻辑漏洞	伪造请求测试	业务流程跳跃
逻辑漏洞	上传文件测试	文件上传漏洞
逻辑漏洞	重放攻击测试	重放攻击漏洞
逻辑漏洞	上传恶意文件测试	pdf-xss漏洞
认证	认证绕过测试	短信验证码绕过
认证	修改密码\重置密码测试	任意密码修改
认证	密码复杂度测试	密码复杂度不足
认证	第三方认证测试	短信炸弹
认证	认证绕过测试	JWT漏洞
认证	认证绕过测试	无双因素认证
认证	认证绕过测试	图形验证码绕过
认证	认证绕过测试	会话ID可预测
认证	账号锁定机制测试	账号解锁绕过
认证	账号锁定机制测试	密码爆破
认证	默认凭证测试	默认密钥
认证	默认凭证测试	默认账号密码
认证	凭证测试	凭证URL传输
认证	凭证测试	密码明文传输

AI	注入攻击	提示词注入
拒绝服务	DOS	拒绝服务攻击

3. 漏洞详情及整改建议

3.1 未授权访问

测试描述：用户无需认证即可访问敏感资源。

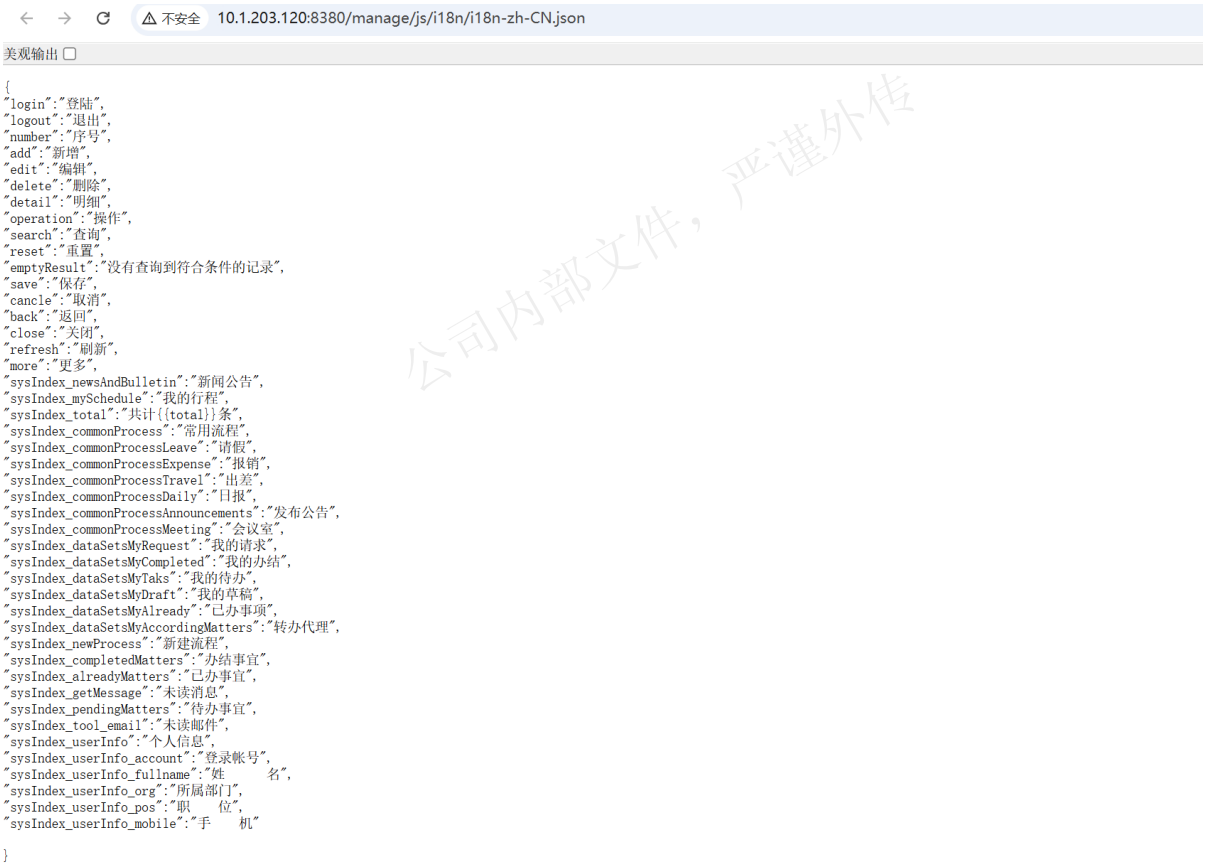
测试地址：http://10.1.203.120:8380/manage/js/i18n/i18n-zh-CN.json

