**MeetHere场馆预约系统**

**非功能性测试报告**

**编写部门：软件测试小组19小组**

**编写地址：C6Ⅱ区507机房**

**编写时间：2023年5月20日**

目录

[1 兼容性测试 4](#_Toc135699761)

[1.1 测试范围与目的 4](#_Toc135699762)

[1.2 可靠性测试用例 4](#_Toc135699763)

[1.3 测试结论 6](#_Toc135699764)

[2 手动抓包测试 6](#_Toc135699765)

[2.1注册抓包 6](#_Toc135699766)

[2.2登录抓包 7](#_Toc135699767)

[2.3预约时间手动抓包进行修改 12](#_Toc135699768)

[2.4进行留言板功能抓包测试 15](#_Toc135699769)

[2.5结论 17](#_Toc135699770)

[3.安全性测试 18](#_Toc135699771)

[3.1 介绍 18](#_Toc135699772)

[3.2 目标 18](#_Toc135699773)

[3.3 管理摘要报告 19](#_Toc135699774)

[3.4 问题的数量（全部 32 ） 19](#_Toc135699775)

[3.5 问题的数量（按照“测试类型”） 19](#_Toc135699776)

[3.6 有漏洞的 URL 和无漏洞的 URL 比较 23](#_Toc135699777)

[3.7 修复任务数量 24](#_Toc135699778)

[3.8 高严重性问题 25](#_Toc135699779)

[3.9 中等级别的安全性问题 25](#_Toc135699780)

[3.10 低级别严重性问题 25](#_Toc135699781)

[3.11 参考信息严重性问题 26](#_Toc135699782)

[3.12 修复任务 27](#_Toc135699783)

[3.13 有漏洞的 URL 28](#_Toc135699784)

[3.14 严重性为高的“问题类型” 29](#_Toc135699785)

[3.15 严重性为中的“问题类型” 34](#_Toc135699788)

[3.16 严重性为低的“问题类型” 34](#_Toc135699789)

[3.17 严重性为参考信息的“问题类型” 152](#_Toc135699834)

[3.18 测试策略 208](#_Toc135699853)

[3.19 高优先级修复任务 234](#_Toc135699854)

[3.20 中优先级修复任务 236](#_Toc135699858)

[3.21 低优先级修复任务 237](#_Toc135699859)

[3.22 参数 252](#_Toc135699893)

[3.23 失败请求 253](#_Toc135699894)

[3.24 注释 291](#_Toc135699895)

[3.25 cookie 295](#_Toc135699896)

[3.26 应用程序 URL 295](#_Toc135699897)

# 1 兼容性测试

## 测试范围与目的

测试范围：操作系统（Windows 10 64bit、Ubuntu 22.04.2 LTS、Android 13），浏览器（Chrome 113、IE 10），分辨率（1280×720、1920×1080、2560×1440），网络环境（Wifi、快速3G、慢速3G、脱机）

目的：测试场馆预约系统在不同的操作系统平台上、不同的浏览器访问、不同的屏幕分辨率下、不同的网络环境中网站是否能正常运行。

**表7-1 因子状态表**

|  |  |  |  |
| --- | --- | --- | --- |
| 操作系统 | Windows 10 64bit | Ubuntu 22.04.2 LTS | Android 13 |
| 分辨率 | 1280×720 | 1920×1080 | 2560×1440 |
| 浏览器 | Chrome 113 | Firefox 113 | IE 10 |

使用正交法设计测试用例，正交表如下所示：

**表7-2 正交表**

|  |  |  |  |
| --- | --- | --- | --- |
| **因素**  **测试编号** | **操作系统** | **分辨率** | **浏览器** |
| 1 | Windows 10 64bit | 1280×720 | Chrome 113 |
| 2 | Windows 10 64bit | 1920×1080 | Firefox 113 |
| 3 | Windows 10 64bit | 2560×1440 | IE 10 |
| 4 | Ubuntu 22.04.2 LTS | 1280×720 | Chrome 113 |
| 5 | Ubuntu 22.04.2 LTS | 1920×1080 | Firefox 113 |
| 6 | Ubuntu 22.04.2 LTS | 2560×1440 | IE 10 |
| 7 | Android 13 | 1280×720 | Chrome 113 |
| 8 | Android 13 | 1920×1080 | Firefox 113 |
| 9 | Android 13 | 2560×1440 | IE 10 |

## 可靠性测试用例

1. 可靠性的测试用例

|  |  |  |  |
| --- | --- | --- | --- |
| 用例ID | RT001 | | |
| 假设名称 | 系统网站在不同操作系统平台、浏览器、分辨率下的测试 | | |
| 用例目的 | 分别使用不同操作系统和浏览器，采用不同分辨率访问系统并验证功能 | | |
| 输入/动作 | | 期望的输出/响应 | 是否能正常运行 |
| 操作系统：Windows 10 64bit  分辨率：1280×720  浏览器：Chrome 113 | | 系统页面访问正常、功能运行正常 | 与期望结果符合 |
| 操作系统：Windows 10 64bit  分辨率：1920×1080  浏览器：Firefox 113 | | 系统页面访问正常、功能运行正常 | 与期望结果符合 |
| 操作系统：Windows 10 64bit  分辨率：2560×1440  浏览器：IE 10 | | 系统页面访问正常、功能运行正常 | 与期望结果符合 |
| 操作系统：Ubuntu 22.04.2 LTS  分辨率：1280×720  浏览器：Chrome 113 | | 系统页面访问正常、功能运行正常 | 与期望结果符合 |
| 操作系统：Ubuntu 22.04.2 LTS  分辨率：1920×1080  浏览器：Firefox 113 | | 系统页面访问正常、功能运行正常 | 与期望结果符合 |
| 操作系统：Ubuntu 22.04.2 LTS  分辨率：2560×1440  浏览器：IE 10 | | 系统页面访问正常、功能运行正常 | 与期望结果符合 |
| 操作系统：Android 13  分辨率：1280×720  浏览器：Chrome 113 | | 系统页面访问正常、功能运行正常 | 系统访问正常，但未作响应式处理 |
| 操作系统：Android 13  分辨率：1920×1080  浏览器：Firefox 113 | | 系统页面访问正常、功能运行正常 | 系统访问正常，但未作响应式处理 |
| 操作系统：Android 13  分辨率：2560×1440  浏览器：IE 10 | | 系统页面访问正常、功能运行正常 | 系统访问正常，但未作响应式处理 |
| 用例ID | RT002 | | |
| 假设名称 | 系统网站网络环境测试 | | |
| 用例目的 | 测试系统网站在不同网络带宽下的响应速度 | | |
| 输入/动作 | | 期望的输出/响应 | 是否能正常运行 |
| Wifi | | 3秒内响应页面 | 与期望结果符合 |
| 3G快速网 | | 3秒内响应页面 | 与期望结果符合 |
| 3G慢速网 | | 3秒内响应页面 | 部分图片加载缓慢或丢失 |
| 脱机 | | 网页访问失败 | 与期望结果符合 |

## 测试结论

根据兼容性测试的结果，以下是一个可能的Web系统兼容性测试结论的示例：

1. 浏览器兼容性：

该Web系统在主流浏览器（如Google Chrome、Mozilla Firefox、Microsoft Edge、Safari等）的最新版本上进行测试，显示正常，没有明显的显示问题或功能错误。

2. 操作系统兼容性：

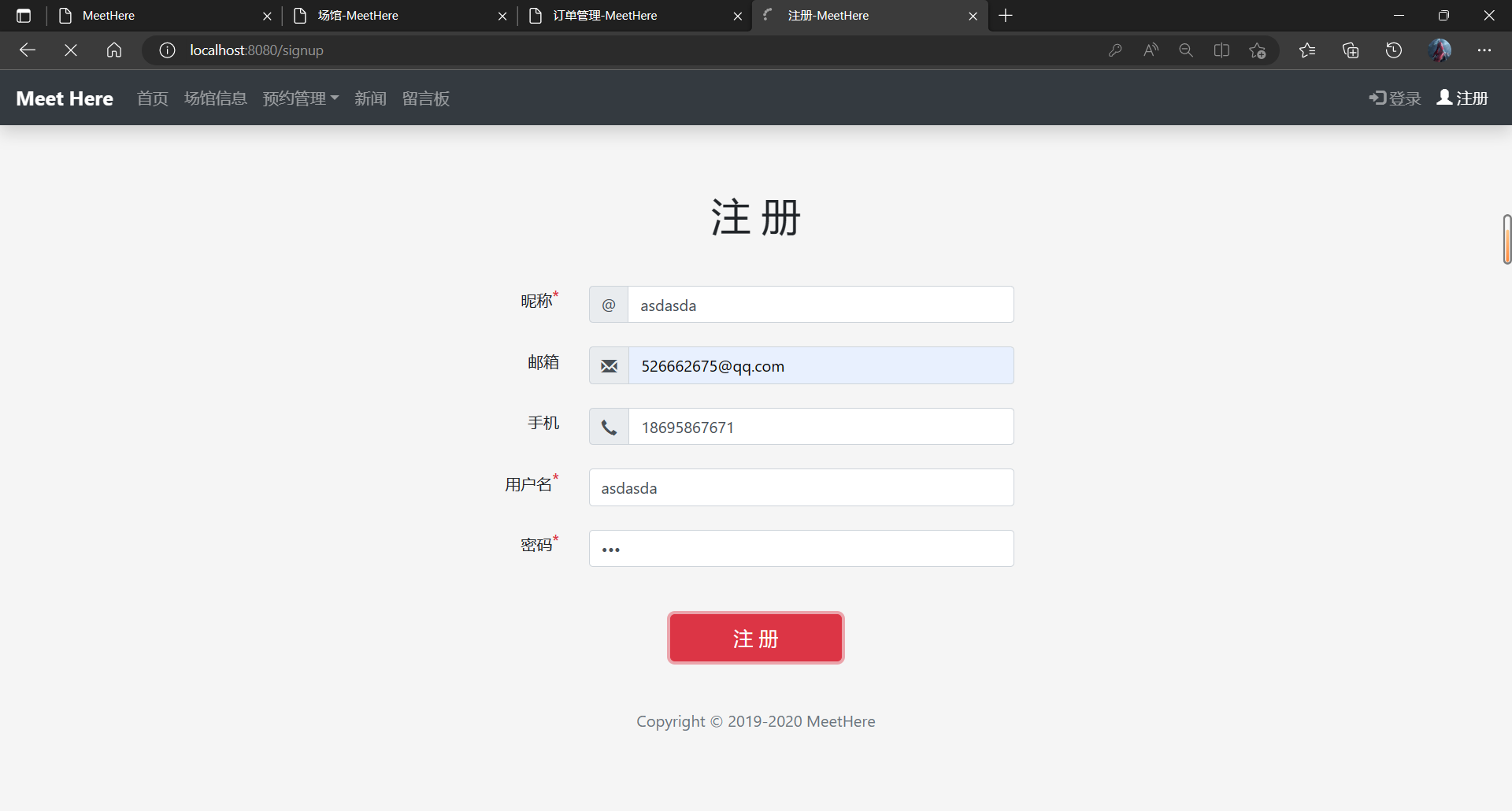
该Web系统在不同操作系统（如Windows、Mac、Linux等）上进行测试，显示正常，没有出现明显的兼容性问题。

