



中国石油大学(北京)克拉玛依校区
CHINA UNIVERSITY OF PETROLEUM - BEIJING AT KARAMAY

《软件质量保证与测试》

上机实验报告[8]

《搬家公司》非功能测试

院（系）： 计 算 机 系

专业年级： 软件工程 2019 级

班 级： 2 班

组 员： 付宇坤 任鹏宇

小组编号： 07

完成日期：2022 年 6 月 6 日

《搬家公司》非功能测试

文档版本号	日期	作者	审核人	说明
V1.0	2022/06/06	任鹏宇	付宇坤	文档编写

目录

一、安全性测试	4
1.1 基本信息	4
1.2 摘要.....	5
1.3 按问题类型分类的问题	8
二、部署测试.....	16
2.1 Linux	16
2.2 windows.....	16
三、兼容性测试	17
3.1 Chrome 浏览器	17
3.2 Firefox 浏览器.....	18
3.3 Edge 浏览器	19
3.4 IE 浏览器	20

一、安全性测试

1.1 基本信息

扫描文件名称	搬家公司
扫描开始时间	2022/6/5 15:39:44
测试策略	Default
测试优化级别	快
主机	localhost
端口	8081
操作系统	Win11
应用程序服务器	JavaAppServer

该安全报告包含由 HCL AppScan Standard 执行的 Web 应用程序安全性扫描的结果。

高严重性问题： 4

中等严重性问题： 4

低严重性问题： 14

参考严重性问题： 1

报告中包含的严重性问题总数： 23

扫描中发现的严重性问题总数： 23

1.2 摘要

问题类型 13

TOC

问题类型		问题的数量
高	已解密的登录请求	4
中	不充分帐户封锁	1
中	会话 ID 未更新	1
中	跨站点请求伪造	2
低	"Content-Security-Policy"头缺失	1
低	"X-Content-Type-Options"头缺失或不安全	1
低	"X-XSS-Protection"头缺失或不安全	1
低	查询中接受的主体参数	4
低	具有不安全、不正确或缺少 SameSite 属性的 Cookie	1
低	跨帧脚本编制防御缺失或不安全	1
低	启用了不安全的"OPTIONS"HTTP 方法	2
低	自动填写未对密码字段禁用的 HTML 属性	3
参	"Referral Policy" Security 头缺失	1

有漏洞的 URL 8

TOC








URL		问题的数量
高	http://localhost:8081/SE22_movingcompany_Web_exploded/login	6
高	http://localhost:8081/SE22_movingcompany_Web_exploded/register	4
中	http://localhost:8081/SE22_movingcompany_Web_exploded/order	2
低	http://localhost:8081/	7
低	http://localhost:8081/SE22_movingcompany_Web_exploded/evaluate	1
低	http://localhost:8081/SE22_movingcompany_Web_exploded/	1
低	http://localhost:8081/SE22_movingcompany_Web_exploded/login.jsp	1
低	http://localhost:8081/SE22_movingcompany_Web_exploded/register.jsp	1

修复任务		问题的数量	
高	发送敏感信息时，始终使用 SSL 和 POST（主体）参数。	4	<div></div>
中	登录之后更改会话 ID 值	1	<div></div>
中	多次登录尝试失败后实施帐户封锁	1	<div></div>
中	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce	2	<div></div>
低	查看将 SameSite Cookie 属性配置为推荐值的可能解决方案	1	<div></div>
低	将“autocomplete”属性正确设置为“off”	3	<div></div>
低	将服务器配置为使用安全策略的“Referrer Policy”头	1	<div></div>
低	将服务器配置为使用安全策略的“Content-Security-Policy”头	1	<div></div>
低	将服务器配置为使用值为 DENY 或 SAMEORIGIN 的“X-Frame-Options”头	1	<div></div>
低	将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头	1	<div></div>
低	将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头	1	<div></div>
低	禁用 WebDAV，或者禁止不需要的 HTTP 方法。	2	<div></div>
低	请勿接受在查询字符串中发送的主体参数	4	<div></div>