风险程度：「高」

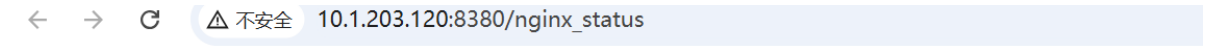
修复建议：
1.实施严格的访问控制。
2.严格验证用户权限。

问题截图：

请全量排查

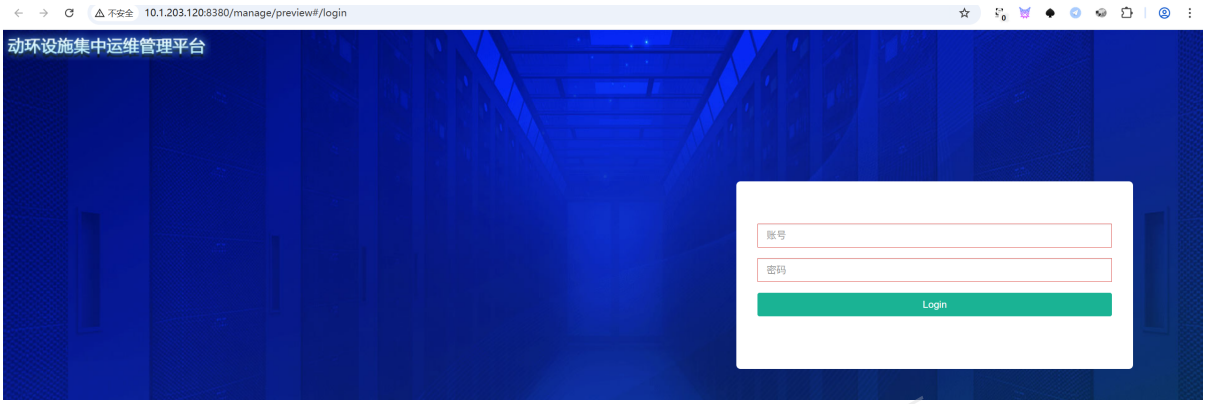


http://10.1.203.120:8380/nginx_status



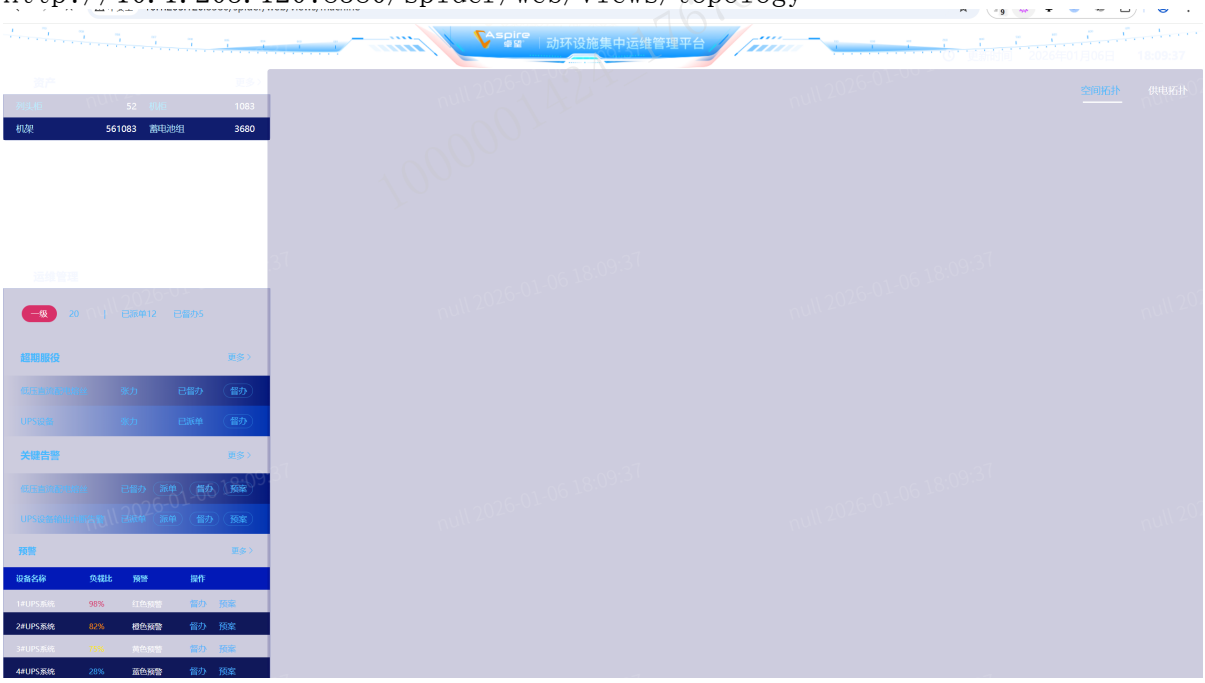

```
Active connections: 43
server accepts handled requests
 25969832 25967766 30636272
Reading: 0 Writing: 15 Waiting: 28
```