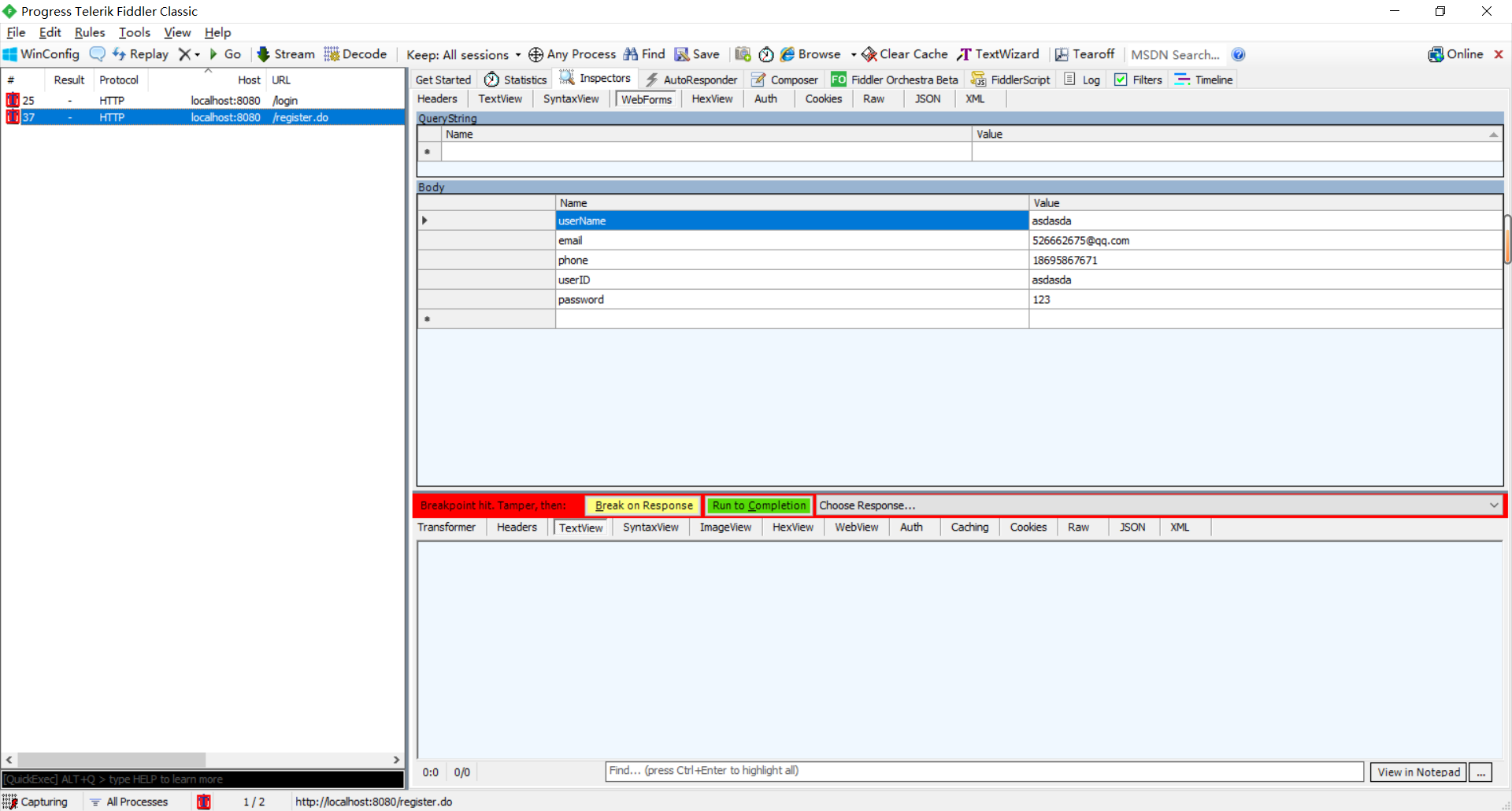
3. 移动设备兼容性：

该Web系统经过移动设备测试，在Android操作系统上系统页面访问正常，但不支持响应式设计。

# 2 手动抓包测试

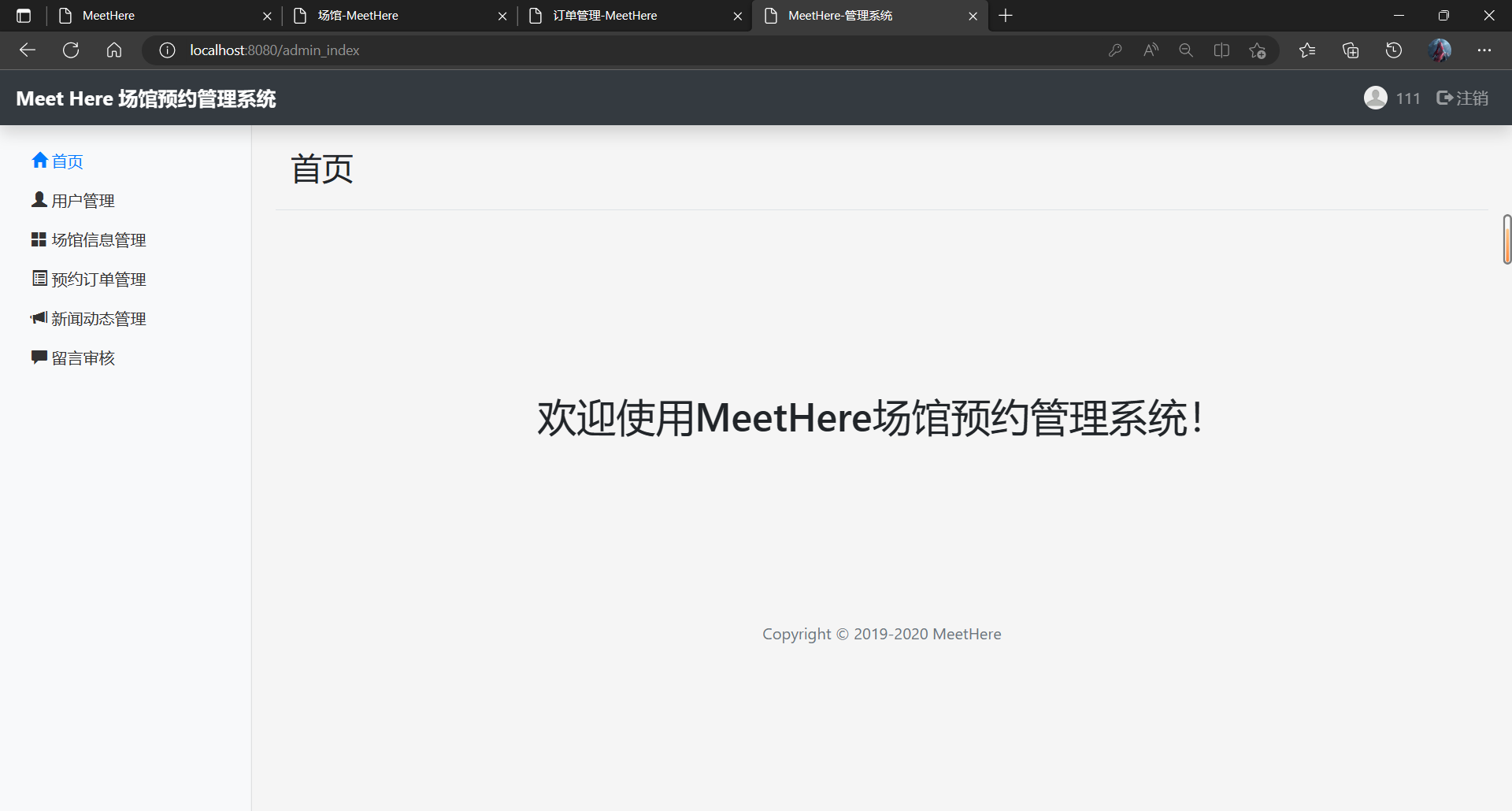
## 2.1注册抓包



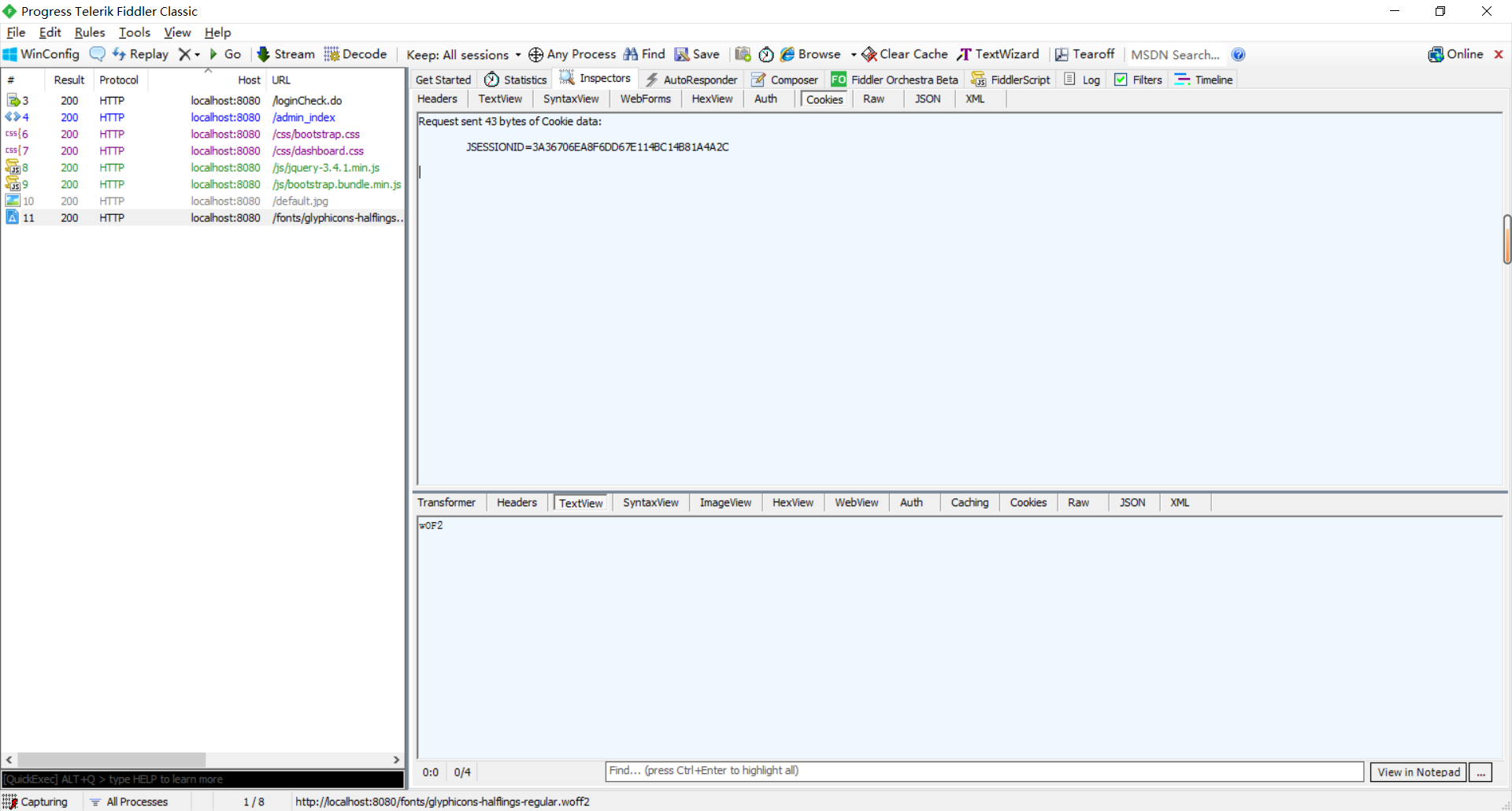


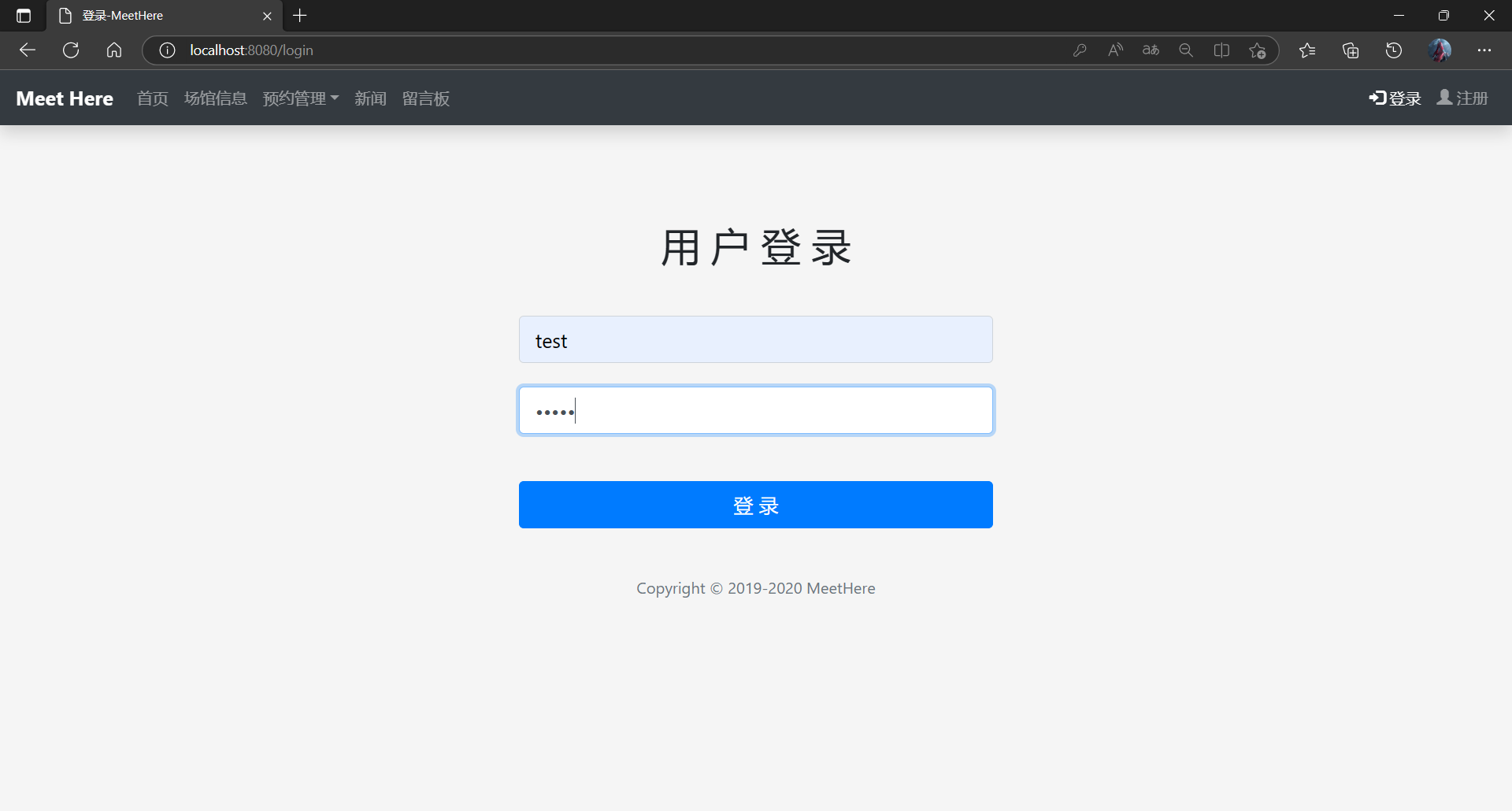
可以在fiddler中看到用户的注册信息

## 2.2登录抓包

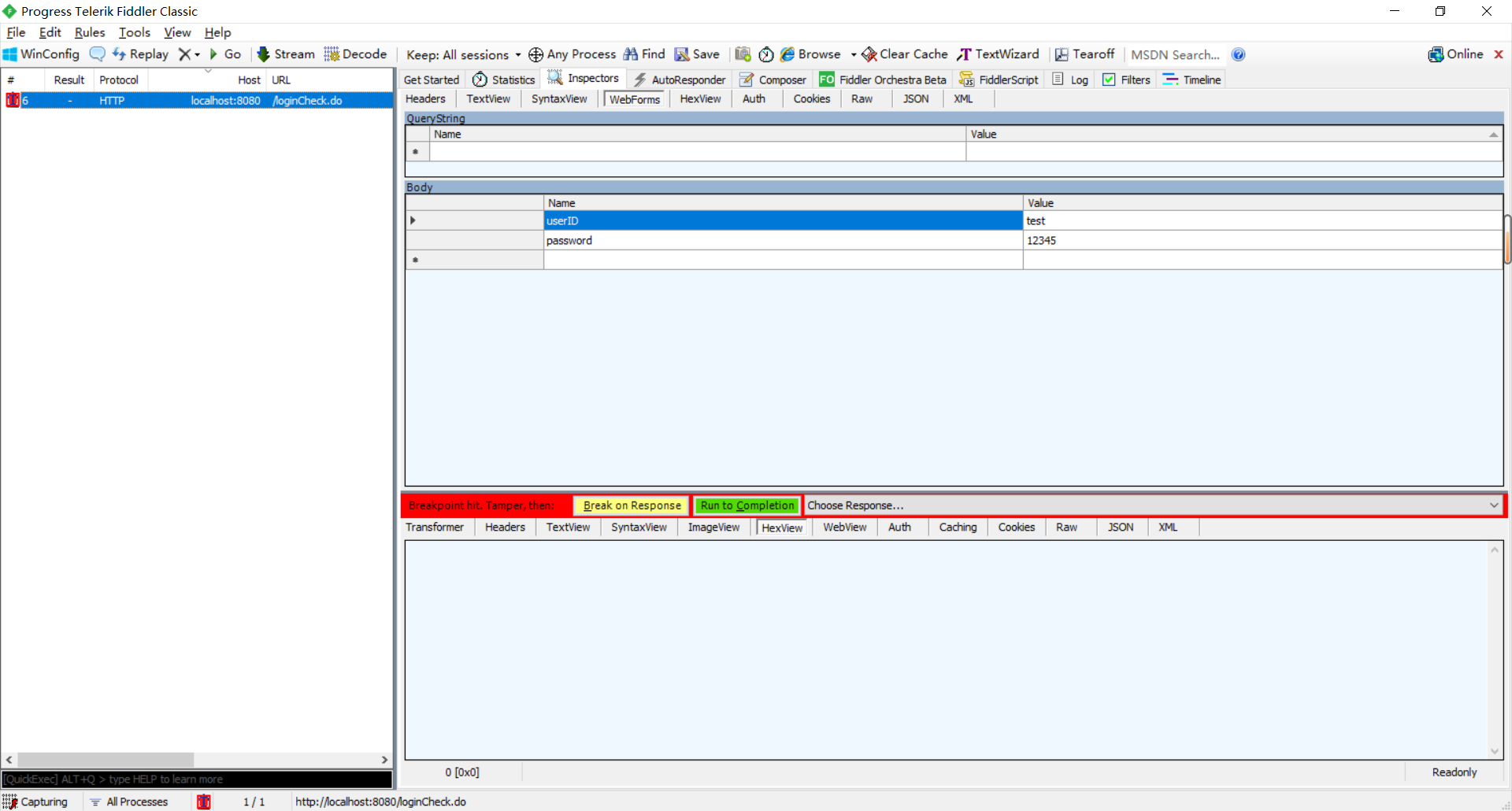


这是后台管理员登陆后的界面，用fiddler进行抓包后拿到cookie

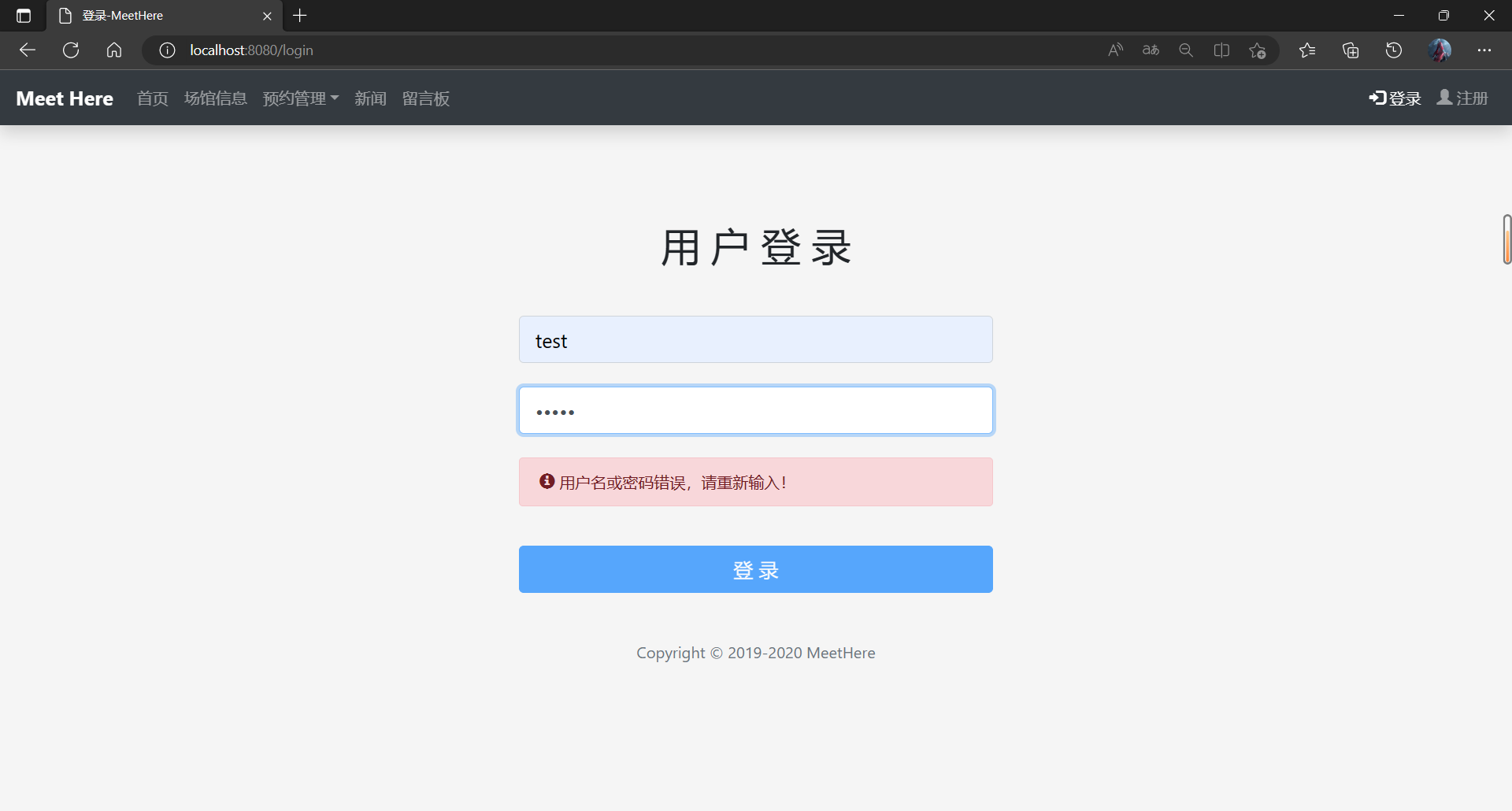


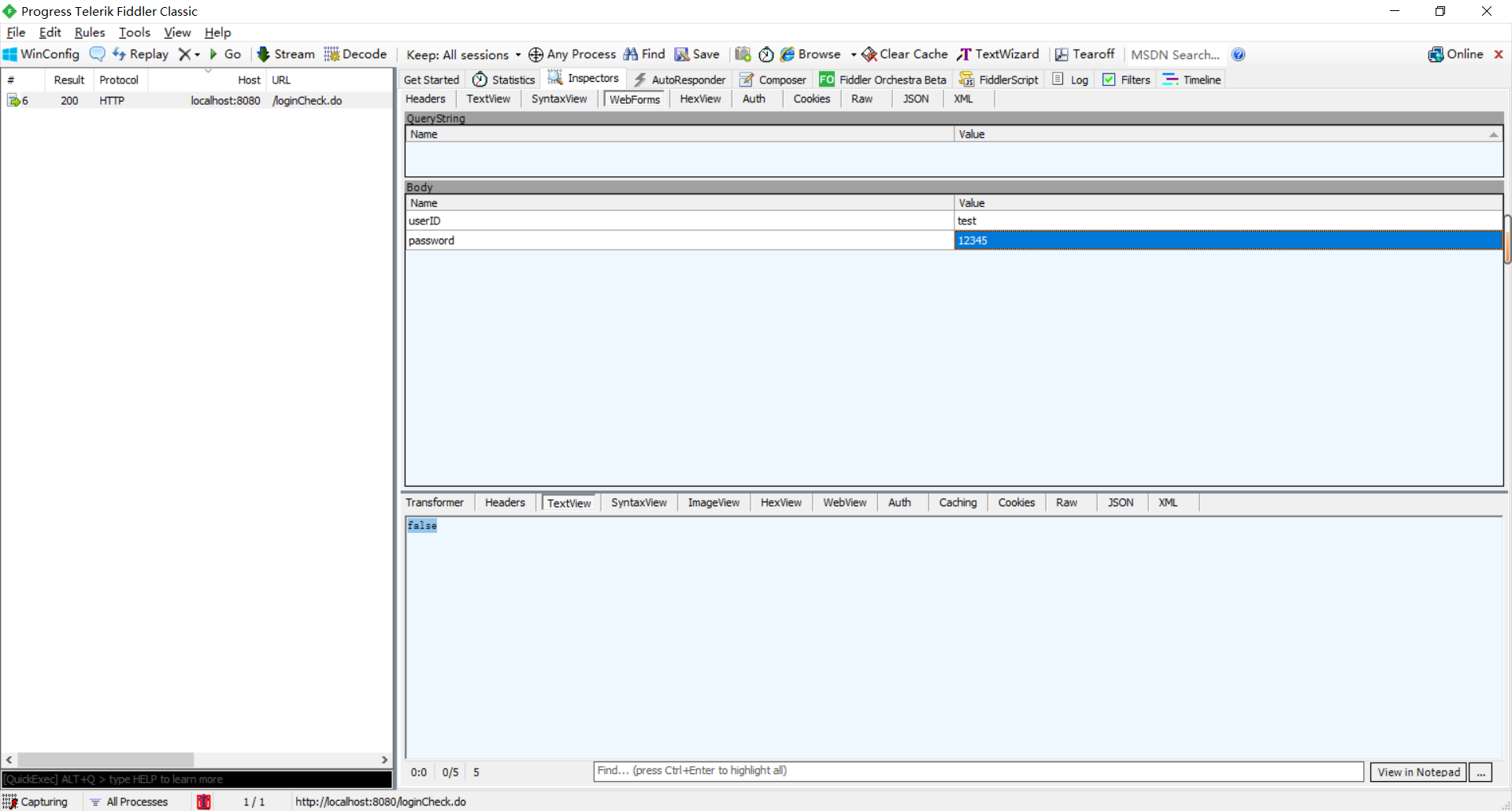


拿到用户登录信息

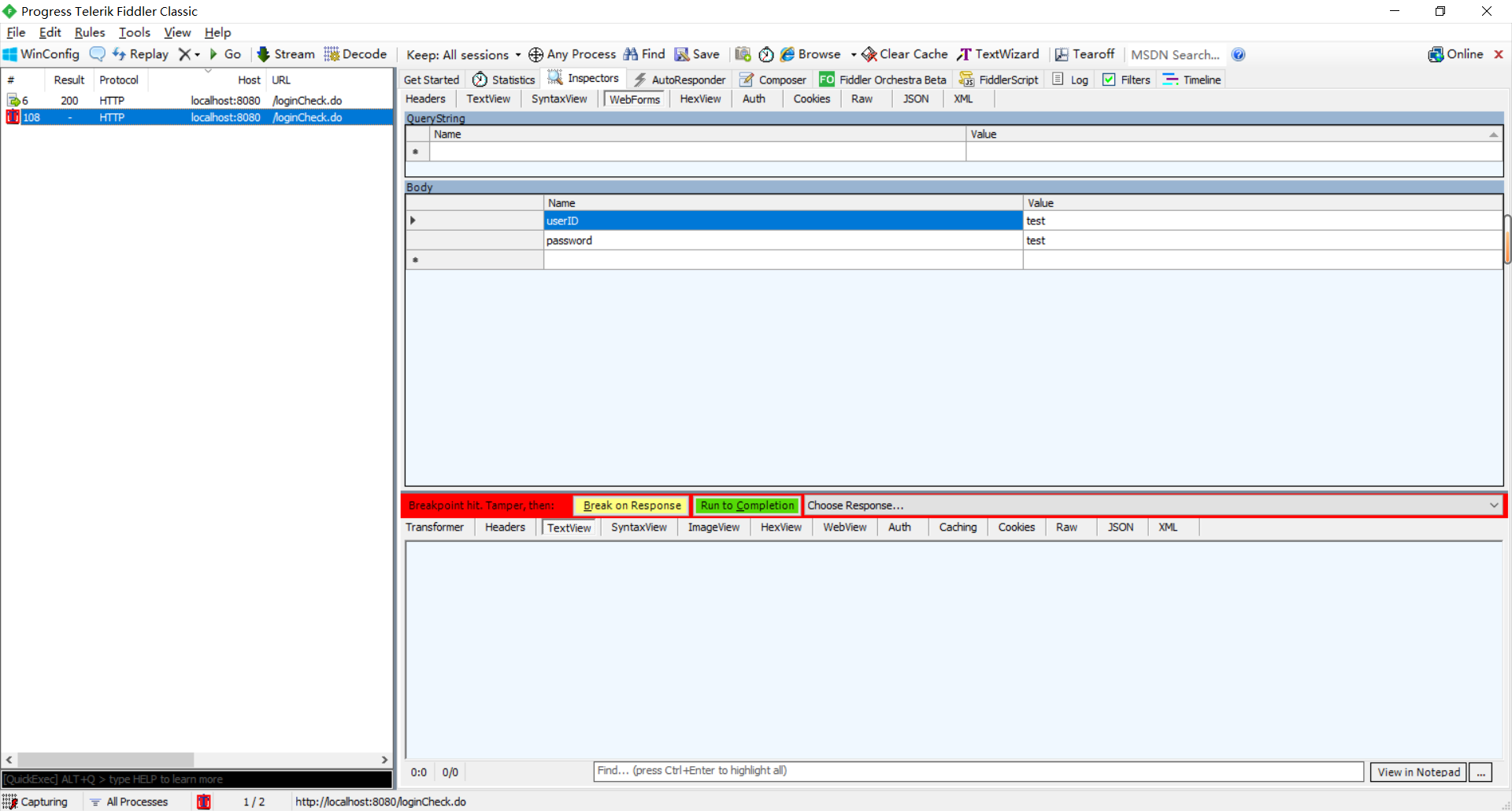


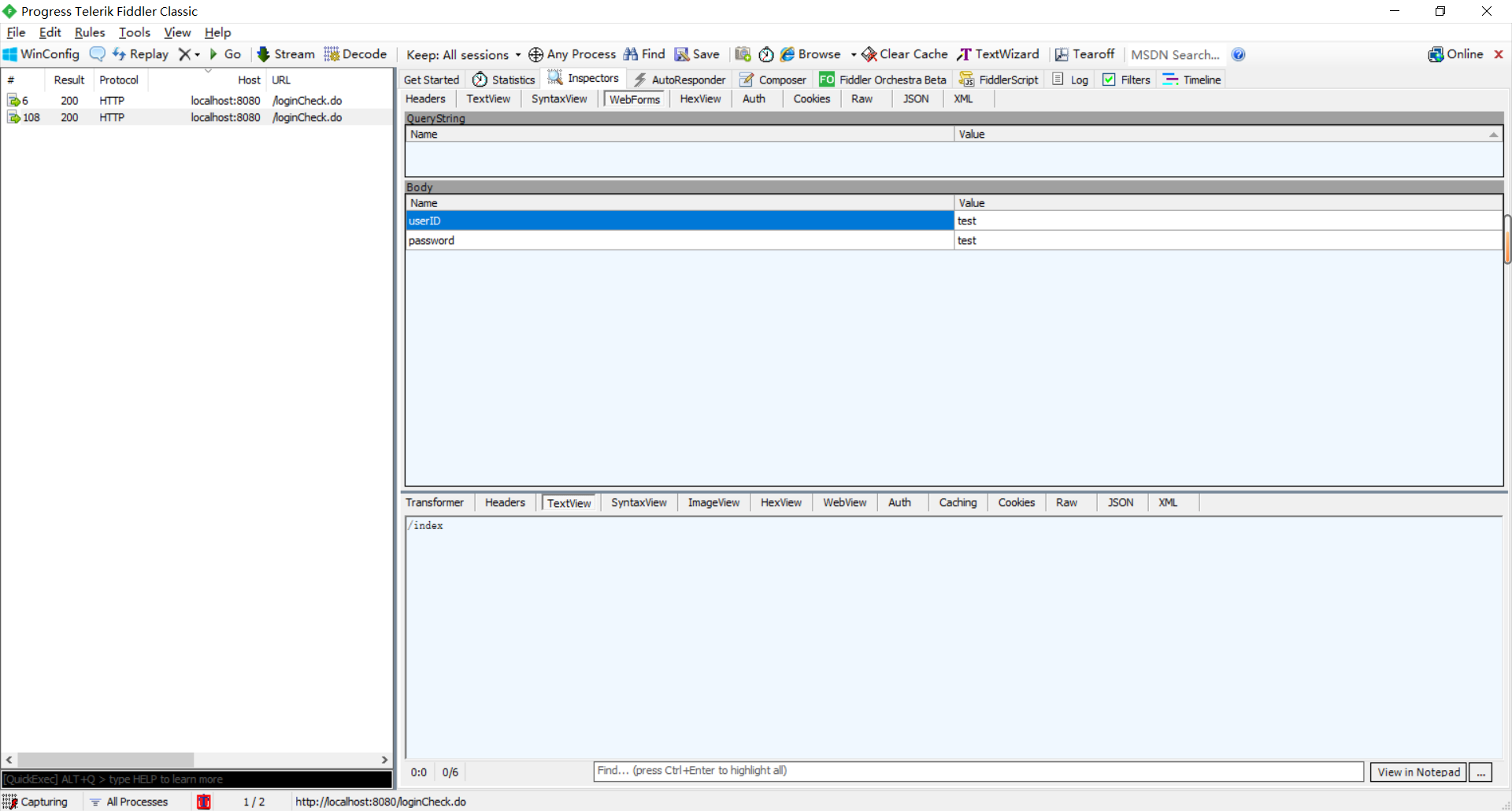
点击Run to Completion

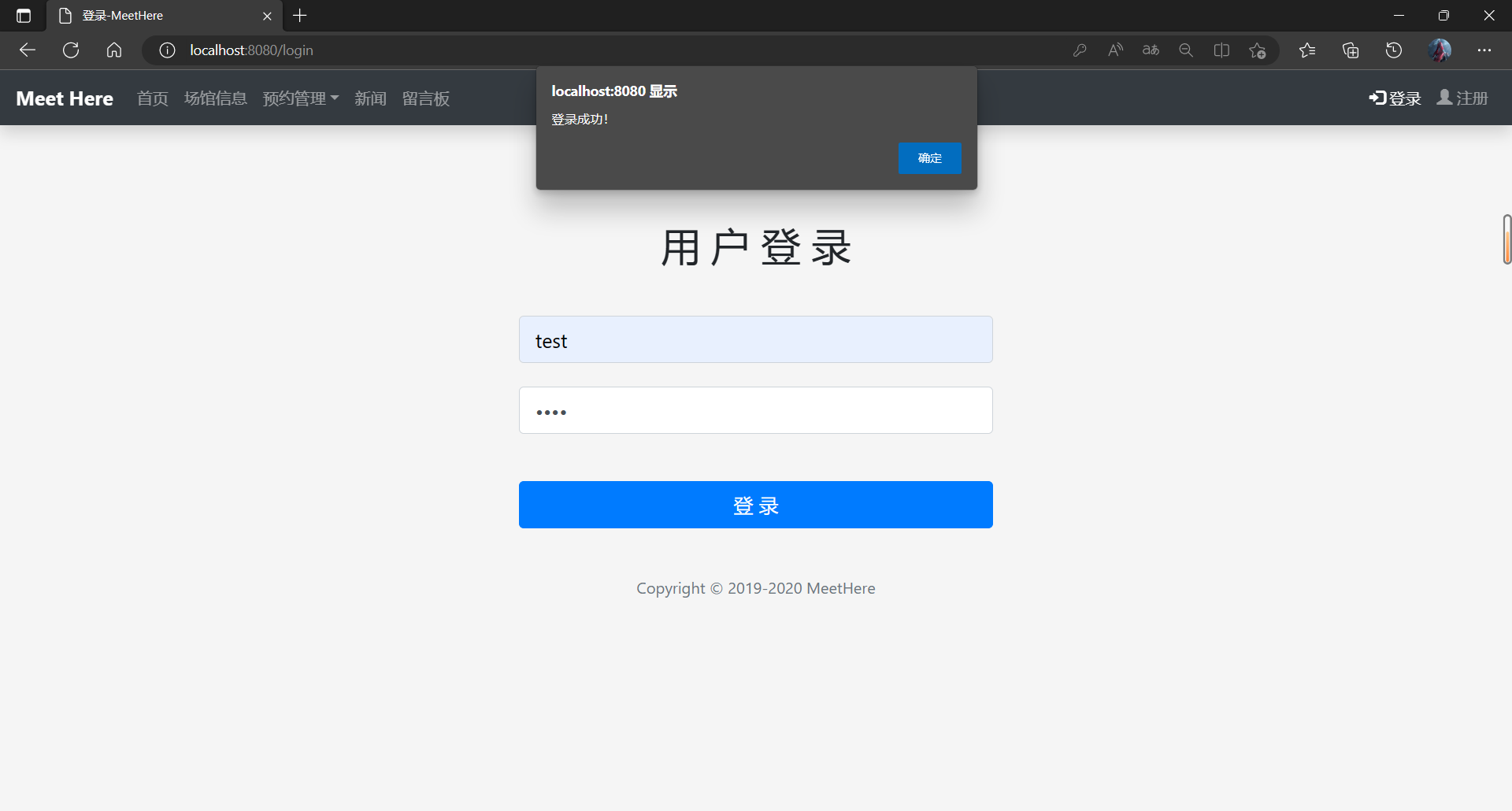




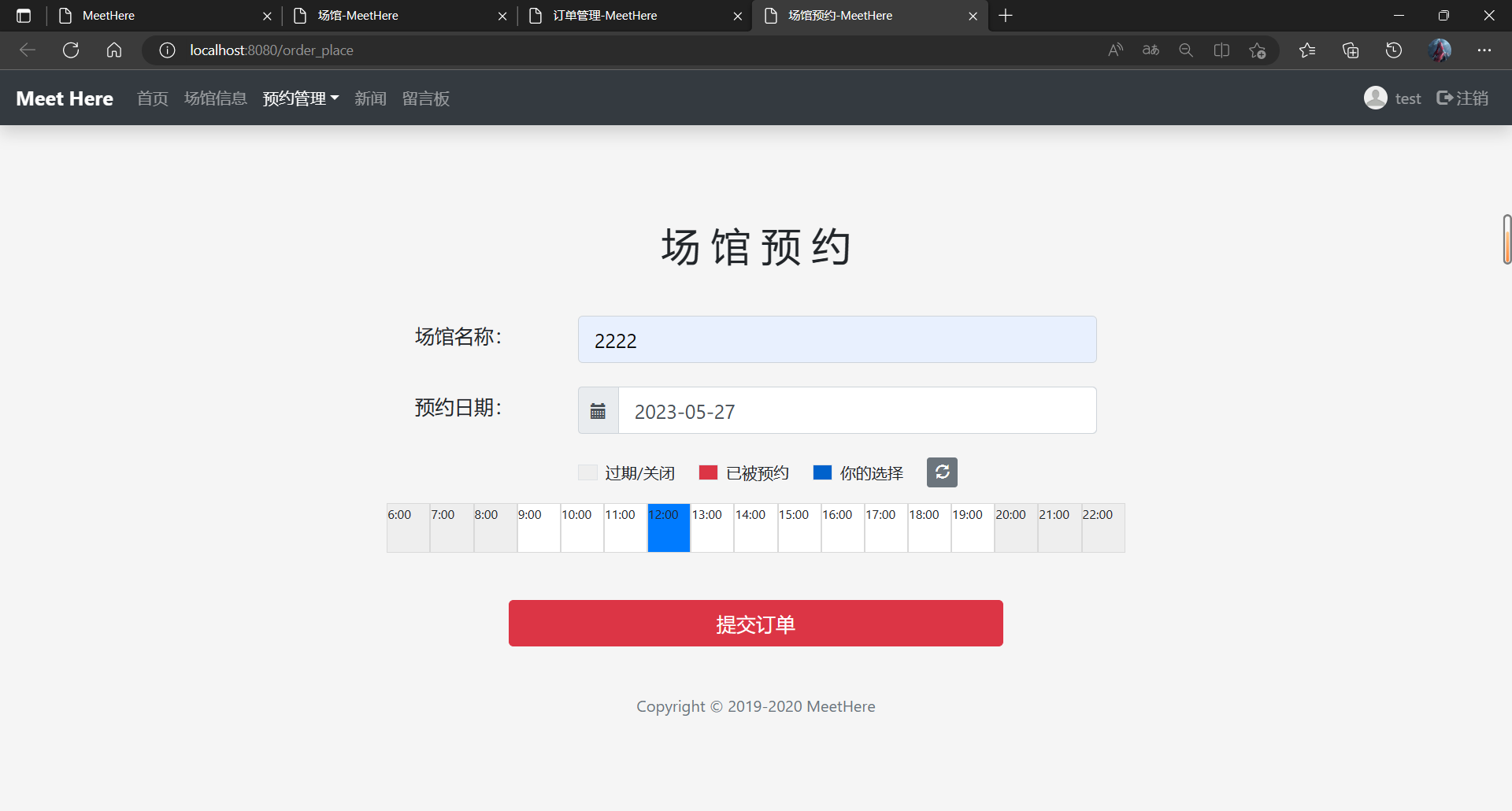
下面为成功登录抓包



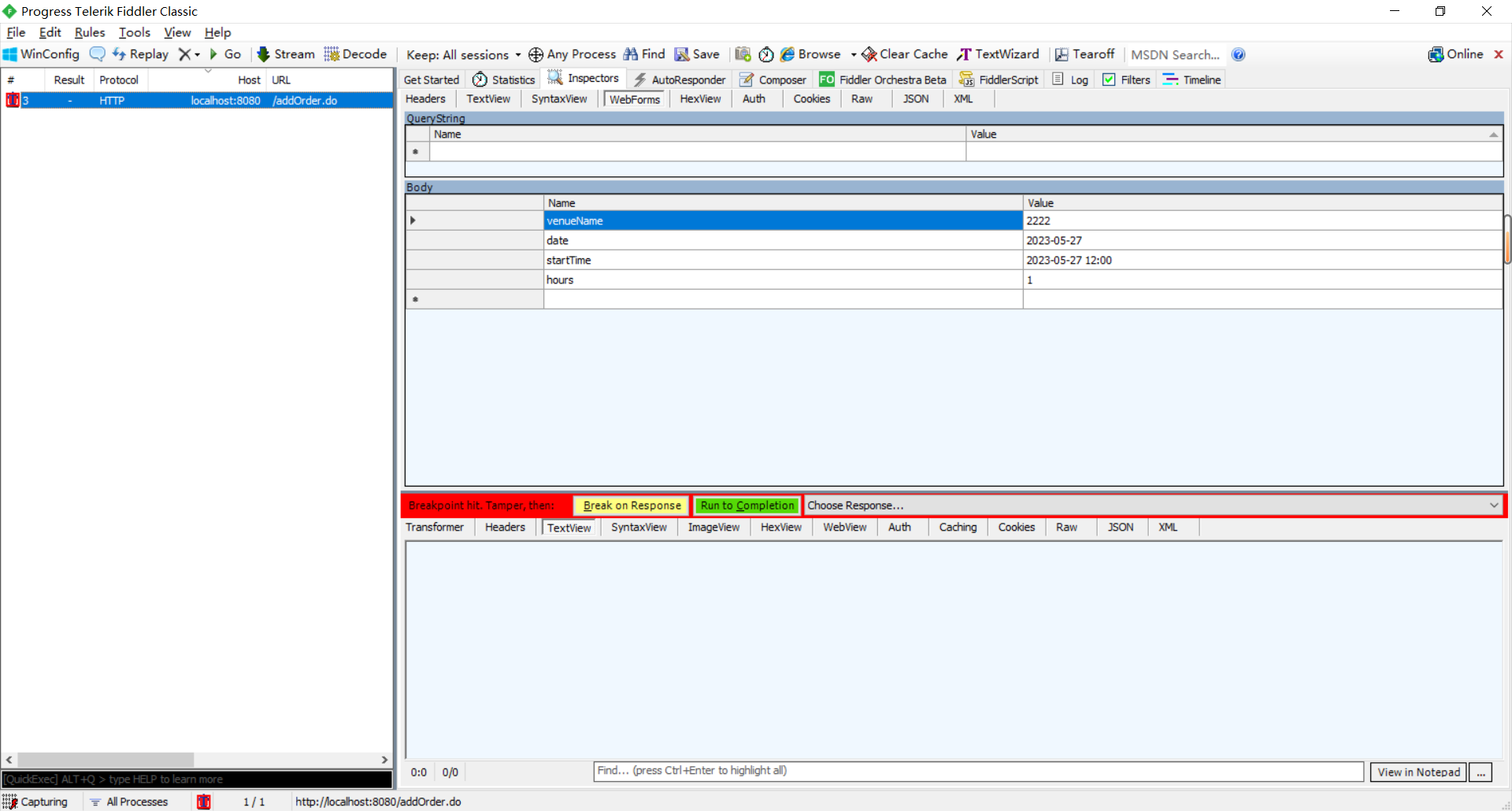




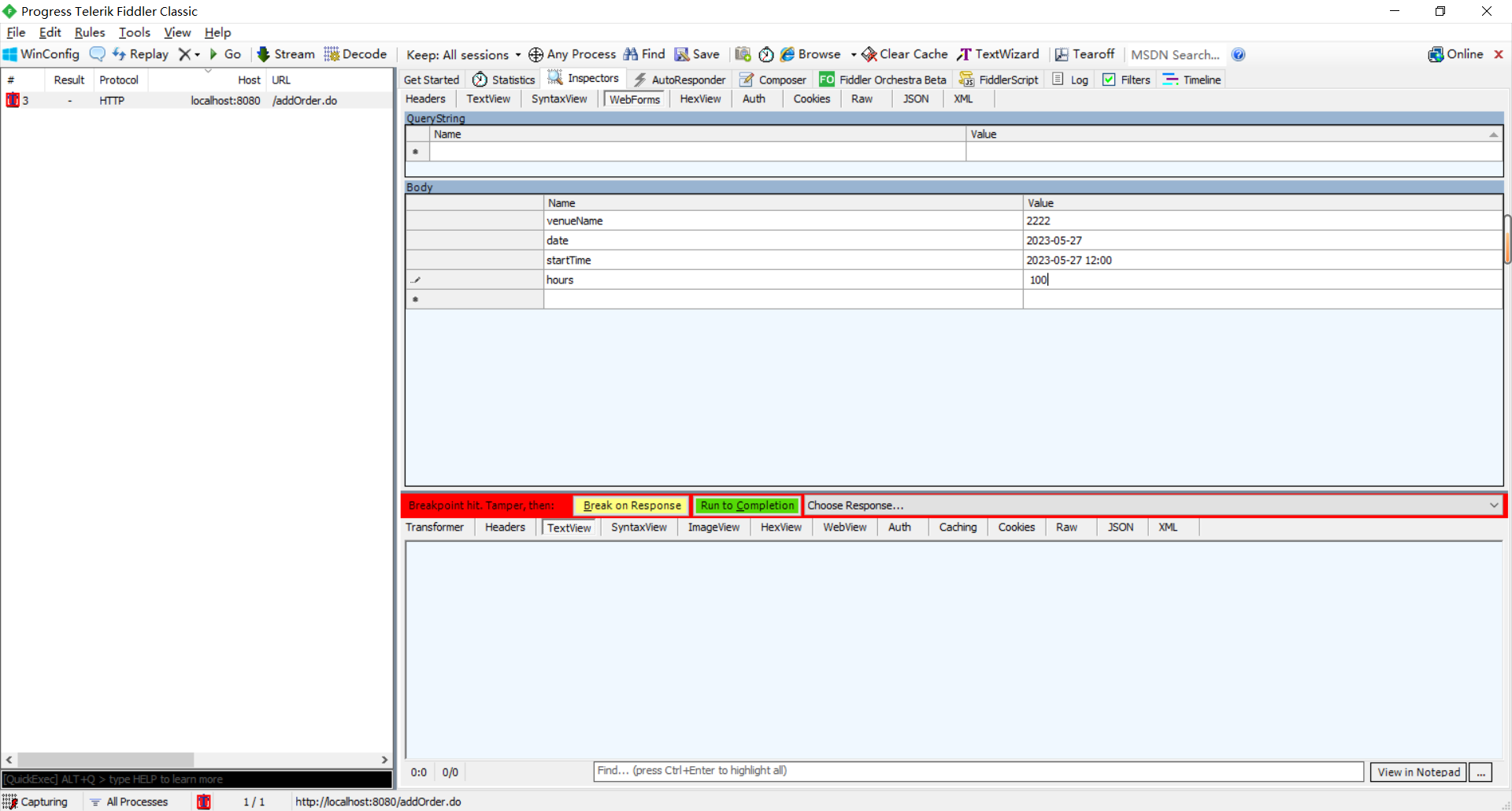
## 2.3预约时间手动抓包进行修改

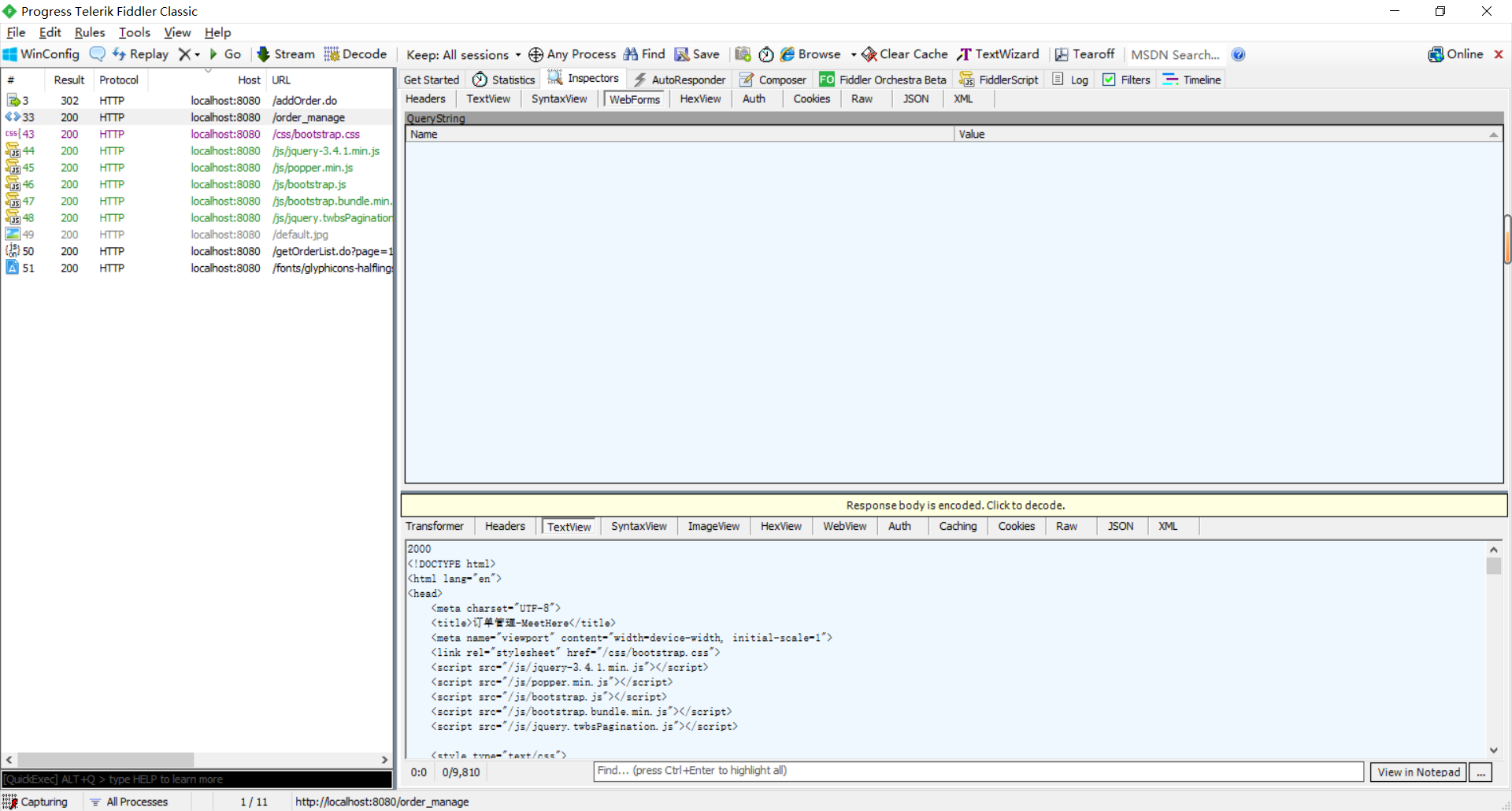


我们对2222场馆进行预约1个小时，然后抓包如下图

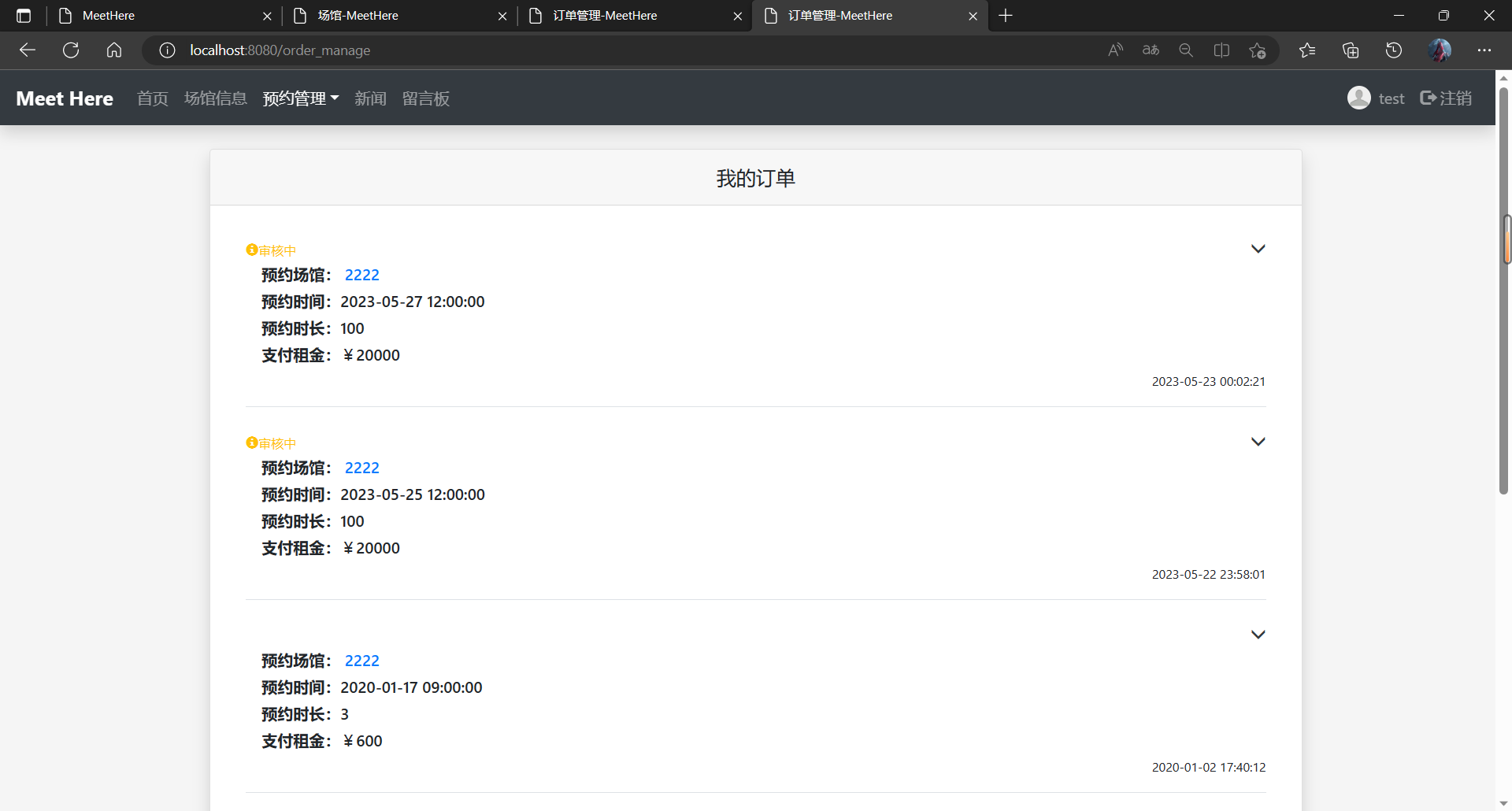


上面显示hour：1h，所以尝试对hour的值进行修改为100h，如下图



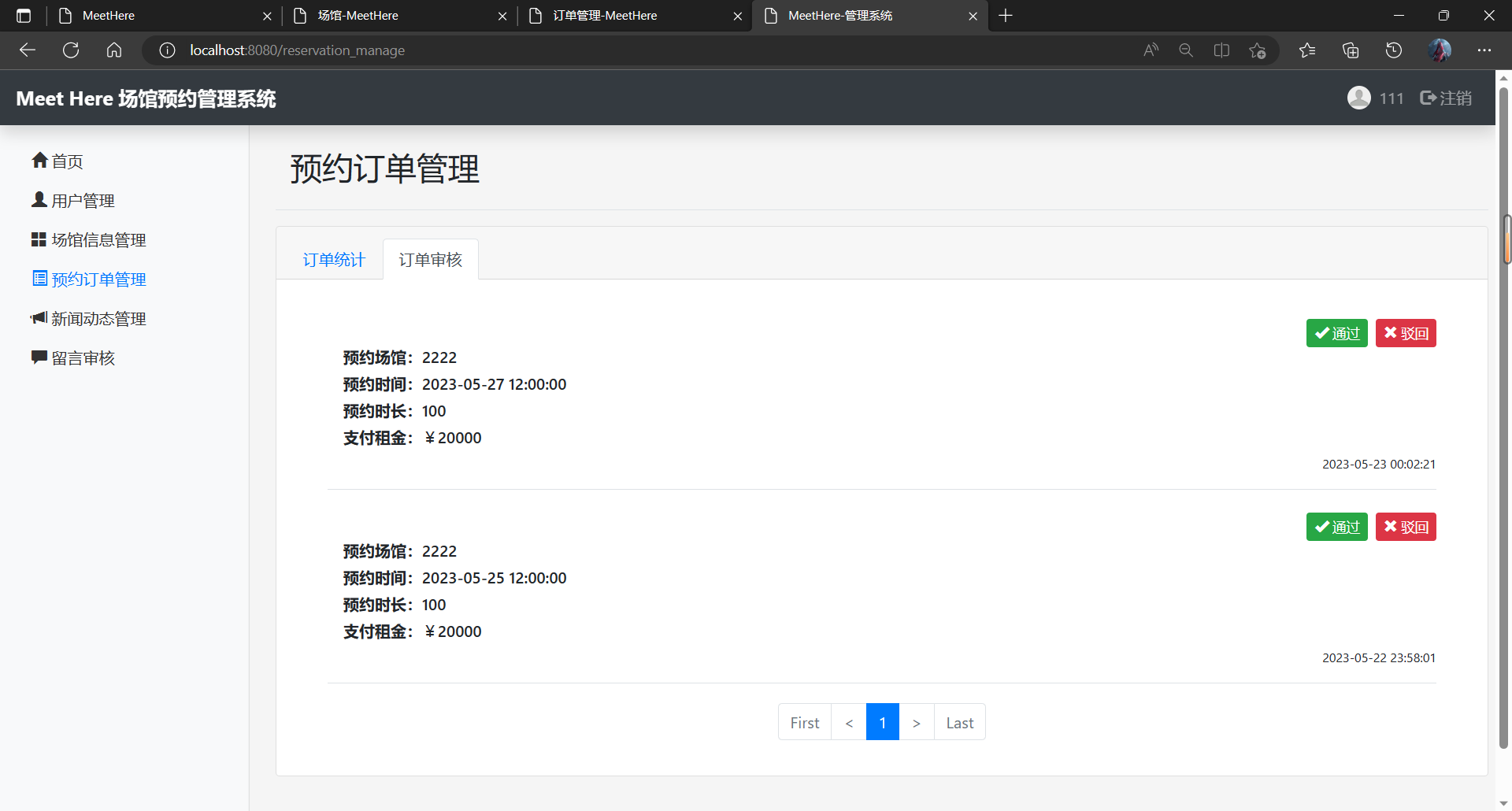


运行后，原网页显示：



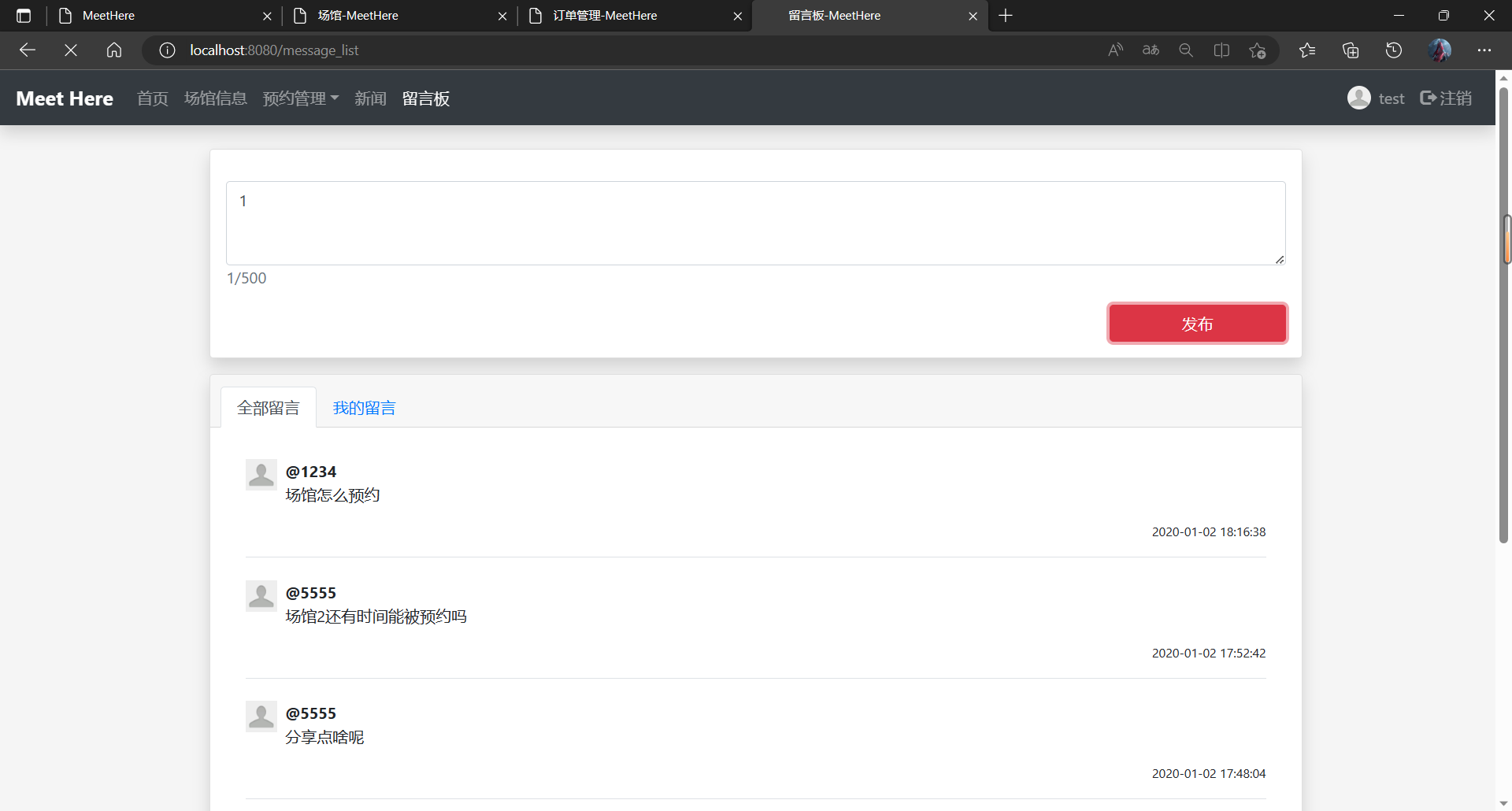
可见，原来我们只是预约1h，但是返回到后台，是100h，所以这里存在安全性漏洞需要修改。

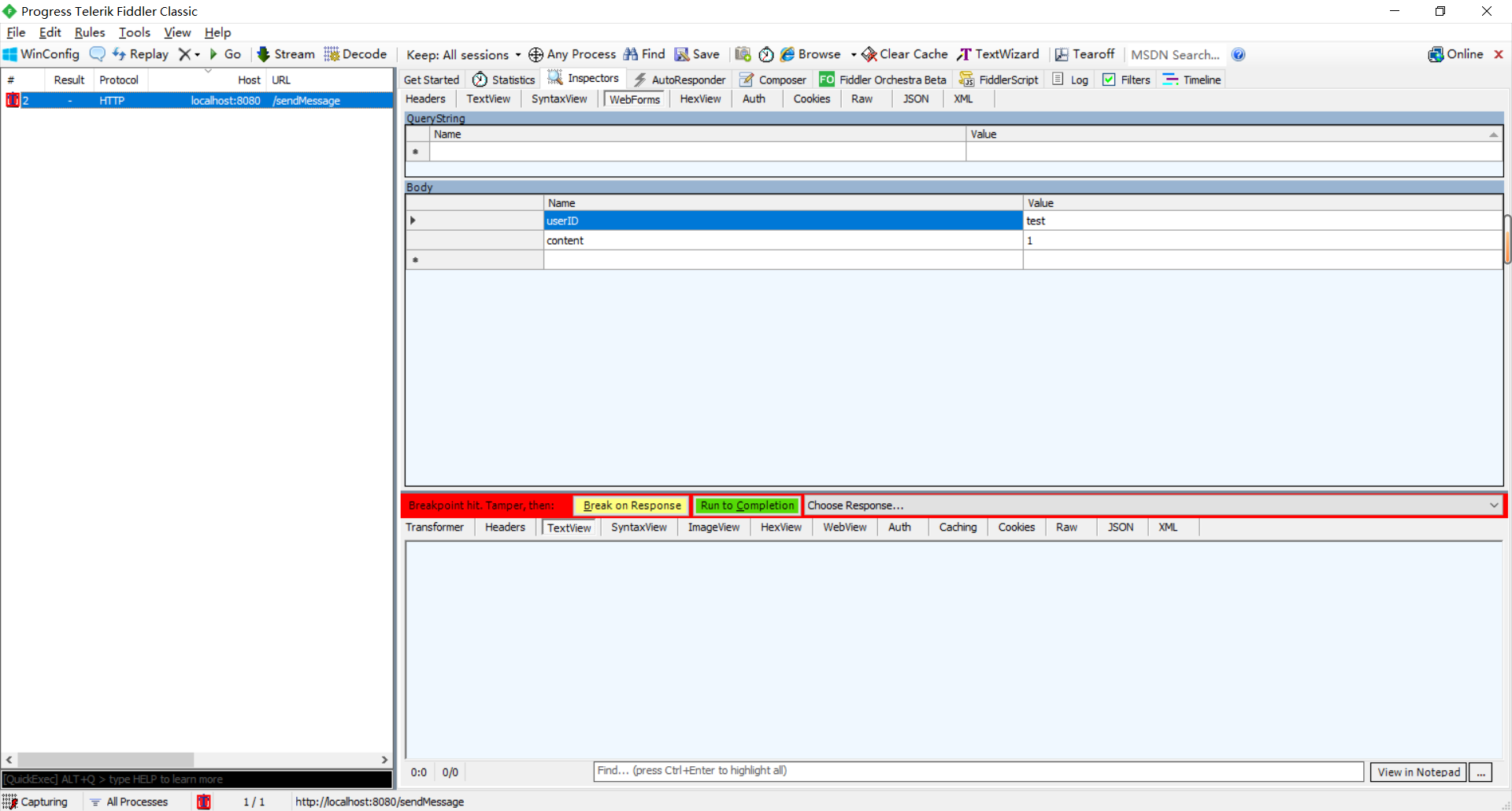
下面登录管理员界面



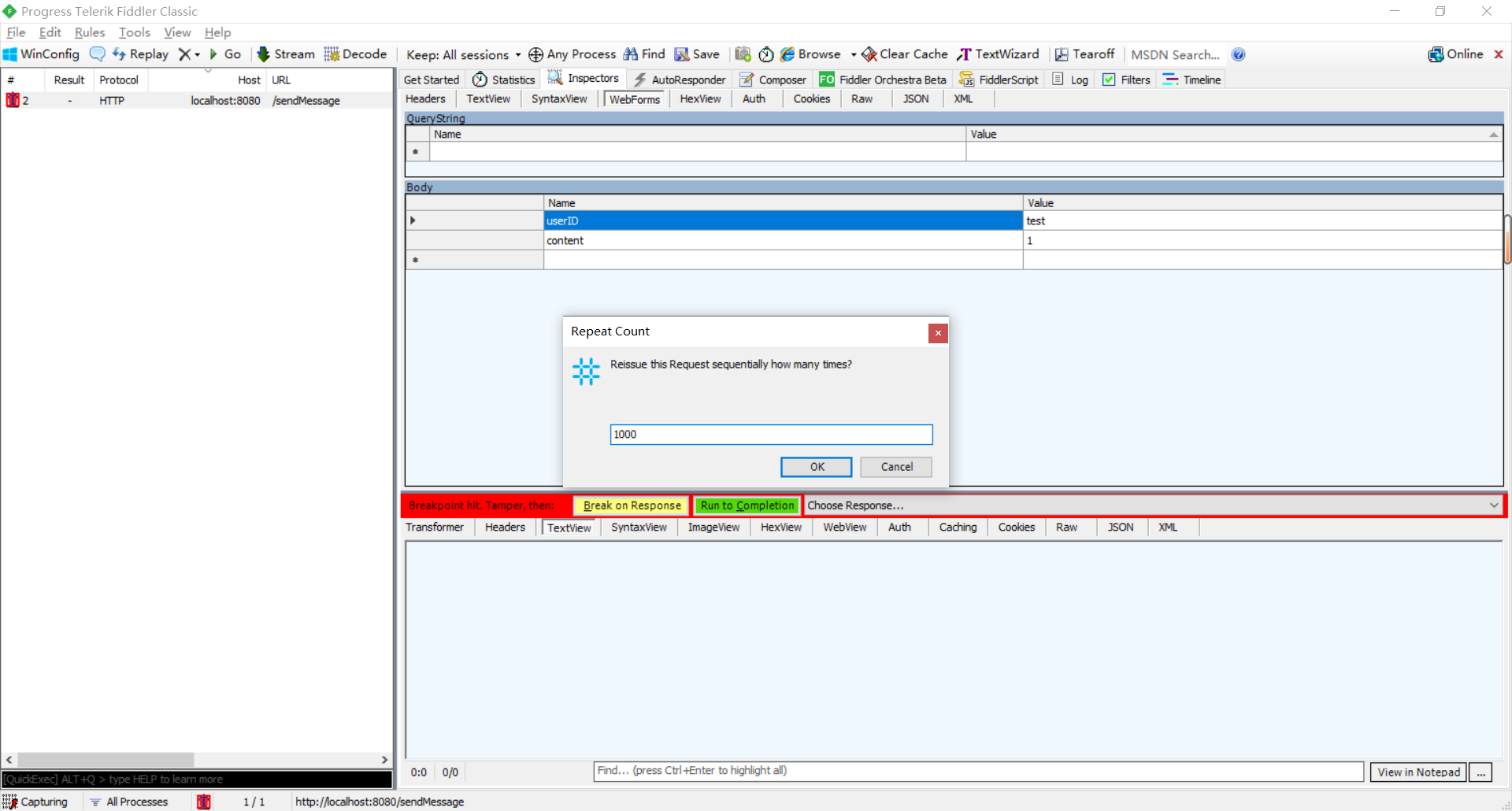
登陆管理员界面后发现，我付出了1h的钱，但是显示我支付了100h的钱，这里有安全漏洞

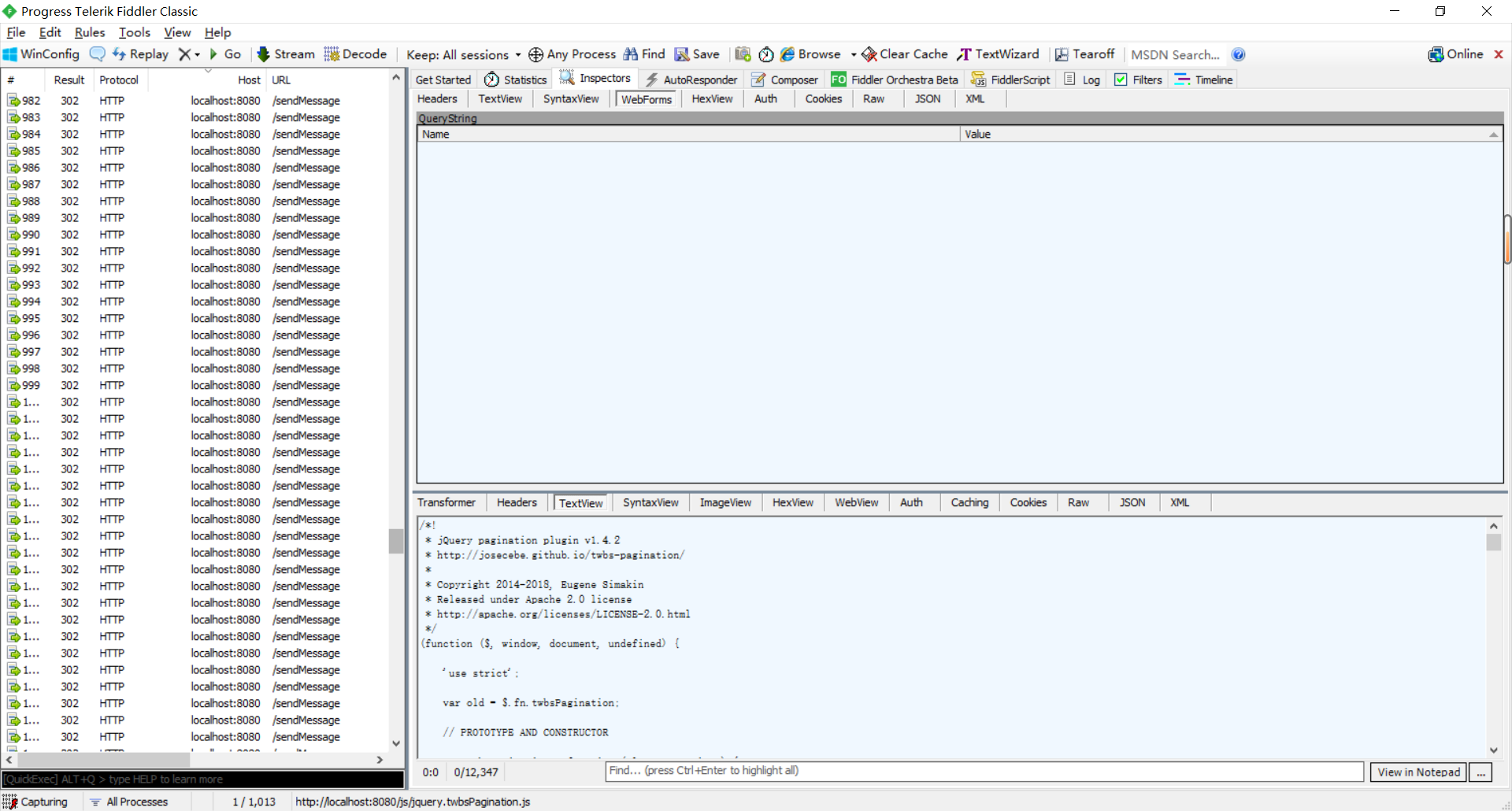
## 2.4进行留言板功能抓包测试



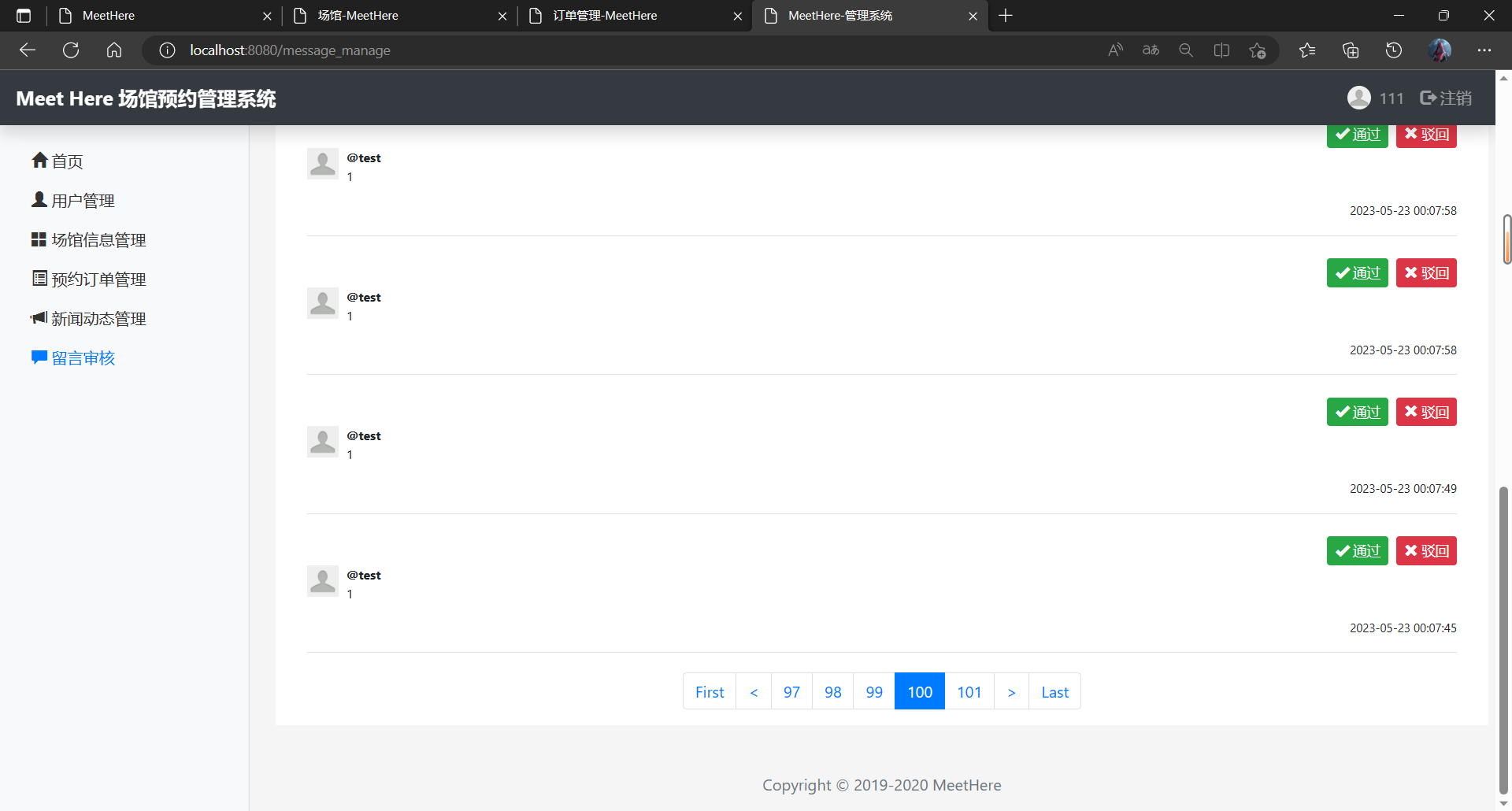


然后在fiddler中我进行一千次如下图





登录管理员界面进行查看



可以看到1000次1，这里也是有安全漏洞需要修改

## 2.5结论

从手动抓包得出，该系统安全性做的不是很好，需要修改的安全漏洞很多。

# 3.安全性测试

## 介绍

该报告会保留由 [公司名称] 安全小组在 [赋值名] 应用程序上执行的 Web 应用程序安全扫描的结果。扫描显示了该应用程序中 1 严重性为高的安全问题、0 严重性为中的安全问题和 22 严重性为低的安全问题。该“管理综合报告”和“详细摘要”已整合查找结果。其他信息包含在该报告的“漏洞详细信息”部分。

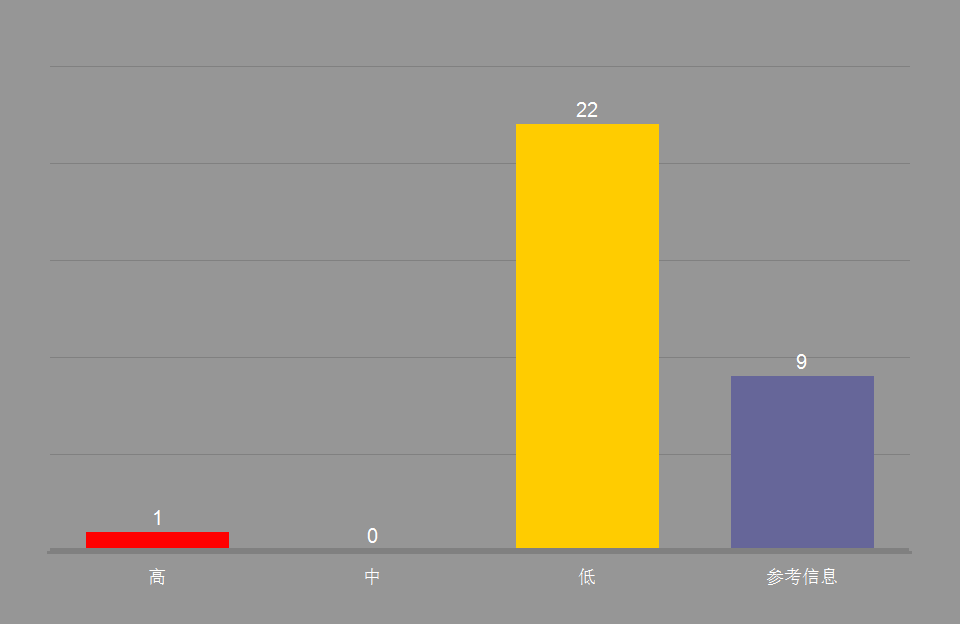
## 目标

[公司名称] 安全小组在 Web 应用程序上执行实时安全评估。这些评估旨在显示已扫描的 Web 应用程序中的任何安全性问题，解释与找到的问题相关联的影响和风险，和提供优先级划分和修复步骤的准则，该赋值的目标是执行控制的攻击和穿透活动，以评估 [赋值名] Web 应用程序的整体安全级别。应用程序的访问凭证和/或应用程序概述已提供/未提供给 [公司名称] 安全小组。该报告包含从已授权/未授权攻击者的角度，对 [赋值名] 应用程序所进行的测试。

## 管理摘要报告

## 问题的数量（全部 32 ）

问题的数量（按照严重性）



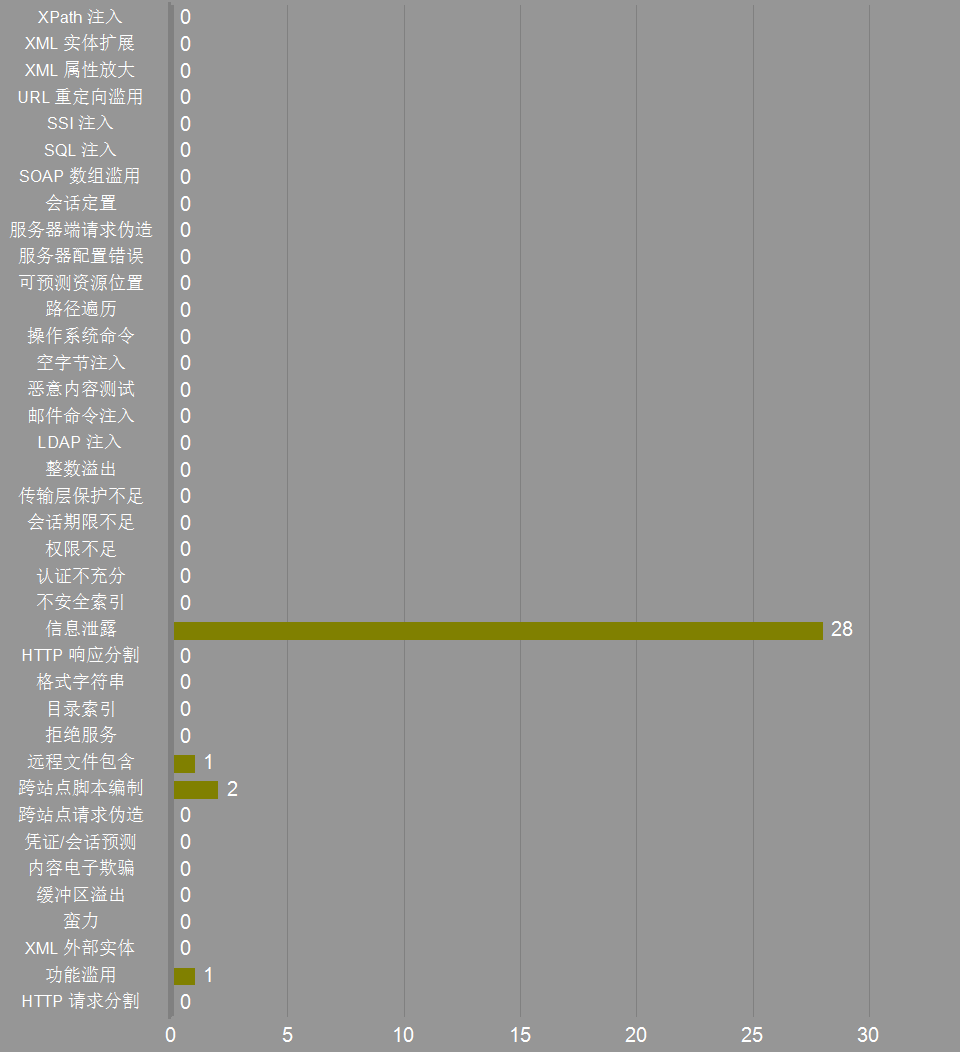
## 问题的数量（按照“测试类型”）

| 类型 | 有漏洞的 URL |
| --- | --- |
| 应用程序 | 28 |
| 基础结构 | 4 |
| 第三方 Web 组件 | 0 |
| 总计 | 32 |

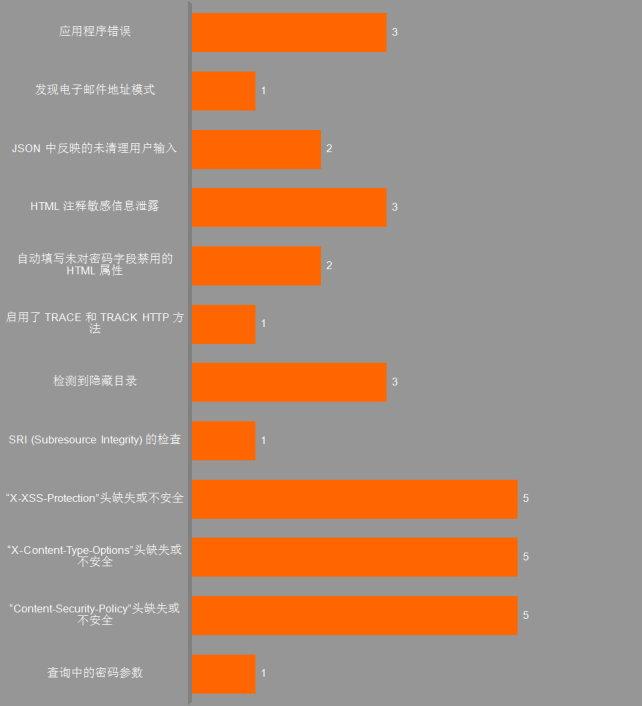
安全性问题（按照“分类”）

安全性问题（按照“问题类型”）

安全性问题（按照“威胁分类”）

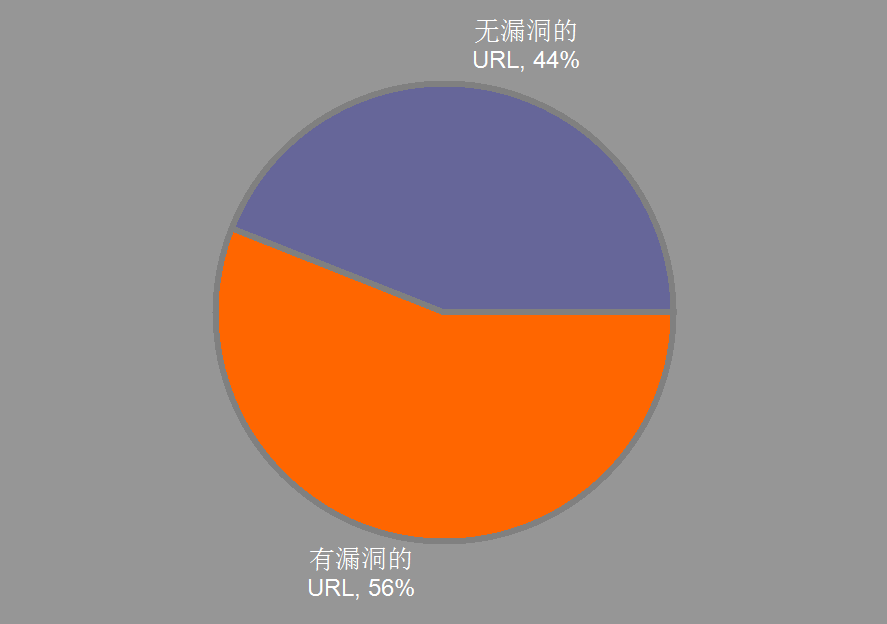


安全性问题（按照“问题类型”）



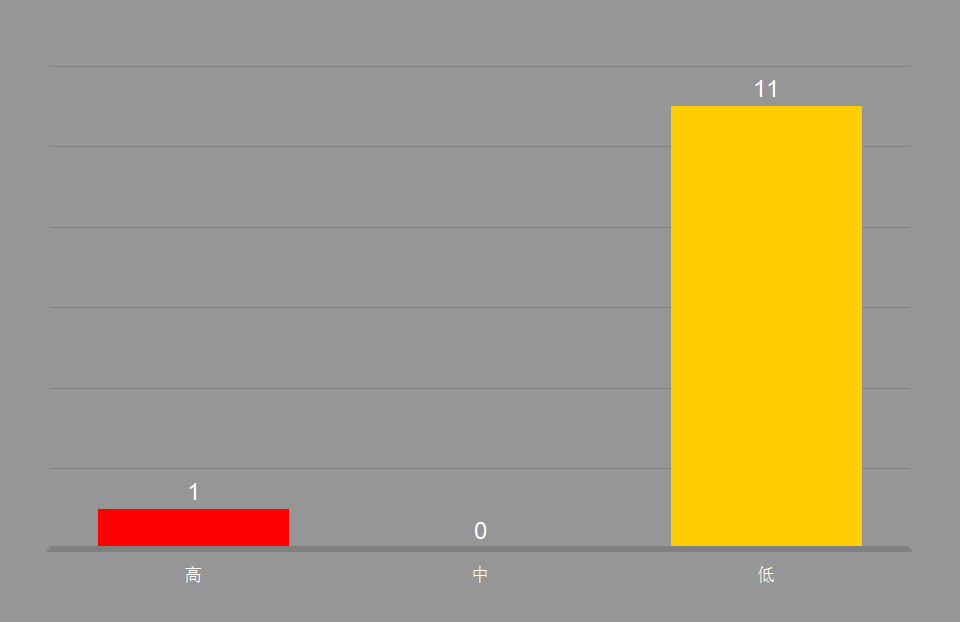
## 有漏洞的 URL 和无漏洞的 URL 比较

有漏洞的 URL 和无漏洞的 URL 比较（% ）



## 修复任务数量

修复任务（按照优先级）



详细摘要

## 高严重性问题

|  | 问题类型 | 问题（所有严重性） |
| --- | --- | --- |
|  | 查询中的密码参数 | 1 |

## 中等级别的安全性问题

|  | 问题类型 | 问题（所有严重性） |
| --- | --- | --- |

## 低级别严重性问题

|  | 问题类型 | 问题（所有严重性） |
| --- | --- | --- |
|  | “Content-Security-Policy”头缺失或不安全 | 5 |
|  | “X-Content-Type-Options”头缺失或不安全 | 5 |
|  | “X-XSS-Protection”头缺失或不安全 | 5 |
|  | SRI (Subresource Integrity) 的检查 | 1 |
|  | 检测到隐藏目录 | 3 |
|  | 启用了 TRACE 和 TRACK HTTP 方法 | 1 |
|  | 自动填写未对密码字段禁用的 HTML 属性 | 2 |