风险		问题的数量	
高	可能会窃取诸如用户名和密码等未经加密即发送了的用户登录信息	4	<div></div>
中	可能会升级用户特权并通过 Web 应用程序获取管理许可权	1	<div></div>
中	可能会窃取或操纵客户会话和 cookie，它们可能用于假冒合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务	1	<div></div>
中	可能会强制最终用户在当前其已通过身份验证的 Web 应用程序上执行不必要的操作。	2	<div></div>
低	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置	9	<div></div>
低	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息	9	<div></div>
低	通过将 Cookie 限制为第一方或同一站点上下文来防止 Cookie 信息泄漏，如果没有额外的保护措施（如反 CSRF 令牌），攻击可能会扩展为跨站点请求伪造 (CSRF) 攻击。	1	<div></div>
低	可能会在 Web 服务器上上载、修改或删除 Web 页面、脚本和文件	2	<div></div>
低	可能会绕过 Web 应用程序的认证机制	3	<div></div>

原因	问题的数量
高 SSL（安全套接字层）可为 HTTP 提供数据机密性和完整性。通过加密 HTTP 消息，SSL 可防止攻击者窃听或更改消息内容。登录页应始终采用 SSL 来保护从客户机传输到服务器的用户名和密码。如果不使用 SSL，会使用户凭证在传输到服务器期间作为明文公开，从而易被窃听。	4 
中 Web 应用程序编程或配置不安全	13 
中 之所以出现此漏洞，是因为应用程序允许用户在不验证请求是否是有意发送的情况下执行某些敏感操作。	2 
中 攻击者可能导致受害者的浏览器向应用程序中的任意 URL 发出 HTTP 请求。从经过身份验证的受害者的浏览器发送此请求时，它	2 
将包括受害者的会话 cookie 或身份验证标头。应用程序将接受此请求作为来自经过身份验证的用户的有效请求。	
中 如果将 Web 服务器设计为接收来自客户端的请求，但缺乏用于验证该请求是否有意发送的机制，则攻击者可能会欺骗客户端从另一个站点发出无意请求，而应用程序会将该请求视为可信请求。可以通过提交表单、加载图像、在 JavaScript 中发送 XMLHttpRequest 等执行此操作。	2 
中 例如，此 IMG 标签可以嵌入到攻击者的网页中，并且受害者的浏览器将提交请求检索该图像。此有效请求将由应用程序处理，并且浏览器不会显示损坏的图像。“”。由此带来的结果是，使用受害者的会话将受害者账户中的资金转移到攻击者的账户中。	2 
低 具有不正确、不安全或缺少 SameSite 属性的敏感 Cookie	1 
低 Web 服务器或应用程序服务器是以不安全的方式配置的	2 
参 不安全的 Web 应用程序编程或配置	1 

WASC 威胁分类

威胁	问题的数量
传输层保护不足	4 
服务器配置错误	1 
会话定置	1 
跨站点请求伪造	2 
蛮力	1 
内容电子欺骗	2 
信息泄露	12 

1.3 按问题类型分类的问题

已解密的登录请求	
严重性:	高
CVSS 分数:	8.5
URL:	http://localhost:8081/SE22_movingcompany_Web_exploded/register
实体:	password (Parameter)
风险:	可能会窃取诸如用户名和密码等未经加密即发送了的用户登录信息
原因:	SSL (安全套接字层) 可为 HTTP 提供数据机密性和完整性。通过加密 HTTP 消息, SSL 可防止攻击者窃听或更改消息内容。登录页应始终采用 SSL 来保护从客户端传输到服务器的用户名和密码。如果不使用 SSL, 会使用户凭证在传输到服务器期间作为明文公开, 从而易被窃听。
固定值:	发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