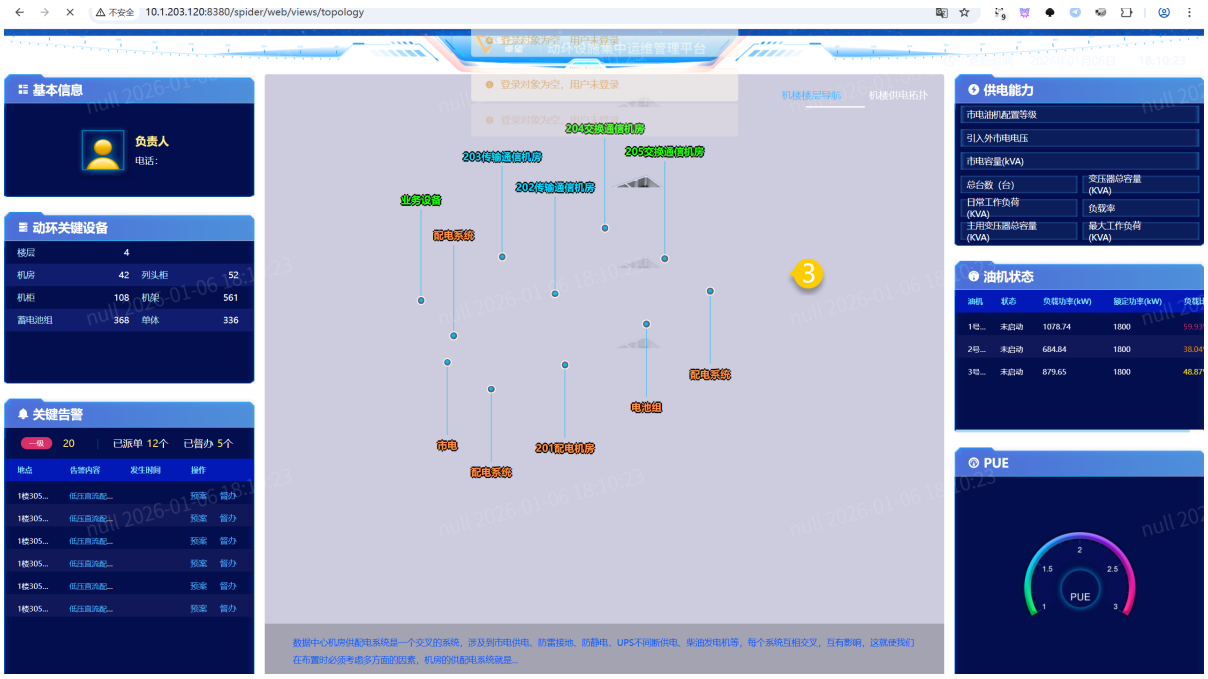
http://10.1.203.120:8380/manage/preview#/login