## 参考信息严重性问题

|  | 问题类型 | 问题（所有严重性） |
| --- | --- | --- |
|  | HTML 注释敏感信息泄露 | 3 |
|  | JSON 中反映的未清理用户输入 | 2 |
|  | 发现电子邮件地址模式 | 1 |
|  | 应用程序错误 | 3 |

## 修复任务

|  | 修复任务 | 计数 | 优先级 |
| --- | --- | --- | --- |
|  | 发送敏感信息时，始终使用 SSL 和 POST（主体）参数。 | 1 | High |
|  | 查看危险字符注入的可能解决方案 | 2 | Low |
|  | 除去 HTML 注释中的敏感信息 | 3 | Low |
|  | 除去 Web 站点中的电子邮件地址 | 1 | Low |
|  | 对禁止的资源发布“404 - Not Found”响应状态代码，或者将其完全除去 | 3 | Low |
|  | 将“autocomplete”属性正确设置为“off” | 2 | Low |
|  | 将服务器配置为使用安全策略的“Content-Security-Policy”头 | 5 | Low |
|  | 将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头 | 5 | Low |
|  | 将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头 | 5 | Low |
|  | 将每个第三方脚本/链接元素支持添加到 SRI(Subresource Integrity)。 | 1 | Low |
|  | 验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常 | 3 | Low |
|  | 在 Web 服务器中禁用 HTTP TRACE 支持 | 1 | Low |

## 有漏洞的 URL

| URL | 问题（类型） | 修复任务（类型） |
| --- | --- | --- |
| http://localhost:8080/login/ | 1 (1) | 1 (1) |
| http://localhost:8080/signup/ | 1 (1) | 1 (1) |
| http://localhost:8080/index/ | 1 (1) | 1 (1) |
| http://localhost:8080/news/getNewsList | 1 (1) | 1 (1) |
| http://localhost:8080/venuelist/getVenueList | 1 (1) | 1 (1) |
| http://localhost:8080/js/jquery-3.4.1.min.js | 1 (1) | 1 (1) |
| http://localhost:8080/venue\_list | 2 (2) | 2 (2) |
| http://localhost:8080/venue | 6 (6) | 6 (6) |
| http://localhost:8080/signup | 4 (4) | 4 (4) |
| http://localhost:8080/register.do | 1 (1) | 1 (1) |
| http://localhost:8080/order\_place | 1 (1) | 1 (1) |
| http://localhost:8080/news\_list | 3 (3) | 3 (3) |
| http://localhost:8080/news | 4 (4) | 4 (4) |
| http://localhost:8080/login | 2 (2) | 2 (2) |
| http://localhost:8080/index | 3 (3) | 3 (3) |

漏洞详细信息

## 严重性为高的“问题类型”

|  |  |
| --- | --- |
|  | 查询中的密码参数 (1/1) |

**咨询和修订建议**

[信息泄露](http://projects.webappsec.org/Information-Leakage)

在应用程序测试过程中，检测到查询字符串中接收到密码参数。由于登录过程所用的部分输入字段（例如：用户名、密码、电子邮件地址、社会保险号码，等等）是个人敏感信息，建议将其放在请求的主体部分或加密连接（如 SSL）中来发送到服务器。任何通过查询字符串传给服务器的信息都可能被窃，稍后可用来电子欺骗身份或伪装用户。

此外，若干隐私权法规指出，用户凭证之类的敏感信息一律以加密方式传给网站。

可能会窃取查询字符串中发送的敏感数据，例如用户名和密码

[金融隐私权：格拉斯-斯蒂格尔法案](http://business.ftc.gov/privacy-and-security/gramm-leach-bliley-act/)

[健康保险可移植性和责任法案 (HIPAA)](http://www.hhs.gov/ocr/hipaa/)

[萨班斯法案](http://www.sec.gov/spotlight/sarbanes-oxley.htm)

[加利福尼亚州 SB1386](http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html)

查询中的密码参数

查询中的密码参数

查询字符串中传递了敏感输入字段（例如用户名、密码和信用卡号）

该问题可能会影响各种类型的产品

#### 受影响的 URL

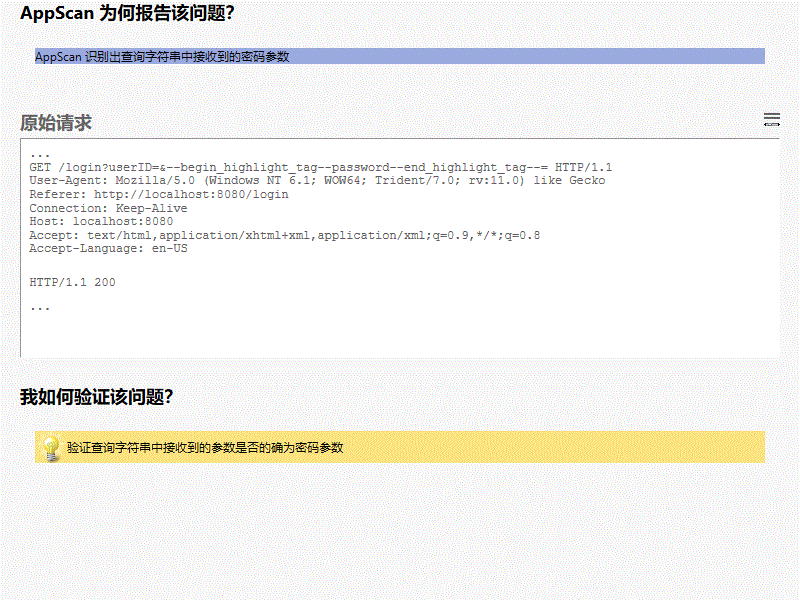
* http://localhost:8080/login

#### 问题 1/1（ http://localhost:8080/login － password ）

#### 严重性： High

#### CVSS 计分： 8.5

#### 图像



**所有变体**

#### 变体差异

变体原因  
AppScan 识别出查询字符串中接收到的密码参数

#### 变体验证

• GET /login?userID=**password**d= HTTP/1.1

变体请求响应  
GET /login?userID=&password= HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

Referer: http://localhost:8080/login

Connection: Keep-Alive

Host: localhost:8080

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Language: en-US

HTTP/1.1 200

Transfer-Encoding: chunked

Connection: keep-alive

Keep-Alive: timeout=60

Content-Language: en-US

Date: Mon, 22 May 2023 08:33:50 GMT

Content-Type: text/html;charset=UTF-8

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<title>登录-MeetHere</title>

<meta name="viewport" content="width=device-width, initial-scale=1">

<link rel="stylesheet" href="/css/bootstrap.css">

<script src="/js/jquery-3.4.1.min.js"></script>

<script src="js/jquery.form.js"></script>

<script src="/js/bootstrap.bundle.min.js"></script>

<style type="text/css">

body{

background-color: #f5f5f5;

}

</style>

</head>

<body>

<div>

<nav class="navbar navbar-expand-sm navbar-dark fixed-top bg-dark shadow" role="navigation">

<div class="navbar-header">

<a class="navbar-brand" href="index" style="font-weight: bold">Meet Here</a>

</div>

<button class="navbar-toggler" data-toggle="collapse" data-target="#navbar">

<span class="navbar-toggler-icon"></span>

</button>

<div class="collapse navbar-collapse" id="navbar">

<ul class="navbar-nav mr-auto">

<li class="nav-item">

<a class="nav-link" href="index">首页</a>

</li>

<li class="nav-item">

<a class="nav-link" href="venue\_list">场馆信息</a>

</li>

<li class="nav-item dropdown">

<a class="nav-link dropdown-toggle" href="#" id="dropdown" data-toggle="dropdown">预约管理</a>

<div class="dropdown-menu">

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_place(false)">场馆预约</a>

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_manage(false)">订单管理</a>

</div>

</li>

<li class="nav-item">

<a class="nav-link" href="news\_list">新闻</a>

</li>

<li class="nav-item">

<a class="nav-link loginfirst" href="#" onclick="javascript:message\_list(false)">留言板</a>

</li>

</ul>

<div>

<ul class="navbar-nav ml-auto">

<li class="nav-item active">

<a class="nav-link" href="login"><span class="glyphicon glyphicon-log-in"></span> 登录</a>

</li>

<li class="nav-item">

<a class="nav-link" href="signup"><span class="glyphicon glyphicon-user"></span> 注册</a>

</li>

</ul>

</div>

</div>

</nav>

<script type="text/javascript">

$('.dropdown-toggle').dropdown();

function message\_list(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/message\_list';

}

}

function order\_manage(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/order\_manage';

}

}

function order\_place(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.open('/order\_place');

// window.location.href = '/order\_place';

}

}

</script>

</div>

<main class="container col-4" style="padding-top: 10%">

<form role="form">

<div class="text-center mb-5">

<h1>用 户 登 录</h1>

</div>

<div class="form-group mb-4">

<label for="userID" class="sr-only">User Name</label>

<input type="text" name="userID" class="form-control form-control-lg" id="userID" placeholder="用户名" required autofocus>

</div>

<div class="form-group mb-4">

<label for="password" class="sr-only">Password</label>

<input type="password" name="password" class="form-control form-control-lg" id="password" placeholder="密码" required>

</div>

<div class="alert alert-danger" hidden><span class="glyphicon glyphicon-info-sign"></span> 用户名或密码错误，请重新输入！</div>

<div class="pt-4">

<button class="btn btn-lg btn-primary btn-block" type="submit" id="submit">登 录</button>

</div>

</form>

</main>

<div>

<footer class="mt-5 mb-3 text-muted text-center">Copyright &copy; 2019-2020 M...

## 严重性为中的“问题类型”

## 严重性为低的“问题类型”

|  |  |
| --- | --- |
|  | “Content-Security-Policy”头缺失或不安全 (1/7) |

##### 咨询和修订建议

[信息泄露](http://projects.webappsec.org/Information-Leakage)

“内容安全策略”标头旨在修改浏览器呈现页面的方式，从而防止各种跨站点注入，包括跨站点脚本。以不妨碍网站正常运行的方式正确设置标头值非常重要。例如，如果将标头设置为阻止执行内联 JavaScript，则网站不得在其页面中使用内联 JavaScript。

为了防止跨站点脚本、跨框架脚本和点击劫持，使用适当的值设置以下策略非常重要：

'default-src' 和 'frame-ancestors'策略、\*或\*所有 'script-src'、'object-src' 和 'frame-ancestors’ 策略。

对于 'default-src'、'script-src' 和 'object-src'，应避免使用不安全的值，例如 '\*'、'data:'、'unsafe-inline' 或 'unsafe-eval'。

对于 'frame-ancestors'，应避免使用不安全的值，例如 '\*' 或 'data:'。

有关更多信息，请参阅以下链接。

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

[有用 HTTP 头列表](https://www.owasp.org/index.php/List_of_useful_HTTP_headers)

[内容安全策略简介](http://www.html5rocks.com/en/tutorials/security/content-security-policy/)

[MDN Web 文档 - 内容安全策略](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy)

“Content-Security-Policy”头缺失或不安全

“Content-Security-Policy”头缺失或不安全

Web 应用程序编程或配置不安全

此问题可能影响不同类型的产品

##### 受影响的 URL

* http://localhost:8080/index
* http://localhost:8080/news
* http://localhost:8080/news\_list
* http://localhost:8080/signup
* http://localhost:8080/venue

##### 问题 1/5（ http://localhost:8080/news\_list － news\_list ）

##### 严重性： Low

##### CVSS 计分： 5

##### 图像



**所有变体**

##### 变体差异

变体原因  
AppScan 检测到 Content-Security-Policy 响应头缺失或具有不安全策略，这可能会更大程度地暴露于各种跨站点注入攻击之下

##### 变体验证

• HTTP/1.1 **200**

变体请求响应  
GET /news\_list HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

Referer: http://localhost:8080/login

Connection: keep-alive

Host: localhost:8080

Upgrade-Insecure-Requests: 1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8

Accept-Language: en-US

HTTP/1.1 200

Transfer-Encoding: chunked

Connection: keep-alive

Keep-Alive: timeout=60

Content-Language: en-US

Date: Mon, 22 May 2023 08:34:10 GMT

Content-Type: text/html;charset=UTF-8

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<title>新闻动态-MeetHere</title>

<meta name="viewport" content="width=device-width, initial-scale=1">

<link rel="stylesheet" href="/css/bootstrap.css">

<script src="/js/jquery-3.4.1.min.js"></script>

<script src="/js/bootstrap.bundle.min.js"></script>

<script src="/js/jquery.twbsPagination.js"></script>

<style type="text/css">

body{

background-color: #f5f5f5;

padding-top: 80px;

}

html {

overflow-y: scroll;

}

:root {

overflow-y: auto;

overflow-x: hidden;

}

:root body {

position: absolute;

}

body {

width: 100vw;

overflow: hidden;

}

</style>

</head>

<body>

<div>

<nav class="navbar navbar-expand-sm navbar-dark fixed-top bg-dark shadow" role="navigation">

<div class="navbar-header">

<a class="navbar-brand" href="index" style="font-weight: bold">Meet Here</a>

</div>

<button class="navbar-toggler" data-toggle="collapse" data-target="#navbar">

<span class="navbar-toggler-icon"></span>

</button>

<div class="collapse navbar-collapse" id="navbar">

<ul class="navbar-nav mr-auto">

<li class="nav-item">

<a class="nav-link" href="index">首页</a>

</li>

<li class="nav-item">

<a class="nav-link" href="venue\_list">场馆信息</a>

</li>

<li class="nav-item dropdown">

<a class="nav-link dropdown-toggle" href="#" id="dropdown" data-toggle="dropdown">预约管理</a>

<div class="dropdown-menu">

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_place(false)">场馆预约</a>

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_manage(false)">订单管理</a>

</div>

</li>

<li class="nav-item active">

<a class="nav-link" href="news\_list">新闻</a>

</li>

<li class="nav-item">

<a class="nav-link loginfirst" href="#" onclick="javascript:message\_list(false)">留言板</a>

</li>

</ul>

<div>

<ul class="navbar-nav ml-auto">

<li class="nav-item">

<a class="nav-link" href="login"><span class="glyphicon glyphicon-log-in"></span> 登录</a>

</li>

<li class="nav-item">

<a class="nav-link" href="signup"><span class="glyphicon glyphicon-user"></span> 注册</a>

</li>

</ul>

</div>

</div>

</nav>

<script type="text/javascript">

$('.dropdown-toggle').dropdown();

function message\_list(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/message\_list';

}

}

function order\_manage(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/order\_manage';

}

}

function order\_place(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.open('/order\_place');

// window.location.href = '/order\_place';

}

}

</script>

</div>

<main role="main" class="container">

<div class="bg-white rounded shadow">

<div class="card-header py-3 text-center bg-danger text-light">

<h5 class="card-title mb-0">新闻</h5>

</div>

<ul class="list-group pt-2 px-3" id="content">

</ul>

<div class="d-flex justify-content-center mt-2" id="pagination-demo"></div>

</div>

</main>

<div>

<footer class="mt-5 mb-3 text-muted text-center">Copyright &copy; 2019-2020 MeetHere</footer>

</div>

<script type="text/javascript">

// $(document).ready(function () {

// getPage(1);

// });

$('#pagination-demo').twbsPagination({

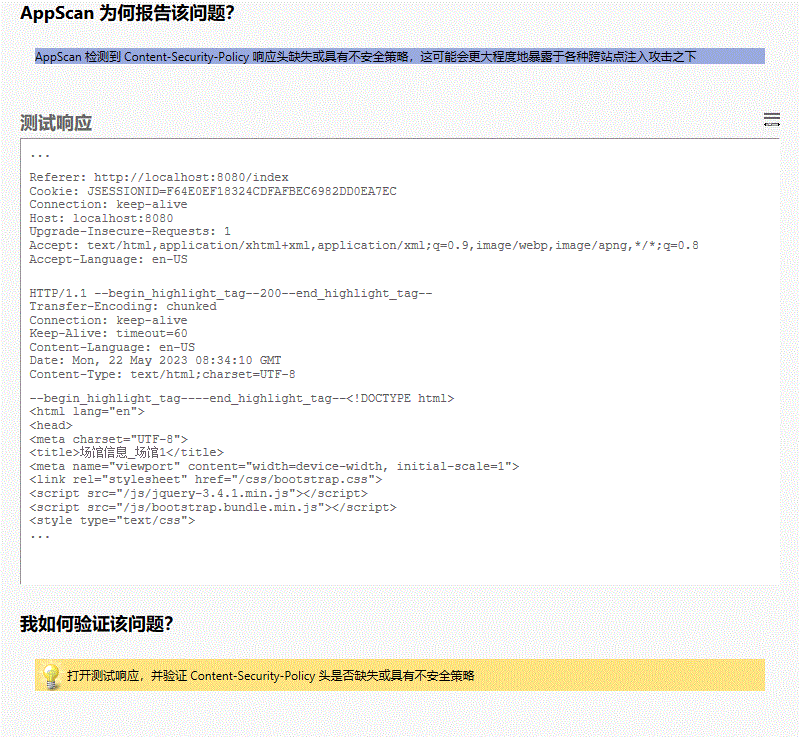
totalP...

##### 问题 2/5（ http://localhost:8080/venue － venue ）

##### 严重性： Low

##### CVSS 计分： 5

##### 图像



**所有变体**

##### 变体差异

变体原因  
AppScan 检测到 Content-Security-Policy 响应头缺失或具有不安全策略，这可能会更大程度地暴露于各种跨站点注入攻击之下

##### 变体验证

• HTTP/1.1 **200**

变体请求响应  
GET /venue?venueID=2 HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

Referer: http://localhost:8080/index

Cookie: JSESSIONID=F64E0EF18324CDFAFBEC6982DD0EA7EC

Connection: keep-alive

Host: localhost:8080

Upgrade-Insecure-Requests: 1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8

Accept-Language: en-US

HTTP/1.1 200

Transfer-Encoding: chunked

Connection: keep-alive

Keep-Alive: timeout=60

Content-Language: en-US

Date: Mon, 22 May 2023 08:34:10 GMT

Content-Type: text/html;charset=UTF-8

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<title>场馆信息\_场馆1</title>

<meta name="viewport" content="width=device-width, initial-scale=1">

<link rel="stylesheet" href="/css/bootstrap.css">

<script src="/js/jquery-3.4.1.min.js"></script>

<script src="/js/bootstrap.bundle.min.js"></script>

<style type="text/css">

body{

background-color: #f5f5f5;

padding-top: 80px;

}

html {

overflow-y: scroll;

}

:root {

overflow-y: auto;

overflow-x: hidden;

}

:root body {

position: absolute;

}

body {

width: 100vw;

overflow: hidden;

}

</style>

</head>

<body>

<div>

<nav class="navbar navbar-expand-sm navbar-dark fixed-top bg-dark shadow" role="navigation">

<div class="navbar-header">

<a class="navbar-brand" href="index" style="font-weight: bold">Meet Here</a>

</div>

<button class="navbar-toggler" data-toggle="collapse" data-target="#navbar">

<span class="navbar-toggler-icon"></span>

</button>

<div class="collapse navbar-collapse" id="navbar">

<ul class="navbar-nav mr-auto">

<li class="nav-item">

<a class="nav-link" href="index">首页</a>

</li>

<li class="nav-item active">

<a class="nav-link" href="venue\_list">场馆信息</a>

</li>

<li class="nav-item dropdown">

<a class="nav-link dropdown-toggle" href="#" id="dropdown" data-toggle="dropdown">预约管理</a>

<div class="dropdown-menu">

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_place(false)">场馆预约</a>

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_manage(false)">订单管理</a>

</div>

</li>

<li class="nav-item">

<a class="nav-link" href="news\_list">新闻</a>

</li>

<li class="nav-item">

<a class="nav-link loginfirst" href="#" onclick="javascript:message\_list(false)">留言板</a>

</li>

</ul>

<div>

<ul class="navbar-nav ml-auto">

<li class="nav-item">

<a class="nav-link" href="login"><span class="glyphicon glyphicon-log-in"></span> 登录</a>

</li>

<li class="nav-item">

<a class="nav-link" href="signup"><span class="glyphicon glyphicon-user"></span> 注册</a>

</li>

</ul>

</div>

</div>

</nav>

<script type="text/javascript">

$('.dropdown-toggle').dropdown();

function message\_list(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/message\_list';

}

}

function order\_manage(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/order\_manage';

}

}

function order\_place(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.open('/order\_place');

// window.location.href = '/order\_place';

}

}

</script>

</div>

<main role="main" class="container-fluid">

<div class="row">

<div class="col-8 mx-auto">

<div class="mb-3 p-4 bg-white rounded shadow-sm">

<div class="media border-bottom border-gray pb-3">

<div class="media-body">

<h4 class="media-heading font-weight-bold pb-3">场馆1</h4>

<h6 class="d-flex">

<p class="font-weight-bold mb-0">场馆位置：</p>

<p class="mb-0">上海市普陀区中山北路3664号</p>

</h6>

<h6 class="d-flex">

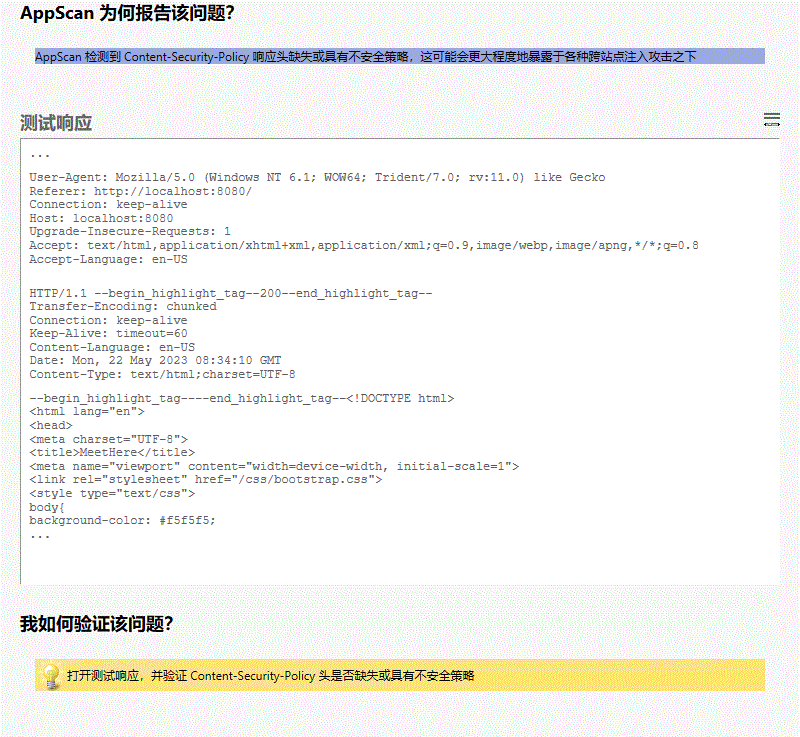
<p class="font-weight-bold...

##### 问题 3/5（ http://localhost:8080/index － index ）

##### 严重性： Low

##### CVSS 计分： 5

##### 图像



**所有变体**

##### 变体差异

变体原因  
AppScan 检测到 Content-Security-Policy 响应头缺失或具有不安全策略，这可能会更大程度地暴露于各种跨站点注入攻击之下

##### 变体验证

• HTTP/1.1 **200**

变体请求响应  
GET /index HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

Referer: http://localhost:8080/

Connection: keep-alive

Host: localhost:8080

Upgrade-Insecure-Requests: 1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8

Accept-Language: en-US

HTTP/1.1 200

Transfer-Encoding: chunked

Connection: keep-alive

Keep-Alive: timeout=60

Content-Language: en-US

Date: Mon, 22 May 2023 08:34:10 GMT

Content-Type: text/html;charset=UTF-8

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<title>MeetHere</title>

<meta name="viewport" content="width=device-width, initial-scale=1">

<link rel="stylesheet" href="/css/bootstrap.css">

<style type="text/css">

body{

background-color: #f5f5f5;

padding-top: 80px;

}

html {

overflow-y: scroll;

}

:root {

overflow-y: auto;

overflow-x: hidden;

}

:root body {

position: absolute;

}

body {

width: 100vw;

overflow: hidden;

}

</style>

<script src="/js/jquery-3.4.1.min.js"></script>

<script src="/js/bootstrap.bundle.min.js"></script>

</head>

<body>

<div>

<nav class="navbar navbar-expand-sm navbar-dark fixed-top bg-dark shadow" role="navigation">

<div class="navbar-header">

<a class="navbar-brand" href="index" style="font-weight: bold">Meet Here</a>

</div>

<button class="navbar-toggler" data-toggle="collapse" data-target="#navbar">

<span class="navbar-toggler-icon"></span>

</button>

<div class="collapse navbar-collapse" id="navbar">

<ul class="navbar-nav mr-auto">

<li class="nav-item active">

<a class="nav-link" href="index">首页</a>

</li>

<li class="nav-item">

<a class="nav-link" href="venue\_list">场馆信息</a>

</li>

<li class="nav-item dropdown">

<a class="nav-link dropdown-toggle" href="#" id="dropdown" data-toggle="dropdown">预约管理</a>

<div class="dropdown-menu">

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_place(false)">场馆预约</a>

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_manage(false)">订单管理</a>

</div>

</li>

<li class="nav-item">

<a class="nav-link" href="news\_list">新闻</a>

</li>

<li class="nav-item">

<a class="nav-link loginfirst" href="#" onclick="javascript:message\_list(false)">留言板</a>

</li>

</ul>

<div>

<ul class="navbar-nav ml-auto">

<li class="nav-item">

<a class="nav-link" href="login"><span class="glyphicon glyphicon-log-in"></span> 登录</a>

</li>

<li class="nav-item">

<a class="nav-link" href="signup"><span class="glyphicon glyphicon-user"></span> 注册</a>

</li>

</ul>

</div>

</div>

</nav>

<script type="text/javascript">

$('.dropdown-toggle').dropdown();

function message\_list(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/message\_list';

}

}

function order\_manage(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/order\_manage';

}

}

function order\_place(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.open('/order\_place');

// window.location.href = '/order\_place';

}

}

</script>

</div>

<main class="container-fluid">

<div class="d-flex">

<div class="col-8">

<!--场馆信息-->

<div class="card shadow">

<div class="card-header py-2 bg-info text-white">

<h6 class="card-title mb-0">场馆信息</h6>

</div>

<ul class="list-group pt-2">

<li class="list-group-item px-3 pt-3 border-0">

<div class="media border-bottom border-gray pb-3">

<div class="media-left mr-3">

<img src="venue.jpg"

alt="" height="100px" width="100px">

</div>

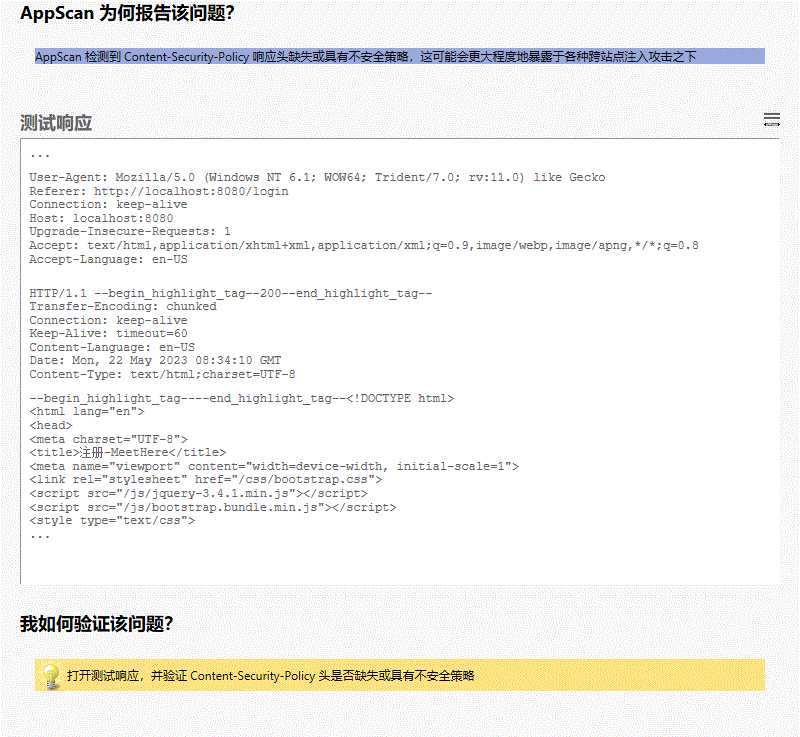
<...

##### 问题 4/5（ http://localhost:8080/signup － signup ）

##### 严重性： Low

##### CVSS 计分： 5

##### 图像



**所有变体**

##### 变体差异

变体原因  
AppScan 检测到 Content-Security-Policy 响应头缺失或具有不安全策略，这可能会更大程度地暴露于各种跨站点注入攻击之下

##### 变体验证

• HTTP/1.1 **200**

变体请求响应  
GET /signup HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

Referer: http://localhost:8080/login

Connection: keep-alive

Host: localhost:8080

Upgrade-Insecure-Requests: 1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8

Accept-Language: en-US

HTTP/1.1 200

Transfer-Encoding: chunked

Connection: keep-alive

Keep-Alive: timeout=60

Content-Language: en-US

Date: Mon, 22 May 2023 08:34:10 GMT

Content-Type: text/html;charset=UTF-8

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<title>注册-MeetHere</title>

<meta name="viewport" content="width=device-width, initial-scale=1">

<link rel="stylesheet" href="/css/bootstrap.css">

<script src="/js/jquery-3.4.1.min.js"></script>

<script src="/js/bootstrap.bundle.min.js"></script>

<style type="text/css">

html {

overflow-y: scroll;

}

:root {

overflow-y: auto;

overflow-x: hidden;

}

:root body {

position: absolute;

}

body {

width: 100vw;

overflow: hidden;

background-color: #f5f5f5;

}

</style>

</head>

<body>

<div>

<nav class="navbar navbar-expand-sm navbar-dark fixed-top bg-dark shadow" role="navigation">

<div class="navbar-header">

<a class="navbar-brand" href="index" style="font-weight: bold">Meet Here</a>

</div>

<button class="navbar-toggler" data-toggle="collapse" data-target="#navbar">

<span class="navbar-toggler-icon"></span>

</button>

<div class="collapse navbar-collapse" id="navbar">

<ul class="navbar-nav mr-auto">

<li class="nav-item">

<a class="nav-link" href="index">首页</a>

</li>

<li class="nav-item">

<a class="nav-link" href="venue\_list">场馆信息</a>

</li>

<li class="nav-item dropdown">

<a class="nav-link dropdown-toggle" href="#" id="dropdown" data-toggle="dropdown">预约管理</a>

<div class="dropdown-menu">

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_place(false)">场馆预约</a>

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_manage(false)">订单管理</a>

</div>

</li>

<li class="nav-item">

<a class="nav-link" href="news\_list">新闻</a>

</li>

<li class="nav-item">

<a class="nav-link loginfirst" href="#" onclick="javascript:message\_list(false)">留言板</a>

</li>

</ul>

<div>

<ul class="navbar-nav ml-auto">

<li class="nav-item">

<a class="nav-link" href="login"><span class="glyphicon glyphicon-log-in"></span> 登录</a>

</li>

<li class="nav-item active">

<a class="nav-link" href="signup"><span class="glyphicon glyphicon-user"></span> 注册</a>

</li>

</ul>

</div>

</div>

</nav>

<script type="text/javascript">

$('.dropdown-toggle').dropdown();

function message\_list(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/message\_list';

}

}

function order\_manage(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/order\_manage';

}

}

function order\_place(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.open('/order\_place');

// window.location.href = '/order\_place';

}

}

</script>

</div>

<main class="container" style="padding-top: 8%">

<form class="col-6 mx-auto" role="form" action="register.do" method="post">

<div class="text-center mb-5">

<h1>注 册</h1>

</div>

<div class="form-group mb-4 row">

<div class="media col-2">

<h6 class="align-self-center ml-auto">昵称</h6>

<h6 class="text-danger">\*</h6>

</div>

<div class="col-10">

<label for="userName" class="sr-only">昵称</label>

<div class="input-group">

<div class="input-group-prepend">

<span class="input-group-text">@</span>

</div>

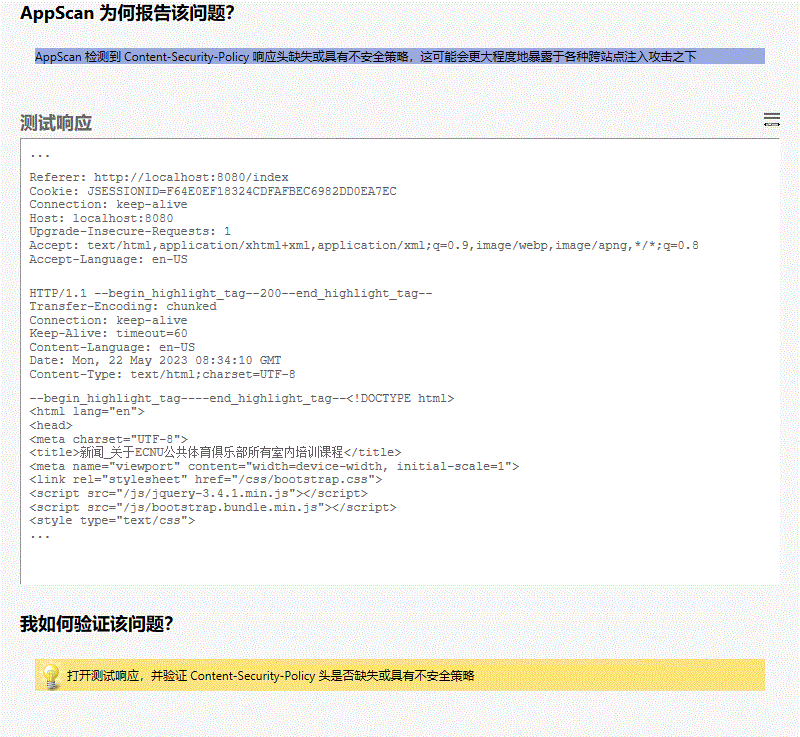
<input type="text" name="userName" class="form-control" ...

##### 问题 5/5（ http://localhost:8080/news － news ）

##### 严重性： Low

##### CVSS 计分： 5

##### 图像



**所有变体**

##### 变体差异

变体原因  
AppScan 检测到 Content-Security-Policy 响应头缺失或具有不安全策略，这可能会更大程度地暴露于各种跨站点注入攻击之下

##### 变体验证

• HTTP/1.1 **200**

变体请求响应  
GET /news?newsID=12 HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

Referer: http://localhost:8080/index

Cookie: JSESSIONID=F64E0EF18324CDFAFBEC6982DD0EA7EC

Connection: keep-alive

Host: localhost:8080

Upgrade-Insecure-Requests: 1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8

Accept-Language: en-US

HTTP/1.1 200

Transfer-Encoding: chunked

Connection: keep-alive

Keep-Alive: timeout=60

Content-Language: en-US

Date: Mon, 22 May 2023 08:34:10 GMT

Content-Type: text/html;charset=UTF-8

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<title>新闻\_关于ECNU公共体育俱乐部所有室内培训课程</title>

<meta name="viewport" content="width=device-width, initial-scale=1">

<link rel="stylesheet" href="/css/bootstrap.css">

<script src="/js/jquery-3.4.1.min.js"></script>

<script src="/js/bootstrap.bundle.min.js"></script>

<style type="text/css">

body{

background-color: #f5f5f5;

padding-top: 80px;

}

html {

overflow-y: scroll;

}

:root {

overflow-y: auto;

overflow-x: hidden;

}

:root body {

position: absolute;

}

body {

width: 100vw;

overflow: hidden;

}

</style>

</head>

<body>

<div>

<nav class="navbar navbar-expand-sm navbar-dark fixed-top bg-dark shadow" role="navigation">

<div class="navbar-header">

<a class="navbar-brand" href="index" style="font-weight: bold">Meet Here</a>

</div>

<button class="navbar-toggler" data-toggle="collapse" data-target="#navbar">

<span class="navbar-toggler-icon"></span>

</button>

<div class="collapse navbar-collapse" id="navbar">

<ul class="navbar-nav mr-auto">

<li class="nav-item">

<a class="nav-link" href="index">首页</a>

</li>

<li class="nav-item">

<a class="nav-link" href="venue\_list">场馆信息</a>

</li>

<li class="nav-item dropdown">

<a class="nav-link dropdown-toggle" href="#" id="dropdown" data-toggle="dropdown">预约管理</a>

<div class="dropdown-menu">

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_place(false)">场馆预约</a>

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_manage(false)">订单管理</a>

</div>

</li>

<li class="nav-item active">

<a class="nav-link" href="news\_list">新闻</a>

</li>

<li class="nav-item">

<a class="nav-link loginfirst" href="#" onclick="javascript:message\_list(false)">留言板</a>

</li>

</ul>

<div>

<ul class="navbar-nav ml-auto">

<li class="nav-item">

<a class="nav-link" href="login"><span class="glyphicon glyphicon-log-in"></span> 登录</a>

</li>

<li class="nav-item">

<a class="nav-link" href="signup"><span class="glyphicon glyphicon-user"></span> 注册</a>

</li>

</ul>

</div>

</div>

</nav>

<script type="text/javascript">

$('.dropdown-toggle').dropdown();

function message\_list(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/message\_list';

}

}

function order\_manage(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/order\_manage';

}

}

function order\_place(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.open('/order\_place');

// window.location.href = '/order\_place';

}

}

</script>

</div>

<main role="main" class="container-fluid">

<div class="row">

<div class="col-8 mx-auto">

<div class="mb-3 p-4 bg-white rounded shadow-sm">

<div class="border-bottom border-gray py-2 mb-0 text-center">

<h4 class="font-weight-bold">关于ECNU公共体育俱乐部所有室内培训课程</h4>

<small>发布时间：</small>

<small>2019-12-17 17:15:26</small>

</div>

<div class="pt-3">

<p style="text-indent: 2em">根据闵行校区体育馆物业办通知，因麻疹疾控需要，体育馆近期限制进出，故11月23日ECNU公共体育俱乐部所有室内培训课程暂停，积分不会因此产生变动，恢复日期另行通知。天气逐渐转寒，请各位同学运动后及时保暖，寝室多开窗门，保持空气流通。</p>

...

|  |  |
| --- | --- |
|  | “X-Content-Type-Options”头缺失或不安全 (2/7) |

##### 咨询和修订建议

[信息泄露](http://projects.webappsec.org/Information-Leakage)

“X-Content-Type-Options”头（具有“nosniff”值）防止 IE 和 Chrome 忽略响应的内容类型。

此操作可能防止不可信内容（例如，用户上载内容）在用户浏览器上执行（例如，在恶意命名之后）。

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

[有用 HTTP 头列表](https://www.owasp.org/index.php/List_of_useful_HTTP_headers)

[减少 MIME 类型安全风险](https://msdn.microsoft.com/en-us/library/gg622941%28v=vs.85%29.aspx)

“X-Content-Type-Options”头缺失或不安全

“X-Content-Type-Options”头缺失或不安全

Web 应用程序编程或配置不安全

此问题可能影响不同类型的产品

##### 受影响的 URL

* http://localhost:8080/index
* http://localhost:8080/news\_list
* http://localhost:8080/signup
* http://localhost:8080/venue
* http://localhost:8080/venue\_list

##### 问题 1/5（ http://localhost:8080/venue － venue ）

##### 严重性： Low

##### CVSS 计分： 5

##### 图像



**所有变体**

##### 变体差异

变体原因  
AppScan 检测到“X-Content-Type-Options”响应头缺失或具有不安全值，这可能会更大程度地暴露于偷渡式下载攻击之下

##### 变体验证

• HTTP/1.1 **200**

变体请求响应  
GET /venue?venueID=2 HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

Referer: http://localhost:8080/index

Cookie: JSESSIONID=F64E0EF18324CDFAFBEC6982DD0EA7EC

Connection: keep-alive

Host: localhost:8080

Upgrade-Insecure-Requests: 1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8

Accept-Language: en-US

HTTP/1.1 200

Transfer-Encoding: chunked

Connection: keep-alive

Keep-Alive: timeout=60

Content-Language: en-US

Date: Mon, 22 May 2023 08:34:10 GMT

Content-Type: text/html;charset=UTF-8

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<title>场馆信息\_场馆1</title>

<meta name="viewport" content="width=device-width, initial-scale=1">

<link rel="stylesheet" href="/css/bootstrap.css">

<script src="/js/jquery-3.4.1.min.js"></script>

<script src="/js/bootstrap.bundle.min.js"></script>

<style type="text/css">

body{

background-color: #f5f5f5;

padding-top: 80px;

}

html {

overflow-y: scroll;

}

:root {

overflow-y: auto;

overflow-x: hidden;

}

:root body {

position: absolute;

}

body {

width: 100vw;

overflow: hidden;

}

</style>

</head>

<body>

<div>

<nav class="navbar navbar-expand-sm navbar-dark fixed-top bg-dark shadow" role="navigation">

<div class="navbar-header">

<a class="navbar-brand" href="index" style="font-weight: bold">Meet Here</a>

</div>

<button class="navbar-toggler" data-toggle="collapse" data-target="#navbar">

<span class="navbar-toggler-icon"></span>

</button>

<div class="collapse navbar-collapse" id="navbar">

<ul class="navbar-nav mr-auto">

<li class="nav-item">

<a class="nav-link" href="index">首页</a>

</li>

<li class="nav-item active">

<a class="nav-link" href="venue\_list">场馆信息</a>

</li>

<li class="nav-item dropdown">

<a class="nav-link dropdown-toggle" href="#" id="dropdown" data-toggle="dropdown">预约管理</a>

<div class="dropdown-menu">

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_place(false)">场馆预约</a>

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_manage(false)">订单管理</a>

</div>

</li>

<li class="nav-item">

<a class="nav-link" href="news\_list">新闻</a>

</li>

<li class="nav-item">

<a class="nav-link loginfirst" href="#" onclick="javascript:message\_list(false)">留言板</a>

</li>

</ul>

<div>

<ul class="navbar-nav ml-auto">

<li class="nav-item">

<a class="nav-link" href="login"><span class="glyphicon glyphicon-log-in"></span> 登录</a>

</li>

<li class="nav-item">

<a class="nav-link" href="signup"><span class="glyphicon glyphicon-user"></span> 注册</a>

</li>

</ul>

</div>

</div>

</nav>

<script type="text/javascript">

$('.dropdown-toggle').dropdown();

function message\_list(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/message\_list';

}

}

function order\_manage(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/order\_manage';

}

}

function order\_place(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.open('/order\_place');

// window.location.href = '/order\_place';

}

}

</script>

</div>

<main role="main" class="container-fluid">

<div class="row">

<div class="col-8 mx-auto">

<div class="mb-3 p-4 bg-white rounded shadow-sm">

<div class="media border-bottom border-gray pb-3">

<div class="media-body">

<h4 class="media-heading font-weight-bold pb-3">场馆1</h4>

<h6 class="d-flex">

<p class="font-weight-bold mb-0">场馆位置：</p>

<p class="mb-0">上海市普陀区中山北路3664号</p>

</h6>

<h6 class="d-flex">

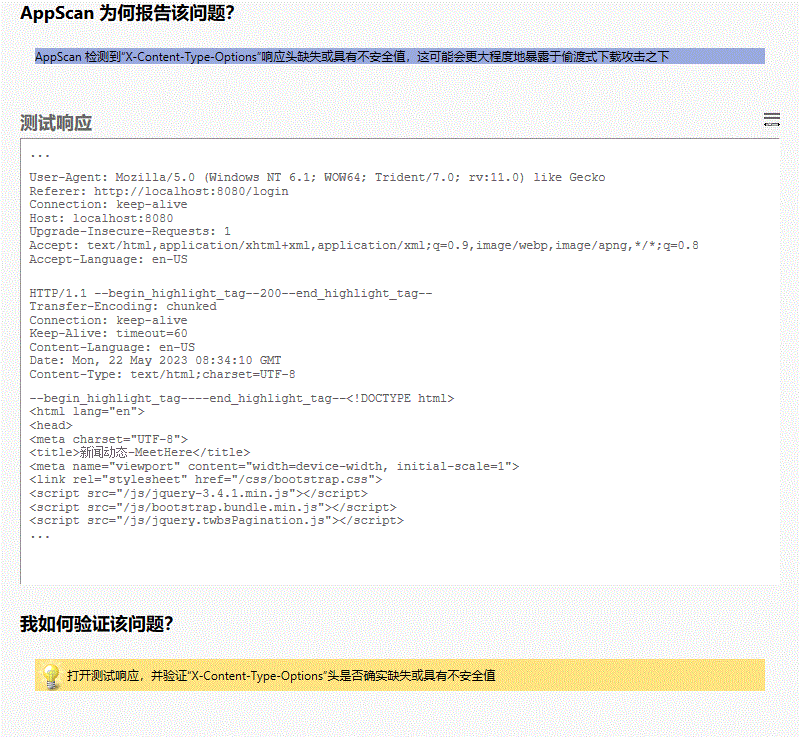
<p class="font-weight-bold...

##### 问题 2/5（ http://localhost:8080/news\_list － news\_list ）

##### 严重性： Low

##### CVSS 计分： 5

##### 图像



**所有变体**

##### 变体差异

变体原因  
AppScan 检测到“X-Content-Type-Options”响应头缺失或具有不安全值，这可能会更大程度地暴露于偷渡式下载攻击之下

##### 变体验证

• HTTP/1.1 **200**

变体请求响应  
GET /news\_list HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

Referer: http://localhost:8080/login

Connection: keep-alive

Host: localhost:8080

Upgrade-Insecure-Requests: 1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8

Accept-Language: en-US

HTTP/1.1 200

Transfer-Encoding: chunked

Connection: keep-alive

Keep-Alive: timeout=60

Content-Language: en-US

Date: Mon, 22 May 2023 08:34:10 GMT

Content-Type: text/html;charset=UTF-8

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<title>新闻动态-MeetHere</title>

<meta name="viewport" content="width=device-width, initial-scale=1">

<link rel="stylesheet" href="/css/bootstrap.css">

<script src="/js/jquery-3.4.1.min.js"></script>

<script src="/js/bootstrap.bundle.min.js"></script>

<script src="/js/jquery.twbsPagination.js"></script>

<style type="text/css">

body{

background-color: #f5f5f5;

padding-top: 80px;

}

html {

overflow-y: scroll;

}

:root {

overflow-y: auto;

overflow-x: hidden;

}

:root body {

position: absolute;

}

body {

width: 100vw;

overflow: hidden;

}

</style>

</head>

<body>

<div>

<nav class="navbar navbar-expand-sm navbar-dark fixed-top bg-dark shadow" role="navigation">

<div class="navbar-header">

<a class="navbar-brand" href="index" style="font-weight: bold">Meet Here</a>

</div>

<button class="navbar-toggler" data-toggle="collapse" data-target="#navbar">

<span class="navbar-toggler-icon"></span>

</button>

<div class="collapse navbar-collapse" id="navbar">

<ul class="navbar-nav mr-auto">

<li class="nav-item">

<a class="nav-link" href="index">首页</a>

</li>

<li class="nav-item">

<a class="nav-link" href="venue\_list">场馆信息</a>

</li>

<li class="nav-item dropdown">

<a class="nav-link dropdown-toggle" href="#" id="dropdown" data-toggle="dropdown">预约管理</a>

<div class="dropdown-menu">

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_place(false)">场馆预约</a>

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_manage(false)">订单管理</a>

</div>

</li>

<li class="nav-item active">

<a class="nav-link" href="news\_list">新闻</a>

</li>

<li class="nav-item">

<a class="nav-link loginfirst" href="#" onclick="javascript:message\_list(false)">留言板</a>

</li>

</ul>

<div>

<ul class="navbar-nav ml-auto">

<li class="nav-item">

<a class="nav-link" href="login"><span class="glyphicon glyphicon-log-in"></span> 登录</a>

</li>

<li class="nav-item">

<a class="nav-link" href="signup"><span class="glyphicon glyphicon-user"></span> 注册</a>

</li>

</ul>

</div>

</div>

</nav>

<script type="text/javascript">

$('.dropdown-toggle').dropdown();

function message\_list(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/message\_list';

}

}

function order\_manage(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/order\_manage';

}

}

function order\_place(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.open('/order\_place');

// window.location.href = '/order\_place';

}

}

</script>

</div>

<main role="main" class="container">

<div class="bg-white rounded shadow">

<div class="card-header py-3 text-center bg-danger text-light">

<h5 class="card-title mb-0">新闻</h5>

</div>

<ul class="list-group pt-2 px-3" id="content">

</ul>

<div class="d-flex justify-content-center mt-2" id="pagination-demo"></div>

</div>

</main>

<div>

<footer class="mt-5 mb-3 text-muted text-center">Copyright &copy; 2019-2020 MeetHere</footer>

</div>

<script type="text/javascript">

// $(document).ready(function () {

// getPage(1);

// });

$('#pagination-demo').twbsPagination({

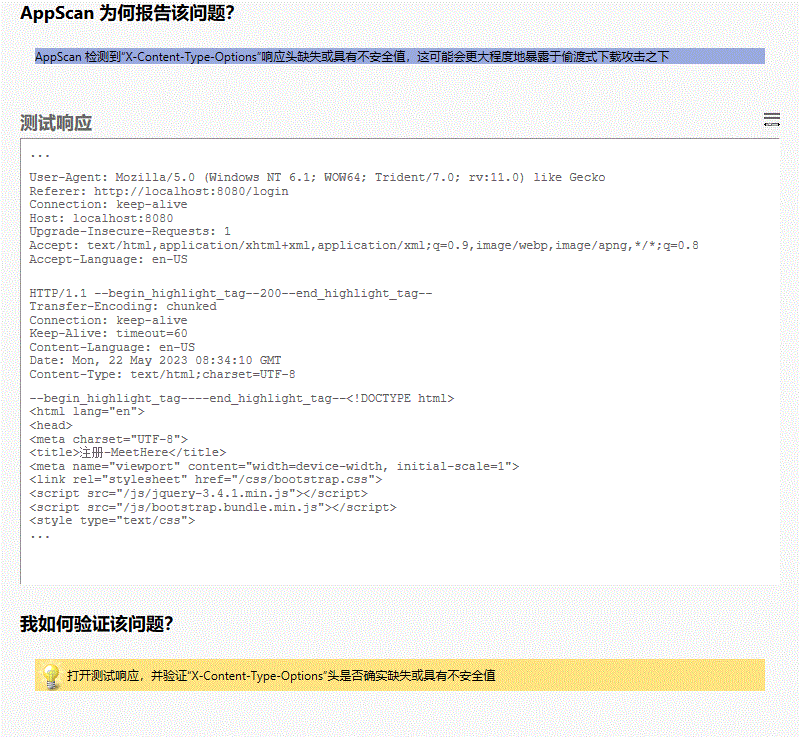
totalP...