中	不充分帐户封锁 1	TOC
---	-----------	-----

问题 1 / 1	TOC
----------	-----

不充分帐户封锁	
严重性:	中
CVSS 分数:	6.4
URL:	http://localhost:8081/SE22_movingcompany_Web_exploded/login
实体:	password (Parameter)
风险:	可能会升级用户特权并通过 Web 应用程序获取管理许可权
原因:	Web 应用程序编程或配置不安全
固定值:	多次登录尝试失败后实施帐户封锁

- 差异: cookie JSESSIONID 已从请求除去:
ADDBF29822D24BA5AB5CBB261B28D1F0
- 参数 password 从以下位置进行控制: **CONFIDENTIAL 0** 至: 4ppSc4n
- 推理: 发送了两次合法的登录尝试, 并且在其间发送了几次错误的登录尝试。最后一个响应与第一个响应相同。这表明存在未充分实施帐户封锁的情况, 从而使登录页面可能受到暴力攻击。(即使第一个响应不是成功的登录页面, 也是如此。)

中	会话 ID 未更新 1	TOC
---	-------------	-----

问题 1 / 1	TOC
----------	-----

会话 ID 未更新	
严重性:	中
CVSS 分数:	6.4
URL:	http://localhost:8081/SE22_movingcompany_Web_exploded/login
实体:	login (Page)
风险:	可能会窃取或操纵客户会话和 cookie，它们可能用于假冒合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因:	Web 应用程序编程或配置不安全
固定值:	登录之后更改会话 ID 值

中 跨站点请求伪造 2

TOC

问题 1 / 2

TOC

跨站点请求伪造	
严重性:	中
CVSS 分数:	6.4
URL:	http://localhost:8081/SE22_movingcompany_Web_exploded/order
实体:	order (Page)
风险:	可能会强制最终用户在当前其已通过身份验证的 Web 应用程序上执行不必要的操作。
原因:	<p>之所以出现此漏洞，是因为应用程序允许用户在不验证请求是否是有意发送的情况下执行某些敏感操作。</p> <p>攻击者可能导致受害者的浏览器向应用程序中的任意 URL 发出 HTTP 请求。从经过身份验证的受害者的浏览器发送此请求时，它将包括受害者的会话 cookie 或身份验证标头。应用程序将接受此请求作为来自经过身份验证的用户的有效请求。</p> <p>如果将 Web 服务器设计为接收来自客户端的请求，但缺乏用于验证该请求是否是有意发送的机制，则攻击者可能会欺骗客户端从另一个站点发出无意请求，而应用程序会将该请求视为可信请求。可以通过提交表单、加载图像、在 JavaScript 中发送 XMLHttpRequest 等执行此操作。</p> <p>例如，此 IMG 标签可以嵌入到攻击者的网页中，并且受害者的浏览器将提交请求检索该图像。此有效请求将由应用程序处理，并且浏览器不会显示损坏的图像。“”。由此带来的结果是，使用受害者的会话将受害者账户中的资金转移到攻击者的账户中。</p>
固定值:	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异: 标题 `Referer` 从以下位置进行控制:

`http://localhost:8081/SE22_movingcompany_Web_exploded/order.js`
`p`

至: `https://bogus.referer.hcl.com`

标题 `Origin` 已添加至请求: `https://bogus.origin.hcl.com`

推理: 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

低

“Content-Security-Policy”头缺失 1

TOC

问题 1 / 1

TOC

“Content-Security-Policy”头缺失

严重性:	低
CVSS 分数:	5.0
URL:	http://localhost:8081/
实体:	localhost (Page)
风险:	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因:	Web 应用程序编程或配置不安全
固定值:	将服务器配置为使用安全策略的“Content-Security-Policy”头

低

“X-Content-Type-Options”头缺失或不安全 1

TOC

问题 1 / 1

TOC

“X-XSS-Protection”头缺失或不安全

严重性:	低
CVSS 分数:	5.0
URL:	http://localhost:8081/
实体:	localhost (Page)
风险:	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因:	Web 应用程序编程或配置不安全
固定值:	将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头