http://10.1.203.120:8380/spider/web/views/machine

http://10.1.203.120:8380/spider/web/views/topology





3.2 敏感信息未脱敏

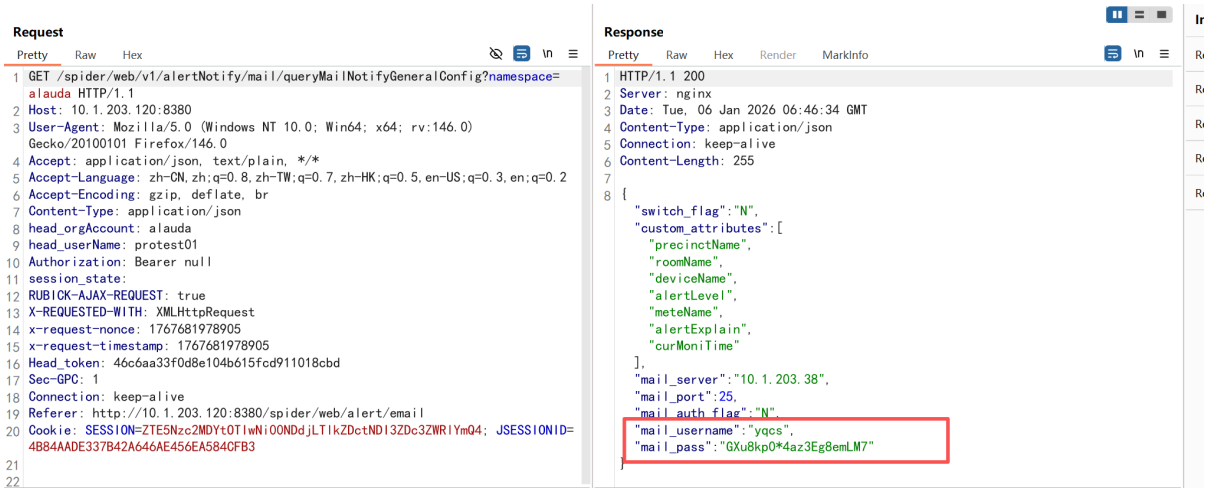
测试描述：敏感信息（如身份证号、手机号）未脱敏显示。

测试地址：http://10.1.203.120:8380/spider/web/v1/alertNotify/mail/queryMailNotifyGeneralConfig?namespace=alauda

风险程度：「高」

修复建议：
1. 对敏感信息进行脱敏处理。
2. 限制敏感信息的访问权限。

问题截图：



Request

Pretty Raw Hex

```
GET /spider/web/v1/alertNotify/mail/queryMailNotifyGeneralConfig?namespace=alauda HTTP/1.1
Host: 10.1.203.120:8380
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:146.0) Gecko/20100101 Firefox/146.0
Accept: application/json, text/plain, */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
head_orgAccount: alauda
head_userName: protest01
Authorization: Bearer null
session_state:
RUBICK-AJAX-REQUEST: true
X-REQUESTED-WITH: XMLHttpRequest
x-request-nonce: 1767681978905
x-request-timestamp: 1767681978905
Head_token: 46c6aa33f0d8e104b615fcd911018cbd
Sec-GPC: 1
Connection: keep-alive
Referer: http://10.1.203.120:8380/spider/web/alert/email
Cookie: SESSION=ZTE5Nzc2MDYtOTIwNi00NDdjLTIkZDctNDI3ZDc3ZWRlYmQ4; JSESSIONID=4B84AADE337B42A646AE456EA584CFB3
```