##### 问题 3/5（ http://localhost:8080/signup － signup ）

##### 严重性： Low

##### CVSS 计分： 5

##### 图像



**所有变体**

##### 变体差异

变体原因  
AppScan 检测到“X-Content-Type-Options”响应头缺失或具有不安全值，这可能会更大程度地暴露于偷渡式下载攻击之下

##### 变体验证

• HTTP/1.1 **200**

变体请求响应  
GET /signup HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

Referer: http://localhost:8080/login

Connection: keep-alive

Host: localhost:8080

Upgrade-Insecure-Requests: 1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8

Accept-Language: en-US

HTTP/1.1 200

Transfer-Encoding: chunked

Connection: keep-alive

Keep-Alive: timeout=60

Content-Language: en-US

Date: Mon, 22 May 2023 08:34:10 GMT

Content-Type: text/html;charset=UTF-8

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<title>注册-MeetHere</title>

<meta name="viewport" content="width=device-width, initial-scale=1">

<link rel="stylesheet" href="/css/bootstrap.css">

<script src="/js/jquery-3.4.1.min.js"></script>

<script src="/js/bootstrap.bundle.min.js"></script>

<style type="text/css">

html {

overflow-y: scroll;

}

:root {

overflow-y: auto;

overflow-x: hidden;

}

:root body {

position: absolute;

}

body {

width: 100vw;

overflow: hidden;

background-color: #f5f5f5;

}

</style>

</head>

<body>

<div>

<nav class="navbar navbar-expand-sm navbar-dark fixed-top bg-dark shadow" role="navigation">

<div class="navbar-header">

<a class="navbar-brand" href="index" style="font-weight: bold">Meet Here</a>

</div>

<button class="navbar-toggler" data-toggle="collapse" data-target="#navbar">

<span class="navbar-toggler-icon"></span>

</button>

<div class="collapse navbar-collapse" id="navbar">

<ul class="navbar-nav mr-auto">

<li class="nav-item">

<a class="nav-link" href="index">首页</a>

</li>

<li class="nav-item">

<a class="nav-link" href="venue\_list">场馆信息</a>

</li>

<li class="nav-item dropdown">

<a class="nav-link dropdown-toggle" href="#" id="dropdown" data-toggle="dropdown">预约管理</a>

<div class="dropdown-menu">

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_place(false)">场馆预约</a>

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_manage(false)">订单管理</a>

</div>

</li>

<li class="nav-item">

<a class="nav-link" href="news\_list">新闻</a>

</li>

<li class="nav-item">

<a class="nav-link loginfirst" href="#" onclick="javascript:message\_list(false)">留言板</a>

</li>

</ul>

<div>

<ul class="navbar-nav ml-auto">

<li class="nav-item">

<a class="nav-link" href="login"><span class="glyphicon glyphicon-log-in"></span> 登录</a>

</li>

<li class="nav-item active">

<a class="nav-link" href="signup"><span class="glyphicon glyphicon-user"></span> 注册</a>

</li>

</ul>

</div>

</div>

</nav>

<script type="text/javascript">

$('.dropdown-toggle').dropdown();

function message\_list(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/message\_list';

}

}

function order\_manage(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/order\_manage';

}

}

function order\_place(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.open('/order\_place');

// window.location.href = '/order\_place';

}

}

</script>

</div>

<main class="container" style="padding-top: 8%">

<form class="col-6 mx-auto" role="form" action="register.do" method="post">

<div class="text-center mb-5">

<h1>注 册</h1>

</div>

<div class="form-group mb-4 row">

<div class="media col-2">

<h6 class="align-self-center ml-auto">昵称</h6>

<h6 class="text-danger">\*</h6>

</div>

<div class="col-10">

<label for="userName" class="sr-only">昵称</label>

<div class="input-group">

<div class="input-group-prepend">

<span class="input-group-text">@</span>

</div>

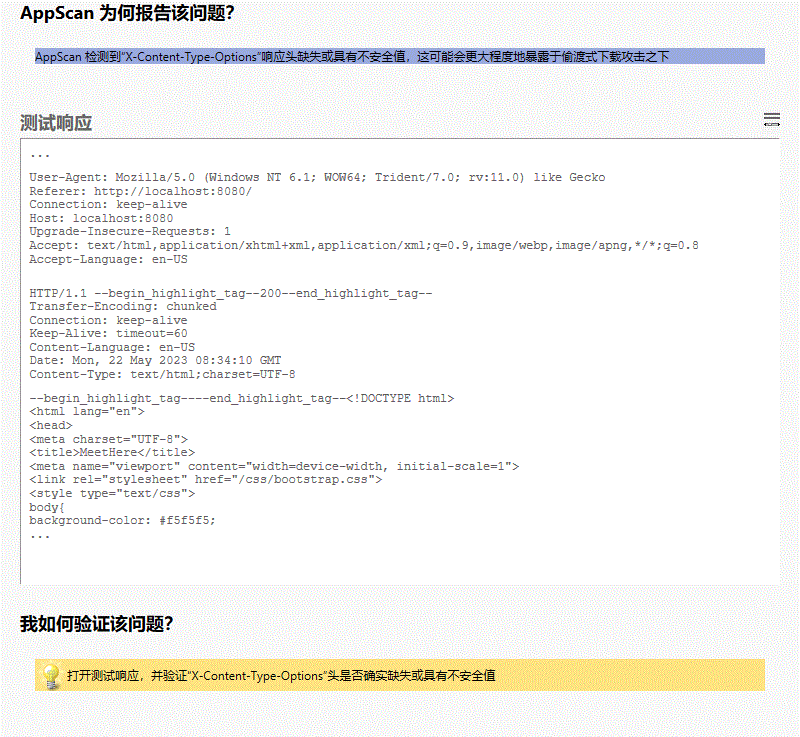
<input type="text" name="userName" class="form-control" ...

##### 问题 4/5（ http://localhost:8080/index － index ）

##### 严重性： Low

##### CVSS 计分： 5

##### 图像



**所有变体**

##### 变体差异

变体原因  
AppScan 检测到“X-Content-Type-Options”响应头缺失或具有不安全值，这可能会更大程度地暴露于偷渡式下载攻击之下

##### 变体验证

• HTTP/1.1 **200**

变体请求响应  
GET /index HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

Referer: http://localhost:8080/

Connection: keep-alive

Host: localhost:8080

Upgrade-Insecure-Requests: 1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8

Accept-Language: en-US

HTTP/1.1 200

Transfer-Encoding: chunked

Connection: keep-alive

Keep-Alive: timeout=60

Content-Language: en-US

Date: Mon, 22 May 2023 08:34:10 GMT

Content-Type: text/html;charset=UTF-8

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<title>MeetHere</title>

<meta name="viewport" content="width=device-width, initial-scale=1">

<link rel="stylesheet" href="/css/bootstrap.css">

<style type="text/css">

body{

background-color: #f5f5f5;

padding-top: 80px;

}

html {

overflow-y: scroll;

}

:root {

overflow-y: auto;

overflow-x: hidden;

}

:root body {

position: absolute;

}

body {

width: 100vw;

overflow: hidden;

}

</style>

<script src="/js/jquery-3.4.1.min.js"></script>

<script src="/js/bootstrap.bundle.min.js"></script>

</head>

<body>

<div>

<nav class="navbar navbar-expand-sm navbar-dark fixed-top bg-dark shadow" role="navigation">

<div class="navbar-header">

<a class="navbar-brand" href="index" style="font-weight: bold">Meet Here</a>

</div>

<button class="navbar-toggler" data-toggle="collapse" data-target="#navbar">

<span class="navbar-toggler-icon"></span>

</button>

<div class="collapse navbar-collapse" id="navbar">

<ul class="navbar-nav mr-auto">

<li class="nav-item active">

<a class="nav-link" href="index">首页</a>

</li>

<li class="nav-item">

<a class="nav-link" href="venue\_list">场馆信息</a>

</li>

<li class="nav-item dropdown">

<a class="nav-link dropdown-toggle" href="#" id="dropdown" data-toggle="dropdown">预约管理</a>

<div class="dropdown-menu">

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_place(false)">场馆预约</a>

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_manage(false)">订单管理</a>

</div>

</li>

<li class="nav-item">

<a class="nav-link" href="news\_list">新闻</a>

</li>

<li class="nav-item">

<a class="nav-link loginfirst" href="#" onclick="javascript:message\_list(false)">留言板</a>

</li>

</ul>

<div>

<ul class="navbar-nav ml-auto">

<li class="nav-item">

<a class="nav-link" href="login"><span class="glyphicon glyphicon-log-in"></span> 登录</a>

</li>

<li class="nav-item">

<a class="nav-link" href="signup"><span class="glyphicon glyphicon-user"></span> 注册</a>

</li>

</ul>

</div>

</div>

</nav>

<script type="text/javascript">

$('.dropdown-toggle').dropdown();

function message\_list(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/message\_list';

}

}

function order\_manage(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/order\_manage';

}

}

function order\_place(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.open('/order\_place');

// window.location.href = '/order\_place';

}

}

</script>

</div>

<main class="container-fluid">

<div class="d-flex">

<div class="col-8">

<!--场馆信息-->

<div class="card shadow">

<div class="card-header py-2 bg-info text-white">

<h6 class="card-title mb-0">场馆信息</h6>

</div>

<ul class="list-group pt-2">

<li class="list-group-item px-3 pt-3 border-0">

<div class="media border-bottom border-gray pb-3">

<div class="media-left mr-3">

<img src="venue.jpg"

alt="" height="100px" width="100px">

</div>

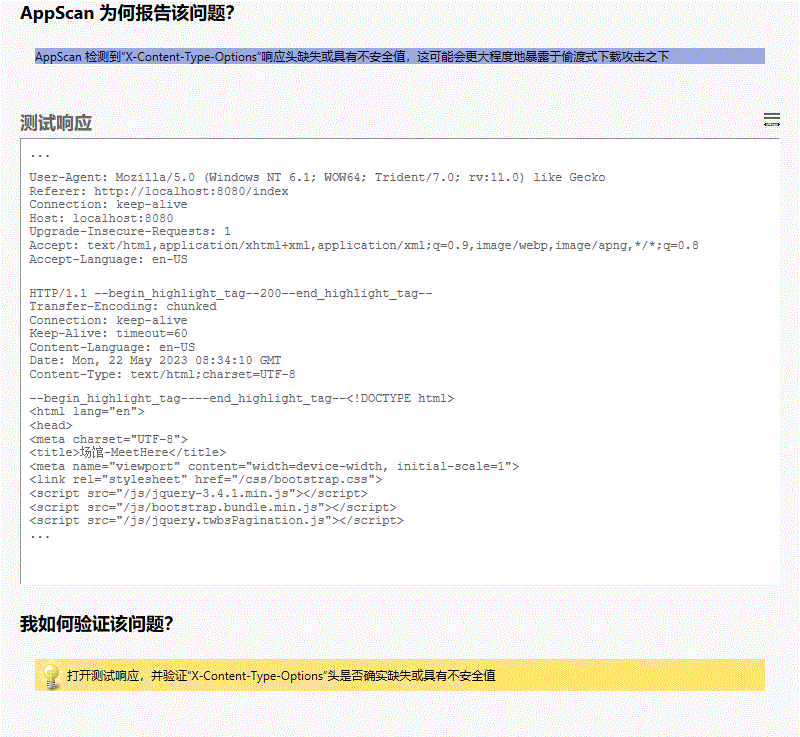
<...

##### 问题 5/5（ http://localhost:8080/venue\_list － venue\_list ）

##### 严重性： Low

##### CVSS 计分： 5

##### 图像



**所有变体**

##### 变体差异

变体原因  
AppScan 检测到“X-Content-Type-Options”响应头缺失或具有不安全值，这可能会更大程度地暴露于偷渡式下载攻击之下

##### 变体验证

• HTTP/1.1 **200**

变体请求响应  
GET /venue\_list HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

Referer: http://localhost:8080/index

Connection: keep-alive

Host: localhost:8080

Upgrade-Insecure-Requests: 1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8

Accept-Language: en-US

HTTP/1.1 200

Transfer-Encoding: chunked

Connection: keep-alive

Keep-Alive: timeout=60

Content-Language: en-US

Date: Mon, 22 May 2023 08:34:10 GMT

Content-Type: text/html;charset=UTF-8

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<title>场馆-MeetHere</title>

<meta name="viewport" content="width=device-width, initial-scale=1">

<link rel="stylesheet" href="/css/bootstrap.css">

<script src="/js/jquery-3.4.1.min.js"></script>

<script src="/js/bootstrap.bundle.min.js"></script>

<script src="/js/jquery.twbsPagination.js"></script>

<style type="text/css">

body{

background-color: #f5f5f5;

padding-top: 80px;

}

html {

overflow-y: scroll;

}

:root {

overflow-y: auto;

overflow-x: hidden;

}

:root body {

position: absolute;

}

body {

width: 100vw;

overflow: hidden;

}

</style>

</head>

<body>

<div>

<nav class="navbar navbar-expand-sm navbar-dark fixed-top bg-dark shadow" role="navigation">

<div class="navbar-header">

<a class="navbar-brand" href="index" style="font-weight: bold">Meet Here</a>

</div>

<button class="navbar-toggler" data-toggle="collapse" data-target="#navbar">

<span class="navbar-toggler-icon"></span>

</button>

<div class="collapse navbar-collapse" id="navbar">

<ul class="navbar-nav mr-auto">

<li class="nav-item">

<a class="nav-link" href="index">首页</a>

</li>

<li class="nav-item active">

<a class="nav-link" href="venue\_list">场馆信息</a>

</li>

<li class="nav-item dropdown">

<a class="nav-link dropdown-toggle" href="#" id="dropdown" data-toggle="dropdown">预约管理</a>

<div class="dropdown-menu">

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_place(false)">场馆预约</a>

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_manage(false)">订单管理</a>

</div>

</li>

<li class="nav-item">

<a class="nav-link" href="news\_list">新闻</a>

</li>

<li class="nav-item">

<a class="nav-link loginfirst" href="#" onclick="javascript:message\_list(false)">留言板</a>

</li>

</ul>

<div>

<ul class="navbar-nav ml-auto">

<li class="nav-item">

<a class="nav-link" href="login"><span class="glyphicon glyphicon-log-in"></span> 登录</a>

</li>

<li class="nav-item">

<a class="nav-link" href="signup"><span class="glyphicon glyphicon-user"></span> 注册</a>

</li>

</ul>

</div>

</div>

</nav>

<script type="text/javascript">

$('.dropdown-toggle').dropdown();

function message\_list(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/message\_list';

}

}

function order\_manage(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/order\_manage';

}

}

function order\_place(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.open('/order\_place');

// window.location.href = '/order\_place';

}

}

</script>

</div>

<main role="main" class="container">

<div class="card bg-white rounded shadow">

<div class="card-header py-3 text-center bg-info text-light">

<h5 class="card-title mb-0">场馆信息</h5>

</div>

<ul class="list-group pt-2 px-3" id="content">

<!-- <li class="list-group-item px-3 pt-3 border-0" th:each="venue : ${venue\_list}">-->

<!-- <div class="media border-bottom border-gray pb-3">-->

<!-- <div class="media-left mr-3">-->

<!-- <img th:src="${venue.picture}"-->

<!-- alt="" height="100px" width="100px">-->

<!-- ...

|  |  |
| --- | --- |
|  | “X-XSS-Protection”头缺失或不安全 (3/7) |

##### 咨询和修订建议

[信息泄露](http://projects.webappsec.org/Information-Leakage)

值为‘1’的“X-XSS-Protection”报头强制跨站点脚本编制过滤器进入启用模式，即使用户已禁用。

此过滤器内置于最新版本的 Web 浏览器（IE 8 +、Chrome 4+）中，在缺省情况下通常为已启用状态。虽然此过滤器不是第一个也不是唯一一个针对跨站点脚本编制的防御程序，但它可以作为额外保护层。

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

[有用 HTTP 头列表](https://www.owasp.org/index.php/List_of_useful_HTTP_headers)

[IE XSS 过滤器](http://blogs.msdn.com/b/ie/archive/2008/07/02/ie8-security-part-iv-the-xss-filter.aspx)

“X-XSS-Protection”报头缺失或不安全

“X-XSS-Protection”头缺失或不安全

Web 应用程序编程或配置不安全

此问题可能影响不同类型的产品

##### 受影响的 URL

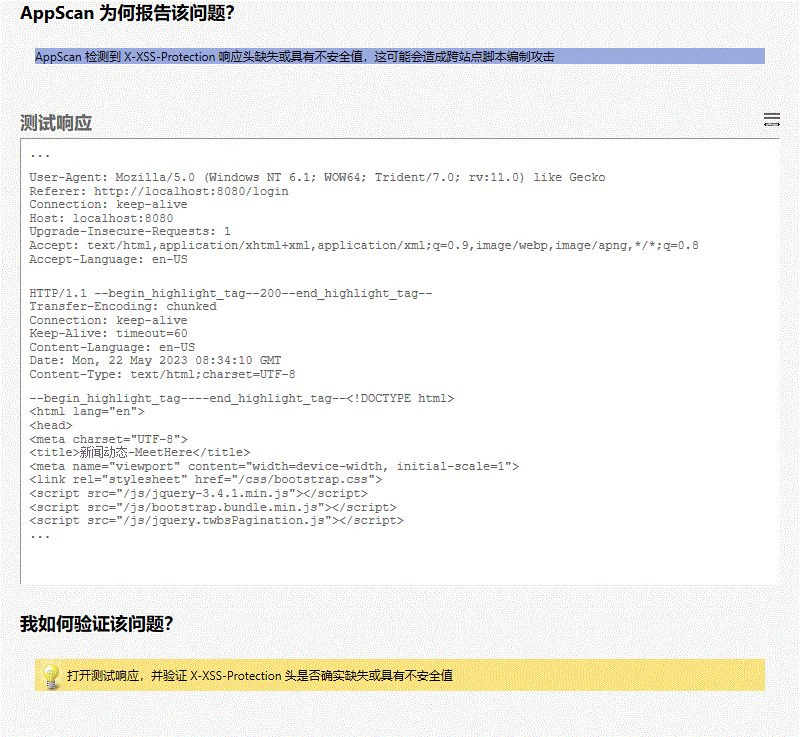
* http://localhost:8080/index
* http://localhost:8080/news
* http://localhost:8080/news\_list
* http://localhost:8080/signup
* http://localhost:8080/venue

##### 问题 1/5（ http://localhost:8080/news\_list － news\_list ）

##### 严重性： Low

##### CVSS 计分： 5

##### 图像



**所有变体**

##### 变体差异

变体原因  
AppScan 检测到 X-XSS-Protection 响应头缺失或具有不安全值，这可能会造成跨站点脚本编制攻击

##### 变体验证

• HTTP/1.1 **200**

变体请求响应  
GET /news\_list HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

Referer: http://localhost:8080/login

Connection: keep-alive

Host: localhost:8080

Upgrade-Insecure-Requests: 1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8

Accept-Language: en-US

HTTP/1.1 200

Transfer-Encoding: chunked

Connection: keep-alive

Keep-Alive: timeout=60

Content-Language: en-US

Date: Mon, 22 May 2023 08:34:10 GMT

Content-Type: text/html;charset=UTF-8

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<title>新闻动态-MeetHere</title>

<meta name="viewport" content="width=device-width, initial-scale=1">

<link rel="stylesheet" href="/css/bootstrap.css">

<script src="/js/jquery-3.4.1.min.js"></script>

<script src="/js/bootstrap.bundle.min.js"></script>

<script src="/js/jquery.twbsPagination.js"></script>

<style type="text/css">

body{

background-color: #f5f5f5;

padding-top: 80px;

}

html {

overflow-y: scroll;

}

:root {

overflow-y: auto;

overflow-x: hidden;

}

:root body {

position: absolute;

}

body {

width: 100vw;

overflow: hidden;

}

</style>

</head>

<body>

<div>

<nav class="navbar navbar-expand-sm navbar-dark fixed-top bg-dark shadow" role="navigation">

<div class="navbar-header">

<a class="navbar-brand" href="index" style="font-weight: bold">Meet Here</a>

</div>

<button class="navbar-toggler" data-toggle="collapse" data-target="#navbar">

<span class="navbar-toggler-icon"></span>

</button>

<div class="collapse navbar-collapse" id="navbar">

<ul class="navbar-nav mr-auto">

<li class="nav-item">

<a class="nav-link" href="index">首页</a>

</li>

<li class="nav-item">

<a class="nav-link" href="venue\_list">场馆信息</a>

</li>

<li class="nav-item dropdown">

<a class="nav-link dropdown-toggle" href="#" id="dropdown" data-toggle="dropdown">预约管理</a>

<div class="dropdown-menu">

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_place(false)">场馆预约</a>

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_manage(false)">订单管理</a>

</div>

</li>

<li class="nav-item active">

<a class="nav-link" href="news\_list">新闻</a>

</li>

<li class="nav-item">

<a class="nav-link loginfirst" href="#" onclick="javascript:message\_list(false)">留言板</a>

</li>

</ul>

<div>

<ul class="navbar-nav ml-auto">

<li class="nav-item">

<a class="nav-link" href="login"><span class="glyphicon glyphicon-log-in"></span> 登录</a>

</li>

<li class="nav-item">

<a class="nav-link" href="signup"><span class="glyphicon glyphicon-user"></span> 注册</a>

</li>

</ul>

</div>

</div>

</nav>

<script type="text/javascript">

$('.dropdown-toggle').dropdown();

function message\_list(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/message\_list';

}

}

function order\_manage(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/order\_manage';

}

}

function order\_place(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.open('/order\_place');

// window.location.href = '/order\_place';

}

}

</script>

</div>

<main role="main" class="container">

<div class="bg-white rounded shadow">

<div class="card-header py-3 text-center bg-danger text-light">

<h5 class="card-title mb-0">新闻</h5>

</div>

<ul class="list-group pt-2 px-3" id="content">

</ul>

<div class="d-flex justify-content-center mt-2" id="pagination-demo"></div>

</div>

</main>

<div>

<footer class="mt-5 mb-3 text-muted text-center">Copyright &copy; 2019-2020 MeetHere</footer>

</div>

<script type="text/javascript">

// $(document).ready(function () {

// getPage(1);

// });

$('#pagination-demo').twbsPagination({

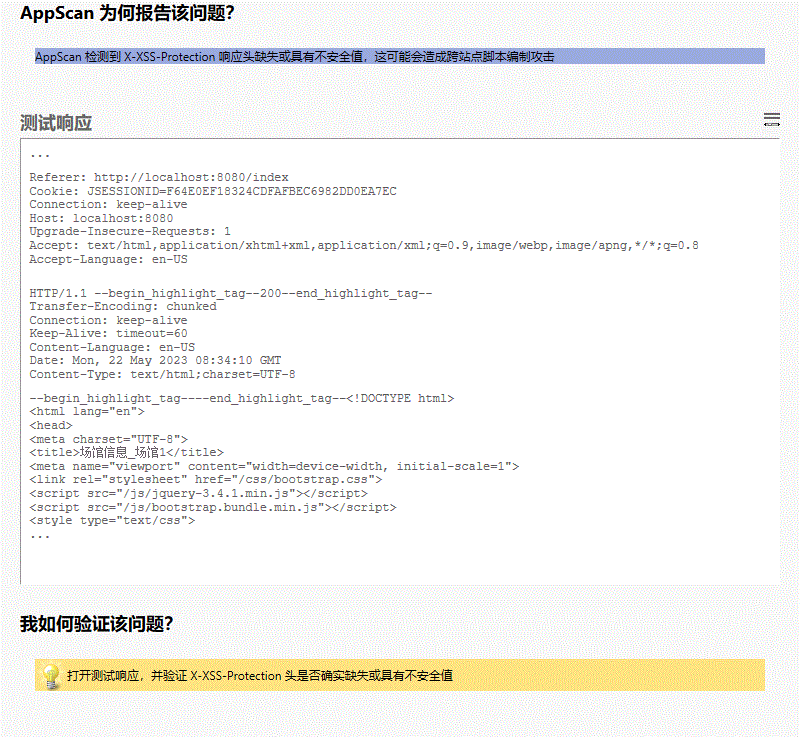
totalP...

##### 问题 2/5（ http://localhost:8080/venue － venue ）

##### 严重性： Low

##### CVSS 计分： 5

##### 图像



**所有变体**

##### 变体差异

变体原因  
AppScan 检测到 X-XSS-Protection 响应头缺失或具有不安全值，这可能会造成跨站点脚本编制攻击

##### 变体验证

• HTTP/1.1 **200**

变体请求响应  
GET /venue?venueID=2 HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

Referer: http://localhost:8080/index

Cookie: JSESSIONID=F64E0EF18324CDFAFBEC6982DD0EA7EC

Connection: keep-alive

Host: localhost:8080

Upgrade-Insecure-Requests: 1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8

Accept-Language: en-US

HTTP/1.1 200

Transfer-Encoding: chunked

Connection: keep-alive

Keep-Alive: timeout=60

Content-Language: en-US

Date: Mon, 22 May 2023 08:34:10 GMT

Content-Type: text/html;charset=UTF-8

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<title>场馆信息\_场馆1</title>

<meta name="viewport" content="width=device-width, initial-scale=1">

<link rel="stylesheet" href="/css/bootstrap.css">

<script src="/js/jquery-3.4.1.min.js"></script>

<script src="/js/bootstrap.bundle.min.js"></script>

<style type="text/css">

body{

background-color: #f5f5f5;

padding-top: 80px;

}

html {

overflow-y: scroll;

}

:root {

overflow-y: auto;

overflow-x: hidden;

}

:root body {

position: absolute;

}

body {

width: 100vw;

overflow: hidden;

}

</style>

</head>

<body>

<div>

<nav class="navbar navbar-expand-sm navbar-dark fixed-top bg-dark shadow" role="navigation">

<div class="navbar-header">

<a class="navbar-brand" href="index" style="font-weight: bold">Meet Here</a>

</div>

<button class="navbar-toggler" data-toggle="collapse" data-target="#navbar">

<span class="navbar-toggler-icon"></span>

</button>

<div class="collapse navbar-collapse" id="navbar">

<ul class="navbar-nav mr-auto">

<li class="nav-item">

<a class="nav-link" href="index">首页</a>

</li>

<li class="nav-item active">

<a class="nav-link" href="venue\_list">场馆信息</a>

</li>

<li class="nav-item dropdown">

<a class="nav-link dropdown-toggle" href="#" id="dropdown" data-toggle="dropdown">预约管理</a>

<div class="dropdown-menu">

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_place(false)">场馆预约</a>

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_manage(false)">订单管理</a>

</div>

</li>

<li class="nav-item">

<a class="nav-link" href="news\_list">新闻</a>

</li>

<li class="nav-item">

<a class="nav-link loginfirst" href="#" onclick="javascript:message\_list(false)">留言板</a>

</li>

</ul>

<div>

<ul class="navbar-nav ml-auto">

<li class="nav-item">

<a class="nav-link" href="login"><span class="glyphicon glyphicon-log-in"></span> 登录</a>

</li>

<li class="nav-item">

<a class="nav-link" href="signup"><span class="glyphicon glyphicon-user"></span> 注册</a>

</li>

</ul>

</div>

</div>

</nav>

<script type="text/javascript">

$('.dropdown-toggle').dropdown();

function message\_list(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/message\_list';

}

}

function order\_manage(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/order\_manage';

}

}

function order\_place(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.open('/order\_place');

// window.location.href = '/order\_place';

}

}

</script>

</div>

<main role="main" class="container-fluid">

<div class="row">

<div class="col-8 mx-auto">

<div class="mb-3 p-4 bg-white rounded shadow-sm">

<div class="media border-bottom border-gray pb-3">

<div class="media-body">

<h4 class="media-heading font-weight-bold pb-3">场馆1</h4>

<h6 class="d-flex">

<p class="font-weight-bold mb-0">场馆位置：</p>

<p class="mb-0">上海市普陀区中山北路3664号</p>

</h6>

<h6 class="d-flex">

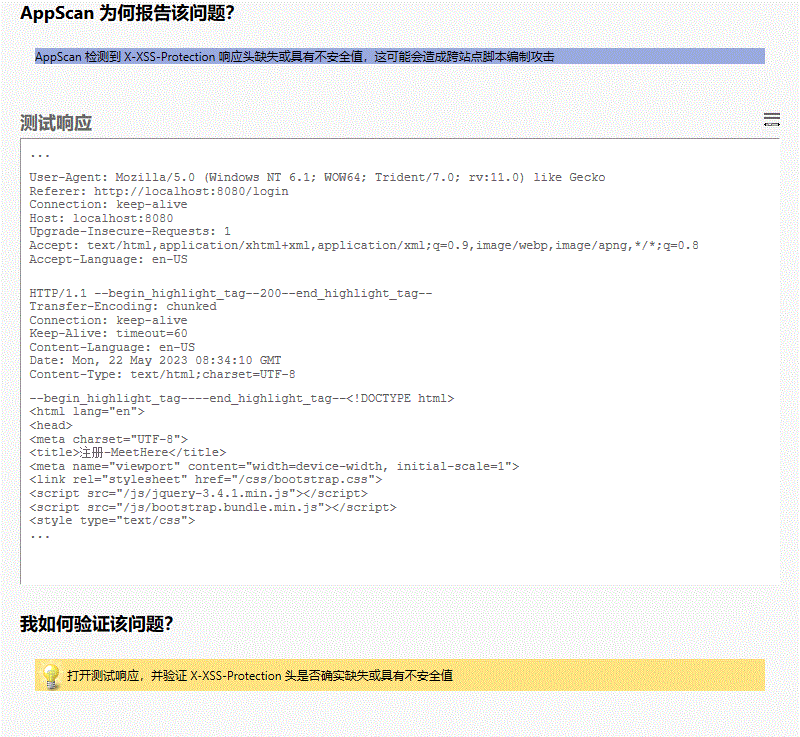
<p class="font-weight-bold...

##### 问题 3/5（ http://localhost:8080/signup － signup ）

##### 严重性： Low

##### CVSS 计分： 5

##### 图像



**所有变体**

##### 变体差异

变体原因  
AppScan 检测到 X-XSS-Protection 响应头缺失或具有不安全值，这可能会造成跨站点脚本编制攻击

##### 变体验证

• HTTP/1.1 **200**

变体请求响应  
GET /signup HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

Referer: http://localhost:8080/login

Connection: keep-alive

Host: localhost:8080

Upgrade-Insecure-Requests: 1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8

Accept-Language: en-US

HTTP/1.1 200

Transfer-Encoding: chunked

Connection: keep-alive

Keep-Alive: timeout=60

Content-Language: en-US

Date: Mon, 22 May 2023 08:34:10 GMT

Content-Type: text/html;charset=UTF-8

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<title>注册-MeetHere</title>

<meta name="viewport" content="width=device-width, initial-scale=1">

<link rel="stylesheet" href="/css/bootstrap.css">

<script src="/js/jquery-3.4.1.min.js"></script>

<script src="/js/bootstrap.bundle.min.js"></script>

<style type="text/css">

html {

overflow-y: scroll;

}

:root {

overflow-y: auto;

overflow-x: hidden;

}

:root body {

position: absolute;

}

body {

width: 100vw;

overflow: hidden;

background-color: #f5f5f5;

}

</style>

</head>

<body>

<div>

<nav class="navbar navbar-expand-sm navbar-dark fixed-top bg-dark shadow" role="navigation">

<div class="navbar-header">

<a class="navbar-brand" href="index" style="font-weight: bold">Meet Here</a>

</div>

<button class="navbar-toggler" data-toggle="collapse" data-target="#navbar">

<span class="navbar-toggler-icon"></span>

</button>

<div class="collapse navbar-collapse" id="navbar">

<ul class="navbar-nav mr-auto">

<li class="nav-item">

<a class="nav-link" href="index">首页</a>

</li>

<li class="nav-item">

<a class="nav-link" href="venue\_list">场馆信息</a>

</li>

<li class="nav-item dropdown">

<a class="nav-link dropdown-toggle" href="#" id="dropdown" data-toggle="dropdown">预约管理</a>

<div class="dropdown-menu">

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_place(false)">场馆预约</a>

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_manage(false)">订单管理</a>

</div>

</li>

<li class="nav-item">

<a class="nav-link" href="news\_list">新闻</a>

</li>

<li class="nav-item">

<a class="nav-link loginfirst" href="#" onclick="javascript:message\_list(false)">留言板</a>

</li>

</ul>

<div>

<ul class="navbar-nav ml-auto">

<li class="nav-item">

<a class="nav-link" href="login"><span class="glyphicon glyphicon-log-in"></span> 登录</a>

</li>

<li class="nav-item active">

<a class="nav-link" href="signup"><span class="glyphicon glyphicon-user"></span> 注册</a>

</li>

</ul>

</div>

</div>

</nav>

<script type="text/javascript">

$('.dropdown-toggle').dropdown();

function message\_list(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/message\_list';

}

}

function order\_manage(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/order\_manage';

}

}

function order\_place(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.open('/order\_place');

// window.location.href = '/order\_place';

}

}

</script>

</div>

<main class="container" style="padding-top: 8%">

<form class="col-6 mx-auto" role="form" action="register.do" method="post">

<div class="text-center mb-5">

<h1>注 册</h1>

</div>

<div class="form-group mb-4 row">

<div class="media col-2">

<h6 class="align-self-center ml-auto">昵称</h6>

<h6 class="text-danger">\*</h6>

</div>

<div class="col-10">

<label for="userName" class="sr-only">昵称</label>

<div class="input-group">

<div class="input-group-prepend">

<span class="input-group-text">@</span>

</div>

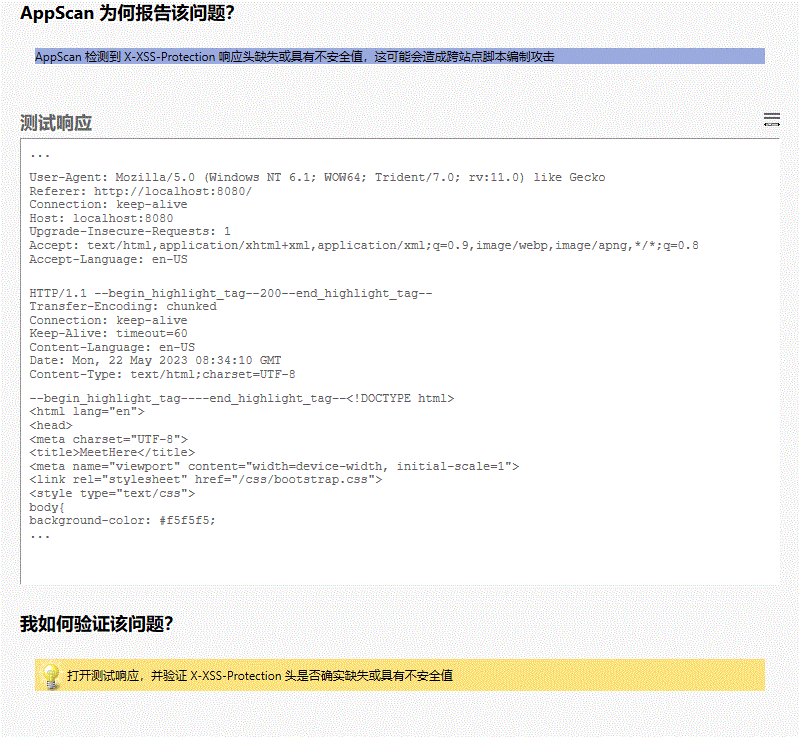
<input type="text" name="userName" class="form-control" ...

##### 问题 4/5（ http://localhost:8080/index － index ）

##### 严重性： Low

##### CVSS 计分： 5

##### 图像



**所有变体**

##### 变体差异

变体原因  
AppScan 检测到 X-XSS-Protection 响应头缺失或具有不安全值，这可能会造成跨站点脚本编制攻击

##### 变体验证

• HTTP/1.1 **200**

变体请求响应  
GET /index HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

Referer: http://localhost:8080/

Connection: keep-alive

Host: localhost:8080

Upgrade-Insecure-Requests: 1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8

Accept-Language: en-US

HTTP/1.1 200

Transfer-Encoding: chunked

Connection: keep-alive

Keep-Alive: timeout=60

Content-Language: en-US

Date: Mon, 22 May 2023 08:34:10 GMT

Content-Type: text/html;charset=UTF-8

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<title>MeetHere</title>

<meta name="viewport" content="width=device-width, initial-scale=1">

<link rel="stylesheet" href="/css/bootstrap.css">

<style type="text/css">

body{

background-color: #f5f5f5;

padding-top: 80px;

}

html {

overflow-y: scroll;

}

:root {

overflow-y: auto;

overflow-x: hidden;

}

:root body {

position: absolute;

}

body {

width: 100vw;

overflow: hidden;

}

</style>

<script src="/js/jquery-3.4.1.min.js"></script>

<script src="/js/bootstrap.bundle.min.js"></script>

</head>

<body>

<div>

<nav class="navbar navbar-expand-sm navbar-dark fixed-top bg-dark shadow" role="navigation">

<div class="navbar-header">

<a class="navbar-brand" href="index" style="font-weight: bold">Meet Here</a>

</div>

<button class="navbar-toggler" data-toggle="collapse" data-target="#navbar">

<span class="navbar-toggler-icon"></span>

</button>

<div class="collapse navbar-collapse" id="navbar">

<ul class="navbar-nav mr-auto">

<li class="nav-item active">

<a class="nav-link" href="index">首页</a>

</li>

<li class="nav-item">

<a class="nav-link" href="venue\_list">场馆信息</a>

</li>

<li class="nav-item dropdown">

<a class="nav-link dropdown-toggle" href="#" id="dropdown" data-toggle="dropdown">预约管理</a>

<div class="dropdown-menu">

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_place(false)">场馆预约</a>

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_manage(false)">订单管理</a>

</div>

</li>

<li class="nav-item">

<a class="nav-link" href="news\_list">新闻</a>

</li>

<li class="nav-item">

<a class="nav-link loginfirst" href="#" onclick="javascript:message\_list(false)">留言板</a>

</li>

</ul>

<div>

<ul class="navbar-nav ml-auto">

<li class="nav-item">

<a class="nav-link" href="login"><span class="glyphicon glyphicon-log-in"></span> 登录</a>

</li>

<li class="nav-item">

<a class="nav-link" href="signup"><span class="glyphicon glyphicon-user"></span> 注册</a>

</li>

</ul>

</div>

</div>

</nav>

<script type="text/javascript">

$('.dropdown-toggle').dropdown();

function message\_list(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/message\_list';

}

}

function order\_manage(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/order\_manage';

}

}

function order\_place(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.open('/order\_place');

// window.location.href = '/order\_place';

}

}

</script>

</div>

<main class="container-fluid">

<div class="d-flex">

<div class="col-8">

<!--场馆信息-->

<div class="card shadow">

<div class="card-header py-2 bg-info text-white">

<h6 class="card-title mb-0">场馆信息</h6>

</div>

<ul class="list-group pt-2">

<li class="list-group-item px-3 pt-3 border-0">

<div class="media border-bottom border-gray pb-3">

<div class="media-left mr-3">

<img src="venue.jpg"

alt="" height="100px" width="100px">

</div>

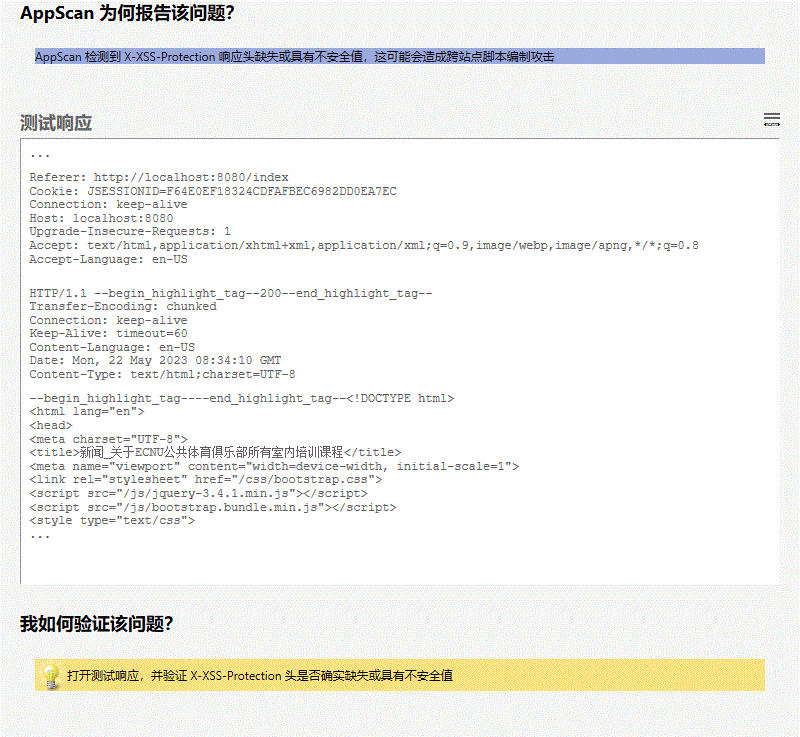
<...

##### 问题 5/5（ http://localhost:8080/news － news ）

##### 严重性： Low

##### CVSS 计分： 5

##### 图像



**所有变体**

##### 变体差异

变体原因  
AppScan 检测到 X-XSS-Protection 响应头缺失或具有不安全值，这可能会造成跨站点脚本编制攻击

##### 变体验证

• HTTP/1.1 **200**

变体请求响应  
GET /news?newsID=12 HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

Referer: http://localhost:8080/index

Cookie: JSESSIONID=F64E0EF18324CDFAFBEC6982DD0EA7EC

Connection: keep-alive

Host: localhost:8080

Upgrade-Insecure-Requests: 1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8

Accept-Language: en-US

HTTP/1.1 200

Transfer-Encoding: chunked

Connection: keep-alive

Keep-Alive: timeout=60

Content-Language: en-US

Date: Mon, 22 May 2023 08:34:10 GMT

Content-Type: text/html;charset=UTF-8

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<title>新闻\_关于ECNU公共体育俱乐部所有室内培训课程</title>

<meta name="viewport" content="width=device-width, initial-scale=1">

<link rel="stylesheet" href="/css/bootstrap.css">

<script src="/js/jquery-3.4.1.min.js"></script>

<script src="/js/bootstrap.bundle.min.js"></script>

<style type="text/css">

body{

background-color: #f5f5f5;

padding-top: 80px;

}

html {

overflow-y: scroll;

}

:root {

overflow-y: auto;

overflow-x: hidden;

}

:root body {

position: absolute;

}

body {

width: 100vw;

overflow: hidden;

}

</style>

</head>

<body>

<div>

<nav class="navbar navbar-expand-sm navbar-dark fixed-top bg-dark shadow" role="navigation">

<div class="navbar-header">

<a class="navbar-brand" href="index" style="font-weight: bold">Meet Here</a>

</div>

<button class="navbar-toggler" data-toggle="collapse" data-target="#navbar">

<span class="navbar-toggler-icon"></span>

</button>

<div class="collapse navbar-collapse" id="navbar">

<ul class="navbar-nav mr-auto">

<li class="nav-item">

<a class="nav-link" href="index">首页</a>

</li>

<li class="nav-item">

<a class="nav-link" href="venue\_list">场馆信息</a>

</li>

<li class="nav-item dropdown">

<a class="nav-link dropdown-toggle" href="#" id="dropdown" data-toggle="dropdown">预约管理</a>

<div class="dropdown-menu">

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_place(false)">场馆预约</a>

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_manage(false)">订单管理</a>

</div>

</li>

<li class="nav-item active">

<a class="nav-link" href="news\_list">新闻</a>

</li>

<li class="nav-item">

<a class="nav-link loginfirst" href="#" onclick="javascript:message\_list(false)">留言板</a>

</li>

</ul>

<div>

<ul class="navbar-nav ml-auto">

<li class="nav-item">

<a class="nav-link" href="login"><span class="glyphicon glyphicon-log-in"></span> 登录</a>

</li>

<li class="nav-item">

<a class="nav-link" href="signup"><span class="glyphicon glyphicon-user"></span> 注册</a>

</li>

</ul>

</div>

</div>

</nav>

<script type="text/javascript">

$('.dropdown-toggle').dropdown();

function message\_list(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/message\_list';

}

}

function order\_manage(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/order\_manage';

}

}

function order\_place(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.open('/order\_place');

// window.location.href = '/order\_place';

}

}

</script>

</div>

<main role="main" class="container-fluid">

<div class="row">

<div class="col-8 mx-auto">

<div class="mb-3 p-4 bg-white rounded shadow-sm">

<div class="border-bottom border-gray py-2 mb-0 text-center">

<h4 class="font-weight-bold">关于ECNU公共体育俱乐部所有室内培训课程</h4>

<small>发布时间：</small>

<small>2019-12-17 17:15:26</small>

</div>

<div class="pt-3">

<p style="text-indent: 2em">根据闵行校区体育馆物业办通知，因麻疹疾控需要，体育馆近期限制进出，故11月23日ECNU公共体育俱乐部所有室内培训课程暂停，积分不会因此产生变动，恢复日期另行通知。天气逐渐转寒，请各位同学运动后及时保暖，寝室多开窗门，保持空气流通。</p>

...

|  |  |
| --- | --- |
|  | SRI (Subresource Integrity) 的检查 (4/7) |

##### 咨询和修订建议

[远程文件包含](http://projects.webappsec.org/Remote-File-Inclusion)

来自其他域的脚本和链接标标签标记不支持完整性检查。

如果包含脚本的服务出现弱点，则这一点可能被利用。、

不支持 SRI 的样本脚本元素：

<script src="https://example.com/example-framework.js"

crossorigin="anonymous"></script>

支持 SRI 的样本脚本元素：

<script src="https://example.com/example-framework.js"

integrity="sha384-Li9vy3DqF8tnTXuiaAJuML3ky+er10rcgNR/VqsVpcw+ThHmYcwiB1pbOxEbzJr7"

crossorigin="anonymous"></script>

user-agent 无法通过第三方服务来验证脚本。

如果是第三方服务出现弱点，那么用户无法受到保护。

[FrontPage 服务器扩展：安全考虑](https://www.w3.org/TR/SRI/)

[解释](https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity)

检查是否支持 SRI（子资源完整性）

SRI (Subresource Integrity) 的检查

不支持子资源完整性。

该问题可能会影响各种类型的产品。

##### 受影响的 URL

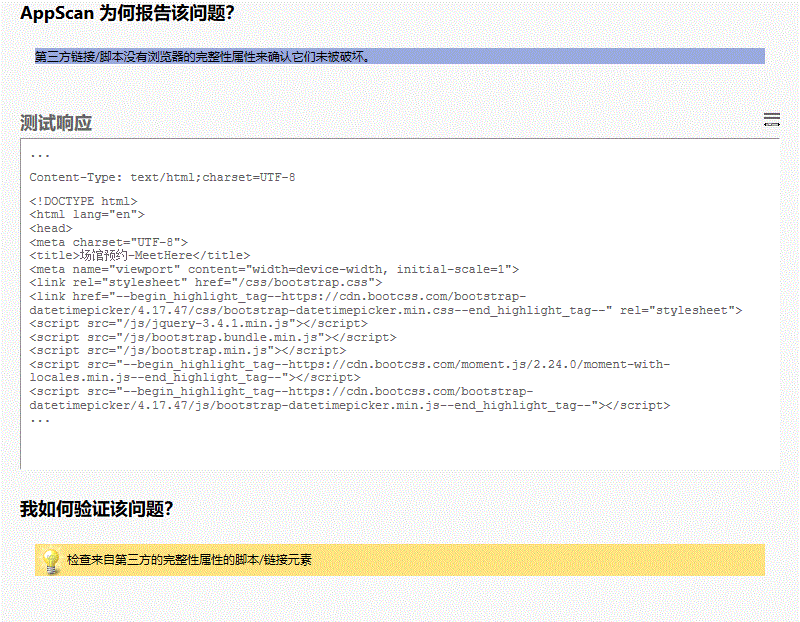
* http://localhost:8080/order\_place

##### 问题 1/1（ http://localhost:8080/order\_place － order\_place ）

##### 严重性： Low

##### CVSS 计分： 5

##### 图像



**所有变体**

##### 变体差异

变体原因  
第三方链接/脚本没有浏览器的完整性属性来确认它们未被破坏。

##### 变体验证

• vice-width, initial-scale=1">

<link rel="stylesheet" href="/css/bootstrap.css">

<link href="**https://cdn.bootcss.com/bootstrap-datetimepicker/4.17.47/css/bootstrap-datetimepicker.min.css**" rel="stylesheet">

<script src="/js/jquery-3.4.1.min.js"></script>

<script src="/js/bootstr

• ootstrap.bundle.min.js"></script>

<script src="/js/bootstrap.min.js"></script>

<script src="**https://cdn.bootcss.com/moment.js/2.24.0/moment-with-locales.min.js**"></script>

<script src="https://cdn.bootcss.com/bootstrap-datetimepicker/4.17.47/js/bootstrap-d

• rc="https://cdn.bootcss.com/moment.js/2.24.0/moment-with-locales.min.js"></script>

