报告编号：

**北京联通产互中心**

**可信移动**

**安全渗透测试技术报告**



国家信息技术安全研究中心

2022年01月

**声 明**

本报告包含北京联通单位敏感信息，未经许可严禁向无关人员借阅、复制。在任何情况下，若需引用本报告中的测试结果或结论都应保持其原有的意义，不得对相关内容擅自进行增加、修改和伪造或掩盖本报告的原有内容。

报告中给出的检测结论仅对被测信息系统当时的安全状态有效。当渗透测试工作完成后，当信息系统发生变更时，本报告不再适用。

未经国家信息技术安全研究中心同意，不得部分或全文复制本报告。如违反规定致使北京联通单位敏感信息泄露，造成严重后果的，依照法律追究当事人相关责任。

本报告若无签字及公章，均属无效。

国家信息技术安全研究中心

（加盖单位公章）

2022年01月

**签 署 页**

**编写： 时间：**

**审核： 时间：**

**批准： 时间：**

**目 录**

[1 概述 1](#_Toc93910087)

[1.1 任务属性 1](#_Toc93910088)

[1.2 测试时间 1](#_Toc93910089)

[1.3 测试流程 1](#_Toc93910090)

[1.4 测试对象 2](#_Toc93910091)

[1.5 测试结果 2](#_Toc93910092)

[2 检测结果 3](#_Toc93910093)

[2.1 可信移动 3](#_Toc93910094)

[2.1.1 检测目标 3](#_Toc93910095)

[2.1.2 检测结果 3](#_Toc93910096)

[3 整改建议 4](#_Toc93910097)

# 概述

* 1. 任务属性

经中国联通北京分公司（以下简称“北京联通”）授权，国家信息技术安全研究中心（以下简称“国信中心”）对中国联通北京市分公司可信移动开展渗透测试，测试结果由国信中心对北京联通单位负责。

* 1. 测试时间

表 1‑1 渗透测试时间

| **渗透测试时间** | |
| --- | --- |
| 起始时间 | 2022年01月17日 |
| 结束时间 | 2022年01月21日 |

* 1. 测试流程

（1）信息收集：进行必要的信息收集，如IP地址、DNS记录、软件版本信息、IP段等。

（2）渗透测试：根据收集的信息对网络、系统进行漏洞测试。

（3）本地信息收集：进行本地信息收集，用于下一阶段的权限提升。

（4）权限提升：尝试将测试阶段可能获得的普通权限提升为管理员权限，获得对系统的完全控制权。在时间许可的情况下，必要时从第一阶段重新进行。

（5）痕迹清除：清除中间数据。

（6）输出报告：根据测试的结果编写测试技术报告。

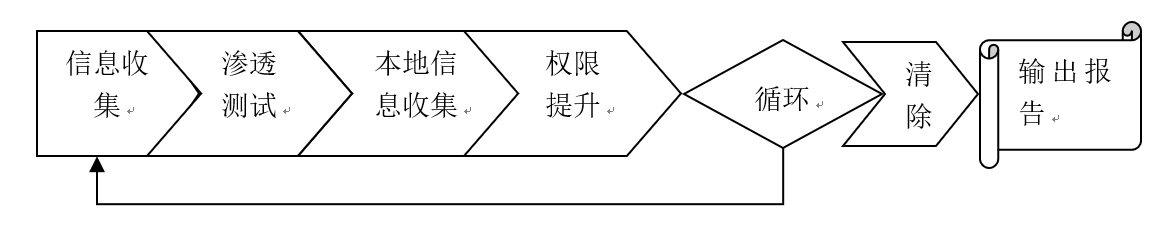


图 1‑1 渗透测试流程

* 1. 测试对象

此次测试目标为北京联通单位网站及相关网络和信息系统，系统列表1-2所示：

表 1‑2 渗透测试对象

| **序号** | **测试对象**  **系统功能描述** | **测试地址** |
| --- | --- | --- |
| 1 | 可信移动 | 61.49.87.218  61.49.87.137  61.49.87.185 |

* 1. 测试结果

在本次对可信移动渗透测试中发现，部分互联网系统安全防护体系较好，但部分环节尚存不足，主要问题如表1-3所示：

表 1‑3 渗透测试结果统计

| **序号** | **系统名称** | **漏洞名称** | **漏洞危害** |
| --- | --- | --- | --- |
| 1 | 可信移动 | 应用程序错误 | 低 |