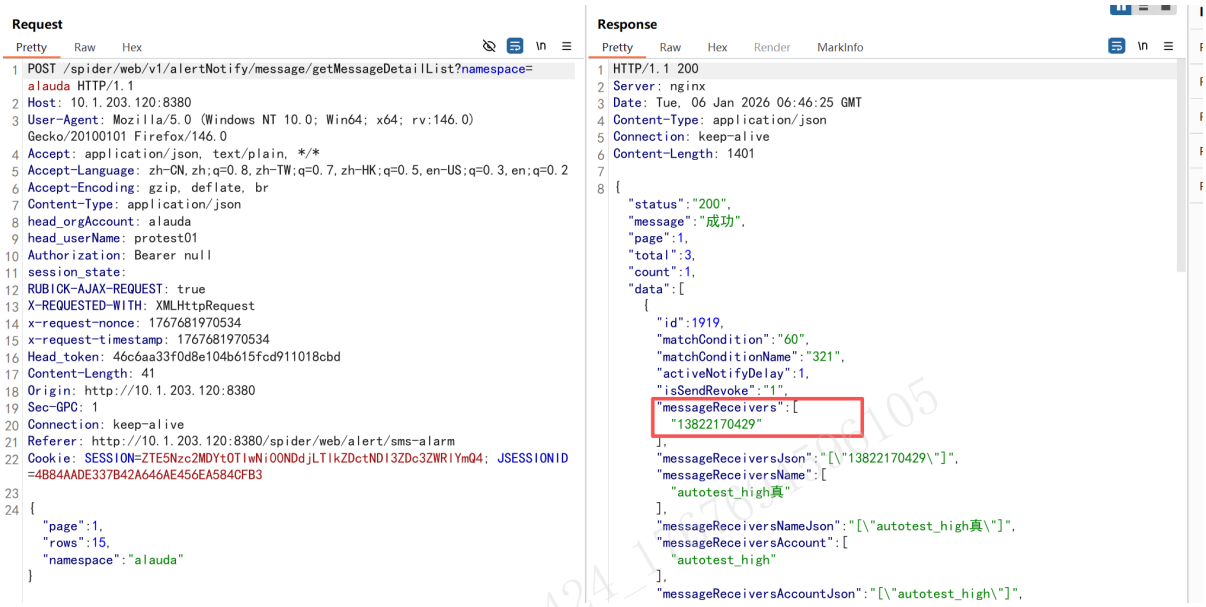
Response

Pretty Raw Hex Render MarkInfo

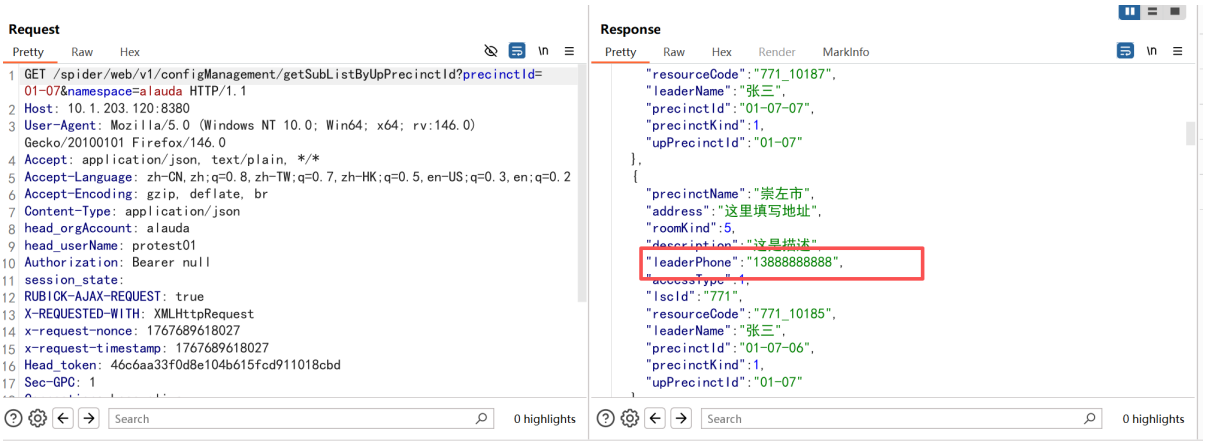
```
HTTP/1.1 200
Server: nginx
Date: Tue, 06 Jan 2026 06:46:34 GMT
Content-Type: application/json
Connection: keep-alive
Content-Length: 255

{
  "switch_flag":"N",
  "custom_attributes":[
    "precinctName",
    "roomName",
    "deviceName",
    "alertLevel",
    "meteName",
    "alertExplain",
    "curMoniTime"
  ],
  "mail_server":"10.1.203.38",
  "mail_port":25,
  "mail_auth_flag":"N",
  "mail_username":"yqcs",
  "mail_pass":"GXu8kp0*4az3Eg8emLM7"
}
```

http://10.1.203.120:8380/spider/web/v1/alertNotify/message/getMessageDetailList?namespace=alauda



http://10.1.203.120:8380/spider/web/v1/configManagement/getSubListByUpPrecinctId?precinctId=01-07&namespace=alauda