<script src="**https://cdn.bootcss.com/bootstrap-datetimepicker/4.17.47/js/bootstrap-datetimepicker.min.js**"></script>

<style type="text/css">

body{

background-color: #f5f5f5;

变体请求响应  
GET /order\_place HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

Referer: http://localhost:8080/login?userID=&password=

Connection: Keep-Alive

Host: localhost:8080

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Language: en-US

HTTP/1.1 200

Transfer-Encoding: chunked

Connection: keep-alive

Keep-Alive: timeout=60

Content-Language: en-US

Date: Mon, 22 May 2023 08:34:40 GMT

Content-Type: text/html;charset=UTF-8

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<title>场馆预约-MeetHere</title>

<meta name="viewport" content="width=device-width, initial-scale=1">

<link rel="stylesheet" href="/css/bootstrap.css">

<link href="https://cdn.bootcss.com/bootstrap-datetimepicker/4.17.47/css/bootstrap-datetimepicker.min.css" rel="stylesheet">

<script src="/js/jquery-3.4.1.min.js"></script>

<script src="/js/bootstrap.bundle.min.js"></script>

<script src="/js/bootstrap.min.js"></script>

<script src="https://cdn.bootcss.com/moment.js/2.24.0/moment-with-locales.min.js"></script>

<script src="https://cdn.bootcss.com/bootstrap-datetimepicker/4.17.47/js/bootstrap-datetimepicker.min.js"></script>

<style type="text/css">

body{

background-color: #f5f5f5;

}

.timebar{

width:750px;

height:auto;

margin:0;

padding:0;

font-size: 0;

/\*需设置定位\*/

position:relative;

}

.time-item{

width:50px;

height:50px;

margin:0;

padding:0;

display:inline-block;

vertical-align: top;

font-size: 13px;

background-color: white;

border:1px solid #d9d9d9;

user-select: none;

}

#moveSelected{

position:absolute;

background-color: blue;

opacity:0.3;

top:0;

left:0;

}

.selected{

background-color: #007bff;

}

.occupied{

background-color: #dc3545;

}

.banned{

background-color: #eeeeee;

}

html {

overflow-y: scroll;

}

:root {

overflow-y: auto;

overflow-x: hidden;

}

:root body {

position: absolute;

}

body {

width: 100vw;

overflow: hidden;

}

</style>

</head>

<body>

<div>

<nav class="navbar navbar-expand-sm navbar-dark fixed-top bg-dark shadow" role="navigation">

<div class="navbar-header">

<a class="navbar-brand" href="index" style="font-weight: bold">Meet Here</a>

</div>

<button class="navbar-toggler" data-toggle="collapse" data-target="#navbar">

<span class="navbar-toggler-icon"></span>

</button>

<div class="collapse navbar-collapse" id="navbar">

<ul class="navbar-nav mr-auto">

<li class="nav-item">

<a class="nav-link" href="index">首页</a>

</li>

<li class="nav-item">

<a class="nav-link" href="venue\_list">场馆信息</a>

</li>

<li class="nav-item dropdown active">

<a class="nav-link dropdown-toggle" href="#" id="dropdown" data-toggle="dropdown">预约管理</a>

<div class="dropdown-menu">

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_place(false)">场馆预约</a>

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_manage(false)">订单管理</a>

</div>

</li>

<li class="nav-item">

<a class="nav-link" href="news\_list">新闻</a>

</li>

<li class="nav-item">

<a class="nav-link loginfirst" href="#" onclick="javascript:message\_list(false)">留言板</a>

</li>

</ul>

<div>

<ul class="navbar-nav ml-auto">

<li class="nav-item">

<a class="nav-link" href="login"><span class="glyphicon glyphicon-log-in"></span> 登录</a>

</li>

<li class="nav-item">

<a class="nav-link" href="signup"><span class="glyphicon glyphicon-user"></span> 注册</a>

</li>

</ul>

</div>

</div>

</nav>

<script type="text/javascript">

$('.dropdown-toggle').dropdown();

function message\_list(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/message\_list';

}

}

function order\_manage(flag){

if(!flag){

...

|  |  |
| --- | --- |
|  | 检测到隐藏目录 (5/7) |

##### 咨询和修订建议

[信息泄露](http://projects.webappsec.org/Information-Leakage)

Web 应用程序显现了站点中的目录。虽然目录并没有列出其内容，但此信息可以帮助攻击者发展对站点进一步的攻击。例如，知道目录名称之后，攻击者便可以猜测它的内容类型，也许还能猜出其中的文件名或子目录，并尝试访问它们。

内容的敏感度越高，此问题也可能越严重。

可能会检索有关站点文件系统结构的信息，这可能会帮助攻击者映射此 Web 站点

检测到隐藏目录

检测到隐藏目录

Web 服务器或应用程序服务器是以不安全的方式配置的

该问题可能会影响各种类型的产品。

##### 受影响的 URL

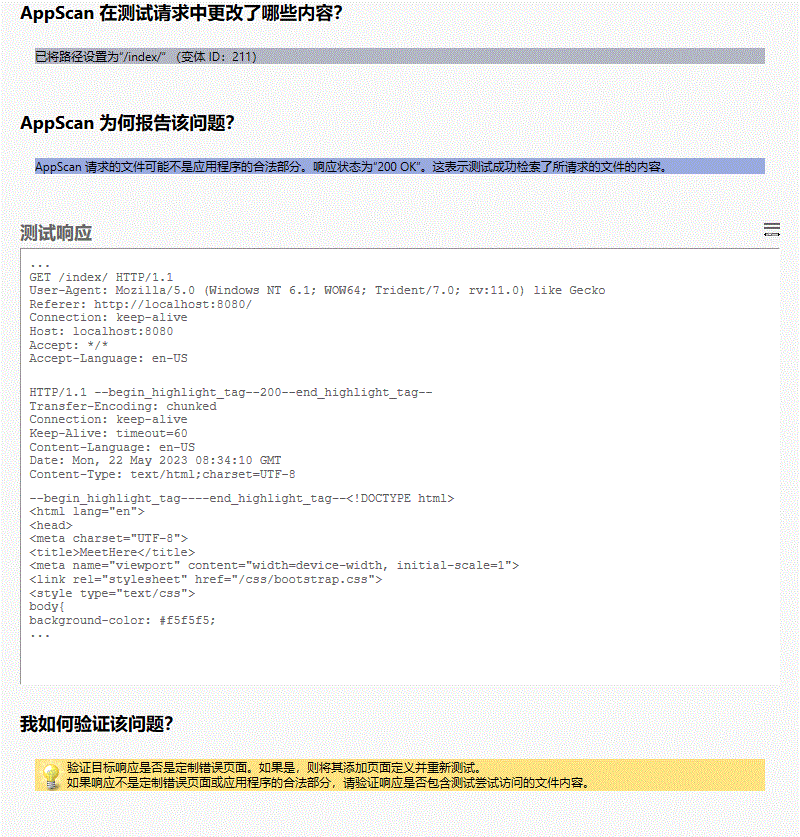
* http://localhost:8080/index/
* http://localhost:8080/login/
* http://localhost:8080/signup/

##### 问题 1/3（ http://localhost:8080/index/ － index/ ）

##### 严重性： Low

##### CVSS 计分： 5

##### 图像



**所有变体**

##### 变体差异

• 已将路径设置为“/index/”

变体原因  
AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

##### 变体验证

• HTTP/1.1 **200**

变体请求响应  
GET /index/ HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

Referer: http://localhost:8080/

Connection: keep-alive

Host: localhost:8080

Accept: \*/\*

Accept-Language: en-US

HTTP/1.1 200

Transfer-Encoding: chunked

Connection: keep-alive

Keep-Alive: timeout=60

Content-Language: en-US

Date: Mon, 22 May 2023 08:34:10 GMT

Content-Type: text/html;charset=UTF-8

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<title>MeetHere</title>

<meta name="viewport" content="width=device-width, initial-scale=1">

<link rel="stylesheet" href="/css/bootstrap.css">

<style type="text/css">

body{

background-color: #f5f5f5;

padding-top: 80px;

}

html {

overflow-y: scroll;

}

:root {

overflow-y: auto;

overflow-x: hidden;

}

:root body {

position: absolute;

}

body {

width: 100vw;

overflow: hidden;

}

</style>

<script src="/js/jquery-3.4.1.min.js"></script>

<script src="/js/bootstrap.bundle.min.js"></script>

</head>

<body>

<div>

<nav class="navbar navbar-expand-sm navbar-dark fixed-top bg-dark shadow" role="navigation">

<div class="navbar-header">

<a class="navbar-brand" href="index" style="font-weight: bold">Meet Here</a>

</div>

<button class="navbar-toggler" data-toggle="collapse" data-target="#navbar">

<span class="navbar-toggler-icon"></span>

</button>

<div class="collapse navbar-collapse" id="navbar">

<ul class="navbar-nav mr-auto">

<li class="nav-item active">

<a class="nav-link" href="index">首页</a>

</li>

<li class="nav-item">

<a class="nav-link" href="venue\_list">场馆信息</a>

</li>

<li class="nav-item dropdown">

<a class="nav-link dropdown-toggle" href="#" id="dropdown" data-toggle="dropdown">预约管理</a>

<div class="dropdown-menu">

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_place(false)">场馆预约</a>

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_manage(false)">订单管理</a>

</div>

</li>

<li class="nav-item">

<a class="nav-link" href="news\_list">新闻</a>

</li>

<li class="nav-item">

<a class="nav-link loginfirst" href="#" onclick="javascript:message\_list(false)">留言板</a>

</li>

</ul>

<div>

<ul class="navbar-nav ml-auto">

<li class="nav-item">

<a class="nav-link" href="login"><span class="glyphicon glyphicon-log-in"></span> 登录</a>

</li>

<li class="nav-item">

<a class="nav-link" href="signup"><span class="glyphicon glyphicon-user"></span> 注册</a>

</li>

</ul>

</div>

</div>

</nav>

<script type="text/javascript">

$('.dropdown-toggle').dropdown();

function message\_list(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/message\_list';

}

}

function order\_manage(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/order\_manage';

}

}

function order\_place(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.open('/order\_place');

// window.location.href = '/order\_place';

}

}

</script>

</div>

<main class="container-fluid">

<div class="d-flex">

<div class="col-8">

<!--场馆信息-->

<div class="card shadow">

<div class="card-header py-2 bg-info text-white">

<h6 class="card-title mb-0">场馆信息</h6>

</div>

<ul class="list-group pt-2">

<li class="list-group-item px-3 pt-3 border-0">

<div class="media border-bottom border-gray pb-3">

<div class="media-left mr-3">

<img src="venue.jpg"

alt="" height="100px" width="100px">

</div>

<div class="media-body">

<h5 class="media-heading font-weight-bold pb-3">

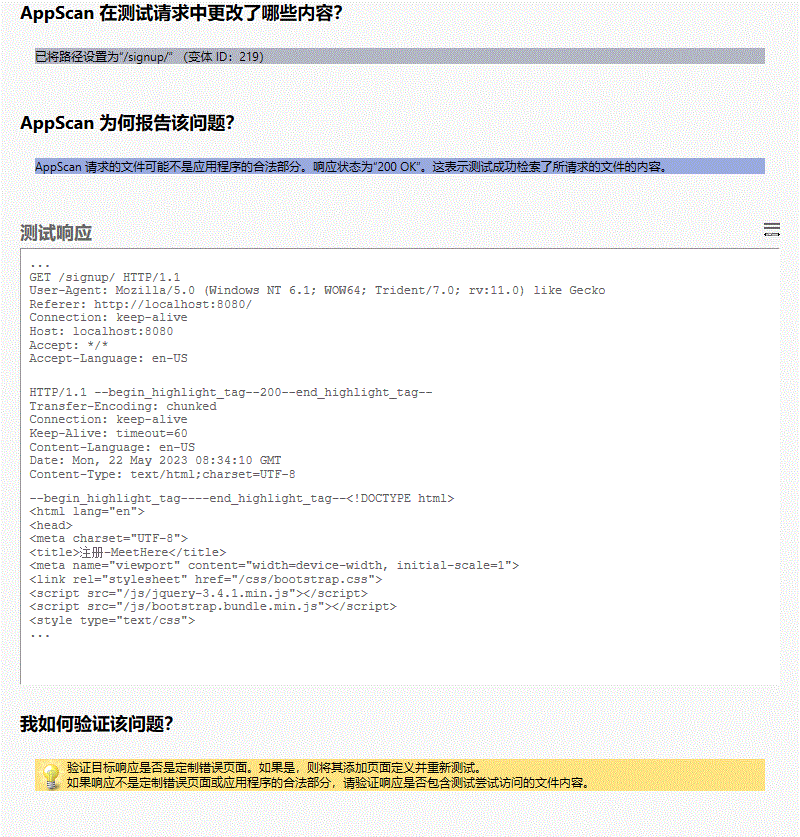
...

##### 问题 2/3（ http://localhost:8080/signup/ － signup/ ）

##### 严重性： Low

##### CVSS 计分： 5

##### 图像



**所有变体**

##### 变体差异

• 已将路径设置为“/signup/”

变体原因  
AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

##### 变体验证

• HTTP/1.1 **200**

变体请求响应  
GET /signup/ HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

Referer: http://localhost:8080/

Connection: keep-alive

Host: localhost:8080

Accept: \*/\*

Accept-Language: en-US

HTTP/1.1 200

Transfer-Encoding: chunked

Connection: keep-alive

Keep-Alive: timeout=60

Content-Language: en-US

Date: Mon, 22 May 2023 08:34:10 GMT

Content-Type: text/html;charset=UTF-8

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<title>注册-MeetHere</title>

<meta name="viewport" content="width=device-width, initial-scale=1">

<link rel="stylesheet" href="/css/bootstrap.css">

<script src="/js/jquery-3.4.1.min.js"></script>

<script src="/js/bootstrap.bundle.min.js"></script>

<style type="text/css">

html {

overflow-y: scroll;

}

:root {

overflow-y: auto;

overflow-x: hidden;

}

:root body {

position: absolute;

}

body {

width: 100vw;

overflow: hidden;

background-color: #f5f5f5;

}

</style>

</head>

<body>

<div>

<nav class="navbar navbar-expand-sm navbar-dark fixed-top bg-dark shadow" role="navigation">

<div class="navbar-header">

<a class="navbar-brand" href="index" style="font-weight: bold">Meet Here</a>

</div>

<button class="navbar-toggler" data-toggle="collapse" data-target="#navbar">

<span class="navbar-toggler-icon"></span>

</button>

<div class="collapse navbar-collapse" id="navbar">

<ul class="navbar-nav mr-auto">

<li class="nav-item">

<a class="nav-link" href="index">首页</a>

</li>

<li class="nav-item">

<a class="nav-link" href="venue\_list">场馆信息</a>

</li>

<li class="nav-item dropdown">

<a class="nav-link dropdown-toggle" href="#" id="dropdown" data-toggle="dropdown">预约管理</a>

<div class="dropdown-menu">

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_place(false)">场馆预约</a>

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_manage(false)">订单管理</a>

</div>

</li>

<li class="nav-item">

<a class="nav-link" href="news\_list">新闻</a>

</li>

<li class="nav-item">

<a class="nav-link loginfirst" href="#" onclick="javascript:message\_list(false)">留言板</a>

</li>

</ul>

<div>

<ul class="navbar-nav ml-auto">

<li class="nav-item">

<a class="nav-link" href="login"><span class="glyphicon glyphicon-log-in"></span> 登录</a>

</li>

<li class="nav-item active">

<a class="nav-link" href="signup"><span class="glyphicon glyphicon-user"></span> 注册</a>

</li>

</ul>

</div>

</div>

</nav>

<script type="text/javascript">

$('.dropdown-toggle').dropdown();

function message\_list(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/message\_list';

}

}

function order\_manage(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/order\_manage';

}

}

function order\_place(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.open('/order\_place');

// window.location.href = '/order\_place';

}

}

</script>

</div>

<main class="container" style="padding-top: 8%">

<form class="col-6 mx-auto" role="form" action="register.do" method="post">

<div class="text-center mb-5">

<h1>注 册</h1>

</div>

<div class="form-group mb-4 row">

<div class="media col-2">

<h6 class="align-self-center ml-auto">昵称</h6>

<h6 class="text-danger">\*</h6>

</div>

<div class="col-10">

<label for="userName" class="sr-only">昵称</label>

<div class="input-group">

<div class="input-group-prepend">

<span class="input-group-text">@</span>

</div>

<input type="text" name="userName" class="form-control" id="userName" required

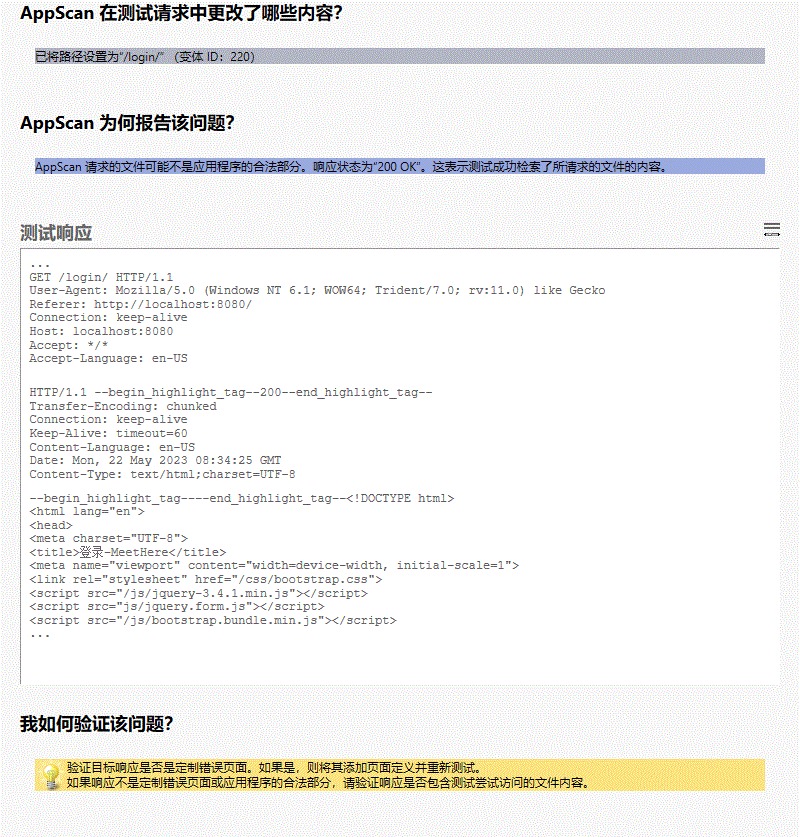
data-toggle="tooltip" title="最多18个字符" data-placement="right" data-...

##### 问题 3/3（ http://localhost:8080/login/ － login/ ）

##### 严重性： Low

##### CVSS 计分： 5

##### 图像



**所有变体**

##### 变体差异

• 已将路径设置为“/login/”

变体原因  
AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

##### 变体验证

• HTTP/1.1 **200**

变体请求响应  
GET /login/ HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

Referer: http://localhost:8080/

Connection: keep-alive

Host: localhost:8080

Accept: \*/\*

Accept-Language: en-US

HTTP/1.1 200

Transfer-Encoding: chunked

Connection: keep-alive

Keep-Alive: timeout=60

Content-Language: en-US

Date: Mon, 22 May 2023 08:34:25 GMT

Content-Type: text/html;charset=UTF-8

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<title>登录-MeetHere</title>

<meta name="viewport" content="width=device-width, initial-scale=1">

<link rel="stylesheet" href="/css/bootstrap.css">

<script src="/js/jquery-3.4.1.min.js"></script>

<script src="js/jquery.form.js"></script>

<script src="/js/bootstrap.bundle.min.js"></script>

<style type="text/css">

body{

background-color: #f5f5f5;

}

</style>

</head>

<body>

<div>

<nav class="navbar navbar-expand-sm navbar-dark fixed-top bg-dark shadow" role="navigation">

<div class="navbar-header">

<a class="navbar-brand" href="index" style="font-weight: bold">Meet Here</a>

</div>

<button class="navbar-toggler" data-toggle="collapse" data-target="#navbar">

<span class="navbar-toggler-icon"></span>

</button>

<div class="collapse navbar-collapse" id="navbar">

<ul class="navbar-nav mr-auto">

<li class="nav-item">

<a class="nav-link" href="index">首页</a>

</li>

<li class="nav-item">

<a class="nav-link" href="venue\_list">场馆信息</a>

</li>

<li class="nav-item dropdown">

<a class="nav-link dropdown-toggle" href="#" id="dropdown" data-toggle="dropdown">预约管理</a>

<div class="dropdown-menu">

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_place(false)">场馆预约</a>

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_manage(false)">订单管理</a>

</div>

</li>

<li class="nav-item">

<a class="nav-link" href="news\_list">新闻</a>

</li>

<li class="nav-item">

<a class="nav-link loginfirst" href="#" onclick="javascript:message\_list(false)">留言板</a>

</li>

</ul>

<div>

<ul class="navbar-nav ml-auto">

<li class="nav-item active">

<a class="nav-link" href="login"><span class="glyphicon glyphicon-log-in"></span> 登录</a>

</li>

<li class="nav-item">

<a class="nav-link" href="signup"><span class="glyphicon glyphicon-user"></span> 注册</a>

</li>

</ul>

</div>

</div>

</nav>

<script type="text/javascript">

$('.dropdown-toggle').dropdown();

function message\_list(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/message\_list';

}

}

function order\_manage(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/order\_manage';

}

}

function order\_place(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.open('/order\_place');

// window.location.href = '/order\_place';

}

}

</script>

</div>

<main class="container col-4" style="padding-top: 10%">

<form role="form">

<div class="text-center mb-5">

<h1>用 户 登 录</h1>

</div>

<div class="form-group mb-4">

<label for="userID" class="sr-only">User Name</label>

<input type="text" name="userID" class="form-control form-control-lg" id="userID" placeholder="用户名" required autofocus>

</div>

<div class="form-group mb-4">

<label for="password" class="sr-only">Password</label>

<input type="password" name="password" class="form-control form-control-lg" id="password" placeholder="密码" required>

</div>

<div class="alert alert-danger" hidden><span class="glyphicon glyphicon-info-sign"></span> 用户名或密码错误，请重新输入！</div>

<div class="pt-4">

<button class="btn btn-lg btn-primary btn-block" type="submit" id="submit">登 录</button>

</div>

</form>

</main>

<div>

<footer class="mt-5 mb-3 text-muted text-center">Copyright &copy; 2019-2020 MeetHere</footer>

</div>

<script type="text/javascript">

$("#userID").keyup(fu...

|  |  |
| --- | --- |
|  | 启用了 TRACE 和 TRACK HTTP 方法 (6/7) |

##### 咨询和修订建议

[功能滥用](http://projects.webappsec.org/Abuse-of-Functionality)

RFC2616 指出（第 9.8 节 － HTTP“TRACE”方法）： “TRACE 方法用于调用请求消息的远程应用层回送。请求的最终接收方应该以 200（OK）响应的实体主体向客户端反映接收到的消息... TRACE 可让客户端查看在请求链的另一端收到什么，并将这项数据用于测试或诊断信息...”如 RFC2616 所指定，完整的 HTTP 请求（包括 HTTP 头）是在 TACE 响应的主体中送回。HTTP 头可包括会话令牌、cookie 或认证凭证之类的敏感信息。由于脚本代码可以通过 DOM（文档对象模型）来访问 TRACE 响应的主体，因此，攻击者有可能滥用 Web 浏览器问题（跨域问题）来读取敏感的头信息，并略过 Microsoft Internet Explorer 6.0 SP1 所引进的“HttpOnly”cookie 属性。

可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，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

[CERT 问题注释](http://www.kb.cert.org/vuls/id/867593)

[XST 文章，作者：WhiteHat Security](http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf)

[Bugtraq 消息](http://archives.neohapsis.com/archives/bugtraq/2003-01/0230.html)

[RFC2616](http://www.ietf.org/rfc/rfc2616.txt)

启用了 TRACE 和 TRACK HTTP 方法

启用了 TRACE 和 TRACK HTTP 方法

Web 服务器或应用程序服务器是以不安全的方式配置的

该问题可能会影响各种类型的产品

##### 受影响的 URL

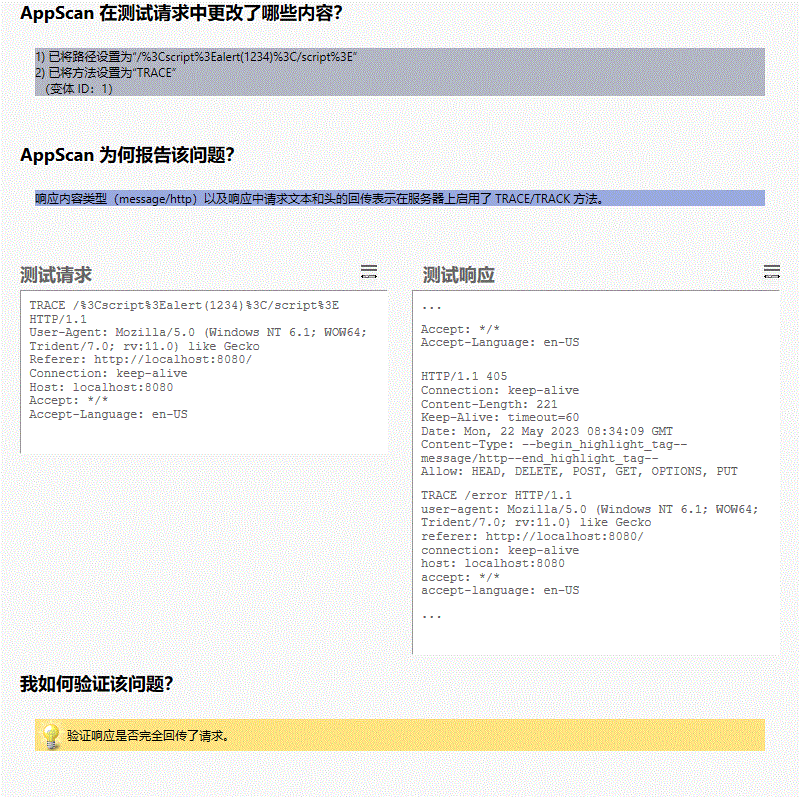
* http://localhost:8080/js/jquery-3.4.1.min.js

##### 问题 1/1（ http://localhost:8080/js/jquery-3.4.1.min.js － localhost ）

##### 严重性： Low

##### CVSS 计分： 5

##### 图像



**所有变体**

##### 变体差异

• 已将路径设置为“/%3Cscript%3Ealert(1234)%3C/script%3E”

• 已将方法设置为“TRACE”

变体原因  
响应内容类型（message/http）以及响应中请求文本和头的回传表示在服务器上启用了 TRACE/TRACK 方法。

##### 变体验证

• Content-Type: **message/http**

变体请求响应  
TRACE /%3Cscript%3Ealert(1234)%3C/script%3E HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

Referer: http://localhost:8080/

Connection: keep-alive

Host: localhost:8080

Accept: \*/\*

Accept-Language: en-US

HTTP/1.1 405

Connection: keep-alive

Content-Length: 221

Keep-Alive: timeout=60

Date: Mon, 22 May 2023 08:34:09 GMT

Content-Type: message/http

Allow: HEAD, DELETE, POST, GET, OPTIONS, PUT

TRACE /error HTTP/1.1

user-agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

referer: http://localhost:8080/

connection: keep-alive

host: localhost:8080

accept: \*/\*

accept-language: en-US

|  |  |
| --- | --- |
|  | 自动填写未对密码字段禁用的 HTML 属性 (7/7) |

##### 咨询和修订建议

[信息泄露](http://projects.webappsec.org/Information-Leakage)

“autocomplete”属性已在 HTML5 标准中进行规范。W3C 的站点声明该属性有两种状态：“on”和“off”，完全忽略时等同于设置为“on”。

该页面易受攻击，因为“input”元素的“password”字段中的“autocomplete”属性没有设置为“off”。

这可能会使未授权用户（具有授权客户机的本地访问权）能够自动填写用户名和密码字段，并因此登录站点。

可能会绕开 Web 应用程序的认证机制

自动填写未对密码字段禁用的 HTML 属性

自动填写未对密码字段禁用的 HTML 属性

Web 应用程序编程或配置不安全

不适用

##### 受影响的 URL

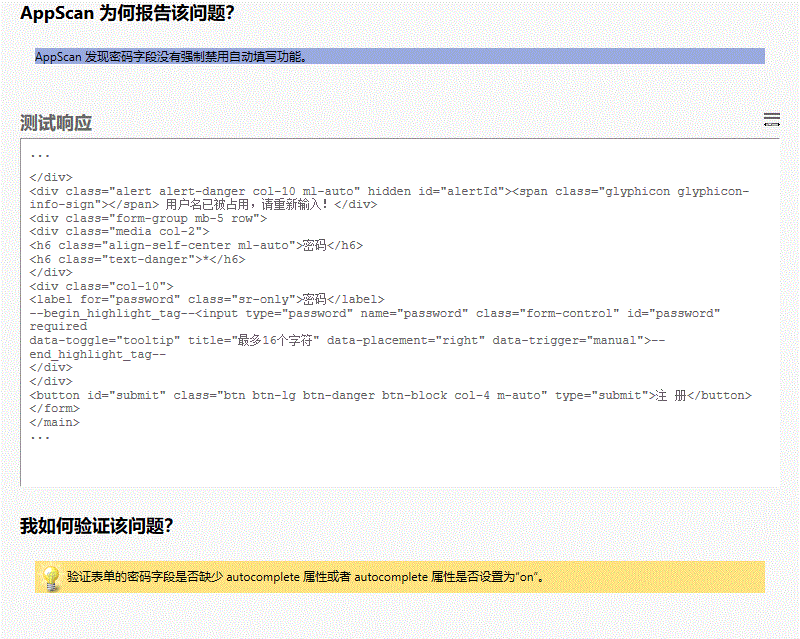
* http://localhost:8080/login
* http://localhost:8080/signup

##### 问题 1/2（ http://localhost:8080/signup － signup ）

##### 严重性： Low

##### CVSS 计分： 5

##### 图像



**所有变体**

##### 变体差异

变体原因  
AppScan 发现密码字段没有强制禁用自动填写功能。

##### 变体验证

• iv class="col-10">

<label for="password" class="sr-only">密码</label>

**<input type="password" name="password" class="form-control" id="password" required**

**data-toggle="tooltip" title="最多16个字符" data-placement="right" data-trigger="manual">**

</div>

</div>

<button id="submit" class="btn btn-lg btn-danger btn-bloc

变体请求响应  
GET /signup HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

Referer: http://localhost:8080/login

Connection: keep-alive

Host: localhost:8080

Upgrade-Insecure-Requests: 1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8

Accept-Language: en-US

HTTP/1.1 200

Transfer-Encoding: chunked

Connection: keep-alive

Keep-Alive: timeout=60

Content-Language: en-US

Date: Mon, 22 May 2023 08:34:10 GMT

Content-Type: text/html;charset=UTF-8

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<title>注册-MeetHere</title>

<meta name="viewport" content="width=device-width, initial-scale=1">

<link rel="stylesheet" href="/css/bootstrap.css">

<script src="/js/jquery-3.4.1.min.js"></script>

<script src="/js/bootstrap.bundle.min.js"></script>

<style type="text/css">

html {

overflow-y: scroll;

}

:root {

overflow-y: auto;

overflow-x: hidden;

}

:root body {

position: absolute;

}

body {

width: 100vw;

overflow: hidden;

background-color: #f5f5f5;

}

</style>

</head>

<body>

<div>

<nav class="navbar navbar-expand-sm navbar-dark fixed-top bg-dark shadow" role="navigation">

<div class="navbar-header">

<a class="navbar-brand" href="index" style="font-weight: bold">Meet Here</a>

</div>

<button class="navbar-toggler" data-toggle="collapse" data-target="#navbar">

<span class="navbar-toggler-icon"></span>

</button>

<div class="collapse navbar-collapse" id="navbar">

<ul class="navbar-nav mr-auto">

<li class="nav-item">

<a class="nav-link" href="index">首页</a>

</li>

<li class="nav-item">

<a class="nav-link" href="venue\_list">场馆信息</a>

</li>

<li class="nav-item dropdown">

<a class="nav-link dropdown-toggle" href="#" id="dropdown" data-toggle="dropdown">预约管理</a>

<div class="dropdown-menu">

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_place(false)">场馆预约</a>

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_manage(false)">订单管理</a>

</div>

</li>

<li class="nav-item">

<a class="nav-link" href="news\_list">新闻</a>

</li>

<li class="nav-item">

<a class="nav-link loginfirst" href="#" onclick="javascript:message\_list(false)">留言板</a>

</li>

</ul>

<div>

<ul class="navbar-nav ml-auto">

<li class="nav-item">

<a class="nav-link" href="login"><span class="glyphicon glyphicon-log-in"></span> 登录</a>

</li>

<li class="nav-item active">

<a class="nav-link" href="signup"><span class="glyphicon glyphicon-user"></span> 注册</a>

</li>

</ul>

</div>

</div>

</nav>

<script type="text/javascript">

$('.dropdown-toggle').dropdown();

function message\_list(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/message\_list';

}

}

function order\_manage(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/order\_manage';

}

}

function order\_place(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.open('/order\_place');

// window.location.href = '/order\_place';

}

}

</script>

</div>

<main class="container" style="padding-top: 8%">

<form class="col-6 mx-auto" role="form" action="register.do" method="post">

<div class="text-center mb-5">

<h1>注 册</h1>

</div>

<div class="form-group mb-4 row">

<div class="media col-2">

<h6 class="align-self-center ml-auto">昵称</h6>

<h6 class="text-danger">\*</h6>

</div>

<div class="col-10">

<label for="userName" class="sr-only">昵称</label>

<div class="input-group">

<div class="input-group-prepend">

<span class="input-group-text">@</span>

</div>

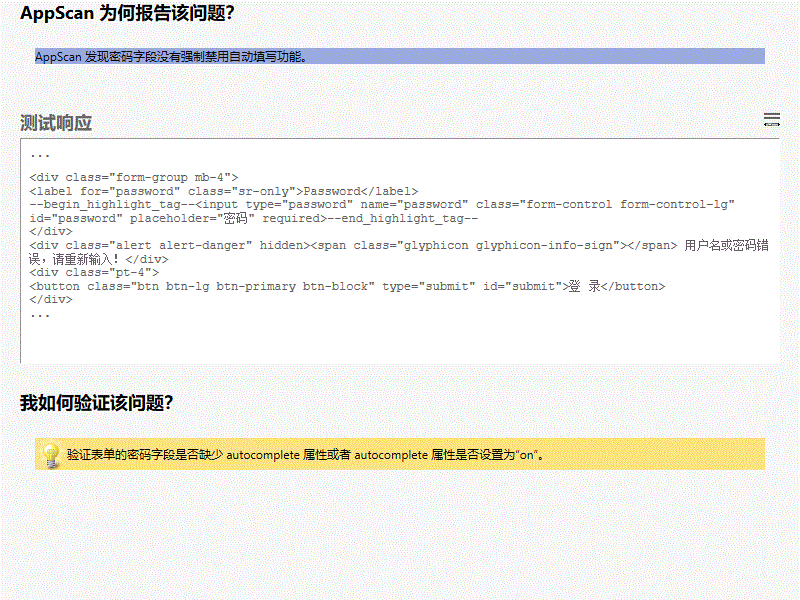
<input type="text" name="userName" class="form-control" ...

##### 问题 2/2（ http://localhost:8080/login － login ）

##### 严重性： Low

##### CVSS 计分： 5

##### 图像



**所有变体**

##### 变体差异

变体原因  
AppScan 发现密码字段没有强制禁用自动填写功能。

##### 变体验证

• s="form-group mb-4">

<label for="password" class="sr-only">Password</label>

**<input type="password" name="password" class="form-control form-control-lg" id="password" placeholder="密码" required>**

</div>

<div class="alert alert-danger" hidden><span class="glyphicon glyphicon-info

变体请求响应  
GET /login HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

Referer: http://localhost:8080/register.do

Connection: Keep-Alive

Host: localhost:8080

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Language: en-US

HTTP/1.1 200

Transfer-Encoding: chunked

Connection: keep-alive

Keep-Alive: timeout=60

Content-Language: en-US

Date: Mon, 22 May 2023 08:34:25 GMT

Content-Type: text/html;charset=UTF-8

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<title>登录-MeetHere</title>

<meta name="viewport" content="width=device-width, initial-scale=1">

<link rel="stylesheet" href="/css/bootstrap.css">

<script src="/js/jquery-3.4.1.min.js"></script>

<script src="js/jquery.form.js"></script>

<script src="/js/bootstrap.bundle.min.js"></script>

<style type="text/css">

body{

background-color: #f5f5f5;

}

</style>

</head>

<body>

<div>

<nav class="navbar navbar-expand-sm navbar-dark fixed-top bg-dark shadow" role="navigation">

<div class="navbar-header">

<a class="navbar-brand" href="index" style="font-weight: bold">Meet Here</a>

</div>

<button class="navbar-toggler" data-toggle="collapse" data-target="#navbar">

<span class="navbar-toggler-icon"></span>

</button>

<div class="collapse navbar-collapse" id="navbar">

<ul class="navbar-nav mr-auto">

<li class="nav-item">

<a class="nav-link" href="index">首页</a>

</li>

<li class="nav-item">

<a class="nav-link" href="venue\_list">场馆信息</a>

</li>

<li class="nav-item dropdown">

<a class="nav-link dropdown-toggle" href="#" id="dropdown" data-toggle="dropdown">预约管理</a>

<div class="dropdown-menu">

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_place(false)">场馆预约</a>

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_manage(false)">订单管理</a>

</div>

</li>

<li class="nav-item">

<a class="nav-link" href="news\_list">新闻</a>

</li>

<li class="nav-item">

<a class="nav-link loginfirst" href="#" onclick="javascript:message\_list(false)">留言板</a>

</li>

</ul>

<div>

<ul class="navbar-nav ml-auto">

<li class="nav-item active">

<a class="nav-link" href="login"><span class="glyphicon glyphicon-log-in"></span> 登录</a>

</li>

<li class="nav-item">

<a class="nav-link" href="signup"><span class="glyphicon glyphicon-user"></span> 注册</a>

</li>

</ul>

</div>

</div>

</nav>

<script type="text/javascript">

$('.dropdown-toggle').dropdown();

function message\_list(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/message\_list';

}

}

function order\_manage(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/order\_manage';

}

}

function order\_place(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.open('/order\_place');

// window.location.href = '/order\_place';

}

}

</script>

</div>

<main class="container col-4" style="padding-top: 10%">

<form role="form">

<div class="text-center mb-5">

<h1>用 户 登 录</h1>

</div>

<div class="form-group mb-4">

<label for="userID" class="sr-only">User Name</label>

<input type="text" name="userID" class="form-control form-control-lg" id="userID" placeholder="用户名" required autofocus>

</div>

<div class="form-group mb-4">

<label for="password" class="sr-only">Password</label>

<input type="password" name="password" class="form-control form-control-lg" id="password" placeholder="密码" required>

</div>

<div class="alert alert-danger" hidden><span class="glyphicon glyphicon-info-sign"></span> 用户名或密码错误，请重新输入！</div>

<div class="pt-4">

<button class="btn btn-lg btn-primary btn-block" type="submit" id="submit">登 录</button>

</div>

</form>

</main>

<div>

<footer class="mt-5 mb-3 text-muted text-center">Copyright &copy; 2019-2020 MeetHere</foo...

## 严重性为参考信息的“问题类型”

|  |  |
| --- | --- |
|  | HTML 注释敏感信息泄露 (1/4) |

##### 咨询和修订建议

[信息泄露](http://projects.webappsec.org/Information-Leakage)

很多 Web 应用程序程序员使用 HTML 注释，以在需要时帮助调试应用程序。尽管添加常规注释有助于调试应用程序，但一些程序员往往会遗留重要数据（例如：与 Web 应用程序相关的文件名、旧的链接或原非供用户浏览的链接、旧的代码片段等）。

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

[WASC 威胁分类：信息泄露](http://www.webappsec.org/projects/threat/classes/information_leakage.shtml)

HTML 注释敏感信息泄露

HTML 注释敏感信息泄露

程序员在 Web 页面上留下调试信息

该问题可能会影响各种类型的产品。

##### 受影响的 URL

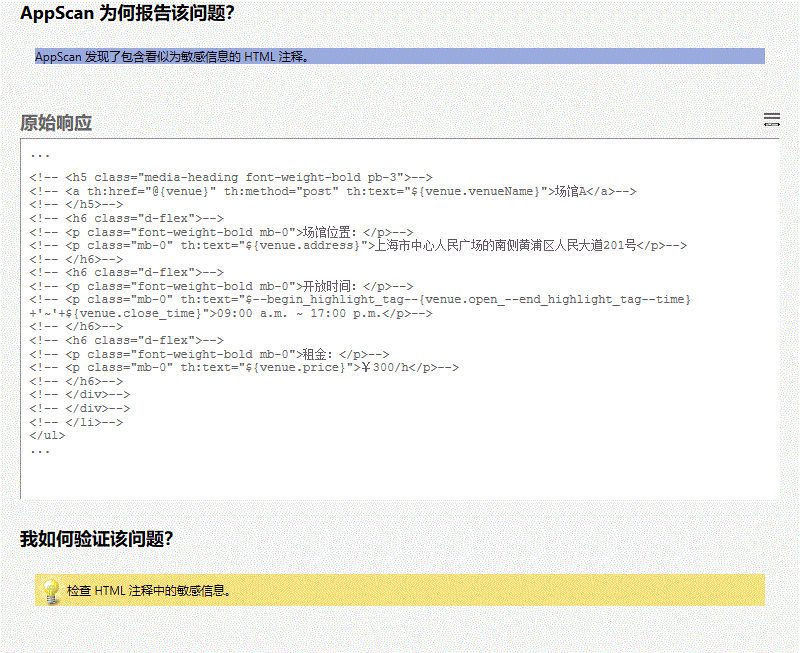
* http://localhost:8080/news
* http://localhost:8080/venue
* http://localhost:8080/venue\_list

##### 问题 1/3（ http://localhost:8080/venue\_list － <p class="mb-0" th:text="${venue.open\_time}+'~'+${venue.close\_time}">09:00 a.m. ~ 17:00 p.m.</p> ）

##### 严重性： Informational

##### CVSS 计分： 手动计分

##### 图像



**所有变体**

##### 变体差异

变体原因  
AppScan 发现了包含看似为敏感信息的 HTML 注释。

##### 变体验证

• lass="font-weight-bold mb-0">开放时间：</p>-->

<!-- <p class="mb-0" th:text="$**{venue.open\_**time}+'~'+${venue.close\_time}">09:00 a.m. ~ 17:00 p.m.</p>-->

<!-- </h6>-->

<

变体请求响应  
GET /venue\_list HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

Referer: http://localhost:8080/index

Connection: keep-alive

Host: localhost:8080

Upgrade-Insecure-Requests: 1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8

Accept-Language: en-US

HTTP/1.1 200

Transfer-Encoding: chunked

Connection: keep-alive

Keep-Alive: timeout=60

Content-Language: en-US

Date: Mon, 22 May 2023 08:34:10 GMT

Content-Type: text/html;charset=UTF-8

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<title>场馆-MeetHere</title>

<meta name="viewport" content="width=device-width, initial-scale=1">

<link rel="stylesheet" href="/css/bootstrap.css">

<script src="/js/jquery-3.4.1.min.js"></script>

<script src="/js/bootstrap.bundle.min.js"></script>

<script src="/js/jquery.twbsPagination.js"></script>

<style type="text/css">

body{

background-color: #f5f5f5;

padding-top: 80px;

}

html {

overflow-y: scroll;

}

:root {

overflow-y: auto;

overflow-x: hidden;

}

:root body {

position: absolute;

}

body {

width: 100vw;

overflow: hidden;

}

</style>

</head>

<body>

<div>

<nav class="navbar navbar-expand-sm navbar-dark fixed-top bg-dark shadow" role="navigation">

<div class="navbar-header">

<a class="navbar-brand" href="index" style="font-weight: bold">Meet Here</a>

</div>

<button class="navbar-toggler" data-toggle="collapse" data-target="#navbar">

<span class="navbar-toggler-icon"></span>

</button>

<div class="collapse navbar-collapse" id="navbar">

<ul class="navbar-nav mr-auto">

<li class="nav-item">

<a class="nav-link" href="index">首页</a>

</li>

<li class="nav-item active">

<a class="nav-link" href="venue\_list">场馆信息</a>

</li>

<li class="nav-item dropdown">

<a class="nav-link dropdown-toggle" href="#" id="dropdown" data-toggle="dropdown">预约管理</a>

<div class="dropdown-menu">

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_place(false)">场馆预约</a>

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_manage(false)">订单管理</a>

</div>

</li>

<li class="nav-item">

<a class="nav-link" href="news\_list">新闻</a>

</li>

<li class="nav-item">

<a class="nav-link loginfirst" href="#" onclick="javascript:message\_list(false)">留言板</a>

</li>

</ul>

<div>

<ul class="navbar-nav ml-auto">

<li class="nav-item">

<a class="nav-link" href="login"><span class="glyphicon glyphicon-log-in"></span> 登录</a>

</li>

<li class="nav-item">

<a class="nav-link" href="signup"><span class="glyphicon glyphicon-user"></span> 注册</a>

</li>

</ul>

</div>

</div>

</nav>

<script type="text/javascript">

$('.dropdown-toggle').dropdown();

function message\_list(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/message\_list';

}

}

function order\_manage(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/order\_manage';

}

}

function order\_place(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.open('/order\_place');

// window.location.href = '/order\_place';

}

}

</script>

</div>

<main role="main" class="container">

<div class="card bg-white rounded shadow">

<div class="card-header py-3 text-center bg-info text-light">

<h5 class="card-title mb-0">场馆信息</h5>

</div>

<ul class="list-group pt-2 px-3" id="content">

<!-- <li class="list-group-item px-3 pt-3 border-0" th:each="venue : ${venue\_list}">-->

<!-- <div class="media border-bottom border-gray pb-3">-->

<!-- <div class="media-left mr-3">-->

<!-- <img th:src="${venue.picture}"-->

<!-- alt="" height="100px" width="100px">-->

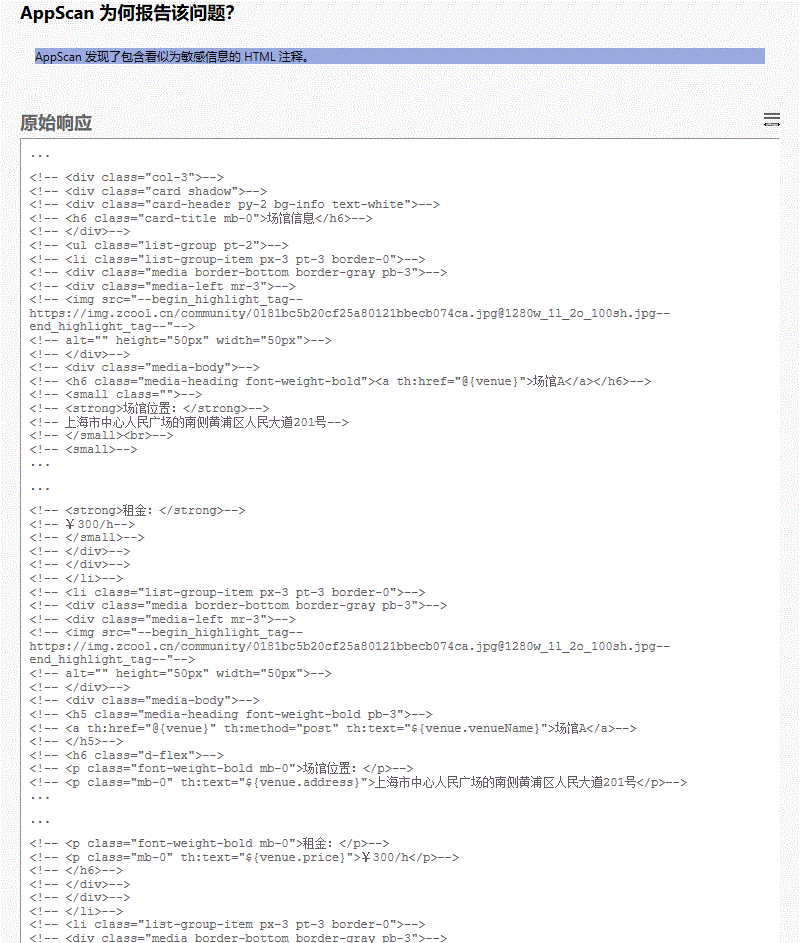
<!-- ...