漏洞危害风险等级划分标准如表1-4所示。

表 1‑4 漏洞风险等级划分

| **风险等级** | **等级划分依据** |
| --- | --- |
| 高风险 | 直接导致系统内容被修改、系统被控制、数据被破坏或者利用漏洞触发用户的敏感信息泄露，一旦发生，就是严重的安全事件。 |
| 中风险 | 可能导致重要信息的泄漏或有可能导致系统被控制。利用漏洞攻击间接影响应用系统运行或引起客户敏感信息外泄。 |
| 低风险 | 非重要信息泄漏或轻微安全问题，一般不会导致严重的安全事件 |

# 检测结果

* 1. 可信移动
     1. 检测目标

**目标地址：**

61.49.87.185

* + 1. 检测结果
       1. 应用程序错误

检测分析发现，目标主机存在应用程序错误漏洞，如果攻击者通过伪造包含非应用程序预期的参数或参数值的请求来探测应用程序，那么应用程序可能会进入易受攻击的未定义状态。

**漏洞链接：**

https://61.49.87.185:44433/uni\_auth/v1/captcha?jr=%bf

https://61.49.87.185:54434/uni\_auth/v1/captcha?jr=%bf

**漏洞分析与取证：**

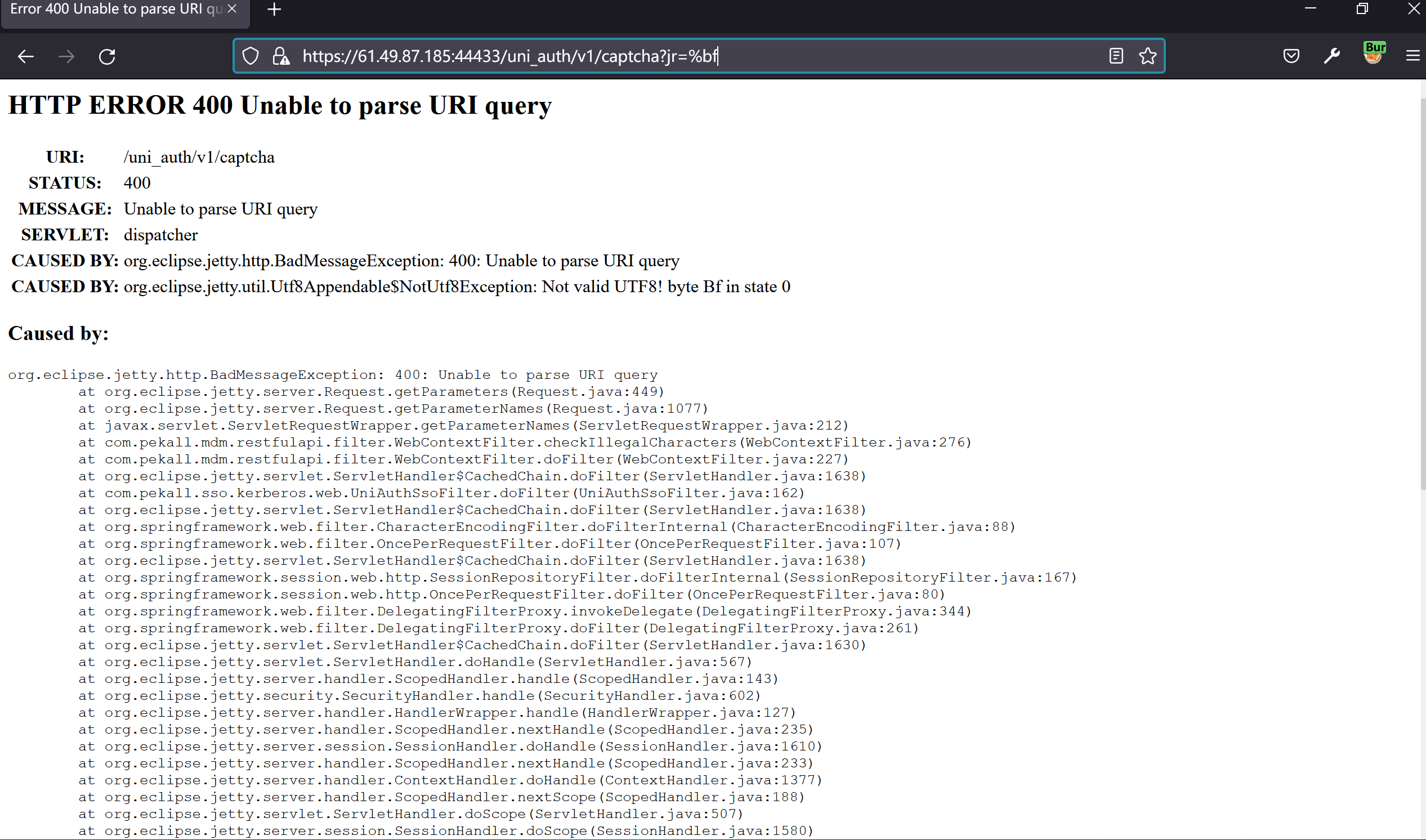


图 2‑1应用程序错误

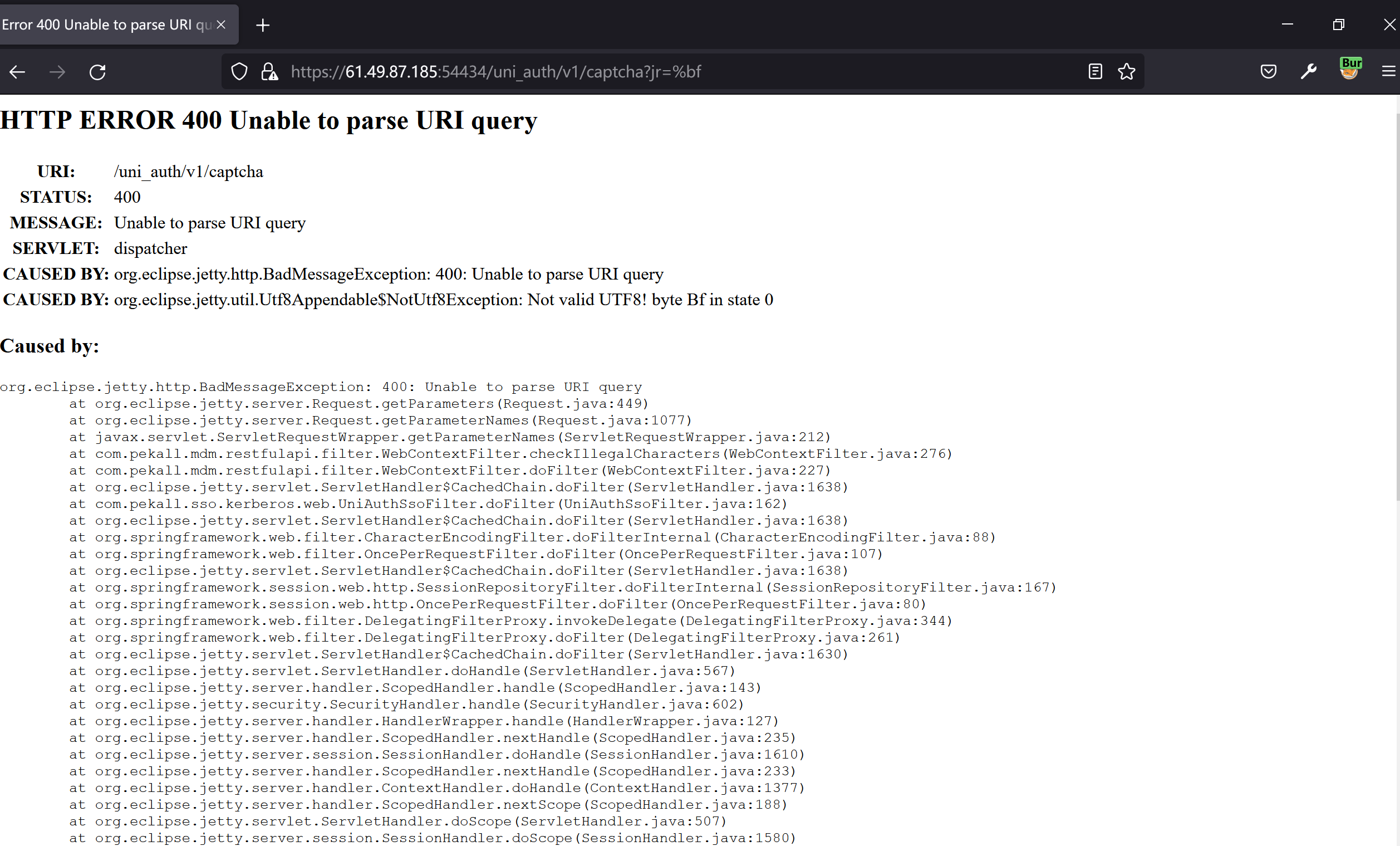


图 2‑2应用程序错误

**漏洞危害：**

攻击者利用该漏洞可以从应用程序对该请求的响应中获取有用的信息，且可利用该信息，以找出应用程序的弱点。

# 整改建议

漏洞整改建议如表3-1所示。

表 3‑1 整改建议

| **序号** | **系统名称** | **漏洞名称** | **整改建议** |
| --- | --- | --- | --- |
|  | 可信移动 | 应用程序错误 | 应用程序应验证其输入是否由有效字符组成，对输入数据进行过滤，请勿在生产环境中输出调试错误消息和异常，自定义错误页面。 |

=========此文档结束，以下无正文========