3.3 文件上传漏洞

测试描述：攻击者上传非预期类型文件或者恶意文件执行代码。

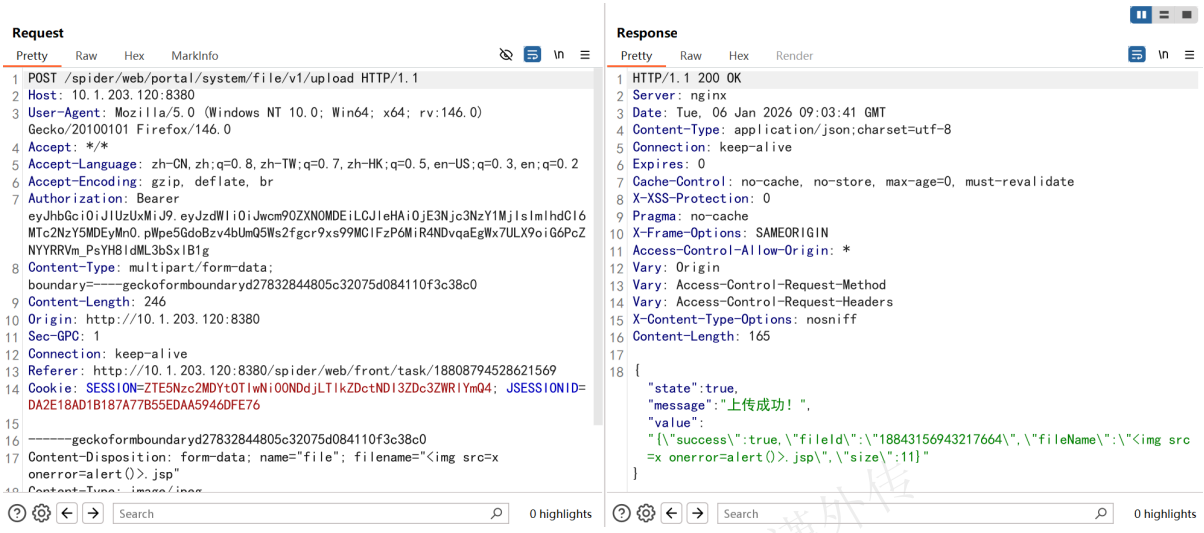
测试地址：http://10.1.203.120:8380/spider/web/portal/system/file/v1/upload

风险程度：「高」

修复建议：

1. 对上传文件进行严格的类型和内容验证。
2. 将上传文件存储在非Web可访问目录。
3. 使用对象存储上传文件。
4. 确保上传目录无执行权限。

问题截图：



Request

Pretty Raw Hex MarkInfo

```
POST /spider/web/portal/system/file/v1/upload HTTP/1.1
Host: 10.1.203.120:8380
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:146.0)
Gecko/20100101 Firefox/146.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Authorization: Bearer
eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJwcm9OZXNOMDEiLCJleHAiOjE3Njc3NzY1MjIsImlhdCI6
MTc2NzY5MDEyMn0.pWpe5GdoBzv4bUmQ5Ws2fgcr9xs99MCIFzP6MiR4NDvqaEgWx7ULX9oiG6PcZ
NYYRRVm_PsYH8ldML3bSxlB1g
Content-Type: multipart/form-data;
boundary=----geckoformboundaryd27832844805c32075d084110f3c38c0
Content-Length: 246
Origin: http://10.1.203.120:8380
Sec-GPC: 1
Connection: keep-alive
Referer: http://10.1.203.120:8380/spider/web/front/task/18808794528621569
Cookie: SESSION=ZTE5Nzc2MDYtOTIwNiOONDdjLTIkZDctNDI3ZDc3ZWRlYmQ4; JSESSIONID=
DA2E18AD1B187A77B55EDAA5946DFE76

------geckoformboundaryd27832844805c32075d084110f3c38c0
Content-Disposition: form-data; name="file"; filename="<img src=x
onerror=alert()>.jsp"
```

Search 0 highlights

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Server: nginx
Date: Tue, 06 Jan 2026 09:03:41 GMT
Content-Type: application/json;charset=utf-8
Connection: keep-alive
Expires: 0
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
X-XSS-Protection: 0
Pragma: no-cache
X-Frame-Options: SAMEORIGIN
Access-Control-Allow-Origin: *
Vary: Origin
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
X-Content-Type-Options: nosniff
Content-Length: 165

{
  "state":true,
  "message":"上传成功！",
  "value":
  "{\"success\":true,\"fileId\":\"18843156943217664\",\"fileName\":\"<img src
  =x onerror=alert()>.jsp\",\"size\":11}"
}
```

Search 0 highlights

4. 结果综述

4.1漏洞分布与修复

漏洞名称	风险级别	复测一	复测二	复测三
未授权访问	高			
文件上传漏洞	高			
敏感信息未脱敏	高			

4.2漏洞汇总

漏洞类型	漏洞数	高	中	低
逻辑漏洞	1	1	0	0
授权	1	1	0	0
数据保护	1	1	0	0
合计	3	3	0	0

4.3 测试结果

测试结论	不通过