查询中接受的主体参数

严重性:	低
CVSS 分数:	5.0
URL:	http://localhost:8081/SE22_movingcompany_Web_exploded/order
实体:	order (Page)
风险:	可能会收集有关 Web 应用程序的敏感信息, 如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因:	Web 应用程序编程或配置不安全
固定值:	请勿接受在查询字符串中发送的主体参数

差异: 主体参数 已从请求除去: 中国
查询参数 已添加至请求: 中国
主体参数 已从请求除去: 上海市
查询参数 已添加至请求: 上海市
主体参数 已从请求除去: 浦东新区
查询参数 已添加至请求: 浦东新区
主体参数 已从请求除去: 中国
查询参数 已添加至请求: 中国
主体参数 已从请求除去: 南昌
查询参数 已添加至请求: 南昌
主体参数 已从请求除去: 南昌大学
查询参数 已添加至请求: 南昌大学
主体参数 已从请求除去: 1234
查询参数 已添加至请求: 1234
主体参数 已从请求除去: 付宇坤
查询参数 已添加至请求: 付宇坤
主体参数 已从请求除去: 10
查询参数 已添加至请求: 10
主体参数 已从请求除去: 10000000000
查询参数 已添加至请求: 10000000000
方法 从以下位置进行控制: POST 至: GET

推理: 测试结果似乎指示存在脆弱性, 因为“测试响应”与“原始响应”类似, 这表明应用程序处理了查询总提交的主体参数。

查询中接受的主体参数

严重性: **低**

CVSS 分数: 5.0

URL: http://localhost:8081/SE22_movingcompany_Web_exploded/evaluate

实体: evaluate (Page)

风险: 可能会收集有关 Web 应用程序的敏感信息, 如用户名、密码、机器名和/或敏感文件位置
可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 请勿接受在查询字符串中发送的主体参数

差异: 主体参数 已从请求除去: 555

查询参数 已添加至请求: 555

方法 从以下位置进行控制: POST 至: GET

推理: 测试结果似乎指示存在脆弱性, 因为“测试响应”与“原始响应”类似, 这表明应用程序处理了查询总提交的主体参数。

问题 3 / 4

TOC

查询中接受的主体参数

严重性: **低**

CVSS 分数: 5.0

URL: http://localhost:8081/SE22_movingcompany_Web_exploded/register

实体: register (Page)

风险: 可能会收集有关 Web 应用程序的敏感信息, 如用户名、密码、机器名和/或敏感文件位置
可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息

原因: Web 应用程序编程或配置不安全

固定值: 请勿接受在查询字符串中发送的主体参数

差异: 主体参数 已从请求除去: xiaoming

查询参数 已添加至请求: xiaoming

主体参数 已从请求除去: **CONFIDENTIAL 0**

查询参数 已添加至请求: **CONFIDENTIAL 0**

主体参数 已从请求除去: **CONFIDENTIAL 0**

查询参数 已添加至请求: **CONFIDENTIAL 0**

主体参数 已从请求除去: 25

查询参数 已添加至请求: 25

方法 从以下位置进行控制: POST 至: GET

推理: 测试结果似乎指示存在脆弱性, 因为“测试响应”与“原始响应”类似, 这表明应用程序处理了查询总提交的主体参数。

查询中接受的主体参数	
严重性:	低
CVSS 分数:	5.0
URL:	http://localhost:8081/SE22_movingcompany_Web_exploded/login
实体:	login (Page)
风险:	可能会收集有关 Web 应用程序的敏感信息, 如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因:	Web 应用程序编程或配置不安全
固定值:	请勿接受在查询字符串中发送的主体参数

差异: cookie JSESSIONID 已从请求除去:

ADDBF29822D24BA5AB5CBB261B28D1F0

主体参数 已从请求除去: xiaoming

查询参数 已添加至请求: xiaoming

主体参数 已从请求除去: **CONFIDENTIAL 0**

查询参数 已添加至请求: **CONFIDENTIAL 0**

方法 从以下位置进行控制: POST 至: GET

推理: 测试结果似乎指示存在脆弱性, 因为“测试响应”与“原始响应”类似, 这表明应用程序处理了查询总提交的主体参数。

低 具有不安全、不正确或缺少 SameSite 属性的 Cookie 1 TOC

问题 1 / 1

TOC

具有不安全、不正确或缺少 SameSite 属性的 Cookie	
严重性:	低
CVSS 分数:	4.1
URL:	http://localhost:8081/
实体:	JSESSIONID (Cookie)
风险:	通过将 Cookie 限制为第一方或同一站点上下文来防止 Cookie 信息泄漏, 如果没有额外的保护措施 (如反 CSRF 令牌), 攻击可能会扩展为跨站点请求伪造 (CSRF) 攻击。
原因:	具有不正确、不安全或缺少 SameSite 属性的敏感 Cookie
固定值:	查看将 SameSite Cookie 属性配置为推荐值的可能解决方案

问题 1 / 1

TOC

跨帧脚本编制防御缺失或不安全

严重性:	低
CVSS 分数:	5.0
URL:	http://localhost:8081/
实体:	localhost (Page)
风险:	可能会收集有关 Web 应用程序的敏感信息, 如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因:	Web 应用程序编程或配置不安全
固定值:	将服务器配置为使用值为 DENY 或 SAMEORIGIN 的“X-Frame-Options”头

问题 1 / 2

TOC

启用了不安全的“OPTIONS”HTTP 方法

严重性:	低
CVSS 分数:	5.0
URL:	http://localhost:8081/SE22_movingcompany_Web_exploded/
实体:	SE22_movingcompany_Web_exploded/ (Page)
风险:	可能会在 Web 服务器上上载、修改或删除 Web 页面、脚本和文件
原因:	Web 服务器或应用程序服务器是以不安全的方式配置的
固定值:	禁用 WebDAV, 或者禁止不需要的 HTTP 方法。

差异: 路径 从以下位置进行控制: [/SE22_movingcompany_Web_exploded/](#) 至: *

方法 从以下位置进行控制: GET 至: OPTIONS

推理: Allow 头显示危险的 HTTP 选项是已允许的, 这表示在服务器上启用了 WebDAV。

启用了不安全的“OPTIONS”HTTP 方法	
严重性:	低
CVSS 分数:	5.0
URL:	http://localhost:8081/
实体:	SE22_movingcompany_Web_exploded/ (Page)
风险:	可能会在 Web 服务器上上载、修改或删除 Web 页面、脚本和文件
原因:	Web 服务器或应用程序服务器是以不安全的方式配置的
固定值:	禁用 WebDAV，或者禁止不需要的 HTTP 方法。

差异: 路径 从以下位置进行控制: /SE22_movingcompany_Web_exploded/ 至: *

方法 从以下位置进行控制: GET 至: OPTIONS

推理: Allow 头显示危险的 HTTP 选项是已允许的，这表示在服务器上启用了 WebDAV。

低

自动填写未对密码字段禁用的 HTML 属性 3

TOC

自动填写未对密码字段禁用的 HTML 属性	
严重性:	低
CVSS 分数:	5.0
URL:	http://localhost:8081/SE22_movingcompany_Web_exploded/login.jsp
实体:	login.jsp (Page)
风险:	可能会绕过 Web 应用程序的认证机制
原因:	Web 应用程序编程或配置不安全
固定值:	将“autocomplete”属性正确设置为“off”

参

"Referral Policy" Security 头缺失 1

TOC

"Referral Policy" Security 头缺失	
严重性:	参考
CVSS 分数:	0.0
URL:	http://localhost:8081/
实体:	localhost (Page)
风险:	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因:	不安全的 Web 应用程序编程或配置
固定值:	将服务器配置为使用安全策略的 "Referrer Policy" 头