##### 问题 2/3（ http://localhost:8080/venue － <img src="https://img.zcool.cn/community/0181bc5b20cf25a80121bbecb074ca.jpg@1280w\_1l\_2o\_100sh.jpg" ）

##### 严重性： Informational

##### CVSS 计分： 手动计分

##### 图像



**所有变体**

##### 变体差异

变体原因  
AppScan 发现了包含看似为敏感信息的 HTML 注释。

##### 变体验证

• <div class="media-left mr-3">-->

<!-- <img src="**https://img.zcool.cn/community/0181bc5b20cf25a80121bbecb074ca.jpg@1280w\_1l\_2o\_100sh.jpg**"-->

<!-- alt="" height="50px" width="50px">-->

<!--

• <div class="media-left mr-3">-->

<!-- <img src="**https://img.zcool.cn/community/0181bc5b20cf25a80121bbecb074ca.jpg@1280w\_1l\_2o\_100sh.jpg**"-->

<!-- alt="" height="50px" width="50px">-->

<!--

• <div class="media-left mr-3">-->

<!-- <img src="**https://img.zcool.cn/community/0181bc5b20cf25a80121bbecb074ca.jpg@1280w\_1l\_2o\_100sh.jpg**"-->

<!-- alt="" height="50px" width="50px">-->

<!--

变体请求响应  
GET /venue?venueID=2 HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

Referer: http://localhost:8080/index

Cookie: JSESSIONID=F64E0EF18324CDFAFBEC6982DD0EA7EC

Connection: keep-alive

Host: localhost:8080

Upgrade-Insecure-Requests: 1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8

Accept-Language: en-US

HTTP/1.1 200

Transfer-Encoding: chunked

Connection: keep-alive

Keep-Alive: timeout=60

Content-Language: en-US

Date: Mon, 22 May 2023 08:34:10 GMT

Content-Type: text/html;charset=UTF-8

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<title>场馆信息\_场馆1</title>

<meta name="viewport" content="width=device-width, initial-scale=1">

<link rel="stylesheet" href="/css/bootstrap.css">

<script src="/js/jquery-3.4.1.min.js"></script>

<script src="/js/bootstrap.bundle.min.js"></script>

<style type="text/css">

body{

background-color: #f5f5f5;

padding-top: 80px;

}

html {

overflow-y: scroll;

}

:root {

overflow-y: auto;

overflow-x: hidden;

}

:root body {

position: absolute;

}

body {

width: 100vw;

overflow: hidden;

}

</style>

</head>

<body>

<div>

<nav class="navbar navbar-expand-sm navbar-dark fixed-top bg-dark shadow" role="navigation">

<div class="navbar-header">

<a class="navbar-brand" href="index" style="font-weight: bold">Meet Here</a>

</div>

<button class="navbar-toggler" data-toggle="collapse" data-target="#navbar">

<span class="navbar-toggler-icon"></span>

</button>

<div class="collapse navbar-collapse" id="navbar">

<ul class="navbar-nav mr-auto">

<li class="nav-item">

<a class="nav-link" href="index">首页</a>

</li>

<li class="nav-item active">

<a class="nav-link" href="venue\_list">场馆信息</a>

</li>

<li class="nav-item dropdown">

<a class="nav-link dropdown-toggle" href="#" id="dropdown" data-toggle="dropdown">预约管理</a>

<div class="dropdown-menu">

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_place(false)">场馆预约</a>

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_manage(false)">订单管理</a>

</div>

</li>

<li class="nav-item">

<a class="nav-link" href="news\_list">新闻</a>

</li>

<li class="nav-item">

<a class="nav-link loginfirst" href="#" onclick="javascript:message\_list(false)">留言板</a>

</li>

</ul>

<div>

<ul class="navbar-nav ml-auto">

<li class="nav-item">

<a class="nav-link" href="login"><span class="glyphicon glyphicon-log-in"></span> 登录</a>

</li>

<li class="nav-item">

<a class="nav-link" href="signup"><span class="glyphicon glyphicon-user"></span> 注册</a>

</li>

</ul>

</div>

</div>

</nav>

<script type="text/javascript">

$('.dropdown-toggle').dropdown();

function message\_list(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/message\_list';

}

}

function order\_manage(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/order\_manage';

}

}

function order\_place(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.open('/order\_place');

// window.location.href = '/order\_place';

}

}

</script>

</div>

<main role="main" class="container-fluid">

<div class="row">

<div class="col-8 mx-auto">

<div class="mb-3 p-4 bg-white rounded shadow-sm">

<div class="media border-bottom border-gray pb-3">

<div class="media-body">

<h4 class="media-heading font-weight-bold pb-3">场馆1</h4>

<h6 class="d-flex">

<p class="font-weight-bold mb-0">场馆位置：</p>

<p class="mb-0">上海市普陀区中山北路3664号</p>

</h6>

<h6 class="d-flex">

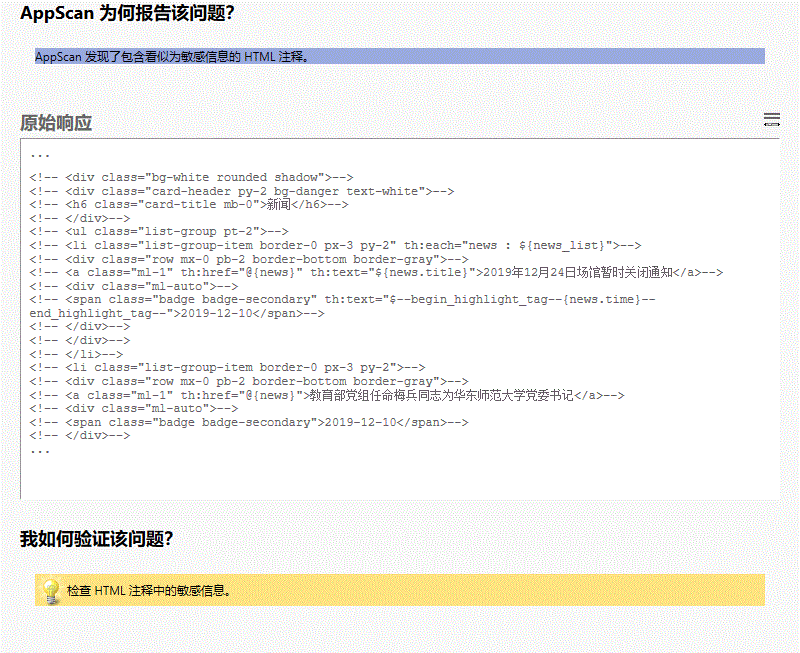
<p class="font-weight-bold...

##### 问题 3/3（ http://localhost:8080/news － <span class="badge badge-secondary" th:text="${news.time}">2019-12-10</span> ）

##### 严重性： Informational

##### CVSS 计分： 手动计分

##### 图像



**所有变体**

##### 变体差异

变体原因  
AppScan 发现了包含看似为敏感信息的 HTML 注释。

##### 变体验证

• ass="ml-auto">-->

<!-- <span class="badge badge-secondary" th:text="$**{news.time}**">2019-12-10</span>-->

<!-- </div>-->

<!-- </div>-

变体请求响应  
GET /news?newsID=12 HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

Referer: http://localhost:8080/index

Cookie: JSESSIONID=F64E0EF18324CDFAFBEC6982DD0EA7EC

Connection: keep-alive

Host: localhost:8080

Upgrade-Insecure-Requests: 1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8

Accept-Language: en-US

HTTP/1.1 200

Transfer-Encoding: chunked

Connection: keep-alive

Keep-Alive: timeout=60

Content-Language: en-US

Date: Mon, 22 May 2023 08:34:10 GMT

Content-Type: text/html;charset=UTF-8

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<title>新闻\_关于ECNU公共体育俱乐部所有室内培训课程</title>

<meta name="viewport" content="width=device-width, initial-scale=1">

<link rel="stylesheet" href="/css/bootstrap.css">

<script src="/js/jquery-3.4.1.min.js"></script>

<script src="/js/bootstrap.bundle.min.js"></script>

<style type="text/css">

body{

background-color: #f5f5f5;

padding-top: 80px;

}

html {

overflow-y: scroll;

}

:root {

overflow-y: auto;

overflow-x: hidden;

}

:root body {

position: absolute;

}

body {

width: 100vw;

overflow: hidden;

}

</style>

</head>

<body>

<div>

<nav class="navbar navbar-expand-sm navbar-dark fixed-top bg-dark shadow" role="navigation">

<div class="navbar-header">

<a class="navbar-brand" href="index" style="font-weight: bold">Meet Here</a>

</div>

<button class="navbar-toggler" data-toggle="collapse" data-target="#navbar">

<span class="navbar-toggler-icon"></span>

</button>

<div class="collapse navbar-collapse" id="navbar">

<ul class="navbar-nav mr-auto">

<li class="nav-item">

<a class="nav-link" href="index">首页</a>

</li>

<li class="nav-item">

<a class="nav-link" href="venue\_list">场馆信息</a>

</li>

<li class="nav-item dropdown">

<a class="nav-link dropdown-toggle" href="#" id="dropdown" data-toggle="dropdown">预约管理</a>

<div class="dropdown-menu">

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_place(false)">场馆预约</a>

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_manage(false)">订单管理</a>

</div>

</li>

<li class="nav-item active">

<a class="nav-link" href="news\_list">新闻</a>

</li>

<li class="nav-item">

<a class="nav-link loginfirst" href="#" onclick="javascript:message\_list(false)">留言板</a>

</li>

</ul>

<div>

<ul class="navbar-nav ml-auto">

<li class="nav-item">

<a class="nav-link" href="login"><span class="glyphicon glyphicon-log-in"></span> 登录</a>

</li>

<li class="nav-item">

<a class="nav-link" href="signup"><span class="glyphicon glyphicon-user"></span> 注册</a>

</li>

</ul>

</div>

</div>

</nav>

<script type="text/javascript">

$('.dropdown-toggle').dropdown();

function message\_list(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/message\_list';

}

}

function order\_manage(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/order\_manage';

}

}

function order\_place(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.open('/order\_place');

// window.location.href = '/order\_place';

}

}

</script>

</div>

<main role="main" class="container-fluid">

<div class="row">

<div class="col-8 mx-auto">

<div class="mb-3 p-4 bg-white rounded shadow-sm">

<div class="border-bottom border-gray py-2 mb-0 text-center">

<h4 class="font-weight-bold">关于ECNU公共体育俱乐部所有室内培训课程</h4>

<small>发布时间：</small>

<small>2019-12-17 17:15:26</small>

</div>

<div class="pt-3">

<p style="text-indent: 2em">根据闵行校区体育馆物业办通知，因麻疹疾控需要，体育馆近期限制进出，故11月23日ECNU公共体育俱乐部所有室内培训课程暂停，积分不会因此产生变动，恢复日期另行通知。天气逐渐转寒，请各位同学运动后及时保暖，寝室多开窗门，保持空气流通。</p>

...

|  |  |
| --- | --- |
|  | JSON 中反映的未清理用户输入 (2/4) |

#### 咨询和修订建议

[跨站点脚本编制](http://projects.webappsec.org/Cross-Site+Scripting)

AppScan 检测到在将用户可控制输入放入 JSON 响应中提供的输出中之前应用程序没有正确中和该输入。

虽然浏览器不会显示 JSON 响应，但是应用程序可能会在其他地方利用不可信输入，这可能导致跨站点脚本编制攻击成功。

在以下情况下会出现跨站点脚本编制 (XSS) 漏洞：

[1] Web 应用程序中输入不可信数据，通常来自 Web 请求。

[2] Web 应用程序动态生成一个包含这些不可信数据的网页。

[3] 在页面生成期间，应用程序没有阻止数据包含 Web 浏览器可执行的内容，如 JavaScript、HTML 标记、HTML 属性、鼠标事件、Flash、ActiveX。

[4] 受害者通过 Web 浏览器访问生成的网页，该网页包含使用不可信数据注入的恶意脚本。

[5] 因为脚本来自 Web 服务器发送的网页，所以受害者的 Web 浏览器会在 Web 服务器的域环境中执行该恶意脚本。

[6] 这实际上违反了 Web 浏览器同源策略的意图，同源策略声明一个域中的脚本不能在另一个域中访问资源或运行代码。

注入恶意脚本后，攻击者便可以进行各种恶意活动了。攻击者可以将私人信息（如可能包含会话信息的 cookie）从受害机器发送给攻击者。攻击者可以用受害者的身份向网站发送恶意请求，如果受害者拥有管理该网站的管理员权限，则这可能对网站特别危险。

钓鱼攻击可用于模仿可信网站并哄骗受害者输入密码，从而允许攻击者在该网站上盗用受害者的帐户。最后，该脚本可以攻击 Web 浏览器本身的漏洞，从而可能接管受害者的机器（有时被称为“路过式入侵”）。

XSS 有三种主要类型：

类型 1：反射型 XSS（也称为“非持久性”）

服务器直接从 HTTP 请求读取数据并在 HTTP 响应中将其反射回去。攻击者导致受害者向易受攻击的 Web 应用程序提供危险内容时，会发生反射型 XSS 攻击，这些危险内容之后会反射回给受害者并由 Web 浏览器执行。提供恶意内容的最常见途径是将恶意内容作为参数包含在公开发布的 URL 中，或者直接通过电子邮件发送给受害者。以这种方式构建的 URL 构成了许多网络钓鱼方案的核心，攻击者借此说服受害者访问易受攻击站点的 URL。在该站点将攻击者的内容反射回给受害者后，受害者的浏览器会执行这些内容。

类型 2：存储型 XSS（也称为“持久性”）

应用程序在数据库、消息论坛、访问者日志或其他可信数据存储中存储危险数据。稍后，应用程序会重新读取这些危险数据并将其包含在动态内容中。从攻击者的角度来说，注入恶意内容的最佳位置位于面向许多用户或攻击者特别感兴趣的用户显示的区域。攻击者感兴趣的用户通常拥有应用程序的提升特权，或者能与易受攻击者攻击的敏感数据互动。如果这些用户之一执行了恶意内容，则攻击者就可能能够以该用户的身份执行特权操作，或者获得访问属于该用户的敏感数据的权限。例如，攻击者可能将 XSS 注入管理员查看日志时可能没有正确处理的日志消息中。

类型 0：基于 DOM 的 XSS

在基于 DOM 的 XSS 中，由客户机执行页面中的 XSS 注入；而在其他类型 XSS 中，则由服务器执行注入。基于 DOM 的 XSS 通常涉及发送给客户机的受服务器控制的可信脚本，如在用户提交表单之前对表单执行完整性检查的 Javascript。如果服务器提供的脚本处理用户提供的数据，然后再将这些数据注入回网页（如使用动态 HTML）中，则可能会发生基于 DOM 的 XSS 攻击。

下面的示例显示了一个在响应中返回了一个参数值的脚本。

该参数值通过使用 GET 请求发送给该脚本，然后在响应中嵌入在 HTML 中返回。

[REQUEST]

GET /index.aspx?name=JSmith HTTP/1.1

[RESPONSE]

HTTP/1.1 200 OK

Server: SomeServer

Date: Sun, 01 Jan 2002 00:31:19 GMT

Content-Type: text/html

Accept-Ranges: bytes

Content-Length: 27

<HTML>

Hello JSmith

</HTML>

攻击者可能利用类似这样的攻击：

[ATTACK REQUEST]

GET /index.aspx?name=>"'><script>alert('PWND')</script> HTTP/1.1

[ATTACK RESPONSE]

HTTP/1.1 200 OK

Server: SomeServer

Date: Sun, 01 Jan 2002 00:31:19 GMT

Content-Type: text/html

Accept-Ranges: bytes

Content-Length: 83

<HTML>

Hello >"'><script>alert('PWND')</script>

</HTML>

在这种情况下，JavaScript 代码将由浏览器执行（在此处 >"'> 部分不相关）。

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

[CERT Advisory CA-2000-02](http://www.cert.org/advisories/CA-2000-02.html)

[微软如何在 ASP.NET 中防止跨站点脚本编制](http://msdn2.microsoft.com/en-us/library/ms998274.aspx)

[微软如何在 ASP.NET 中防止注入攻击](http://msdn2.microsoft.com/en-us/library/Bb355989.aspx)

[微软如何在 ASP.NET 中使用正则表达式限制输入](http://msdn2.microsoft.com/en-us/library/ms998267.aspx)

JSON 中反映的未清理用户输入

JSON 中反映的未清理用户输入

未对用户输入正确执行危险字符清理

此问题可能影响不同类型的产品。

#### 受影响的 URL

* http://localhost:8080/news/getNewsList
* http://localhost:8080/venuelist/getVenueList

#### 问题 1/2（ http://localhost:8080/venuelist/getVenueList － page ）

#### 严重性： Informational

#### CVSS 计分： 手动计分

#### 图像



**所有变体**

#### 变体差异

• 已将参数“page”的值设置为“2%3Cscript%3Ealert%28218%29%3C%2Fscript%3E”

变体原因  
测试结果似乎指示存在脆弱性，因为“全局验证”功能发现在响应中嵌入了脚本，该脚本可能是由先前的测试注入的。

#### 变体验证

• Content-Type: **application/json**

• "message": "Failed to convert value of type 'java.lang.String' to required type 'int'; nested exception is java.lang.NumberFormatException: For input string: \"2**<script>alert(218)</script>**\"",

• ' to required type 'int'; nested exception is java.lang.NumberFormatException: For input string: \"2**<script>alert(218)</script>**\"\r\n\tat org.springframework.web.method.annotation.AbstractNamedValueMethodArgumentResolver.resolv

• ang.Thread.run(Thread.java:834)\r\nCaused by: java.lang.NumberFormatException: For input string: \"2**<script>alert(218)</script>**\"\r\n\tat java.base/java.lang.NumberFormatException.forInputString(NumberFormatException.java:65)\r

变体请求响应  
GET /venuelist/getVenueList?page=2%3Cscript%3Ealert%28218%29%3C%2Fscript%3E HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

Referer: http://localhost:8080/venue\_list

Cookie: JSESSIONID=F64E0EF18324CDFAFBEC6982DD0EA7EC

Connection: keep-alive

Host: localhost:8080

X-Requested-With: XMLHttpRequest

Accept: application/json, text/javascript, \*/\*; q=0.01

Accept-Language: en-US

HTTP/1.1 400

Transfer-Encoding: chunked

Connection: close

Date: Mon, 22 May 2023 08:34:13 GMT

Content-Type: application/json

{

"timestamp": "2023-05-22T08:34:14.354+0000",

"status": 400,

"error": "Bad Request",

"message": "Failed to convert value of type 'java.lang.String' to required type 'int'; nested exception is java.lang.NumberFormatException: For input string: \"2<script>alert(218)</script>\"",

"trace": "org.springframework.web.method.annotation.MethodArgumentTypeMismatchException: Failed to convert value of type 'java.lang.String' to required type 'int'; nested exception is java.lang.NumberFormatException: For input string: \"2<script>alert(218)</script>\"\r\n\tat org.springframework.web.method.annotation.AbstractNamedValueMethodArgumentResolver.resolveArgument(AbstractNamedValueMethodArgumentResolver.java:133)\r\n\tat org.springframework.web.method.support.HandlerMethodArgumentResolverComposite.resolveArgument(HandlerMethodArgumentResolverComposite.java:121)\r\n\tat org.springframework.web.method.support.InvocableHandlerMethod.getMethodArgumentValues(InvocableHandlerMethod.java:167)\r\n\tat org.springframework.web.method.support.InvocableHandlerMethod.invokeForRequest(InvocableHandlerMethod.java:134)\r\n\tat org.springframework.web.servlet.mvc.method.annotation.ServletInvocableHandlerMethod.invokeAndHandle(ServletInvocableHandlerMethod.java:106)\r\n\tat org.springframework.web.servlet.mvc.method.annotation.RequestMappingHandlerAdapter.invokeHandlerMethod(RequestMappingHandlerAdapter.java:888)\r\n\tat org.springframework.web.servlet.mvc.method.annotation.RequestMappingHandlerAdapter.handleInternal(RequestMappingHandlerAdapter.java:793)\r\n\tat org.springframework.web.servlet.mvc.method.AbstractHandlerMethodAdapter.handle(AbstractHandlerMethodAdapter.java:87)\r\n\tat org.springframework.web.servlet.DispatcherServlet.doDispatch(DispatcherServlet.java:1040)\r\n\tat org.springframework.web.servlet.DispatcherServlet.doService(DispatcherServlet.java:943)\r\n\tat org.springframework.web.servlet.FrameworkServlet.processRequest(FrameworkServlet.java:1006)\r\n\tat org.springframework.web.servlet.FrameworkServlet.doGet(FrameworkServlet.java:898)\r\n\tat javax.servlet.http.HttpServlet.service(HttpServlet.java:634)\r\n\tat org.springframework.web.servlet.FrameworkServlet.service(FrameworkServlet.java:883)\r\n\tat javax.servlet.http.HttpServlet.service(HttpServlet.java:741)\r\n\tat org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:231)\r\n\tat org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:166)\r\n\tat org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:53)\r\n\tat org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:193)\r\n\tat org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:166)\r\n\tat org.springframework.web.filter.RequestContextFilter.doFilterInternal(RequestContextFilter.java:100)\r\n\tat org.springframework.web.filter.OncePerRequestFilter.doFilter(OncePerRequestFilter.java:119)\r\n\tat org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:193)\r\n\tat org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:166)\r\n\tat org.springframework.web.filter.FormContentFilter.doFilterInternal(FormContentFilter.java:93)\r\n\tat org.springframework.web.filter.OncePerRequestFilter.doFilter(OncePerRequestFilter.java:119)\r\n\tat org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:193)\r\n\tat org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:166)\r\n\tat org.springframework.web.filter.CharacterEncodingFilter.doFilterInternal(CharacterEncodingFilter.java:201)\r\n\tat org.springframework.web.filter.OncePerRequestFilter.doFilter(OncePerRequestFilter.java:119)\r\n\tat org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:193)\r\n\tat org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:166)\r\n\tat org.apache.catalina.core.StandardWrapperValve.invoke(StandardWrapperValve.java:202)\r\n\tat org.apache.catalina.core.StandardContextValve.invoke(StandardContextValve.java:96)\r\n\tat org.apache.catalina.authenticator.AuthenticatorBase.invoke(AuthenticatorBase.java:526)\r\n\tat org.apache.catalina.core.StandardHostValve.invoke(StandardHostValve.java:139)\r\n\tat org.apache.catalina.valves.ErrorReportValve.invoke...

#### 问题 2/2（ http://localhost:8080/news/getNewsList － page ）

#### 严重性： Informational

#### CVSS 计分： 手动计分

#### 图像



**所有变体**

#### 变体差异

• 已将参数“page”的值设置为“1%3Cscript%3Ealert%28374%29%3C%2Fscript%3E”

变体原因  
测试结果似乎指示存在脆弱性，因为“全局验证”功能发现在响应中嵌入了脚本，该脚本可能是由先前的测试注入的。

#### 变体验证

• Content-Type: **application/json**

• "message": "Failed to convert value of type 'java.lang.String' to required type 'int'; nested exception is java.lang.NumberFormatException: For input string: \"1**<script>alert(374)</script>**\"",

• ' to required type 'int'; nested exception is java.lang.NumberFormatException: For input string: \"1**<script>alert(374)</script>**\"\r\n\tat org.springframework.web.method.annotation.AbstractNamedValueMethodArgumentResolver.resolv

• ang.Thread.run(Thread.java:834)\r\nCaused by: java.lang.NumberFormatException: For input string: \"1**<script>alert(374)</script>**\"\r\n\tat java.base/java.lang.NumberFormatException.forInputString(NumberFormatException.java:65)\r

变体请求响应  
GET /news/getNewsList?page=1%3Cscript%3Ealert%28374%29%3C%2Fscript%3E HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

Referer: http://localhost:8080/news\_list

Cookie: JSESSIONID=F64E0EF18324CDFAFBEC6982DD0EA7EC

Connection: keep-alive

Host: localhost:8080

X-Requested-With: XMLHttpRequest

Accept: application/json, text/javascript, \*/\*; q=0.01

Accept-Language: en-US

HTTP/1.1 400

Transfer-Encoding: chunked

Connection: close

Date: Mon, 22 May 2023 08:34:20 GMT

Content-Type: application/json

{

"timestamp": "2023-05-22T08:34:21.383+0000",

"status": 400,

"error": "Bad Request",

"message": "Failed to convert value of type 'java.lang.String' to required type 'int'; nested exception is java.lang.NumberFormatException: For input string: \"1<script>alert(374)</script>\"",

"trace": "org.springframework.web.method.annotation.MethodArgumentTypeMismatchException: Failed to convert value of type 'java.lang.String' to required type 'int'; nested exception is java.lang.NumberFormatException: For input string: \"1<script>alert(374)</script>\"\r\n\tat org.springframework.web.method.annotation.AbstractNamedValueMethodArgumentResolver.resolveArgument(AbstractNamedValueMethodArgumentResolver.java:133)\r\n\tat org.springframework.web.method.support.HandlerMethodArgumentResolverComposite.resolveArgument(HandlerMethodArgumentResolverComposite.java:121)\r\n\tat org.springframework.web.method.support.InvocableHandlerMethod.getMethodArgumentValues(InvocableHandlerMethod.java:167)\r\n\tat org.springframework.web.method.support.InvocableHandlerMethod.invokeForRequest(InvocableHandlerMethod.java:134)\r\n\tat org.springframework.web.servlet.mvc.method.annotation.ServletInvocableHandlerMethod.invokeAndHandle(ServletInvocableHandlerMethod.java:106)\r\n\tat org.springframework.web.servlet.mvc.method.annotation.RequestMappingHandlerAdapter.invokeHandlerMethod(RequestMappingHandlerAdapter.java:888)\r\n\tat org.springframework.web.servlet.mvc.method.annotation.RequestMappingHandlerAdapter.handleInternal(RequestMappingHandlerAdapter.java:793)\r\n\tat org.springframework.web.servlet.mvc.method.AbstractHandlerMethodAdapter.handle(AbstractHandlerMethodAdapter.java:87)\r\n\tat org.springframework.web.servlet.DispatcherServlet.doDispatch(DispatcherServlet.java:1040)\r\n\tat org.springframework.web.servlet.DispatcherServlet.doService(DispatcherServlet.java:943)\r\n\tat org.springframework.web.servlet.FrameworkServlet.processRequest(FrameworkServlet.java:1006)\r\n\tat org.springframework.web.servlet.FrameworkServlet.doGet(FrameworkServlet.java:898)\r\n\tat javax.servlet.http.HttpServlet.service(HttpServlet.java:634)\r\n\tat org.springframework.web.servlet.FrameworkServlet.service(FrameworkServlet.java:883)\r\n\tat javax.servlet.http.HttpServlet.service(HttpServlet.java:741)\r\n\tat org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:231)\r\n\tat org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:166)\r\n\tat org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:53)\r\n\tat org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:193)\r\n\tat org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:166)\r\n\tat org.springframework.web.filter.RequestContextFilter.doFilterInternal(RequestContextFilter.java:100)\r\n\tat org.springframework.web.filter.OncePerRequestFilter.doFilter(OncePerRequestFilter.java:119)\r\n\tat org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:193)\r\n\tat org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:166)\r\n\tat org.springframework.web.filter.FormContentFilter.doFilterInternal(FormContentFilter.java:93)\r\n\tat org.springframework.web.filter.OncePerRequestFilter.doFilter(OncePerRequestFilter.java:119)\r\n\tat org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:193)\r\n\tat org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:166)\r\n\tat org.springframework.web.filter.CharacterEncodingFilter.doFilterInternal(CharacterEncodingFilter.java:201)\r\n\tat org.springframework.web.filter.OncePerRequestFilter.doFilter(OncePerRequestFilter.java:119)\r\n\tat org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:193)\r\n\tat org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:166)\r\n\tat org.apache.catalina.core.StandardWrapperValve.invoke(StandardWrapperValve.java:202)\r\n\tat org.apache.catalina.core.StandardContextValve.invoke(StandardContextValve.java:96)\r\n\tat org.apache.catalina.authenticator.AuthenticatorBase.invoke(AuthenticatorBase.java:526)\r\n\tat org.apache.catalina.core.StandardHostValve.invoke(StandardHostValve.java:139)\r\n\tat org.apache.catalina.valves.ErrorReportValve.invoke(ErrorR...

|  |  |
| --- | --- |
|  | 发现电子邮件地址模式 (3/4) |

#### 咨询和修订建议

[信息泄露](http://projects.webappsec.org/Information-Leakage)

Spambot 搜寻因特网站点，开始查找电子邮件地址来构建发送自发电子邮件（垃圾邮件）的邮件列表。

AppScan 检测到含有一或多个电子邮件地址的响应，可供利用以发送垃圾邮件。

而且，找到的电子邮件地址也可能是专用电子邮件地址，对于一般大众应是不可访问的。

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

[Spambot 的定义（维基百科）](http://en.wikipedia.org/wiki/Spambot)

发现电子邮件地址模式

发现电子邮件地址模式

Web 应用程序编程或配置不安全

该问题可能会影响各种类型的产品。

#### 受影响的 URL

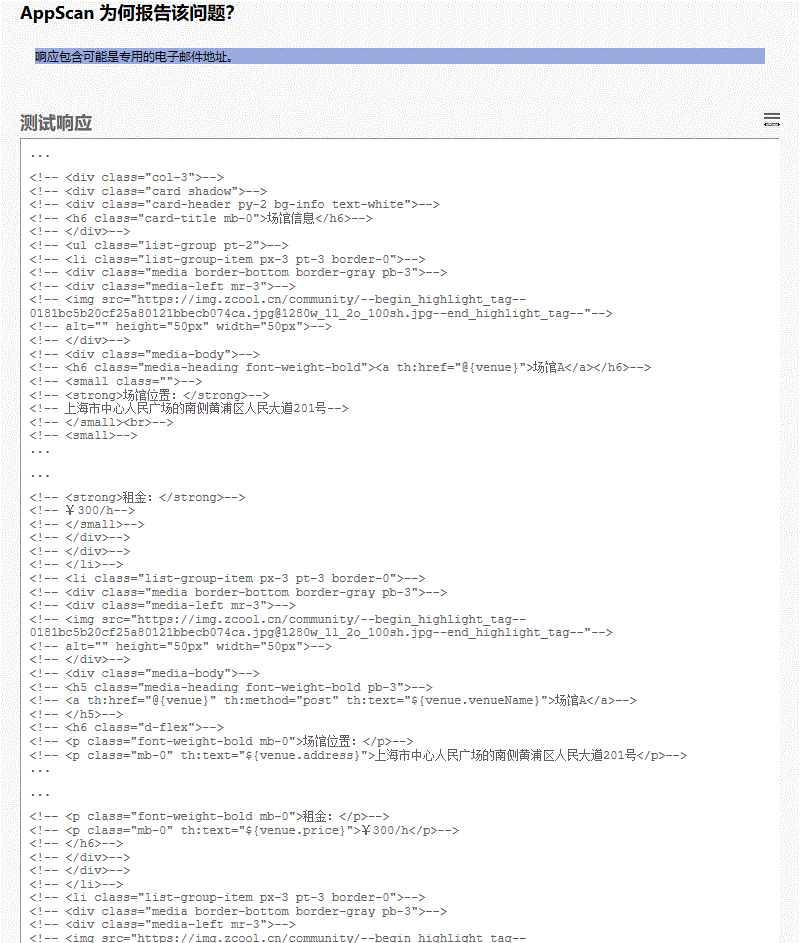
* http://localhost:8080/venue

#### 问题 1/1（ http://localhost:8080/venue － venue ）

#### 严重性： Informational

#### CVSS 计分： 手动计分

#### 图像



**所有变体**

#### 变体差异

变体原因  
响应包含可能是专用的电子邮件地址。

#### 变体验证

• ="media-left mr-3">-->

<!-- <img src="https://img.zcool.cn/community/**0181bc5b20cf25a80121bbecb074ca.jpg@1280w\_1l\_2o\_100sh.jpg**"-->

<!-- alt="" height="50px" width="50px">-->

<!--

• ="media-left mr-3">-->

<!-- <img src="https://img.zcool.cn/community/**0181bc5b20cf25a80121bbecb074ca.jpg@1280w\_1l\_2o\_100sh.jpg**"-->

<!-- alt="" height="50px" width="50px">-->

<!--

• ="media-left mr-3">-->

<!-- <img src="https://img.zcool.cn/community/**0181bc5b20cf25a80121bbecb074ca.jpg@1280w\_1l\_2o\_100sh.jpg**"-->

<!-- alt="" height="50px" width="50px">-->

<!--

变体请求响应  
GET /venue?venueID=2 HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

Referer: http://localhost:8080/index

Cookie: JSESSIONID=F64E0EF18324CDFAFBEC6982DD0EA7EC

Connection: keep-alive

Host: localhost:8080

Upgrade-Insecure-Requests: 1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8

Accept-Language: en-US

HTTP/1.1 200

Transfer-Encoding: chunked

Connection: keep-alive

Keep-Alive: timeout=60

Content-Language: en-US

Date: Mon, 22 May 2023 08:34:10 GMT

Content-Type: text/html;charset=UTF-8

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<title>场馆信息\_场馆1</title>

<meta name="viewport" content="width=device-width, initial-scale=1">

<link rel="stylesheet" href="/css/bootstrap.css">

<script src="/js/jquery-3.4.1.min.js"></script>

<script src="/js/bootstrap.bundle.min.js"></script>

<style type="text/css">

body{

background-color: #f5f5f5;

padding-top: 80px;

}

html {

overflow-y: scroll;

}

:root {

overflow-y: auto;

overflow-x: hidden;

}

:root body {

position: absolute;

}

body {

width: 100vw;

overflow: hidden;

}

</style>

</head>

<body>

<div>

<nav class="navbar navbar-expand-sm navbar-dark fixed-top bg-dark shadow" role="navigation">

<div class="navbar-header">

<a class="navbar-brand" href="index" style="font-weight: bold">Meet Here</a>

</div>

<button class="navbar-toggler" data-toggle="collapse" data-target="#navbar">

<span class="navbar-toggler-icon"></span>

</button>

<div class="collapse navbar-collapse" id="navbar">

<ul class="navbar-nav mr-auto">

<li class="nav-item">

<a class="nav-link" href="index">首页</a>

</li>

<li class="nav-item active">

<a class="nav-link" href="venue\_list">场馆信息</a>

</li>

<li class="nav-item dropdown">

<a class="nav-link dropdown-toggle" href="#" id="dropdown" data-toggle="dropdown">预约管理</a>

<div class="dropdown-menu">

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_place(false)">场馆预约</a>

<a class="dropdown-item loginfirst" href="#" onclick="javascript:order\_manage(false)">订单管理</a>

</div>

</li>

<li class="nav-item">

<a class="nav-link" href="news\_list">新闻</a>

</li>

<li class="nav-item">

<a class="nav-link loginfirst" href="#" onclick="javascript:message\_list(false)">留言板</a>

</li>

</ul>

<div>

<ul class="navbar-nav ml-auto">

<li class="nav-item">

<a class="nav-link" href="login"><span class="glyphicon glyphicon-log-in"></span> 登录</a>

</li>

<li class="nav-item">

<a class="nav-link" href="signup"><span class="glyphicon glyphicon-user"></span> 注册</a>

</li>

</ul>

</div>

</div>

</nav>

<script type="text/javascript">

$('.dropdown-toggle').dropdown();

function message\_list(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/message\_list';

}

}

function order\_manage(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.location.href = '/order\_manage';

}

}

function order\_place(flag){

if(!flag){

alert("请登录！");

window.location.href = '/login';

}

else{

window.open('/order\_place');

// window.location.href = '/order\_place';

}

}

</script>

</div>

<main role="main" class="container-fluid">

<div class="row">

<div class="col-8 mx-auto">

<div class="mb-3 p-4 bg-white rounded shadow-sm">

<div class="media border-bottom border-gray pb-3">

<div class="media-body">

<h4 class="media-heading font-weight-bold pb-3">场馆1</h4>

<h6 class="d-flex">

<p class="font-weight-bold mb-0">场馆位置：</p>

<p class="mb-0">上海市普陀区中山北路3664号</p>

</h6>

<h6 class="d-flex">

<p class="font-weight-bold...

|  |  |
| --- | --- |
|  | 应用程序错误 (4/4) |

#### 咨询和修订建议

[信息泄露](http://projects.webappsec.org/Information-Leakage)

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（如以下示例所示），那么应用程序可能会进入易受攻击的未定义状态。 攻击者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。

例如，如果参数字段是单引号括起来的字符串（如在 ASP 脚本或 SQL 查询中），那么注入的单引号将会提前终止字符串流，从而更改脚本的正常流程/语法。

错误消息中泄露重要信息的另一个原因，是脚本编制引擎、Web 服务器或数据库配置错误。

以下是一些不同的变体：

[1] 除去参数

[2] 除去参数值

[3] 将参数值设置为空值

[4] 将参数值设置为数字溢出（+/- 99999999）

[5] 将参数值设置为危险字符，如 ' " \' \" ) ;

[6] 将某字符串附加到数字参数值

[7] 在参数名称后追加“.”（点）或“[]”（尖括号）

可能会收集敏感的调试信息

[使用单引号入侵站点的示例，可参阅“How I hacked PacketStorm (by Rain Forest Puppy), RFP's site”](http://archives.neohapsis.com/archives/win2ksecadvice/2000-q1/0085.html)

[“Web Application Disassembly with ODBC Error Messages”（作者：David Litchfield）](http://www.cgisecurity.com/lib/webappdis.doc)

[CERT 咨询（CA-1997-25）：清理 CGI 脚本中用户提供的数据](http://www.cert.org/advisories/CA-1997-25.html)

应用程序错误

应用程序错误

未对入局参数值执行适当的边界检查

该问题可能会影响各种类型的产品。

#### 受影响的 URL

* http://localhost:8080/news
* http://localhost:8080/register.do
* http://localhost:8080/venue

#### 问题 1/3（ http://localhost:8080/venue － venueID ）

#### 严重性： Informational

#### CVSS 计分： 手动计分

#### 图像



**所有变体**

#### 变体差异

• 已除去参数“venueID”

变体原因  
应用程序以错误消息响应，表示可能会泄露敏感信息的未定义状态。

#### 变体验证

• HTTP/1.1 **500**

变体请求响应  
GET /venue? HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

Referer: http://localhost:8080/index

Cookie: JSESSIONID=F64E0EF18324CDFAFBEC6982DD0EA7EC

Connection: keep-alive

Host: localhost:8080

Upgrade-Insecure-Requests: 1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8

Accept-Language: en-US

HTTP/1.1 500

Connection: close

Content-Length: 5688

Content-Language: en-US

Date: Mon, 22 May 2023 08:34:19 GMT

Content-Type: text/html;charset=UTF-8

<html><body><h1>Whitelabel Error Page</h1><p>This application has no explicit mapping for /error, so you are seeing this as a fallback.</p><div id='created'>Mon May 22 16:34:20 CST 2023</div><div>There was an unexpected error (type=Internal Server Error, status=500).</div><div>Optional int parameter &#39;venueID&#39; is present but cannot be translated into a null value due to being declared as a primitive type. Consider declaring it as object wrapper for the corresponding primitive type.</div><div style='white-space:pre-wrap;'>java.lang.IllegalStateException: Optional int parameter &#39;venueID&#39; is present but cannot be translated into a null value due to being declared as a primitive type. Consider declaring it as object wrapper for the corresponding primitive type.

at org.springframework.web.method.annotation.AbstractNamedValueMethodArgumentResolver.handleNullValue(AbstractNamedValueMethodArgumentResolver.java:245)

at org.springframework.web.method.annotation.AbstractNamedValueMethodArgumentResolver.resolveArgument(AbstractNamedValueMethodArgumentResolver.java:116)

at org.springframework.web.method.support.HandlerMethodArgumentResolverComposite.resolveArgument(HandlerMethodArgumentResolverComposite.java:121)

at org.springframework.web.method.support.InvocableHandlerMethod.getMethodArgumentValues(InvocableHandlerMethod.java:167)

at org.springframework.web.method.support.InvocableHandlerMethod.invokeForRequest(InvocableHandlerMethod.java:134)

at org.springframework.web.servlet.mvc.method.annotation.ServletInvocableHandlerMethod.invokeAndHandle(ServletInvocableHandlerMethod.java:106)

at org.springframework.web.servlet.mvc.method.annotation.RequestMappingHandlerAdapter.invokeHandlerMethod(RequestMappingHandlerAdapter.java:888)

at org.springframework.web.servlet.mvc.method.annotation.RequestMappingHandlerAdapter.handleInternal(RequestMappingHandlerAdapter.java:793)

at org.springframework.web.servlet.mvc.method.AbstractHandlerMethodAdapter.handle(AbstractHandlerMethodAdapter.java:87)

at org.springframework.web.servlet.DispatcherServlet.doDispatch(DispatcherServlet.java:1040)

at org.springframework.web.servlet.DispatcherServlet.doService(DispatcherServlet.java:943)

at org.springframework.web.servlet.FrameworkServlet.processRequest(FrameworkServlet.java:1006)

at org.springframework.web.servlet.FrameworkServlet.doGet(FrameworkServlet.java:898)

at javax.servlet.http.HttpServlet.service(HttpServlet.java:634)

at org.springframework.web.servlet.FrameworkServlet.service(FrameworkServlet.java:883)

at javax.servlet.http.HttpServlet.service(HttpServlet.java:741)

at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:231)

at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:166)

at org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:53)

at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:193)

at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:166)

at org.springframework.web.filter.RequestContextFilter.doFilterInternal(RequestContextFilter.java:100)

at org.springframework.web.filter.OncePerRequestFilter.doFilter(OncePerRequestFilter.java:119)

at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:193)

at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:166)

at org.springframework.web.filter.FormContentFilter.doFilterInternal(FormContentFilter.java:93)

at org.springframework.web.filter.OncePerRequestFilter.doFilter(OncePerRequestFilter.java:119)

at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:193)

at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:166)

at org.springframework.web.filter.CharacterEncodingFilter.doFilterInternal(CharacterEncodingFilter.java:201)

at org.springframework.web.filter.OncePerRequestFilter.doFilter(OncePerRequestFilter.java:119)

at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:193)

at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:166)

at org.apache.catalina.core.StandardWrapperValve.invoke(StandardWrapperValve.java:202)

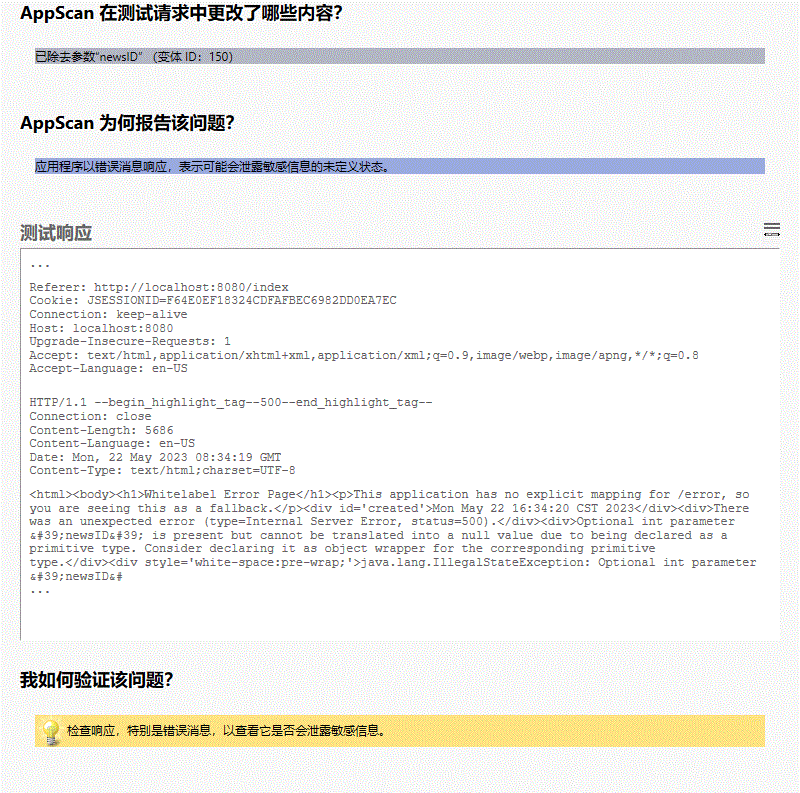
at org.apache.catalina.core.StandardContextValve.invok...

#### 问题 2/3（ http://localhost:8080/news － newsID ）

#### 严重性： Informational

#### CVSS 计分： 手动计分

#### 图像



**所有变体**

#### 变体差异

• 已除去参数“newsID”

变体原因  
应用程序以错误消息响应，表示可能会泄露敏感信息的未定义状态。

#### 变体验证

• HTTP/1.1 **500**

变体请求响应  
GET /news? HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

Referer: http://localhost:8080/index

Cookie: JSESSIONID=F64E0EF18324CDFAFBEC6982DD0EA7EC

Connection: keep-alive

Host: localhost:8080

Upgrade-Insecure-Requests: 1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8

Accept-Language: en-US

HTTP/1.1 500

Connection: close

Content-Length: 5686

Content-Language: en-US

Date: Mon, 22 May 2023 08:34:19 GMT

Content-Type: text/html;charset=UTF-8

<html><body><h1>Whitelabel Error Page</h1><p>This application has no explicit mapping for /error, so you are seeing this as a fallback.</p><div id='created'>Mon May 22 16:34:20 CST 2023</div><div>There was an unexpected error (type=Internal Server Error, status=500).</div><div>Optional int parameter &#39;newsID&#39; is present but cannot be translated into a null value due to being declared as a primitive type. Consider declaring it as object wrapper for the corresponding primitive type.</div><div style='white-space:pre-wrap;'>java.lang.IllegalStateException: Optional int parameter &#39;newsID&#39; is present but cannot be translated into a null value due to being declared as a primitive type. Consider declaring it as object wrapper for the corresponding primitive type.

at org.springframework.web.method.annotation.AbstractNamedValueMethodArgumentResolver.handleNullValue(AbstractNamedValueMethodArgumentResolver.java:245)

at org.springframework.web.method.annotation.AbstractNamedValueMethodArgumentResolver.resolveArgument(AbstractNamedValueMethodArgumentResolver.java:116)

at org.springframework.web.method.support.HandlerMethodArgumentResolverComposite.resolveArgument(HandlerMethodArgumentResolverComposite.java:121)

at org.springframework.web.method.support.InvocableHandlerMethod.getMethodArgumentValues(InvocableHandlerMethod.java:167)

at org.springframework.web.method.support.InvocableHandlerMethod.invokeForRequest(InvocableHandlerMethod.java:134)

at org.springframework.web.servlet.mvc.method.annotation.ServletInvocableHandlerMethod.invokeAndHandle(ServletInvocableHandlerMethod.java:106)

at org.springframework.web.servlet.mvc.method.annotation.RequestMappingHandlerAdapter.invokeHandlerMethod(RequestMappingHandlerAdapter.java:888)

at org.springframework.web.servlet.mvc.method.annotation.RequestMappingHandlerAdapter.handleInternal(RequestMappingHandlerAdapter.java:793)

at org.springframework.web.servlet.mvc.method.AbstractHandlerMethodAdapter.handle(AbstractHandlerMethodAdapter.java:87)

at org.springframework.web.servlet.DispatcherServlet.doDispatch(DispatcherServlet.java:1040)

at org.springframework.web.servlet.DispatcherServlet.doService(DispatcherServlet.java:943)

at org.springframework.web.servlet.FrameworkServlet.processRequest(FrameworkServlet.java:1006)

at org.springframework.web.servlet.FrameworkServlet.doGet(FrameworkServlet.java:898)

at javax.servlet.http.HttpServlet.service(HttpServlet.java:634)

at org.springframework.web.servlet.FrameworkServlet.service(FrameworkServlet.java:883)

at javax.servlet.http.HttpServlet.service(HttpServlet.java:741)

at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:231)

at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:166)

at org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:53)

at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:193)

at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:166)

at org.springframework.web.filter.RequestContextFilter.doFilterInternal(RequestContextFilter.java:100)

at org.springframework.web.filter.OncePerRequestFilter.doFilter(OncePerRequestFilter.java:119)

at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:193)

at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:166)

at org.springframework.web.filter.FormContentFilter.doFilterInternal(FormContentFilter.java:93)

at org.springframework.web.filter.OncePerRequestFilter.doFilter(OncePerRequestFilter.java:119)

at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:193)

at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:166)

at org.springframework.web.filter.CharacterEncodingFilter.doFilterInternal(CharacterEncodingFilter.java:201)

at org.springframework.web.filter.OncePerRequestFilter.doFilter(OncePerRequestFilter.java:119)

at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:193)

at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:166)

at org.apache.catalina.core.StandardWrapperValve.invoke(StandardWrapperValve.java:202)

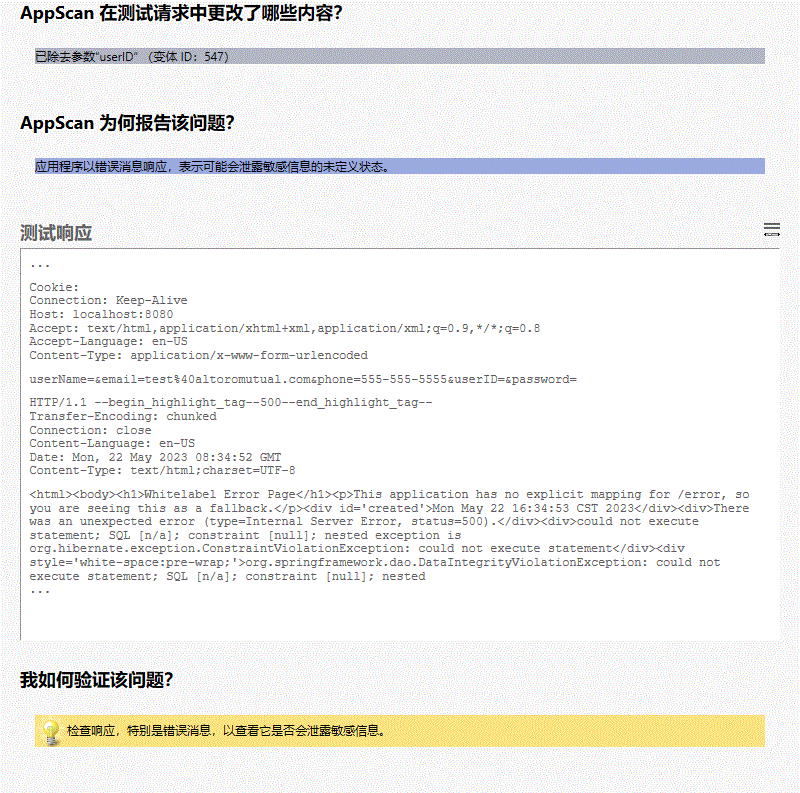
at org.apache.catalina.core.StandardContextValve.invoke(S...

#### 问题 3/3（ http://localhost:8080/register.do － userID ）

#### 严重性： Informational

#### CVSS 计分： 手动计分

#### 图像



**所有变体**

#### 变体差异

• 已除去参数“userID”

变体原因  
应用程序以错误消息响应，表示可能会泄露敏感信息的未定义状态。

#### 变体验证

• HTTP/1.1 **500**

变体请求响应  
POST /register.do HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

Referer: http://localhost:8080/signup

Cookie:

Connection: Keep-Alive

Host: localhost:8080

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Language: en-US

Content-Type: application/x-www-form-urlencoded

userName=&email=test%40altoromutual.com&phone=555-555-5555&userID=&password=

HTTP/1.1 500

Transfer-Encoding: chunked

Connection: close

Content-Language: en-US

Date: Mon, 22 May 2023 08:34:52 GMT

Content-Type: text/html;charset=UTF-8

<html><body><h1>Whitelabel Error Page</h1><p>This application has no explicit mapping for /error, so you are seeing this as a fallback.</p><div id='created'>Mon May 22 16:34:53 CST 2023</div><div>There was an unexpected error (type=Internal Server Error, status=500).</div><div>could not execute statement; SQL [n/a]; constraint [null]; nested exception is org.hibernate.exception.ConstraintViolationException: could not execute statement</div><div style='white-space:pre-wrap;'>org.springframework.dao.DataIntegrityViolationException: could not execute statement; SQL [n/a]; constraint [null]; nested exception is org.hibernate.exception.ConstraintViolationException: could not execute statement

at org.springframework.orm.jpa.vendor.HibernateJpaDialect.convertHibernateAccessException(HibernateJpaDialect.java:298)

at org.springframework.orm.jpa.vendor.HibernateJpaDialect.translateExceptionIfPossible(HibernateJpaDialect.java:255)

at org.springframework.orm.jpa.AbstractEntityManagerFactoryBean.translateExceptionIfPossible(AbstractEntityManagerFactoryBean.java:528)

at org.springframework.dao.support.ChainedPersistenceExceptionTranslator.translateExceptionIfPossible(ChainedPersistenceExceptionTranslator.java:61)

at org.springframework.dao.support.DataAccessUtils.translateIfNecessary(DataAccessUtils.java:242)

at org.springframework.dao.support.PersistenceExceptionTranslationInterceptor.invoke(PersistenceExceptionTranslationInterceptor.java:153)

at org.springframework.aop.framework.ReflectiveMethodInvocation.proceed(ReflectiveMethodInvocation.java:186)

at org.springframework.data.jpa.repository.support.CrudMethodMetadataPostProcessor$CrudMethodMetadataPopulatingMethodInterceptor.invoke(CrudMethodMetadataPostProcessor.java:178)

at org.springframework.aop.framework.ReflectiveMethodInvocation.proceed(ReflectiveMethodInvocation.java:186)

at org.springframework.aop.interceptor.ExposeInvocationInterceptor.invoke(ExposeInvocationInterceptor.java:93)

at org.springframework.aop.framework.ReflectiveMethodInvocation.proceed(ReflectiveMethodInvocation.java:186)

at org.springframework.aop.framework.JdkDynamicAopProxy.invoke(JdkDynamicAopProxy.java:212)

at com.sun.proxy.$Proxy106.save(Unknown Source)

at com.meethere.service.impl.UserServiceImpl.create(UserServiceImpl.java:38)

at com.meethere.controller.user.UserController.register(UserController.java:65)

at jdk.internal.reflect.GeneratedMethodAccessor158.invoke(Unknown Source)

at java.base/jdk.internal.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)

at java.base/java.lang.reflect.Method.invoke(Method.java:566)

at org.springframework.web.method.support.InvocableHandlerMethod.doInvoke(InvocableHandlerMethod.java:190)

at org.springframework.web.method.support.InvocableHandlerMethod.invokeForRequest(InvocableHandlerMethod.java:138)

at org.springframework.web.servlet.mvc.method.annotation.ServletInvocableHandlerMethod.invokeAndHandle(ServletInvocableHandlerMethod.java:106)

at org.springframework.web.servlet.mvc.method.annotation.RequestMappingHandlerAdapter.invokeHandlerMethod(RequestMappingHandlerAdapter.java:888)

at org.springframework.web.servlet.mvc.method.annotation.RequestMappingHandlerAdapter.handleInternal(RequestMappingHandlerAdapter.java:793)

at org.springframework.web.servlet.mvc.method.AbstractHandlerMethodAdapter.handle(AbstractHandlerMethodAdapter.java:87)

at org.springframework.web.servlet.DispatcherServlet.doDispatch(DispatcherServlet.java:1040)

at org.springframework.web.servlet.DispatcherServlet.doService(DispatcherServlet.java:943)

at org.springframework.web.servlet.FrameworkServlet.processRequest(FrameworkServlet.java:1006)

at org.springframework.web.servlet.FrameworkServlet.doPost(FrameworkServlet.java:909)

at javax.servlet.http.HttpServlet.service(HttpServlet.java:660)

at org.springframework.web.servlet.FrameworkServlet.service(FrameworkServlet.java:883)

at javax.servlet.http.HttpServlet.service(HttpServlet.java:741)

at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:231)

at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:166)

at org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:53)

at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:193)

...