二、部署测试

2.1 Linux

软件环境	华为云服务器
系统版本	EulerOS
软件名称	搬家公司
硬件环境	
CPU	Intel(R) Xeon(R) CPU E5-2680 v4 @ 2.40GHz
内存	1.4GB
硬盘	40GB
网络环境	100MB 广域网

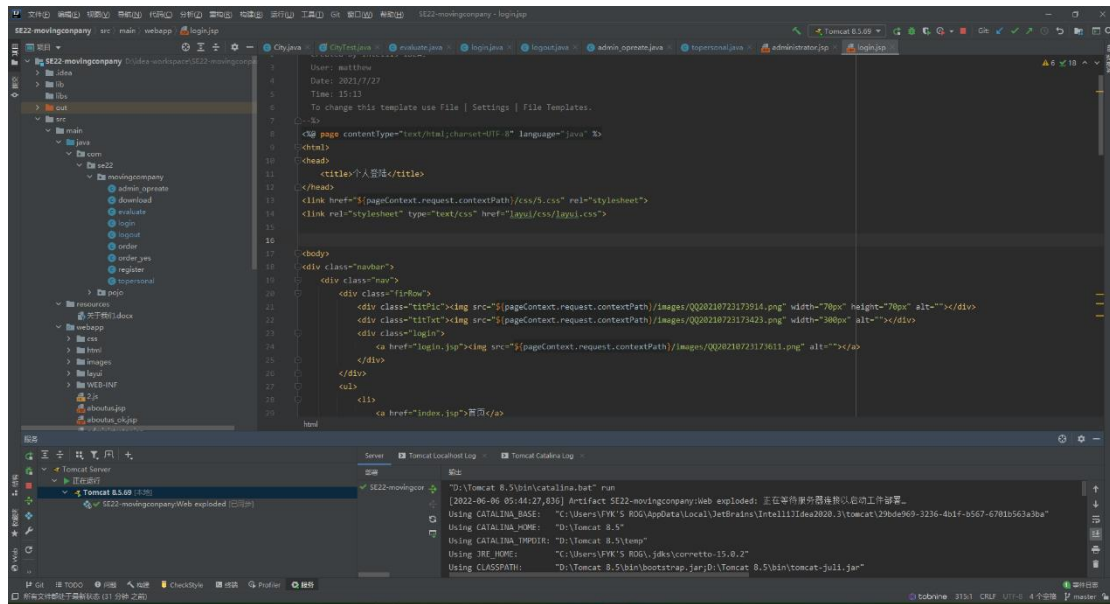
测试结果：

可以正常部署使用。

2.2 windows

软件环境	Microsoft Windows 11 家庭中文版
硬件环境	
CPU	Intel(R) Core(TM) i7-10870H CPU @ 2.20GHz 2.21 GHz
内存	16GB
硬盘	1TB
网络环境	100MB 广域网

测试结果

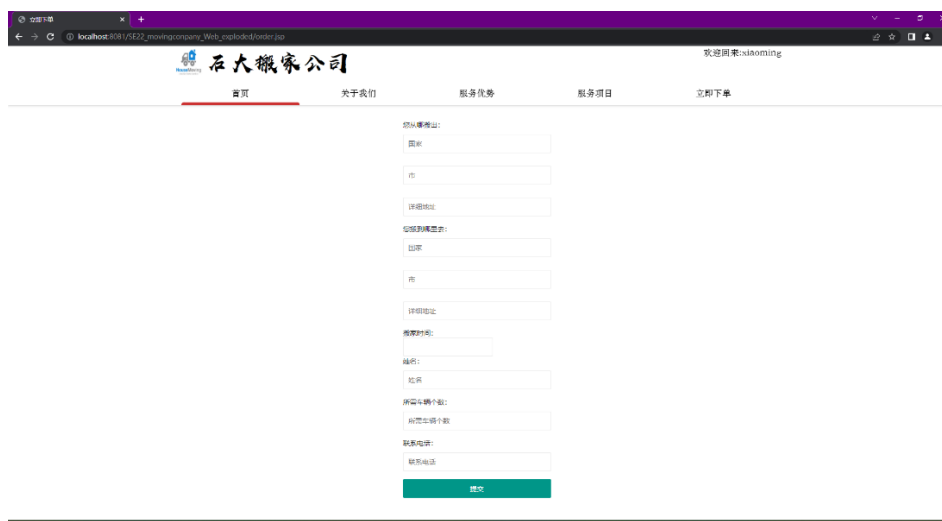


可以正常部署使用。

三、兼容性测试

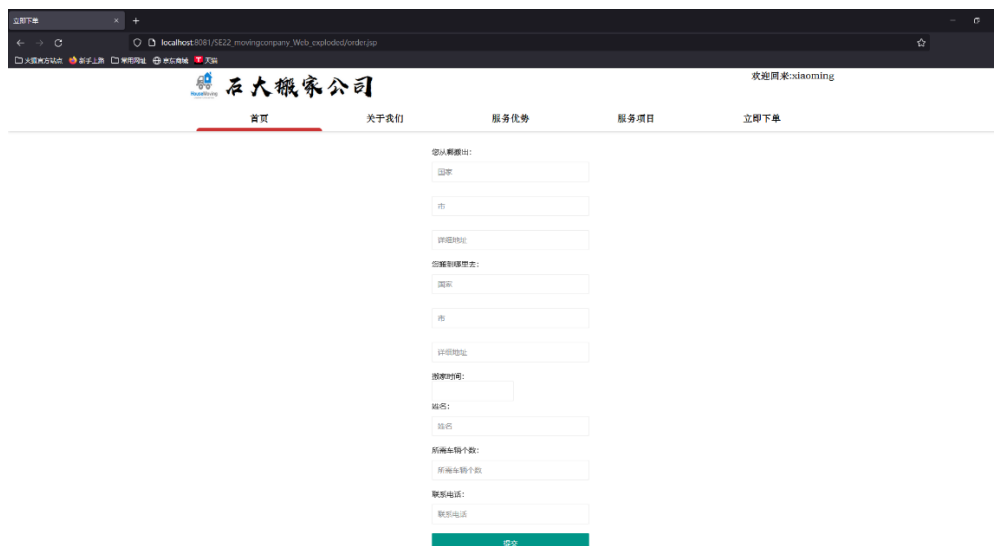
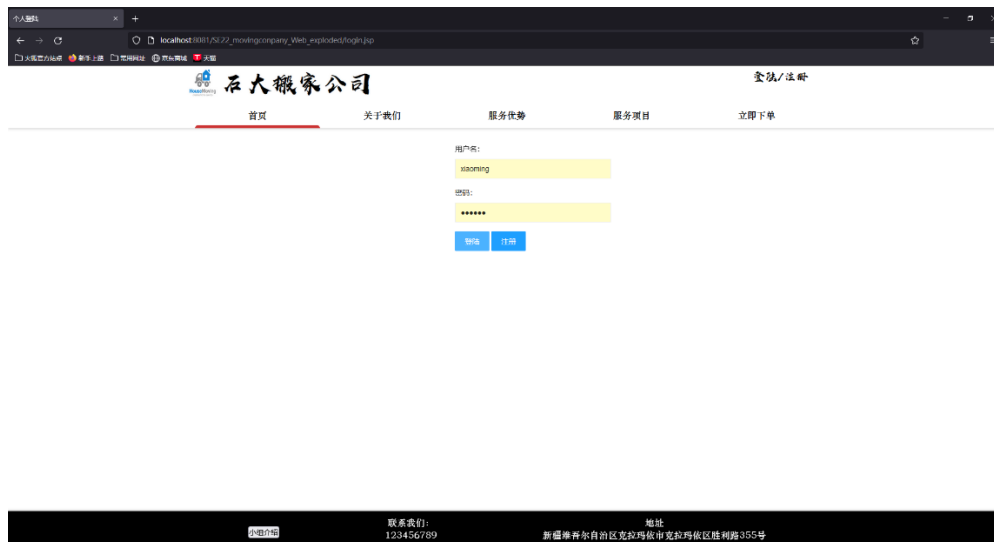
3.1 Chrome 浏览器