## 测试策略

名称： Default

描述： 该策略包含所有测试，但侵入式和端口侦听器测试除外。

测试（ 154 ）：

| 名称 | 严重性 |
| --- | --- |
| 应用程序调试方式实施 | Low |
| 电子邮件参数电子欺骗 | Informational |
| 文件上载 | High |
| File Upload With XXE | High |
| 电子盗窃 | Low |
| 检测到 HTTP 请求转发（Web 代理） | Informational |
| 启用了 TRACE 和 TRACK HTTP 方法 | Low |
| 发现 IBM WebSphere 样本站点 | High |
| Oracle Application Server SOAP 管理 | High |
| 远程 RSS 订阅源包含 | Informational |
| 非 SOAP Web Service 访问 | Low |
| 易受攻击的 ActiveX 控件的用途 | Medium |
| 不安全的第三方链接 (target="\_blank") | Low |
| 反映的不安全链接 (target="\_blank") | Medium |
| 已存储的 target='\_blank' 链接 | Medium |
| 不充分帐户封锁 | Medium |
| 可预测的登录凭证 | High |
| IIS localstart.asp 可能的蛮力 | High |
| 登录错误消息凭证枚举 | Medium |
| Microsoft IIS Phone Book Service 缓冲区溢出 | High |
| 启用了不安全的“OPTIONS”HTTP 方法 | Low |
| 链接注入（便于跨站请求伪造） | Medium |
| WebDAV MKCOL 方法站点篡改 | Medium |
| 通过框架钓鱼 | Medium |
| phpPgAdmin redirect.php URL 重定向 | Medium |
| 使用 MD5 作为 SSL 证书签名算法 | Medium |
| 通过管理员控制台进行的 WebSphere 多重链接注入 | Medium |
| 通过管理员控制台进行的 WebSphere 多重网络钓鱼 | Medium |
| WordPress 4.7.0 和 4.7.1 内容注入 | Medium |
| Apache Tomcat 弱缺省管理帐户凭证 | High |
| 跨站点请求伪造 | Medium |
| Silverlight 允许从域进行访问 | Medium |
| AChecker index.php 跨站点脚本编制 | High |
| AContent 多重跨站点脚本编制 | High |
| AMFPHP details.php 跨站点脚本编制 | High |
| 跨站点脚本编制 | High |
| HTTP Referer 头跨站点脚本编制 | High |
| User-Agent Header 跨站点脚本编制 | High |
| AutoIndex index.php 跨站点脚本编制 | High |
| bbsmax post.aspx 跨站点脚本编制 | High |
| Blue Coat ICAP Patience Page 跨站点脚本编制 | High |
| BMForum 多重跨站点脚本编制 | High |
| Campsite index.php 跨站点脚本编制 | High |
| Caucho Resin resin-admin 跨站点脚本编制 | High |
| ClipBucket 多重跨站点脚本编制 | High |
| Comptel Provisioning and Activation index.jsp 跨站点脚本编制 | High |
| Contenido front\_content.php 跨站点脚本编制 | High |
| cPanel autoinstall4imagesgalleryupgrade.php 跨站点脚本编制 | High |
| cPanel dofileop.html 跨站点脚本编制 | High |
| CubeCart index.php 跨站点脚本编制 | High |
| CuteNews index.php 跨站点脚本编制 | High |
| CuteNews 多重跨站点脚本编制 | High |
| Sun Cobalt RaQ 控制面板跨站点脚本编制 | High |
| Sun ONE Web Server 搜索跨站点脚本编制 | High |
| ”IBM WebSphere“..”跨站点脚本编制 | High |
| 路径中的 Datalife Engine 跨站点脚本编制 | High |
| DirectAdmin CMD\_DB\_VIEW 跨站点脚本编制 | High |
| DirectAdmin CMD\_DOMAIN 跨站点脚本编制 | High |
| DocMGR history.php 跨站点脚本编制 | High |
| Dojo 多重跨站点脚本编制 | High |
| Dojo Toolkit 多重跨站点脚本编制 | High |
| 基于 DOM 的跨站点脚本编制 | High |
| Edit-X CMS index.php 跨站点脚本编制 | High |
| eFront 多重跨站点脚本编制 | High |
| Elastix 多重跨站点脚本编制 | High |
| Elxis 多重跨站点脚本编制 | High |
| Etomite index.php 跨站点脚本编制 | High |
| FirePass 4100 SSL VPN 多重跨站点脚本编制 | High |
| FireStats 多重跨站点脚本编制 | High |
| Flash Tag Cloud control for ASP.NET 跨站点脚本编制 | High |
| FortiMail admin.fe 跨站点脚本编制 | High |
| FreeNAS index.php 跨站点脚本编制 | High |
| FuseTalk 多重跨站点脚本编制（版本 3.2） | High |
| Geeklog profiles.php 扩展点脚本编制 | High |
| GlassFish Administration Console 跨站点脚本编制 | High |
| 存储的跨站点脚本编制 | High |
| JSON 中反映的未清理用户输入 | Informational |
| GWExtranet 多重跨站点脚本编制 | High |
| Horde IMP fetchmailprefs.php 跨站点脚本编制 | High |
| Horde Webmail addevent.php 跨站点脚本编制 | High |
| H-Sphere actions.php 跨站点脚本编制 | High |
| H-Sphere login.php 跨站点脚本编制 | High |
| IBM Metrica 跨站点脚本编制 | High |
| IBM WebSphere Portal Server 和 Lotus Web Content Management 跨站点脚本编制 | High |
| Microsoft IIS idc 文件扩展名跨站点脚本编制 | High |
| ImpressCMS CSSTidy css\_optimiser.php 跨站点脚本编制 | High |
| iNet Orkut Clone profile\_social.php 跨站点脚本编制 | High |
| i-Web 套件 default.asp 跨站点脚本编制 | High |
| JavaBB member\_list.jbb 跨站点脚本编制 | High |
| JavaBB pm.externalSend.jbb 跨站点脚本编制 | High |
| JEUS url.jsp 跨站点脚本编制 | High |
| Juniper IVE 跨站点脚本编制 | High |
| Kayako eSupport index.php 跨站点脚本编制 | High |
| KnowledgeTree 多重跨站点脚本编制 | High |
| @mail Webmail Client index.php 跨站点脚本编制 | High |
| Mambo connector.php 跨站点脚本编制 | High |
| Mambo 多重跨站点脚本编制（版本 4.6 RC1） | High |
| MemHT Portal admin.php 跨站点脚本编制 | High |
| MKPortal handler\_image.php 跨站点脚本编制 | High |
| MODx index.php 跨站点脚本编制 (V2.0.2-pl) | High |
| Moodle phpcoverage.remote.top.inc.php 跨站点脚本编制 | High |
| Movable Type MT-Cumulus Plugin tagcloud.swf 跨站点脚本编制 | High |
| MyBB generic\_error.php 跨站点脚本编制 | High |
| MyBB managegroup.php 跨站点脚本编制 | High |
| MyBB moderation.php 跨站点脚本编制 | High |
| NextAge 购物车软件 index.php 跨站点脚本编制 | High |
| Nikira Fraud Management System“prompt”跨站点脚本编制 | High |
| Onyx 多重跨站点脚本编制 | High |
| Open Text ECM 多重跨站点脚本编制 | High |
| Oracle Application Server 10g login.jsp 跨站点脚本编制 | High |
| Oracle Application Server login.jsp 跨站点脚本编制 | High |
| Oracle Application Server welcomeuser.jsp 跨站点脚本编制 | High |
| Oracle Forms ifcgi60.exe 跨站点脚本编制 | High |
| Oracle Fusion Middleware 产品跨站点脚本编制 | High |
| Oracle Portal 10g 跨站点脚本编制 | High |
| Oracle Siebel Loyalty Management start.swe 跨站点脚本编制 | High |
| Orion Network Performance Monitor 多重跨站点脚本编制 | High |
| 路径中的 OSSIM 跨站点脚本编制 | High |
| pfSense 多重跨站点脚本编制 | High |
| Phorum admin.php 跨站点脚本编制（5.1.19 及其以下的版本） | High |
| Phorum 多重跨站点脚本编制 | High |
| Phorum posting.php 跨站点脚本编制 | High |
| PHP Album main.php 跨站点脚本编制 | High |
| phpFreeChat 多重跨站点脚本编制 | High |
| PHP iCalendar 多重跨站点脚本编制 | High |
| PHPShop register.html 跨站点脚本编制 | High |
| PhpWebGallery isadmin.inc.php 跨站点脚本编制 | High |
| Pimcore 跨站点脚本编制 | High |
| Pligg login.php 跨站点脚本编制 | High |
| Pligg 搜索跨站点脚本编制 | High |
| Pligg user.php 跨站点脚本编制 | High |
| Q-Shop search.asp 跨站点脚本编制 | High |
| 使用“恶意 RSS 订阅源包含”的“跨站点脚本编制” | High |
| SAP NetWeaver administration\_setup.jsp 跨站点脚本编制 | High |
| SAP NetWeaver container.jsp 跨站点脚本编制 | High |
| SAP 产品 Cfolders 引擎多重跨站点脚本编制 | High |
| Sawmill 多重跨站点脚本编制 | High |
| Serendipity Freetag 插件跨站点脚本编制 | High |
| SilverStripe form.php 跨站点脚本编制 | High |
| Simple PHP Blog comment\_add\_cgi.php 跨站点脚本编制 | High |
| sNews 跨站点脚本编制 | High |
| Snitz Forums 2000 pop\_send\_to\_friend.asp 跨站点脚本编制 | High |
| Sphider search.php 跨站点脚本编制 | High |
| SPIP spip.php 跨站点脚本编制 | High |
| Splunk segmentation\_performance 跨站点脚本编制 | High |
| 路径中的 Sparta Systems TrackWise TeamAccess 多重跨站点脚本编制 | High |
| 路径中的 Swiki 跨站点脚本编制 | High |
| Tiki Wiki CMS Groupware tiki-edit\_wiki\_section.php 跨站点脚本编制 | High |
| Tmax Soft JEUS url.jsp 跨站点脚本编制 | High |
| Todoyu test.php 跨站点脚本编制 | High |
| TWiki 多重跨站点脚本编制 | High |
| TYPO3 Cumulus Tagcloud 扩展 tagcloud.swf 跨站点脚本编制 | High |
| vBulletin 多重跨站点脚本编制（版本 4.0.2） | High |
| VirtueMart 多重跨站点脚本编制 | High |
| vtiger CRM index.php 跨站点脚本编制 (V5.2.1) | High |
| WeBid confirm.php 跨站点脚本编制 | High |
| 路径中的 WebSVN 跨站点脚本编制 | High |
| Wolf CMS Multiple 跨站点脚本编制 | High |
| WoltLab Burning Board dereferrer.php 跨站点脚本编制 | High |
| WordPress Cover WP Theme 跨站点脚本编制 | High |
| WordPress Daily Maui Photo Widget Plugin wp-dailymaui-widget-control.php 跨站点脚本编制 | High |
| WordPress（通过 Genericons 软件包）基于 DOM 的跨站点脚本编制 | High |
| WordPress FeedList Plugin handler\_image.php 跨站点脚本编制 | High |
| WordPress 多重 base64 重定向跨站点脚本编制 | High |
| WordPress MU wpmu-blogs.php 跨站点脚本编制 | High |
| WordPress Organizer Plugin admin.php 跨站点脚本编制 | High |
| WordPress Twitter Feed Plugin magpie\_debug.php 跨站点脚本编制 | High |
| WordPress Whois Search 插件 wp-whois-ajax.php 跨站点脚本编制 | High |
| WordPress WP Comment Remix 插件跨站点脚本编制 | High |
| DISTINCT | High |
| WordPress WP Photo Album Plugin wppa.php 跨站点脚本编制 | High |
| WordPress WP-StarsRateBox Plugin wp-starsratebox.php 跨站点脚本编制 | High |
| WordPress WP Survey And Quiz Tool Plugin create.php 跨站点脚本编制 | High |
| WordPress WP-UserOnline 插件跨站点脚本编制 | High |
| WordPress WP Featured Post with Thumbnail Plugin timthumb.php 跨站点脚本编制 | High |
| WordPress Pretty Link Lite Plugin pretty-bar.php 跨站点脚本编制 | High |
| 路径中的 Xerox DocuShare 多重跨站点脚本编制 | High |
| 通过远程文件包含进行跨站点脚本编制 | High |
| xt:Commerce advanced\_search\_result.php 跨站点脚本编制 | High |
| zenphoto admin.php 跨站点脚本编制 | High |
| zenphoto 多重跨站点脚本编制 | High |
| Zeus vs\_diag.cgi 跨站点脚本编制 | High |
| WordPress All In One WP Security Plugin aiowpsec.php 跨站点脚本编制 | High |
| WordPress Display Widgets Plugin admin-ajax.php 跨站点脚本编制 | High |
| WordPress Subscribe To Comments Reloaded Plugin options-general.php 跨站点脚本编制 | High |
| WordPress Kiwi Logo Carousel Plugin kiwi\_logo\_carousel\_admin.php 跨站点脚本编制 | High |
| WordPress WP Google Fonts Plugin google-fonts.php 跨站点脚本编制 | High |
| WordPress Google Language Translator Plugin google-language-translator.php跨站点脚本编制 | High |
| WordPress WP-Crontrol Plugin wp-crontrol.php 跨站点脚本编制 | High |
| WordPress Manual Image Crop Plugin manual-image-crop.php 跨站点脚本编制 | High |
| WordPress Easy Coming Soon Plugin desing\_page\_setting.php 跨站点脚本编制 | High |
| WordPress Sound Cloud Is Gold Plugin sound-cloud-gold-functions.php 跨站点脚本编制 | High |
| WordPress Broken Link Manager Plugin functions.php 跨站点脚本编制 | High |
| WordPress Email Encoder bundle Plugin email-encoder-bundle.php 跨站点脚本编制 | High |
| WordPress Olevmedia Shortcodes Plugin interface.php 跨站点脚本编制 | High |
| WordPress Simple Fields Plugin simple\_fields.php 跨站点脚本编制 | High |
| WordPress Crazy Bone Plugin 跨站点脚本编制 | High |
| SRI (Subresource Integrity) 的检查 | Low |
| IPSwitch Imail Imonitor 拒绝服务 | High |
| Allaire ColdFusion 源代码泄露和拒绝服务 | High |
| WordPress load-scripts.php 拒绝服务 | High |
| 使用 URL 编码的 Apache Tomcat 目录列表 | Medium |
| CVS 目录浏览 | Medium |
| 目录列表 | Medium |
| Microsoft IIS Bdir.htr 目录列表 | Medium |
| RCS 目录浏览 | Medium |
| Microsoft FrontPage 目录列表 | Medium |
| BEA WebLogic URL 欺骗目录列表 | Medium |
| MacOS X Finder Apache 目录内容泄露 | Medium |
| 发现目录列表模式 | Low |
| 服务器端 JavaScript 目录列表 | Medium |
| 格式字符串远程命令执行 | High |
| HTTP 响应分割 | Medium |
| 存储的响应分割 | Medium |
| Aardvark Topsites PHP 目录列表 | Low |
| AMFPHP Service Browser 公共访问 | Low |
| Apache access\_log 信息泄露 | Low |
| Apache error\_log 信息泄露 | Low |
| Apache Web 服务器信息披露（又名 OptionsBleed） | Low |
| Apache JServ 环境状态信息泄露 | Low |
| Apache Multiviews 攻击 | Low |
| Apache PHP 源代码泄露 | Low |
| Apache server-info 信息泄露 | Low |
| Apache server-status 信息泄露 | Low |
| Apache stronghold-info 信息泄露 | Low |
| Apache stronghold-status 信息泄露 | Low |
| Apache Tomcat 无效字符路径泄露 | Low |
| ASP.NET 定制错误路径泄露 | Low |
| 检测到 ASP.NET 项目转换报告 | Low |
| 检测到文件替代版本 | Low |
| 发现可高速缓存的登录页面 | Low |
| 发现可高速缓存的 SSL 页面 | Low |
| Cart32 信息泄露、特权升级和拒绝服务 | Low |
| ColdFusion 调试方式信息收集 | Low |
| Global.asa 文件敏感信息检索 | Low |
| 检测到隐藏目录 | Low |
| NT 和 IIS 数据流交替 | Low |
| Microsoft FrontPage 配置信息泄露 | Low |
| Microsoft FrontPage Server Extensions 重要信息泄露 | Low |
| 未实施加密 | Low |
| 不正确的 Lotus Domino 管理数据库访问 | Low |
| iScouter PHP Web Portal MySQL 密码检索 | Low |
| JavaScript 劫持 | Low |
| 客户端（JavaScript）Cookie 引用 | Informational |
| Lotus Domino Web 应用程序访问控制旁路 | Low |
| Lotus Domino 数据库信息收集 | Low |
| Microsoft IIS 4.0 未授权的数据库访问 | Low |
| Talentsoft WebPlus Server 源代码泄露和信息泄露 | Low |
| IBM Net.Data 内部变量显示 | Low |
| Oracle Application Server 脚本/perl 目录映射源代码泄露 | Low |
| 应用程序输入限制旁路 | Low |
| 应用程序逻辑 Subversion | Informational |
| 错误页面路径泄露 | Low |
| Robots.txt 文件 Web 站点结构暴露 | Low |
| HTML 注释敏感信息泄露 | Informational |
| .NET 解决方案文件下载 | Low |
| WS\_FTP.log 文件分析源代码泄露 | Low |
| 发现临时目录 | Low |
| 未授权的 Java Servlet 源代码访问 | Low |
| 应用程序错误 | Informational |
| Xitami Web 服务器信息泄露 | Low |
| PHP phpinfo.php 信息泄露 | Low |
| Bash Shell 历史记录文件检索 | Low |
| BEA WebLogic weblogic.xml 信息泄露 | Low |
| 查询中接受的主体参数 | Low |
| CMME 备份文件下载 | Low |
| Cobalt RaQ 信息泄露 | Low |
| 发现压缩目录 | Low |
| Concrete5 路径泄露 | Low |
| “Content-Security-Policy”头缺失或不安全 | Low |
| “X-Content-Type-Options”头缺失或不安全 | Low |
| 过度许可的 CORS 访问测试 | Low |
| Apache AXIS 样本 Servlet 信息泄露 | Low |
| 包含文件源代码泄露 | Low |
| Microsoft FrontPage Server Extensions 机器名泄露 | Low |
| Global.asa 和 Global.asax 备份副本检索 | Low |
| IIS Global.asa 和 Global.asax 检索 | Low |
| Web 服务器访问控制文件不正确的许可权设置 | Low |
| 含 .NET 的 Microsoft IIS 路径泄露 | Low |
| Microsoft ASP.NET“Application Trace”信息泄露 | Low |
| Microsoft IIS 样本应用程序物理路径泄露 | Low |
| Oracle Application Server 9i PORTAL\_DEMO.ORG\_CHART SQL 注入 | Low |
| Microsoft FrontPage“\_vti\_cnf”信息泄露 | Low |
| Web.config 文件配置设置泄露 | Low |
| BEA WebLogic Server 版本暴露 | Low |
| WS\_FTP.LOG 信息泄露 | Low |
| Zope Additems 脚本环境信息泄露 | Low |
| Zope Server 空上载信息泄露 | Low |
| DigiNotar 发放的 SSL 证书易受攻击 | Low |
| .NET CS 文件下载 | Low |
| 检测到 .NET output-build.txt 文件 | Low |
| .NET VB 文件下载 | Low |
| Drupal“keys”路径泄露 | Low |
| Microsoft FrontPage Server Extensions 编写日志信息泄露 | Low |
| 发现 Apache 缺省安装页面模式 | Informational |
| 自动填写未对密码字段禁用的 HTML 属性 | Low |
| 发现信用卡号模式（American Express） | Low |
| 在未加密连接中发现信用卡号模式 (American Express) | Low |
| 发现信用卡号模式（Diners Club） | Low |
| 在未加密连接中发现信用卡号模式 (Diners Club) | Low |
| 发现信用卡号模式（Discover） | Low |
| 在未加密连接中发现信用卡号模式 (Discover) | Low |
| 发现信用卡号模式（MasterCard） | Low |
| 在未加密连接中发现信用卡号模式 (MasterCard) | Low |
| 发现信用卡号模式 | Low |
| 在未加密连接中发现信用卡号模式 | Low |
| 发现信用卡号模式（Visa） | Low |
| 在未加密连接中发现信用卡号模式 (Visa) | Low |
| 发现电子邮件地址模式 | Informational |
| 发现 IIS 缺省安装页面模式 | Informational |
| 发现内部 IP 泄露模式 | Informational |
| 发现 iPlanet 缺省安装页面模式 | Informational |
| 发现可能的服务器路径泄露模式 | Informational |
| 发现敏感文件 | Informational |
| 发现 Web 应用程序源代码泄露模式 | Low |
| 发现社会保险号模式 | Low |
| 在未加密连接中发现社会保障号码模式 | Low |
| 检测到 Google 站点地图文件 | Low |
| HP Insight Management Agents 路径泄露 | Low |
| HTTP Strict-Transport-Security 头缺失或不安全 | Low |
| IBM WebSphere 配置信息泄露 | Low |
| IBM WebSphere 调试方式实施 | Low |
| 发现 IBM WebSphere 文档 | Low |
| IBM WebSphere 密码存储为明文 | Low |
| Webalizer 用途统计信息的泄露 | Low |
| JBoss 空字节 JSP 源代码泄露 | Low |
| Lotus Domino ?ReadEntries 信息泄露 | Low |
| Microsoft Active Server Pages 信息泄露 | Low |
| 启用了 Microsoft ASP.NET 调试 | Low |
| 发现 Microsoft FrontPage Server Extensions 任务列表 | Low |
| Microsoft IIS servervariables\_vbscript.asp 信息泄露 | Low |
| Microsoft IIS 缺少 Host 头信息泄露 | Low |
| MyBB 多重路径泄露 | Low |
| Netscape Server 配置信息泄露 | Low |
| 发现 Oracle 错误日志 | Low |
| Oracle 日志文件信息泄露 | Low |
| 在参数值中找到了内部 IP 公开模式 | Low |
| 在参数值中找到了社会安全号模式 | Low |
| 查询中的密码参数 | High |
| 各种基于 PHP 的应用程序中的路径泄露 | Low |
| PHPShop 路径泄露 | Low |
| 发现潜在订单信息 | Low |
| 发现潜在注册信息 | Low |
| Sun Java Application Server 路径泄露 | Low |
| TYPO3 Cumulus Tagcloud 扩展路径泄露 | Low |
| VBS 文件源泄露 | Low |
| ViArt 购物车路径泄露 | Low |
| 跨帧脚本编制防御缺失或不安全 | Low |
| “X-XSS-Protection”头缺失或不安全 | Low |
| Zen Cart curltest.php 本地文件包含 | Low |
| Spring Boot Actuator 端点已公开 | Low |
| 不安全索引 | Medium |
| Lotus Domino Web 服务器文件检索 | High |
| Netscape Administration Server 密码检索 | High |
| HTTP PUT 方法站点篡改 | High |
| 使用 HTTP 动词篡改的认证旁路 | Medium |
| 使用 SQL 注入的认证旁路 | High |
| Netscape Enterprise Server/Sun ONE 未授权的管理特权和拒绝服务 | High |
| 使用非认证用户的特权升级 | High |
| 使用特权不足用户的特权升级 | High |
| Apache Tomcat Context Administration Tool 无特权访问 | Medium |
| Banner Rotating 01 特权升级 | Medium |
| 通过 Cookie 操纵的可能的垂直特权升级 | Low |
| Microsoft FrontPage Extensions 站点篡改 | Medium |
| 应用流程 Subversion 所用的 Webevent 管理权 | Medium |
| BEA WebLogic 管理界面 | Medium |
| Microsoft FrontPage Server Extensions 管理界面 | Medium |
| Oracle Application Server 管理界面 | Medium |
| 注销后会话未失效 | High |
| 基本认证未加密 | High |
| SSL 证书将要到期 | Informational |
| SSL 证书到期 | Informational |
| SSL 证书尚未生效 | Informational |
| SSL 证书域名不匹配 | Informational |
| 发现自签署 SSL 证书 | Informational |
| 整数溢出 | Informational |
| LDAP 注入 | High |
| SMTP MX 注入 | High |
| Poison Null Byte Windows 文件检索 | High |
| Poison Null Byte Unix 文件检索 | High |
| Apache Struts2 与 Struts1 插件远程代码执行 | High |
| Apache Struts2 命名空间未定义远程代码执行 | High |
| Apache Struts2 Freemarker 标记远程代码执行 | High |
| Alibaba Web 服务器文件下载和远程命令执行 | High |
| 参数系统调用代码注入 | High |
| Microsoft IIS Unicode 目录遍历 | High |
| 文件参数 Shell 命令注入 | High |
| FormNow CGI Shell 命令执行 | High |
| Java 编组代码执行 | High |
| IBM WebSphere "WASPostParam" Cookie 反序列化拒绝服务 | High |
| Apache Struts2 远程代码执行 | High |
| Apache Struts2 REST 插件 XStream 远程代码执行 | High |
| Nimda 蠕虫远程命令执行 | High |
| Oracle Web Listener 远程命令执行 | High |
| Perl 评估的参数 Shell 命令注入 | High |
| Perl 解释器脚本任意命令执行 | High |
| 端口侦听器命令注入 | High |
| 适用于 Windows 的端口侦听器命令注入 | High |
| Parameter Command Injection | High |
| UtilMind Maillist.cgi 远程命令执行 | High |
| DotNetNuke BDPDT 模块命令执行 | High |
| VirtueMart index.php 命令执行 | High |
| Linux 中的 Oracle WebLogic 服务器远程命令执行 | High |
| Windows 中的 Oracle WebLogic 服务器远程命令执行 | High |
| 未进行认证情况下的 Oracle WebLogic Server 远程命令执行 | High |
| 未进行认证情况下的 Drupal 远程命令执行 (CVE-2018-7600) | High |
| IIS IDQ.DLL 目录遍历 | Medium |
| BigBrother 远程文件下载 | Medium |
| 目录遍历任意文件下载 | Medium |
| Unix 文件参数变更 | Medium |
| Windows 文件参数变更 | Medium |
| Etomite index.php 路径遍历 | Medium |
| Exponent CMS download.php 路径遍历 | Medium |
| F5 Data Manager 多重路径遍历 | Medium |
| Jcow index.php 路径遍历 | Medium |
| Joomla! AllVideos 插件 download.php 路径遍历 | Medium |
| Joomla Canteen 组件 index.php 路径遍历 | Medium |
| Joomla ccNewsletter 组件 index.php 路径遍历 | Medium |
| Joomla! ionFiles 组件 download.php 路径遍历 | Medium |
| Joomla JGrid 组件 index.php 路径遍历 | Medium |
| Joomla MyBlog 组件 index.php 路径遍历 | Medium |
| Joomla Pro Desk 组件 index.php 路径遍历 | Medium |
| JSPWiki Edit.jsp 路径遍历 | Medium |
| LineWeb index.php 路径遍历 | Medium |
| MODx tvs.php 路径遍历 | Medium |
| Namazu 路径遍历 | Medium |
| PhpWebGallery 多重路径遍历 | Medium |
| PostNuke 目录遍历 | Medium |
| SAP Crystal Reports Server 路径遍历 | Medium |
| sendcard 路径遍历 | Medium |
| Tiki Wiki CMS Groupware tiki-jsplugin.php 路径遍历 | Medium |
| TomatoCart json.php 路径遍历 | Medium |
| VirtueMart 多重路径遍历 | Medium |
| vtiger CRM 多重路径遍历 | Medium |
| WeBid active\_auctions.php 路径遍历 | Medium |
| Winmail Server main.php 路径遍历 | Medium |
| WoltLab Burning Board index.php 路径泄露 | Medium |
| WordPress SEO Tools Plugin get\_download.php 路径遍历 | Medium |
| Xoops 多重路径遍历（2.3.x 版本） | Medium |
| Zen Cart initsystem.php 路径遍历 | Medium |
| Zen Cart 多重路径遍历 | Medium |
| 检测到应用程序测试脚本 | Informational |
| 归档文件下载 | Low |
| Visual Studio .NET 文件下载 | Low |
| 包含文件下载 | Low |
| 临时文件下载 | Low |
| 直接访问管理页面 | Low |
| Ariadne CMS view.php 远程文件包含 | High |
| AWStats PHP 命令执行 | High |
| CMME 信息泄露 | High |
| Drake CMS PHP 远程文件包含 | High |
| Joomla Dada Mail Manager 组件 config.dadamail.php 远程文件包含 | High |
| Joomla! index.php 远程文件包含 | High |
| Joomla VirtueMart Google Base 组件 admin.googlebase.php 远程文件包含 | High |
| JSP 文件包含 | High |
| 通过远程文件包含事项进行发布 | High |
| phpPgAdmin redirect.php 远程文件包含 | High |
| PHP 远程文件包含 | High |
| Cookie 上的 PHP 远程文件包含 | High |
| VirtueMart 多远程文件包含 | High |
| XOOPS 多重 PHP 代码注入 | High |
| Windows 上 Apache Tomcat 中的 PUT 请求处理缺陷 | High |
| 备用链式证书伪造 | Medium |
| 支持不推荐使用的 SSL 版本 | Medium |
| 支持较老的 TLS 版本 | Low |
| Decrypting RSA with Obsolete and Weakened eNcryption（即 DROWN) | High |
| 重构 RSA 导出键（又称为 FREAK） | Medium |
| Logjam（Diffie-Hellman 密钥交换降级） | Medium |
| 检测到 RC4 密码套件 | Medium |
| 检测到 SHA-1 密码套件 | Low |
| 支持弱 SSL 密码套件 | Medium |
| 源 IP 已公开 | Medium |
| 探测器端口 8080 | Medium |
| 探测器端口 8880 | Medium |
| 端口侦听器盲 SSRF | Medium |
| ADNS 盲 SSRF | Medium |
| 外部会话 ID 实施 | High |
| 会话 ID 未更新 | Medium |
| 会话定置 | High |
| AdMan editCampaign.php SQL 注入 | High |
| ASPPortal reply.asp SQL 注入 | High |
| aspProductCatalog default.asp SQL 注入 | High |
| SQL 盲注 | High |
| MongoDB NoSQL 注入 | High |
| SQL 注入命令执行 | High |
| SQL 注入 | High |
| ClipBucket 多重 SQL 注入 | High |
| ClipShare channel\_detail.php SQL 注入 | High |
| Concrete5 SQL 注入 | High |
| CubeCart index.php SQL 注入 | High |
| DoceboCMS Accept-Language 头 SQL 注入 | High |
| Dolphin get\_list.php SQL 注入 | High |
| dotProject index.php SQL 注入 | High |
| Drupal Ajax Checklist 模块 SQL 注入 | High |
| e107 Forum Plugin forum\_admin.php SQL 注入 | High |
| e107 Lyrics Plugin lyrics\_song.php SQL 注入 | High |
| e107 多重 SQL 注入 | High |
| e107 User Journals Plugin userjournals.php SQL 注入 | High |
| e107 ZoGo-Shop Plugin product\_details.php SQL 注入 | High |
| easyLink detail.php SQL 注入 | High |
| eFront 多重 SQL 注入 | High |
| Etomite index.php SQL 注入 (V1.1) | High |
| Fusetalk 多重 SQL 注入 | High |
| GForge 多重 SQL 注入 | High |
| 发现数据库错误模式 | Low |
| iNet Orkut Clone profile\_social.php SQL 注入 | High |
| Joomla! Comlantis Visitors Google Map 组件 map\_data.php SQL 注入 | High |
| Joomla! 多重 SQL 注入 | High |
| Joomla! TimeTrack 组件 index.php SQL 注入 | High |
| MemHT Portal index.php SQL 注入 | High |
| MODx“a”参数 (index.php) SQL 注入 | High |
| MODx“id”参数 (index.php) SQL 注入 | High |
| 多重 Joomla! 组件 SQL 注入 | High |
| MyBB managegroup.php SQL 注入 | High |
| MyBB private.php SQL 注入 | High |
| Nuke-Evolution modules.php SQL 注入 | High |
| OneCMS staff.php SQL 注入 | High |
| Oracle Application Server SQL 注入 | High |
| paFileDB articles.php SQL 注入 | High |
| PhotoStore 多重 SQL 注入 | High |
| phpBB memberlist.php SQL 注入 | High |
| PHP-Fusion Book Panel Infusion books.php SQL Injection | High |
| PHP-Fusion Recepies 模块 recept.php SQL 注入 | High |
| PHP-Fusion vArcade 模块 SQL 注入 | High |
| PHP-Nuke BookCatalog 模块 modules.php SQL 注入 | High |
| PHP-Nuke 下载模块 SQL 注入 | High |
| PHP Pro Bid categories.php SQL 注入 | High |
| phpWebSite links.php SQL 注入 | High |
| 探测 MongoDB | High |
| Q-Shop users.asp SQL 注入 | High |
| Simple Machines Forum 外挂 Seo4SMF SQL 注入 | High |
| SimpleNews print.php SQL 注入 | High |
| SourceBans index.php SQL 注入 | High |
| SweetRice index.php SQL 注入 | High |
| vBulletin attachmentpermission.php SQL 注入 | High |
| VirtueMart 多重 SQL 注入 | High |
| WikkaWiki "/UserSettings" SQL 注入 | High |
| WordPress Count Per Day 插件 notes.php SQL 注入 | High |
| WordPress Newsletter Plugin stnl\_iframe.php SQL 注入 | High |
| WordPress“p”SQL 注入 | High |
| WordPress 搜索功能 SQL 注入 | High |
| WordPress WP Comment Remix Plugin SQL 注入 | High |
| WordPress WP e-Commerce 插件 SQL 注入 | High |
| WordPress WP-StarsRateBox Plugin wp-starsratebox.php SQL 注入 | High |
| WordPress Community Events 插件 tracker.php SQL 注入 | High |
| WordPress Filebase 插件 wpfb-ajax.php SQL 注入 | High |
| xbtit index.php SQL 注入 | High |
| Xoops Article 模块多重 SQL 注入 | High |
| XOOPS Makale 模块 makale.php SQL 注入 | High |
| zenphoto full-image.php SQL 注入 | High |
| 服务器端伪指令文件检索 | High |
| 发现不存在的域的链接 | High |
| 通过 URL 重定向钓鱼 | High |
| Comm100 Forum Redirect.aspx URL 重定向 | High |
| Dojo Toolkit URL 重定向 | High |
| Microsoft Outlook Web Access for Exchange URL 重定向 | High |
| Microsoft SharePoint URL 重定向 | High |
| OSSIM index.php URL 重定向 | High |
| WoltLab Burning Board dereferrer.php URL 重定向 | High |
| XML 外部实体文件泄露 | High |
| JSON 端点 XML 外部实体文件泄露 | High |
| Apache AXIS XML 外部实体文件检索 | High |
| XPath 注入 | Medium |

详细的修复任务

## 高优先级修复任务

|  |  |  |
| --- | --- | --- |
|  | 发送敏感信息时，始终使用 SSL 和 POST（主体）参数。 | 1 |

1. 确保所有登录请求都在主体中（并加密）发送到服务器。

2. 请确保敏感信息，例如：

- 用户名

- 密码

- 社会保险号码

- 信用卡号码

- 驾照号码

- 电子邮件地址

- 电话号码

- 邮政编码

始终放在请求主体中（并加密）来发送到服务器。

### 要修订的变量

| 类型 | 名称 | URL |
| --- | --- | --- |
| Parameter | password | http://localhost:8080/login |

### 相关联的问题类型

|  | 问题类型 | 计数 | 严重性 |
| --- | --- | --- | --- |
|  | 查询中的密码参数 | 1 | High |

## 中优先级修复任务

## 低优先级修复任务

|  |  |  |
| --- | --- | --- |
|  | 查看危险字符注入的可能解决方案 | 2 |

有几种缓解技术：

[1] 策略：库或框架

使用经过审查的库或框架，这样的库或框架不允许出现这种漏洞或提供更容易避免这种漏洞的结构。

更容易生成正确编码的输出的库和框架的示例包括微软的反 XSS 库、OWASP ESAPI 编码模块和 Apache Wicket。

[2] 了解您的数据将用于的上下文及预期使用的编码。在不同组件之间传输数据时，或者生成可能同时包含多个编码的输出（如网页或多部分邮件消息）时，这一点特别重要。研究所有预期通信协议和数据表示形式，以确定所需的编码策略。

对于将输出到另一个网页的数据，特别是从外部输入接收到的数据，请对所有非字母数字字符使用相应的编码。

同一个输出文件的各个部分可能需要不同的编码，这会因输出是否处于以下各项中而不同：

[-] HTML 正文

[-] 元素属性（如 src="XYZ"）

[-] URI

[-] JavaScript 部分

[-] 级联样式表和样式属性

请注意，HTML 实体编码仅适用于 HTML 正文。

请参阅 XSS 防御速查表，

http://www.owasp.org/index.php/XSS\_(Cross\_Site\_Scripting)\_Prevention\_Cheat\_Sheet

了解有关所需编码和转义类型的更多详细信息。

[3] 策略：识别并减少攻击面

了解不可信输入可能进入您的软件的所有潜在区域：参数、cookie、从网络读取的任何内容、环境变量、反向 DNS 查找、查询结果、请求头、URL 组件、电子邮件、文件、文件名、数据库和向应用程序提供数据的任何外部系统。请记住，此类输入可能通过 API 调用间接获得。

[4] 策略：输出编码

对于生成的每一个网页，请使用并指定一个字符编码，如 ISO-8859-1 或 UTF-8。未指定编码时，Web 浏览器可能通过猜测网页实际使用了哪个编码，选择另一个编码。这可能导致 Web 浏览器对某些序列特殊对待，从而面向难以察觉的 XSS 攻击敞开客户机。请参阅 CWE-116 了解更多与编码/转义有关的缓解措施。

[5] 策略：识别并减少攻击面

为了帮助缓解针对用户会话 cookie 的 XSS 攻击，请将会话 cookie 设置为 HttpOnly。在支持 HttpOnly 功能的浏览器（如较新版本的 Internet Explorer 和 Firefox ）中，此属性可以防止使用 document.cookie 的恶意客户机端脚本访问用户的会话 cookie。这不是一个完善的解决方案，因为并不是所有的浏览器都支持 HttpOnly。更重要的是，XMLHTTPRequest 和其他功能强大的浏览器技术会向 HTTP 头（包括其中设置了 HttpOnly 标志的 Set-Cookie 头）提供读取权限。

[6] 策略：输入验证

假设所有输入都是恶意输入。使用“接受已知良好输入”输入验证策略：严格符合规范的可接受输入的白名单。拒绝不严格符合规范的所有输入，或者将其转换为严格符合规范的输入。请勿单独依靠列入黑名单的恶意输入或格式不正确的输入。不过，在检测潜在攻击或确定哪些输入格式不正确以至于应彻底拒绝方面，黑名单可能很有用。

执行输入验证时，请考虑所有潜在相关属性，包括长度、输入类型、可接受值的完整范围、缺少或多余的输入、语法、相关字段的一致性和业务规则的符合性。举一个业务规则逻辑的示例，“boat”在语法上可能有效，因为其仅包含字母数字字符，但是如果您期望输入的是颜色，如“red”或“blue”，则其就是无效的。

动态构建网页时，请使用基于请求中参数的预期值限制字符集的严格白名单。应验证并清理所有输入，不仅包括用户预计指定的参数，还包括请求中的所有数据（包括隐藏字段、cookie、头、URL 本身等）。导致持续 XSS 漏洞的常见错误是仅验证预计网站会重新显示的字段。应用程序服务器或应用程序反射请求中的其他数据很常见，开发团队很难预料到这一点。而且未来的开发人员也可能使用当前没有反射的字段。因此，建议验证 HTTP 请求的所有部分。

请注意，虽然输入验证可以提供一些深度防御，但是正确的输出编码、转义和引用才是防止 XSS 的最有效解决方案。输入验证可有效地限制输出中将显示的内容，却无法一直防止 XSS，特别是要求您支持可能包含任意字符的自由格式文本字段的情况。例如，在聊天应用程序中，心形表情符号 ("<3") 很可能会通过验证步骤，因为其经常使用。但是，该符号无法直接插入网页中，因为其包含需要转义或以其他方式处理的 "<" 字符。在这种情况下，删除 "<" 可能降低 XSS 风险，却会产生不正确的行为，因为不会记录表情符号。这似乎只是一个小小的不便之处，但是在希望表示不等式的数学论坛中会更加重要。

即使您在验证中犯了错（如忘记了验证 100 个输入字段的其中一个），正确的编码仍有可能保护您不受基于注入的攻击。只要不孤立进行，输入验证就仍是一种有用的手段，因为其可以显著减少攻击面，可让您检测一些攻击，并提供正确编码无法处理的其他安全优势。

确保您在应用程序内明确定义的界面中执行输入验证。这将有助于保护应用程序，即使重新使用组件或将组件移到别处也如此。

### 要修订的变量

| 类型 | 名称 | URL |
| --- | --- | --- |
| Global | page | http://localhost:8080/venuelist/getVenueList |
| Global | page | http://localhost:8080/news/getNewsList |

### 相关联的问题类型

|  | 问题类型 | 计数 | 严重性 |
| --- | --- | --- | --- |
|  | JSON 中反映的未清理用户输入 | 2 | Informational |

|  |  |  |
| --- | --- | --- |
|  | 除去 HTML 注释中的敏感信息 | 3 |

[1] 请勿在 HTML 注释中遗留任何重要信息（如文件名或文件路径）。

[2] 从生产站点注释中除去以前（或未来）站点链接的跟踪信息。

[3] 避免在 HTML 注释中放置敏感信息。

[4] 确保 HTML 注释不包括源代码片段。

[5] 确保程序员没有遗留重要信息。

### 要修订的变量

| 类型 | 名称 | URL |
| --- | --- | --- |
| Page | <p class="mb-0" th:text="${venue.open\_time}+'~'+${venue.close\_time}">09:00 a.m. ~ 17:00 p.m.</p> | http://localhost:8080/venue\_list |
| Page | <img src="https://img.zcool.cn/community/0181bc5b20cf25a80121bbecb074ca.jpg@1280w\_1l\_2o\_100sh.jpg" | http://localhost:8080/venue |
| Page | <span class="badge badge-secondary" th:text="${news.time}">2019-12-10</span> | http://localhost:8080/news |

### 相关联的问题类型

|  | 问题类型 | 计数 | 严重性 |
| --- | --- | --- | --- |
|  | HTML 注释敏感信息泄露 | 3 | Informational |

|  |  |  |
| --- | --- | --- |
|  | 除去 Web 站点中的电子邮件地址 | 1 |

从 Web 站点中除去任何电子邮件地址，以便其不会被恶意用户利用。

### 要修订的变量

| 类型 | 名称 | URL |
| --- | --- | --- |
| Page | venue | http://localhost:8080/venue |

### 相关联的问题类型

|  | 问题类型 | 计数 | 严重性 |
| --- | --- | --- | --- |
|  | 发现电子邮件地址模式 | 1 | Informational |

|  |  |  |
| --- | --- | --- |
|  | 对禁止的资源发布“404 - Not Found”响应状态代码，或者将其完全除去 | 3 |

如果不需要禁止的资源，请将其从站点中除去。

可能的话，请发出改用“404 － 找不到”响应状态代码，而不是“403 － 禁止”。这项更改会将站点的目录模糊化，可以防止泄漏站点结构。

### 要修订的变量

| 类型 | 名称 | URL |
| --- | --- | --- |
| Page | index/ | http://localhost:8080/index/ |
| Page | signup/ | http://localhost:8080/signup/ |
| Page | login/ | http://localhost:8080/login/ |

### 相关联的问题类型

|  | 问题类型 | 计数 | 严重性 |
| --- | --- | --- | --- |
|  | 检测到隐藏目录 | 3 | Low |

|  |  |  |
| --- | --- | --- |
|  | 将“autocomplete”属性正确设置为“off” | 2 |

如果“input”元素的“password”字段中缺失“autocomplete”属性，请进行添加并将其设置为“off“。

如果“autocomplete”属性设置为“on”，请将其更改为“off”。

例如：易受攻击站点：

<form action="AppScan.html" method="get">

Username: <input type="text" name="firstname" /><br />

Password: <input type="password" name="lastname" />

<input type="submit" value="Submit" />

<form>

非易受攻击站点：

<form action="AppScan.html" method="get">

Username: <input type="text" name="firstname" /><br />

Password: <input type="password" name="lastname" autocomplete="off"/>

<input type="submit" value="Submit" />

<form>

### 要修订的变量

| 类型 | 名称 | URL |
| --- | --- | --- |
| Page | login | http://localhost:8080/login |
| Page | signup | http://localhost:8080/signup |

### 相关联的问题类型

|  | 问题类型 | 计数 | 严重性 |
| --- | --- | --- | --- |
|  | 自动填写未对密码字段禁用的 HTML 属性 | 2 | Low |

|  |  |  |
| --- | --- | --- |
|  | 将服务器配置为使用安全策略的“Content-Security-Policy”头 | 5 |

将服务器配置为发送“Content-Security-Policy”头。

关于 Apache，请参阅：

http://httpd.apache.org/docs/2.2/mod/mod\_headers.html

关于 IIS，请参阅：

https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx

关于 nginx，请参阅：

http://nginx.org/en/docs/http/ngx\_http\_headers\_module.html

### 要修订的变量

| 类型 | 名称 | URL |
| --- | --- | --- |
| Page | index | http://localhost:8080/index |
| Page | news\_list | http://localhost:8080/news\_list |
| Page | signup | http://localhost:8080/signup |
| Page | venue | http://localhost:8080/venue |
| Page | news | http://localhost:8080/news |

### 相关联的问题类型

|  | 问题类型 | 计数 | 严重性 |
| --- | --- | --- | --- |
|  | “Content-Security-Policy”头缺失或不安全 | 5 | Low |

|  |  |  |
| --- | --- | --- |
|  | 将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头 | 5 |

配置您的服务器，以确保在所有传出请求上发送值为“1”（即已启用）的“X-XSS-Protection”报头。

关于 Apache，请参阅：

http://httpd.apache.org/docs/2.2/mod/mod\_headers.html

关于 IIS，请参阅：

https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx

关于 nginx，请参阅：

http://nginx.org/en/docs/http/ngx\_http\_headers\_module.html

### 要修订的变量

| 类型 | 名称 | URL |
| --- | --- | --- |
| Page | index | http://localhost:8080/index |
| Page | news\_list | http://localhost:8080/news\_list |
| Page | signup | http://localhost:8080/signup |
| Page | venue | http://localhost:8080/venue |
| Page | news | http://localhost:8080/news |

### 相关联的问题类型

|  | 问题类型 | 计数 | 严重性 |
| --- | --- | --- | --- |
|  | “X-XSS-Protection”头缺失或不安全 | 5 | Low |

|  |  |  |
| --- | --- | --- |
|  | 将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头 | 5 |

将服务器配置为针对所有外发请求发送具有值“nosniff”的“X-Content-Type-Options”头。

关于 Apache，请参阅：

http://httpd.apache.org/docs/2.2/mod/mod\_headers.html

关于 IIS，请参阅：

https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx

关于 nginx，请参阅：

http://nginx.org/en/docs/http/ngx\_http\_headers\_module.html

### 要修订的变量

| 类型 | 名称 | URL |
| --- | --- | --- |
| Page | index | http://localhost:8080/index |
| Page | venue\_list | http://localhost:8080/venue\_list |
| Page | news\_list | http://localhost:8080/news\_list |
| Page | signup | http://localhost:8080/signup |
| Page | venue | http://localhost:8080/venue |

### 相关联的问题类型

|  | 问题类型 | 计数 | 严重性 |
| --- | --- | --- | --- |
|  | “X-Content-Type-Options”头缺失或不安全 | 5 | Low |

|  |  |  |
| --- | --- | --- |
|  | 将每个第三方脚本/链接元素支持添加到 SRI(Subresource Integrity)。 | 1 |

将子资源完整性添加到源不在您的域中的每个脚本/链接。

W3C 子资源完整性：

https://www.w3.org/TR/SRI/

SRI 散列生成器：

https://srihash.org

不支持 SRI 的样本脚本元素：

<script src="https://example.com/example-framework.js"

crossorigin="anonymous"></script>

支持 SRI 的样本脚本元素：

<script src="https://example.com/example-framework.js"

integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQlGYl1kPzQho1wx4JwY8wC"

crossorigin="anonymous"></script>

### 要修订的变量

| 类型 | 名称 | URL |
| --- | --- | --- |
| Page | order\_place | http://localhost:8080/order\_place |

### 相关联的问题类型

|  | 问题类型 | 计数 | 严重性 |
| --- | --- | --- | --- |
|  | SRI (Subresource Integrity) 的检查 | 1 | Low |

|  |  |  |
| --- | --- | --- |
|  | 验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常 | 3 |