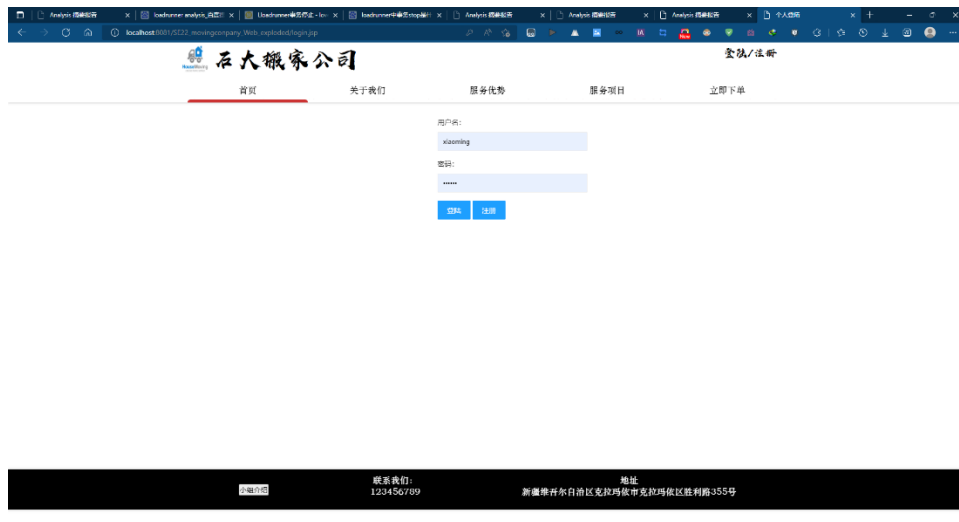
3.2 Firefox 浏览器



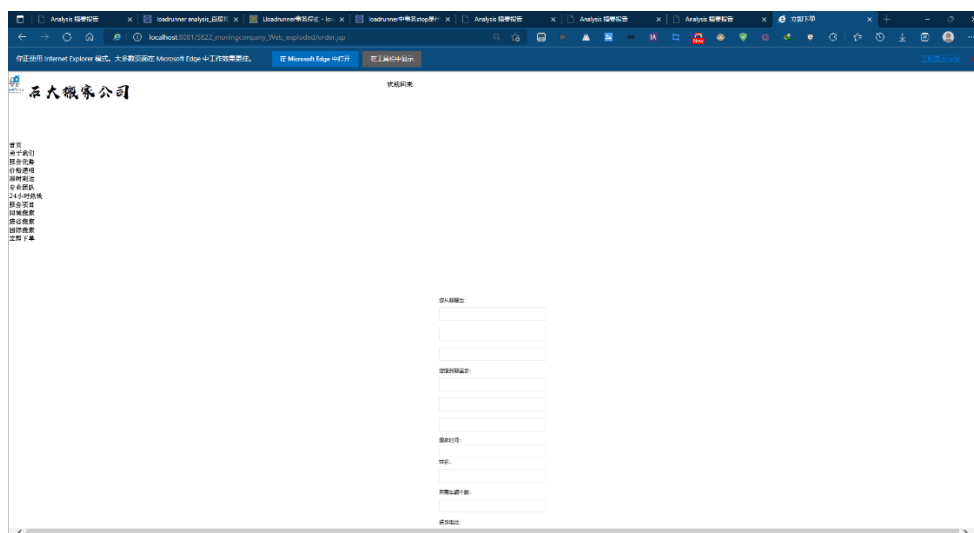


3.3 Edge 浏览器





3.4 IE 浏览器





结论：除了 IE 浏览器网页图片和文字布局出现异常之外，其余浏览器均正常运行，故兼容性测试通过。