[1] 检查入局请求，以了解所有预期的参数和值是否存在。 当参数缺失时，发出适当的错误消息，或使用缺省值。

[2] 应用程序应验证其输入是否由有效字符组成（解码后）。 例如，应拒绝包含空字节（编码为 %00）、单引号、引号等的输入值。

[3] 确保值符合预期范围和类型。 如果应用程序预期特定参数具有特定集合中的值，那么该应用程序应确保其接收的值确实属于该集合。 例如，如果应用程序预期值在 10..99 范围内，那么就该确保该值确实是数字，且在 10..99 范围内。

[4] 验证数据是否属于提供给客户端的集合。

[5] 请勿在生产环境中输出调试错误消息和异常。

### 要修订的变量

| 类型 | 名称 | URL |
| --- | --- | --- |
| Parameter | venueID | http://localhost:8080/venue |
| Parameter | newsID | http://localhost:8080/news |
| Parameter | userID | http://localhost:8080/register.do |

### 相关联的问题类型

|  | 问题类型 | 计数 | 严重性 |
| --- | --- | --- | --- |
|  | 应用程序错误 | 3 | Informational |

|  |  |  |
| --- | --- | --- |
|  | 在 Web 服务器中禁用 HTTP TRACE 支持 | 1 |

禁用 Web 服务器中的 HTTP TRACE 支持。

针对 Apache Web 服务器和 Microsoft IIS 的可能的变通方法如下：

- Apache HTTP Server：利用 Apache mod\_rewrite 模块来拒绝 HTTP TRACE 请求，或只允许符合网站需求和策略的方法。

- Microsoft Internet Information Services（IIS）：利用 URLScan 工具来拒绝 HTTP TRACE 请求，或只允许符合站点需求和策略的方法。

### 要修订的变量

| 类型 | 名称 | URL |
| --- | --- | --- |
| Page | localhost | http://localhost:8080/js/jquery-3.4.1.min.js |

### 相关联的问题类型

|  | 问题类型 | 计数 | 严重性 |
| --- | --- | --- | --- |
|  | 启用了 TRACE 和 TRACK HTTP 方法 | 1 | Low |

应用程序数据

## 参数

| 名称 | 值 | 类型 | URL |
| --- | --- | --- | --- |
| password |  | 密码 | http://localhost:8080/register.do |
| userID |  | 文本 | http://localhost:8080/register.do |
| page | 1  2 | 简单链接 | http://localhost:8080/venuelist/getVenueList?page=1 |
| phone | 555-555-5555 | 文本 | http://localhost:8080/register.do |
| page | 1 | 简单链接 | http://localhost:8080/news/getNewsList?page=1 |
| userName |  | 文本 | http://localhost:8080/register.do |
| email | test@altoromutual.com | 文本 | http://localhost:8080/register.do |
| newsID | 12 | 简单链接 | http://localhost:8080/news?newsID=12 |
| venueID | 2 | 简单链接 | http://localhost:8080/venue?venueID=2 |
| password |  | 密码 | http://localhost:8080/login?userID=&password= |
| userID |  | 文本 | http://localhost:8080/login?userID=&password= |

## 失败请求

| 原因 | URL |
| --- | --- |
| 响应状态“500” － 内部服务器错误 | http://localhost:8080/message\_list |
| 响应状态“500” － 内部服务器错误 | http://localhost:8080/addOrder.do |
| 响应状态“404” － 找不到 | http://localhost:8080/js/popper.js |

JavaScript

| 脚本 | URL |
| --- | --- |
| /\*! jQuery v3.4.1 | (c) JS Foundation and other contributors | jquery.org/license \*/  !function(e,t){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=e.document?t(e,!0):function(e){if(!e.document)throw new Error("jQuery requires a window with a document");return t(e)}:t(e)}("undefined"!=typeof window?window:this,function(C,e){"use strict";var t=[],E=C.document,r=Object.getPrototypeOf,s=t.slice,g=t.concat,u=t.push,i=t.indexOf,n={},o=n.toString,v=n.hasOwnProperty,a=v.toString,l=a.call(Object),y={},m=function(e){return"function"==typeof e&&"number"!=typeof e.nodeType},x=function(e){return null!=e&&e===e.window},c={type:!0,src:!0,nonce:!0,noModule:!0};function b(e,t,n){var r,i,o=(n=n||E).createElement("script");if(o.text=e,t)for(r in c)(i=t[r]||t.getAttribute&&t.getAttribute(r))&&o.setAttribute(r,i);n.head.appendChild(o).parentNode.removeChild(o)}function w(e){return null==e?e+"":"object"==typeof e||"function"==typeof e?n[o.call(e)]||"object":typeof e}var f="3.4.1",k=function(e,t){return new k.fn.init(e,t)},p=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g;function d(e){var t=!!e&&"length"in e&&e.length,n=w(e);return!m(e)&&!x(e)&&("array"===n||0===t||"number"==typeof t&&0<t&&t-1 in e)}k.fn=k.prototype={jquery:f,constructor:k,length:0,toArray:function(){return s.call(this)},get:function(e){return null==e?s.call(this):e<0?this[e+this.length]:this[e]},pushStack:function(e){var t=k.merge(this.constructor(),e);return t.prevObject=this,t},each:function(e){return k.each(this,e)},map:function(n){return this.pushStack(k.map(this,function(e,t){return n.call(e,t,e)}))},slice:function(){return this.pushStack(s.apply(this,arguments))},first:function(){return this.eq(0)},last:function(){return this.eq(-1)},eq:function(e){var t=this.length,n=+e+(e<0?t:0);return this.pushStack(0<=n&&n<t?[this[n]]:[])},end:function(){return this.prevObject||this.constructor()},push:u,sort:t.sort,splice:t.splice},k.extend=k.fn.extend=function(){var e,t,n,r,i,o,a=arguments[0]||{},s=1,u=arguments.length,l=!1;for("boolean"==typeof a&&(l=a,a=arguments[s]||{},s++),"object"==typeof a||m(a)||(a={}),s===u&&(a=this,s--);s<u;s++)if(null!=(e=arguments[s]))for(t in e)r=e[t],"\_\_proto\_\_"!==t&&a!==r&&(l&&r&&(k.isPlainObject(r)||(i=Array.isArray(r)))?(n=a[t],o=i&&!Array.isArray(n)?[]:i||k.isPlainObject(n)?n:{},i=!1,a[t]=k.extend(l,o,r)):void 0!==r&&(a[t]=r));return a},k.extend({expando:"jQuery"+(f+Math.random()).replace(/\D/g,""),isReady:!0,error:function(e){throw new Error(e)},noop:function(){},isPlainObject:function(e){var t,n;return!(!e||"[object Object]"!==o.call(e))&&(!(t=r(e))||"function"==typeof(n=v.call(t,"constructor")&&t.constructor)&&a.call(n)===l)},isEmptyObject:function(e){var t;for(t in e)return!1;return!0},globalEval:function(e,t){b(e,{nonce:t&&t.nonce})},each:function(e,t){var n,r=0;if(d(e)){for(n=e.length;r<n;r++)if(!1===t.call(e[r],r,e[r]))break}else for(r in e)if(!1===t.call(e[r],r,e[r]))break;return e},trim:function(e){return null==e?"":(e+"").replace(p,"")},makeArray:function(e,t){var n=t||[];return null!=e&&(d(Object(e))?k.merge(n,"string"==typeof e?[e]:e):u.call(n,e)),n},inArray:function(e,t,n){return null==t?-1:i.call(t,e,n)},merge:function(e,t){for(var n=+t.length,r=0,i=e.length;r<n;r++)e[i++]=t[r];return e.length=i,e},grep:function(e,t,n){for(var r=[],i=0,o=e.length,a=!n;i<o;i++)!t(e[i],i)!==a&&r.push(e[i]);return r},map:function(e,t,n){var r,i,o=0,a=[];if(d(e))for(r=e.length;o<r;o++)null!=(i=t(e[o],o,n))&&a.push(i);else for(o in e)null!=(i=t(e[o],o,n))&&a.push(i);return g.apply([],a)},guid:1,support:y}),"function"==typeof Symbol&&(k.fn[Symbol.iterator]=t[Symbol.iterator]),k.each("Boolean Number String Function Array Date RegExp Object Error Symbol".split(" "),function(e,t){n["[object "+t+"]"]=t.toLowerCase()});var h=function(n){var e,d,b,o,i,h,f,g,w,u,l,T,C,a,E,v,s,c,y,k="sizzle"+1\*new Date,m=n.document,S=0,r=0,p=ue(),x=ue(),N=ue(),A=ue(),D=function(e,t){return e===t&&(l=!0),0},j={}.hasOwnProperty,t=[],q=t.pop,L=t.push,H=t.push,O=t.slice,P=function(e,t){for(var n=0,r=e.length;n<r;n++)if(e[n]===t)return n;return-1},R="checked|selected|async|autofocus|autoplay|controls|defer|disabled|hidden|ismap|loop|multiple|open|readonly|required|scoped",M="[\\x20\\t\\r\\n\\f]",I="(?:\\\\.|[\\w-]|[^\0-\\xa0])+",W="\\["+M+"\*("+I+")(?:"+M+"\*([\*^$|!~]?=)"+M+"\*(?:'((?:\\\\.|[^\\\\'])\*)'|\"((?:\\\\.|[^\\\\\"])\*)\"|("+I+"))|)"+M+"\*\\]",$=":("+I+")(?:\\((('((?:\\\\.|[^\\\\'])\*)'|\"((?:\\\\.|[^\\\\\"])\*)\")|((?:\\\\.|[^\\\\()[\\]]|"+W+")\*)|.\*)\\)|)",F=new RegExp(M+"+","g"),B=new RegExp("^"+M+"+|((?:^|[^\\\\])(?:\\\\.)\*)"+M+"+$","g"),\_=new RegExp("^"+M+"\*,"+M+"\*"),z=new RegExp("^"+M+"\*([>+~]|"+M+")"+M+"\*"),U=new RegExp(M+"|>"),X=new RegExp($),V=new RegExp("^"+I+"$"),G={ID:new RegExp("^#("+I+")"),CLASS:new RegExp("^\\.("+I+")"),TAG:new RegExp("^("+I+"|[\*])"),ATTR:new RegExp("^"+W),PSEUDO:new RegExp("^"+$),CHILD:new RegExp("^:(only|first|last|nth|nth-last)-(child|of-type)(?:\\("+M+"\*(even|odd|(([+-]|)(\\d\*)n|)"+M+"\*(?:([+-]|)"+M+"\*(\\d+)... | http://localhost:8080/js/jquery-3.4.1.min.js |
| /\*!  \* Bootstrap v4.3.1 (https://getbootstrap.com/)  \* Copyright 2011-2019 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors)  \* Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE)  \*/  !function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports,require("jquery")):"function"==typeof define&&define.amd?define(["exports","jquery"],e):e((t=t||self).bootstrap={},t.jQuery)}(this,function(t,p){"use strict";function i(t,e){for(var n=0;n<e.length;n++){var i=e[n];i.enumerable=i.enumerable||!1,i.configurable=!0,"value"in i&&(i.writable=!0),Object.defineProperty(t,i.key,i)}}function s(t,e,n){return e&&i(t.prototype,e),n&&i(t,n),t}function l(o){for(var t=1;t<arguments.length;t++){var r=null!=arguments[t]?arguments[t]:{},e=Object.keys(r);"function"==typeof Object.getOwnPropertySymbols&&(e=e.concat(Object.getOwnPropertySymbols(r).filter(function(t){return Object.getOwnPropertyDescriptor(r,t).enumerable}))),e.forEach(function(t){var e,n,i;e=o,i=r[n=t],n in e?Object.defineProperty(e,n,{value:i,enumerable:!0,configurable:!0,writable:!0}):e[n]=i})}return o}p=p&&p.hasOwnProperty("default")?p.default:p;var e="transitionend";function n(t){var e=this,n=!1;return p(this).one(m.TRANSITION\_END,function(){n=!0}),setTimeout(function(){n||m.triggerTransitionEnd(e)},t),this}var m={TRANSITION\_END:"bsTransitionEnd",getUID:function(t){for(;t+=~~(1e6\*Math.random()),document.getElementById(t););return t},getSelectorFromElement:function(t){var e=t.getAttribute("data-target");if(!e||"#"===e){var n=t.getAttribute("href");e=n&&"#"!==n?n.trim():""}try{return document.querySelector(e)?e:null}catch(t){return null}},getTransitionDurationFromElement:function(t){if(!t)return 0;var e=p(t).css("transition-duration"),n=p(t).css("transition-delay"),i=parseFloat(e),o=parseFloat(n);return i||o?(e=e.split(",")[0],n=n.split(",")[0],1e3\*(parseFloat(e)+parseFloat(n))):0},reflow:function(t){return t.offsetHeight},triggerTransitionEnd:function(t){p(t).trigger(e)},supportsTransitionEnd:function(){return Boolean(e)},isElement:function(t){return(t[0]||t).nodeType},typeCheckConfig:function(t,e,n){for(var i in n)if(Object.prototype.hasOwnProperty.call(n,i)){var o=n[i],r=e[i],s=r&&m.isElement(r)?"element":(a=r,{}.toString.call(a).match(/\s([a-z]+)/i)[1].toLowerCase());if(!new RegExp(o).test(s))throw new Error(t.toUpperCase()+': Option "'+i+'" provided type "'+s+'" but expected type "'+o+'".')}var a},findShadowRoot:function(t){if(!document.documentElement.attachShadow)return null;if("function"!=typeof t.getRootNode)return t instanceof ShadowRoot?t:t.parentNode?m.findShadowRoot(t.parentNode):null;var e=t.getRootNode();return e instanceof ShadowRoot?e:null}};p.fn.emulateTransitionEnd=n,p.event.special[m.TRANSITION\_END]={bindType:e,delegateType:e,handle:function(t){if(p(t.target).is(this))return t.handleObj.handler.apply(this,arguments)}};var o="alert",r="bs.alert",a="."+r,c=p.fn[o],h={CLOSE:"close"+a,CLOSED:"closed"+a,CLICK\_DATA\_API:"click"+a+".data-api"},u="alert",f="fade",d="show",g=function(){function i(t){this.\_element=t}var t=i.prototype;return t.close=function(t){var e=this.\_element;t&&(e=this.\_getRootElement(t)),this.\_triggerCloseEvent(e).isDefaultPrevented()||this.\_removeElement(e)},t.dispose=function(){p.removeData(this.\_element,r),this.\_element=null},t.\_getRootElement=function(t){var e=m.getSelectorFromElement(t),n=!1;return e&&(n=document.querySelector(e)),n||(n=p(t).closest("."+u)[0]),n},t.\_triggerCloseEvent=function(t){var e=p.Event(h.CLOSE);return p(t).trigger(e),e},t.\_removeElement=function(e){var n=this;if(p(e).removeClass(d),p(e).hasClass(f)){var t=m.getTransitionDurationFromElement(e);p(e).one(m.TRANSITION\_END,function(t){return n.\_destroyElement(e,t)}).emulateTransitionEnd(t)}else this.\_destroyElement(e)},t.\_destroyElement=function(t){p(t).detach().trigger(h.CLOSED).remove()},i.\_jQueryInterface=function(n){return this.each(function(){var t=p(this),e=t.data(r);e||(e=new i(this),t.data(r,e)),"close"===n&&e[n](this)})},i.\_handleDismiss=function(e){return function(t){t&&t.preventDefault(),e.close(this)}},s(i,null,[{key:"VERSION",get:function(){return"4.3.1"}}]),i}();p(document).on(h.CLICK\_DATA\_API,'[data-dismiss="alert"]',g.\_handleDismiss(new g)),p.fn[o]=g.\_jQueryInterface,p.fn[o].Constructor=g,p.fn[o].noConflict=function(){return p.fn[o]=c,g.\_jQueryInterface};var \_="button",v="bs.button",y="."+v,E=".data-api",b=p.fn[\_],w="active",C="btn",T="focus",S='[data-toggle^="button"]',D='[data-toggle="buttons"]',I='input:not([type="hidden"])',A=".active",O=".btn",N={CLICK\_DATA\_API:"click"+y+E,FOCUS\_BLUR\_DATA\_API:"focus"+y+E+" blur"+y+E},k=function(){function n(t){this.\_element=t}var t=n.prototype;return t.toggle=function(){var t=!0,e=!0,n=p(this.\_element).closest(D)[0];if(n){var i=this.\_element.querySelector(I);if(i){if("radio"===i.type)if(i.checked&&this.\_element.classList.contains(w))t=!1;else{var o=n.querySelector(A);o&&p(o).removeClass(w)}if(t){if(i.hasAttribute("disabled")||n.hasAttribute("... | http://localhost:8080/js/bootstrap.bundle.min.js |
| $('.dropdown-toggle').dropdown(); function message\_list(flag){ if(!flag){ alert("请登录！"); window.location.href = '/login'; } else{ window.location.href = '/message\_list'; } } function order\_manage(flag){ if(!flag){ alert("请登录！"); window.location.href = '/login'; } else{ window.location.href = '/order\_manage'; } } function order\_place(flag){ if(!flag){ alert("请登录！"); window.location.href = '/login'; } else{ window.open('/order\_place'); // window.location.href = '/order\_place'; } } | http://localhost:8080/ |
| function message\_list(){ let flag = $("#user").html() == ''; if(flag){ alert("请登录！"); window.location.href = '/login'; } else{ window.location.href = '/message\_list'; } } | http://localhost:8080/ |
| javascript:order\_place(false) | http://localhost:8080/ |
| javascript:order\_manage(false) | http://localhost:8080/ |
| javascript:message\_list(false) | http://localhost:8080/ |
| message\_list() | http://localhost:8080/ |
| /\*!  \* jQuery pagination plugin v1.4.2  \* http://josecebe.github.io/twbs-pagination/  \*  \* Copyright 2014-2018, Eugene Simakin  \* Released under Apache 2.0 license  \* http://apache.org/licenses/LICENSE-2.0.html  \*/  (function ($, window, document, undefined) {  'use strict';  var old = $.fn.twbsPagination;  // PROTOTYPE AND CONSTRUCTOR  var TwbsPagination = function (element, options) {  this.$element = $(element);  this.options = $.extend({}, $.fn.twbsPagination.defaults, options);  if (this.options.startPage < 1 || this.options.startPage > this.options.totalPages) {  throw new Error('Start page option is incorrect');  }  this.options.totalPages = parseInt(this.options.totalPages);  if (isNaN(this.options.totalPages)) {  throw new Error('Total pages option is not correct!');  }  this.options.visiblePages = parseInt(this.options.visiblePages);  if (isNaN(this.options.visiblePages)) {  throw new Error('Visible pages option is not correct!');  }  if (this.options.beforePageClick instanceof Function) {  this.$element.first().on('beforePage', this.options.beforePageClick);  }  if (this.options.onPageClick instanceof Function) {  this.$element.first().on('page', this.options.onPageClick);  }  // hide if only one page exists  if (this.options.hideOnlyOnePage && this.options.totalPages == 1) {  if (this.options.initiateStartPageClick) {  this.$element.trigger('page', 1);  }  return this;  }  if (this.options.href) {  this.options.startPage = this.getPageFromQueryString();  if (!this.options.startPage) {  this.options.startPage = 1;  }  }  var tagName = (typeof this.$element.prop === 'function') ?  this.$element.prop('tagName') : this.$element.attr('tagName');  if (tagName === 'UL') {  this.$listContainer = this.$element;  } else {  var elements = this.$element;  var $newListContainer = $([]);  elements.each(function(index) {  var $newElem = $("<ul></ul>");  $(this).append($newElem);  $newListContainer.push($newElem[0]);  });  this.$listContainer = $newListContainer;  this.$element = $newListContainer;  }  this.$listContainer.addClass(this.options.paginationClass);  if (this.options.initiateStartPageClick) {  this.show(this.options.startPage);  } else {  this.currentPage = this.options.startPage;  this.render(this.getPages(this.options.startPage));  this.setupEvents();  }  return this;  };  TwbsPagination.prototype = {  constructor: TwbsPagination,  destroy: function () {  this.$element.empty();  this.$element.removeData('twbs-pagination');  this.$element.off('page');  return this;  },  show: function (page) {  if (page < 1 || page > this.options.totalPages) {  throw new Error('Page is incorrect.');  }  this.currentPage = page;  this.$element.trigger('beforePage', page);  var pages = this.getPages(page);  this.render(pages);  this.setupEvents();  this.$element.trigger('page', page);  return pages;  },  enable: function () {  this.show(this.currentPage);  },  disable: function () {  var \_this = this;  this.$listContainer.off('click').on('click', 'li', function (evt) {  evt.preventDefault();  });  this.$listContainer.children().each(function () {  var $this = $(this);  if (!$this.hasClass(\_this.options.activeClass)) {  $(this).addClass(\_this.options.disabledClass);  }  });  },  buildListItems: function (pages) {  var listItems = [];  if (this.options.first) {  listItems.push(this.buildItem('first', 1));  }  if (this.options.prev) {  var prev = pages.currentPage > 1 ? pages.currentPage - 1 : this.options.loop ? this.options.totalPages : 1;  listItems.push(this.buildItem('prev', prev));  }  for (var i = 0; i < pages.numeric.length; i++) {  listItems.push(this.buildItem('page', pages.numeric[i]));  }  if (this.options.next) {  var next = pages.currentPage < this.options.totalPages ? pages.currentPage + 1 : this.options.loop ? 1 : this.options.totalPages;  listItems.push(this.buildItem('next', next));  }  ... | http://localhost:8080/js/jquery.twbsPagination.js |
| // $(document).ready(function () { // getPage(1); // }); $('#pagination-demo').twbsPagination({ totalPages: 2, visiblePages: 5, onPageClick: function (event, page) { getPage(page); } }); function getPage(page){ $.ajax({//根据page去后台加载数据 url : "/venuelist/getVenueList", type : "get", dataType : "json", data : {"page" : page}, success : function(data) { appendHtml(data.content);//处理数据 console.log(data); } }); } function appendHtml(list) {//此函数用于处理后台返回的数据，根据自己需求来实现页面拼接 let tableShow = ''; for (let i = 0; i < list.length; i++) { tableShow += '<li class="list-group-item px-3 pt-3 border-0">\n' + ' <div class="media border-bottom border-gray pb-3">\n' + ' <div class="media-left mr-3">\n'; if(list[i].picture == '') tableShow += '<img src="venue.jpg" alt="" height="100px" width="100px">\n'; else tableShow += '<img src="'+list[i].picture+'" alt="" height="100px" width="100px">\n'; tableShow += '</div>\n' + ' <div class="media-body">\n' + ' <h5 class="media-heading font-weight-bold pb-3">\n' + ' <a href="/venue?venueID='+list[i].venueID+'" target="\_blank">'+list[i].venueName+'</a>\n' + ' </h5>\n' + ' <h6 class="d-flex">\n' + ' <p class="font-weight-bold mb-0">场馆位置：</p>\n' + ' <p class="mb-0">'+list[i].address+'</p>\n' + ' </h6>\n' + ' <h6 class="d-flex">\n' + ' <p class="font-weight-bold mb-0">开放时间：</p>\n' + ' <p class="mb-0">'+list[i].open\_time+' ~ '+list[i].close\_time+'</p>\n' + ' </h6>\n' + ' <h6 class="d-flex">\n' + ' <p class="font-weight-bold mb-0">租金：</p>\n' + ' <p class="mb-0">￥'+list[i].price+'/h</p>\n' + ' </h6>\n' + ' </div>\n' + ' </div>\n' + ' </li>\n'; } $('#content').html(tableShow); } | http://localhost:8080/venue\_list |
| /\*!  \* jQuery Form Plugin  \* version: 3.51.0-2014.06.20  \* Requires jQuery v1.5 or later  \* Copyright (c) 2014 M. Alsup  \* Examples and documentation at: http://malsup.com/jquery/form/  \* Project repository: https://github.com/malsup/form  \* Dual licensed under the MIT and GPL licenses.  \* https://github.com/malsup/form#copyright-and-license  \*/  /\*global ActiveXObject \*/  // AMD support  (function (factory) {  "use strict";  if (typeof define === 'function' && define.amd) {  // using AMD; register as anon module  define(['jquery'], factory);  } else {  // no AMD; invoke directly  factory( (typeof(jQuery) != 'undefined') ? jQuery : window.Zepto );  }  }  (function($) {  "use strict";  /\*  Usage Note:  -----------  Do not use both ajaxSubmit and ajaxForm on the same form. These  functions are mutually exclusive. Use ajaxSubmit if you want  to bind your own submit handler to the form. For example,  $(document).ready(function() {  $('#myForm').on('submit', function(e) {  e.preventDefault(); // <-- important  $(this).ajaxSubmit({  target: '#output'  });  });  });  Use ajaxForm when you want the plugin to manage all the event binding  for you. For example,  $(document).ready(function() {  $('#myForm').ajaxForm({  target: '#output'  });  });  You can also use ajaxForm with delegation (requires jQuery v1.7+), so the  form does not have to exist when you invoke ajaxForm:  $('#myForm').ajaxForm({  delegation: true,  target: '#output'  });  When using ajaxForm, the ajaxSubmit function will be invoked for you  at the appropriate time.  \*/  /\*\*  \* Feature detection  \*/  var feature = {};  feature.fileapi = $("<input type='file'/>").get(0).files !== undefined;  feature.formdata = window.FormData !== undefined;  var hasProp = !!$.fn.prop;  // attr2 uses prop when it can but checks the return type for  // an expected string. this accounts for the case where a form  // contains inputs with names like "action" or "method"; in those  // cases "prop" returns the element  $.fn.attr2 = function() {  if ( ! hasProp ) {  return this.attr.apply(this, arguments);  }  var val = this.prop.apply(this, arguments);  if ( ( val && val.jquery ) || typeof val === 'string' ) {  return val;  }  return this.attr.apply(this, arguments);  };  /\*\*  \* ajaxSubmit() provides a mechanism for immediately submitting  \* an HTML form using AJAX.  \*/  $.fn.ajaxSubmit = function(options) {  /\*jshint scripturl:true \*/  // fast fail if nothing selected (http://dev.jquery.com/ticket/2752)  if (!this.length) {  log('ajaxSubmit: skipping submit process - no element selected');  return this;  }  var method, action, url, $form = this;  if (typeof options == 'function') {  options = { success: options };  }  else if ( options === undefined ) {  options = {};  }  method = options.type || this.attr2('method');  action = options.url || this.attr2('action');  url = (typeof action === 'string') ? $.trim(action) : '';  url = url || window.location.href || '';  if (url) {  // clean url (don't include hash vaue)  url = (url.match(/^([^#]+)/)||[])[1];  }  options = $.extend(true, {  url: url,  success: $.ajaxSettings.success,  type: method || $.ajaxSettings.type,  iframeSrc: /^https/i.test(window.location.href || '') ? 'javascript:false' : 'about:blank'  }, options);  // hook for manipulating the form data before it is extracted;  // convenient for use with rich editors like tinyMCE or FCKEditor  var veto = {};  this.trigger('form-pre-serialize', [this, options, veto]);  if (veto.veto) {  log('ajaxSubmit: submit vetoed via form-pre-serialize trigger');  return this;  }  // provide opportunity to alter form data before it is serialized  if (options.beforeSerialize && options.beforeSerialize(this, options) === false) {  log('ajaxSubmit: submit aborted via beforeSerialize callback');  return this;  }  var traditional = options.traditional;  if ( traditional === undefined ) {  traditional = $.ajaxSettings.traditional;  }  var elements = [];  var qx, a = this.formToArray(options.semantic, elements);  if (options.data) {  options.extraData = options.data;  qx = $.param(options.data, traditional);  }  // give pre-submit callback an opportunity to abort the submit  if (options.beforeSubmit && options.beforeSubmit(a, this, options) === false) {  log('ajaxSubmit: submit aborted via beforeSubmit callback');  return this;  }  // fire vetoable 'validate' event  this.trigger('form-submit-validate', [a, this, options, veto]);  if (veto.veto) {  log('ajaxSubmit: submit vetoed via form-submit-validate tri... | http://localhost:8080/js/jquery.form.js |
| $("#userID").keyup(function(){ let len = $(this).val().length; if(len > 31){ $(this).val($(this).val().substring(0,32)); } }); $("#password").keyup(function(){ let len = $(this).val().length; if(len > 15){ $(this).val($(this).val().substring(0,16)); } }); $("input").change(function () { $(".alert").attr('hidden', 'hidden'); $("#submit").removeAttr("disabled"); // alert("登陆失败"); }); $("form").submit(function () { $("form").ajaxSubmit({ url:"loginCheck.do", dataType: "text", type: "post", success: function(data){ console.log(data); if(data == 'false') { $(".alert").removeAttr('hidden'); $("#submit").attr("disabled", "disabled"); } else{ alert("登录成功！"); window.location.href = data; } } }); return false; }); | http://localhost:8080/login |
| // $(document).ready(function () { // getPage(1); // }); $('#pagination-demo').twbsPagination({ totalPages: 1, visiblePages: 5, onPageClick: function (event, page) { getPage(page); } }); function getPage(page){ $.ajax({//根据page去后台加载数据 url : "/news/getNewsList", type : "get", dataType : "json", data : {"page" : page}, success : function(data) { appendHtml(data.content);//处理数据 console.log(data); } }); } function appendHtml(list) {//此函数用于处理后台返回的数据，根据自己需求来实现页面拼接 let tableShow = ''; for (let i = 0; i < list.length; i++) { tableShow += '<li class="list-group-item border-0 px-3 py-2">\n' + ' <div class="row mx-0 pb-2 border-bottom border-gray">\n' + ' <a class="ml-1" href="/news?newsID='+list[i].newsID+'" target="\_blank">'+list[i].title+'</a>\n' + ' <div class="ml-auto">\n' + ' <span class="badge badge-secondary">'+list[i].time+'</span>\n' + ' </div>\n' + ' </div>\n' + ' </li>\n'; } $('#content').html(tableShow); } | http://localhost:8080/news\_list |
| var flag = [false, false, false]; function justifySubmit() { console.log(flag); for(let i = 0; i < 3; i++){ if(flag[i]){ $("#submit").attr('disabled',true); return; } } $("#submit").attr('disabled',false); } function doVerify(){ let account = $("#userID").val(); // console.log(account); if(account =="") { if (flag[0]) { $("#alertId").attr('hidden', 'hidden'); flag[0] = false; } justifySubmit(); return; } $.ajax({ url:"checkUserID.do", dataType: "Json", type: "post", data:{ userID:account }, success: function(msg){ if(!msg) { // 账号已经存在 if(!flag[0]){ flag[0] = true; $("#alertId").removeAttr('hidden'); } } else{ if(flag[0]){ flag[0] = false; $("#alertId").attr('hidden', 'hidden'); } } justifySubmit(); } }); } function phoneVerify() { var phone = $("#phone").val(); if(phone =="") { if (flag[1]) { $("#alertPhone").attr('hidden', 'hidden'); flag[1] = false; } justifySubmit(); return; } var myreg=/^[1][3,4,5,6,7,8,9][0-9]{9}$/; if (!myreg.test(phone)) { if(!flag[1]){ flag[1] = true; $("#alertPhone").removeAttr('hidden'); } } else { if(flag[1]){ flag[1] = false; $("#alertPhone").attr('hidden', 'hidden'); } } justifySubmit(); } function emailVerify(){ var email = $("#email").val(); if(email =="") { if (flag[2]) { $("#alertEmail").attr('hidden', 'hidden'); flag[2] = false; } justifySubmit(); return; } var reg = /^([a-zA-Z]|[0-9])(\w|\-)+@[a-zA-Z0-9]+\.([a-zA-Z]{2,4})$/; if(!reg.test(email)){ if(!flag[2]){ flag[2] = true; $("#alertEmail").removeAttr('hidden'); } }else{ if(flag[2]){ flag[2] = false; $("#alertEmail").attr('hidden', 'hidden'); } } justifySubmit(); } $("#userName").keyup(function(){ let len = $(this).val().length; if(len > 17){ $(this).val($(this).val().substring(0,18)); $(this).tooltip('show'); setTimeout(function(){ $("#userName").tooltip('hide'); }, 2000); } }); $("#email").keyup(function(){ let len = $(this).val().length; if(len > 31){ $(this).val($(this).val().substring(0,32)); $(this).tooltip('show'); setTimeout(function(){ $("#email").tooltip('hide'); }, 2000); } }); $("#phone").keyup(function(){ let len = $(this).val().length; if(len > 10){ $(this).val($(this).val().substring(0,11)); $(this).tooltip('show'); setTimeout(function(){ $("#phone").tooltip('hide'); }, 2000); } }); $("#userID").keyup(function(){ let len = $(this).val().length; if(len > 31){ $(this).val($(this).val().substring(0,32)); $(this).tooltip('show'); setTimeout(function(){ $("#userID").tooltip('hide'); }, 2000); } }); $("#password").keyup(function(){ let len = $(this).val().length; if(len > 15){ $(this).val($(this).val().substring(0,16)); $(this).tooltip('show'); setTimeout(function(){ $("#password").tooltip('hide'); }, 2000); } }); $("form").submit(function () { alert("注册成功，请登录！"); }); | http://localhost:8080/signup |
| emailVerify() | http://localhost:8080/signup |
| phoneVerify() | http://localhost:8080/signup |
| doVerify() | http://localhost:8080/signup |
| function order\_venue(){ let flag = $("#user").html() == ''; if(flag){ alert("请登录！"); window.location.href = '/login'; } else{ window.open("/order\_place.do?venueID="+2+""); // window.location.href = "/order\_place?venueID=\""+2+"\""; } } | http://localhost:8080/venue |
| order\_venue() | http://localhost:8080/venue |
| $(document).ready(function(){ let moveSelected=$('#moveSelected')[0]; let ifDrag=false;//是搜开启拖拽的标志 let oldLeft=0;//鼠标按下时的left,top let oldTop=0; let selectedList=[];//拖拽多选选中的块集合 $('#date').datetimepicker({ format: 'YYYY-MM-DD', locale: moment.locale('zh-cn'), minDate: new Date(), defaultDate: new Date() }); let selectedOrderList=[];//向后台请求的订单列表 let venueName = $("#venueName").val(); let date = $("#date").val(); let now = new Date().getHours(); let today = date; let selectedVenue = null; $('#date').datetimepicker().on('dp.change', function () { date = $(this).val(); getOrderList(); }); $("#venueName").change(function () { venueName = $(this).val(); getOrderList(); }); if(venueName!=''){ getOrderList(); } function getOrderList() { console.log(date); console.log(venueName); $.ajax({ url : "/order/getOrderList.do", type : "get", dataType : "json", data : {"venueName" : venueName, "date" : date}, success : function(data) { console.log(data); selectedOrderList = data.orders; selectedVenue = data.venue; resetTimebar();//处理数据 } }); } function resetTimebar(){ $(".time-item").removeClass('selected').removeClass('banned').removeClass('occupied'); selectedList=[]; if(selectedVenue != null){//设置开放时间 let start = parseInt(selectedVenue.open\_time.slice(0,2), 10); let end = parseInt(selectedVenue.close\_time.slice(0,2), 10); if(today == date && start <= now) setTimeItem(6, now+1, 'banned'); else setTimeItem(6, start, 'banned'); setTimeItem(end, 23, 'banned'); } for (let i = 0; i < selectedOrderList.length; i++) {//设置已被预约时间 let start = parseInt(selectedOrderList[i].startTime.slice(11,13), 10); let end = start + selectedOrderList[i].hours; setTimeItem(start, end, 'occupied'); } } function setTimeItem(start, end, type){ for(let i = start; i < end; i++){ let id = '#' + i; $(id).addClass(type); } } $("#reload").click(function(){ resetTimebar(); }); // 鼠标按下时开启拖拽多选，将遮罩定位并展现 $(".timebar").mousedown(function(event) { if(selectedList.length>0 || $("#venueName").val()=='') return; ifDrag=true; moveSelected.style.left=event.pageX-$(this).offset().left +'px'; moveSelected.style.height=50+'px'; oldLeft=event.pageX; oldTop=event.pageY; event.preventDefault(); // 阻止默认行为 event.stopPropagation(); // 阻止事件冒泡 }); // 鼠标移动时计算遮罩的位置，宽 高 $(".timebar").mousemove(function(event) { if(!ifDrag) return;//只有开启了拖拽，才进行mouseover操作 if(event.pageX>oldLeft){//向右拖 moveSelected.style.width=(event.pageX-oldLeft)+'px'; } event.preventDefault(); // 阻止默认行为 event.stopPropagation(); // 阻止事件冒泡 }); //鼠标抬起时计算遮罩的right 和 bottom，找出遮罩覆盖的块，关闭拖拽选中开关，清除遮罩数据 $(".timebar").mouseup(function(event) { if(!ifDrag) return; moveSelected.style.right=Number(moveSelected.style.left.split('px')[0])+Number(moveSelected.style.width.split('px')[0])+'px'; findSelected(); ifDrag=false; clearDragData(); event.preventDefault(); // 阻止默认行为 event.stopPropagation(); // 阻止事件冒泡 }); function findSelected(){ let blockList=$('.timebar').find('.time-item'); for(let i=0;i<blockList.length;i++){ if($(blockList[i]).hasClass('banned') || $(blockList[i]).hasClass('occupied')) { if(selectedList.length > 0) break; continue; } //计算每个块的定位信息 let left=$(blockList[i]).offset().left - $(".timebar").offset().left; let right=$(blockList[i]).width()+left; let top=$(blockList[i]).offset().top - $(".timebar").offset().top; let bottom=$(blockList[i]).height()+top; //判断每个块是否被遮罩盖住（即选中） if(moveSelected.style.left.split('px')[0]<=right && moveSelected.style.right.split('px')[0]>=left){ selectedList.push(blockList[i]); $(blockList[i]).addClass('selected'); } } console.log(selectedList); if(selectedList.length > 0){ if($(selectedList[0]).html().... | http://localhost:8080/order\_place |
| /\*!  \* Bootstrap v4.3.1 (https://getbootstrap.com/)  \* Copyright 2011-2019 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors)  \* Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE)  \*/  !function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports,require("jquery"),require("popper.js")):"function"==typeof define&&define.amd?define(["exports","jquery","popper.js"],e):e((t=t||self).bootstrap={},t.jQuery,t.Popper)}(this,function(t,g,u){"use strict";function i(t,e){for(var n=0;n<e.length;n++){var i=e[n];i.enumerable=i.enumerable||!1,i.configurable=!0,"value"in i&&(i.writable=!0),Object.defineProperty(t,i.key,i)}}function s(t,e,n){return e&&i(t.prototype,e),n&&i(t,n),t}function l(o){for(var t=1;t<arguments.length;t++){var r=null!=arguments[t]?arguments[t]:{},e=Object.keys(r);"function"==typeof Object.getOwnPropertySymbols&&(e=e.concat(Object.getOwnPropertySymbols(r).filter(function(t){return Object.getOwnPropertyDescriptor(r,t).enumerable}))),e.forEach(function(t){var e,n,i;e=o,i=r[n=t],n in e?Object.defineProperty(e,n,{value:i,enumerable:!0,configurable:!0,writable:!0}):e[n]=i})}return o}g=g&&g.hasOwnProperty("default")?g.default:g,u=u&&u.hasOwnProperty("default")?u.default:u;var e="transitionend";function n(t){var e=this,n=!1;return g(this).one(\_.TRANSITION\_END,function(){n=!0}),setTimeout(function(){n||\_.triggerTransitionEnd(e)},t),this}var \_={TRANSITION\_END:"bsTransitionEnd",getUID:function(t){for(;t+=~~(1e6\*Math.random()),document.getElementById(t););return t},getSelectorFromElement:function(t){var e=t.getAttribute("data-target");if(!e||"#"===e){var n=t.getAttribute("href");e=n&&"#"!==n?n.trim():""}try{return document.querySelector(e)?e:null}catch(t){return null}},getTransitionDurationFromElement:function(t){if(!t)return 0;var e=g(t).css("transition-duration"),n=g(t).css("transition-delay"),i=parseFloat(e),o=parseFloat(n);return i||o?(e=e.split(",")[0],n=n.split(",")[0],1e3\*(parseFloat(e)+parseFloat(n))):0},reflow:function(t){return t.offsetHeight},triggerTransitionEnd:function(t){g(t).trigger(e)},supportsTransitionEnd:function(){return Boolean(e)},isElement:function(t){return(t[0]||t).nodeType},typeCheckConfig:function(t,e,n){for(var i in n)if(Object.prototype.hasOwnProperty.call(n,i)){var o=n[i],r=e[i],s=r&&\_.isElement(r)?"element":(a=r,{}.toString.call(a).match(/\s([a-z]+)/i)[1].toLowerCase());if(!new RegExp(o).test(s))throw new Error(t.toUpperCase()+': Option "'+i+'" provided type "'+s+'" but expected type "'+o+'".')}var a},findShadowRoot:function(t){if(!document.documentElement.attachShadow)return null;if("function"!=typeof t.getRootNode)return t instanceof ShadowRoot?t:t.parentNode?\_.findShadowRoot(t.parentNode):null;var e=t.getRootNode();return e instanceof ShadowRoot?e:null}};g.fn.emulateTransitionEnd=n,g.event.special[\_.TRANSITION\_END]={bindType:e,delegateType:e,handle:function(t){if(g(t.target).is(this))return t.handleObj.handler.apply(this,arguments)}};var o="alert",r="bs.alert",a="."+r,c=g.fn[o],h={CLOSE:"close"+a,CLOSED:"closed"+a,CLICK\_DATA\_API:"click"+a+".data-api"},f="alert",d="fade",m="show",p=function(){function i(t){this.\_element=t}var t=i.prototype;return t.close=function(t){var e=this.\_element;t&&(e=this.\_getRootElement(t)),this.\_triggerCloseEvent(e).isDefaultPrevented()||this.\_removeElement(e)},t.dispose=function(){g.removeData(this.\_element,r),this.\_element=null},t.\_getRootElement=function(t){var e=\_.getSelectorFromElement(t),n=!1;return e&&(n=document.querySelector(e)),n||(n=g(t).closest("."+f)[0]),n},t.\_triggerCloseEvent=function(t){var e=g.Event(h.CLOSE);return g(t).trigger(e),e},t.\_removeElement=function(e){var n=this;if(g(e).removeClass(m),g(e).hasClass(d)){var t=\_.getTransitionDurationFromElement(e);g(e).one(\_.TRANSITION\_END,function(t){return n.\_destroyElement(e,t)}).emulateTransitionEnd(t)}else this.\_destroyElement(e)},t.\_destroyElement=function(t){g(t).detach().trigger(h.CLOSED).remove()},i.\_jQueryInterface=function(n){return this.each(function(){var t=g(this),e=t.data(r);e||(e=new i(this),t.data(r,e)),"close"===n&&e[n](this)})},i.\_handleDismiss=function(e){return function(t){t&&t.preventDefault(),e.close(this)}},s(i,null,[{key:"VERSION",get:function(){return"4.3.1"}}]),i}();g(document).on(h.CLICK\_DATA\_API,'[data-dismiss="alert"]',p.\_handleDismiss(new p)),g.fn[o]=p.\_jQueryInterface,g.fn[o].Constructor=p,g.fn[o].noConflict=function(){return g.fn[o]=c,p.\_jQueryInterface};var v="button",y="bs.button",E="."+y,C=".data-api",T=g.fn[v],S="active",b="btn",I="focus",D='[data-toggle^="button"]',w='[data-toggle="buttons"]',A='input:not([type="hidden"])',N=".active",O=".btn",k={CLICK\_DATA\_API:"click"+E+C,FOCUS\_BLUR\_DATA\_API:"focus"+E+C+" blur"+E+C},P=function(){function n(t){this.\_element=t}var t=n.prototype;return t.toggle=function(){var t=!0,e=!0,n=g(this.\_element).closest(w)[0];if(n){var i=this.\_element.querySelector(A);if(i){if("radio"===i.type)if(i.checked&&this.\_element.classList.contains(S))t=!1;else{var o=n.quer... | http://localhost:8080/js/bootstrap.min.js |

## 注释

| 注释 | URL |
| --- | --- |
| <!DOCTYPE html> | http://localhost:8080/ |
| 场馆信息 | http://localhost:8080/ |
| 新闻 | http://localhost:8080/ |
| 留言板 | http://localhost:8080/ |
| <li class="list-group-item px-3 pt-3 border-0" th:each="venue : ${venue\_list}"> | http://localhost:8080/venue\_list |
| <div class="media border-bottom border-gray pb-3"> | http://localhost:8080/venue\_list |
| <div class="media-left mr-3"> | http://localhost:8080/venue\_list |
| <img th:src="${venue.picture}" | http://localhost:8080/venue\_list |
| alt="" height="100px" width="100px"> | http://localhost:8080/venue\_list |
| </div> | http://localhost:8080/venue\_list |
| <div class="media-body"> | http://localhost:8080/venue\_list |
| <h5 class="media-heading font-weight-bold pb-3"> | http://localhost:8080/venue\_list |
| <a th:href="@{venue}" th:method="post" th:text="${venue.venueName}">场馆A</a> | http://localhost:8080/venue\_list |
| </h5> | http://localhost:8080/venue\_list |
| <h6 class="d-flex"> | http://localhost:8080/venue\_list |
| <p class="font-weight-bold mb-0">场馆位置：</p> | http://localhost:8080/venue\_list |
| <p class="mb-0" th:text="${venue.address}">上海市中心人民广场的南侧黄浦区人民大道201号</p> | http://localhost:8080/venue\_list |
| </h6> | http://localhost:8080/venue\_list |
| <p class="font-weight-bold mb-0">开放时间：</p> | http://localhost:8080/venue\_list |
| <p class="mb-0" th:text="${venue.open\_time}+'~'+${venue.close\_time}">09:00 a.m. ~ 17:00 p.m.</p> | http://localhost:8080/venue\_list |
| <p class="font-weight-bold mb-0">租金：</p> | http://localhost:8080/venue\_list |
| <p class="mb-0" th:text="${venue.price}">￥300/h</p> | http://localhost:8080/venue\_list |
| </li> | http://localhost:8080/venue\_list |
| <div class="col-3"> | http://localhost:8080/venue |
| <div class="card shadow"> | http://localhost:8080/venue |
| <div class="card-header py-2 bg-info text-white"> | http://localhost:8080/venue |
| <h6 class="card-title mb-0">场馆信息</h6> | http://localhost:8080/venue |
| <ul class="list-group pt-2"> | http://localhost:8080/venue |
| <li class="list-group-item px-3 pt-3 border-0"> | http://localhost:8080/venue |
| <img src="https://img.zcool.cn/community/0181bc5b20cf25a80121bbecb074ca.jpg@1280w\_1l\_2o\_100sh.jpg" | http://localhost:8080/venue |
| alt="" height="50px" width="50px"> | http://localhost:8080/venue |
| <h6 class="media-heading font-weight-bold"><a th:href="@{venue}">场馆A</a></h6> | http://localhost:8080/venue |
| <small class=""> | http://localhost:8080/venue |
| <strong>场馆位置：</strong> | http://localhost:8080/venue |
| 上海市中心人民广场的南侧黄浦区人民大道201号 | http://localhost:8080/venue |
| </small><br> | http://localhost:8080/venue |
| <small> | http://localhost:8080/venue |
| <strong>开放时间：</strong> | http://localhost:8080/venue |
| 09:00 a.m. ~ 17:00 p.m. | http://localhost:8080/venue |
| <strong>租金：</strong> | http://localhost:8080/venue |
| ￥300/h | http://localhost:8080/venue |
| </small> | http://localhost:8080/venue |
| <p class="mb-0" th:text="${venue.openTime}+'~'+${venue.closeTime}">09:00 a.m. ~ 17:00 p.m.</p> | http://localhost:8080/venue |
| <h6 class="media-heading font-weight-bold"><a th:href="@{venue}">场馆C</a></h6> | http://localhost:8080/venue |
| </ul> | http://localhost:8080/venue |
| <div class="card-body text-right pt-0 pb-2"> | http://localhost:8080/venue |
| <h6 class="m-0"><a th:href="@{venue\_list}"><span class="badge">MORE</span></a></h6> | http://localhost:8080/venue |
| 信息来源：新闻网 | http://localhost:8080/news |
| <div class="bg-white rounded shadow"> | http://localhost:8080/news |
| <div class="card-header py-2 bg-danger text-white"> | http://localhost:8080/news |
| <h6 class="card-title mb-0">新闻</h6> | http://localhost:8080/news |
| <li class="list-group-item border-0 px-3 py-2" th:each="news : ${news\_list}"> | http://localhost:8080/news |
| <div class="row mx-0 pb-2 border-bottom border-gray"> | http://localhost:8080/news |
| <a class="ml-1" th:href="@{news}" th:text="${news.title}">2019年12月24日场馆暂时关闭通知</a> | http://localhost:8080/news |
| <div class="ml-auto"> | http://localhost:8080/news |
| <span class="badge badge-secondary" th:text="${news.time}">2019-12-10</span> | http://localhost:8080/news |
| <li class="list-group-item border-0 px-3 py-2"> | http://localhost:8080/news |
| <a class="ml-1" th:href="@{news}">教育部党组任命梅兵同志为华东师范大学党委书记</a> | http://localhost:8080/news |
| <span class="badge badge-secondary">2019-12-10</span> | http://localhost:8080/news |
| <a class="ml-1" th:href="@{news}">“不忘初心、牢记使命”主题教育专题网</a> | http://localhost:8080/news |
| <a class="ml-1" th:href="@{news}">“统计与数据科学前沿理论及应用”教育部重点实验室建设项目通过验收</a> | http://localhost:8080/news |
| <h6 class="m-0"><a th:href="@{news\_list}"><span class="badge">MORE</span></a></h6> | http://localhost:8080/news |

## cookie

| 名称 | 值 | URL |
| --- | --- | --- |
| JSESSIONID | F64E0EF18324CDFAFBEC6982DD0EA7EC | http://localhost:8080/js/jquery.form.js |

## 应用程序 URL

* http://localhost:8080/
* http://localhost:8080/js/jquery-3.4.1.min.js
* http://localhost:8080/js/bootstrap.bundle.min.js
* http://localhost:8080/index
* http://localhost:8080/venue\_list
* http://localhost:8080/js/jquery.twbsPagination.js
* http://localhost:8080/venuelist/getVenueList?page=1
* http://localhost:8080/login
* http://localhost:8080/js/jquery.form.js
* http://localhost:8080/news\_list
* http://localhost:8080/news/getNewsList?page=1
* http://localhost:8080/signup
* http://localhost:8080/js/jquery.form.js
* http://localhost:8080/js/bootstrap.bundle.min.js
* http://localhost:8080/js/jquery-3.4.1.min.js
* http://localhost:8080/venue?venueID=2
* http://localhost:8080/news?newsID=12
* http://localhost:8080/js/jquery.twbsPagination.js
* http://localhost:8080/venuelist/getVenueList?page=1
* http://localhost:8080/venuelist/getVenueList?page=2
* http://localhost:8080/news/getNewsList?page=1
* http://localhost:8080/login?userID=&password=
* http://localhost:8080/register.do
* http://localhost:8080/js/jquery-3.4.1.min.js
* http://localhost:8080/js/jquery.form.js
* http://localhost:8080/js/bootstrap.bundle.min.js
* http://localhost:8080/order\_place
* http://localhost:8080/js/bootstrap.min.js