软件测试与质量保证报告

一、引言

本报告旨在全面阐述针对会员管理系统（部署于 PythonAnywhere 平台）所执行的软件测试与质量保证活动的过程、方法、发现及结论。本次测试活动严格遵循既定的测试计划，以保障系统在上线前满足核心功能需求、性能指标及安全基线为目标。

本次测试的核心目标聚焦于：

- 功能正确性验证：确保系统核心业务流程（如会员注册/登录、管理员用户/课程管理、会员课程预约/个人信息维护等）严格符合需求规格说明书的要求。
- 性能与稳定性评估：通过模拟高并发场景（如用户登录、数据查询），评估系统在负载压力下的响应时间、吞吐量和稳定性，确定其承载能力边界。
- 安全风险识别与防护能力检验：主动探测系统是否存在常见Web安全漏洞（如SQL注入、XSS跨站脚本攻击、身份认证与会话管理缺陷等），验证其安全防护机制的有效性。
- 跨平台兼容性保障：确保系统在不同操作系统（Windows, Android, iOS/iPadOS）及主流浏览器（Chrome, Edge, Firefox, Safari, QQ浏览器等）环境下功能完整、界面兼容。

测试范围覆盖了**功能测试（黑盒测试）、性能测试（负载测试）、兼容性测试及安全测试（工具扫描与手工渗透）**四大关键领域。测试过程中综合运用了包括 **k6（性能测试）、OWASP ZAP（安全扫描）**在内的自动化工具，并结合详尽的手工测试用例执行（覆盖等价类划分、边界值分析、错误注入等）。

主要成果概述：

- 功能测试验证了核心业务流程（注册登录、信息管理、课程预约等）符合预期，并修复了若干关键功能缺陷（如报错页面、数据约束缺失）。
- 性能测试表明系统在1000用户并发场景下能维持高成功率（>99.9%）和毫秒级平均响应时间（~316ms），预估承载上限约为950-1000并发用户。
- 兼容性测试确认系统在目标PC端及移动端平台的主流浏览器上功能完整运行。
- 安全测试识别并确认了若干中低风险配置问题（如CSP缺失、Anti-CSRF不足），并通过手工渗透测试验证了系统对SQL注入、XSS等常见攻击具备有效防御能力。所有发现的缺陷均已跟踪并修复。

本报告后续章节将详细阐述测试计划、方法、工具选型、具体测试用例设计、执行结果分析（含性能、兼容性、安全测试数据）、缺陷跟踪记录以及最终的质量评估结论。

二、测试计划

- **测试目标**：
  - 验证系统功能是否符合需求（如会员注册、权限管理）
  - 评估系统性能（如并发登录、数据查询响应时间）
  - 检查安全性（如SQL注入、权限漏洞）
- **测试范围**：
  - 功能测试（核心业务流程）
  - 性能测试（负载测试）
  - 兼容性测试（浏览器、设备适配）

- 安全性测试（漏洞测试）

三、测试方法与工具

- 测试方法：
  - 黑盒测试：功能测试、边界值分析、等价类划分
  - 负载测试
  - 跨平台兼容性测试
  - 漏洞扫描与渗透测试
- 测试工具：
  - 性能测试：k6
  - 安全测试：OWASP ZAP

四、测试用例与结果分析

1. 功能测试

此项目测试以功能验证为主，使用更加简便快捷的黑盒测试对模块功能集成测试。**黑盒测试**主要关注软件系统的输入和输出，测试是否满足规定的功能需求和性能要求，能够发现系统中的逻辑错误、功能缺陷、性能瓶颈等问题。主要使用等价类划分法和边界值分析法。

（1）注册登录功能

- 注册界面包括：用户名、密码、确认密码、手机号、年龄（选填）、性别（选填）。可输入任意字符，注册成功的条件为比对密码和确认密码是否一致。
- 登录界面包括：用户名、密码，可输入任意字符，登录成功的条件为用户名和密码已注册。密码可以显示输入。
- 其中已有输入要求与功能：用户名超过8个字则无法输入；性别只能选择男女；密码可以显示输入；必填项不输入则无法登入与注册。

  据此划分为有效等价类和无效等价类。

输入条件	有效等价类	无效等价类
输入信息是否有效	注册密码 == 注册确认密码(1) 密码需包含两种字符且在6-20位(2) 用户名不存在于登录信息(3) 手机号 == 11位数字(4) 用户名字符个数不超过8个(5) 登录用户信息存在于注册账号信息中(6) 登录密码正确(7)	注册密码 != 注册确认密码(8) 密码长度小于6位(9) 密码长度大于10位（10） 密码含有空格（11） 密码含有少于2种不同类型的字符（12） 用户名已存在于登录信息(13) 手机号位数不等于11位(14) 手机号位数符合但含有非数字（15） 用户名字符个数超过8个（16） 登录用户信息不存在于注册账号信息中(17) 登录密码错误(18)

注册界面测试用例

编号	测试输入	覆盖等价类	期待输出	实际输出
T01	用户名：77 密码：qwert123 确认密码：qwert123 电话：22222222222 年龄：20 性别：男	(1)(2)(3)(4)(5)	注册成功	注册成功
T02	用户名：77 密码：qwert123 确认密码：QWERT123 电话：22222222222	(2)(3)(4)(5)(7)	注册失败（密码与确认密码不一致）	注册失败（密码与确认密码不一致）
T03	用户名：77 密码：qwer1 确认密码：qwer1 电话：222222222222	(1)(3)(4)(5)(9)	注册失败（密码长度小于6位）	注册失败（密码长度小于6位）
T04	用户名：77 密码：qwert1111122222333333 确认密码：qwert1111122222333333 电话：222222222222	(1)(3)(4)(5)(10)	注册失败（密码长度大于10位）	注册失败（密码长度大于10位）
T05	用户名：77 密码：qwert 123 确认密码：qwert 123 电话：222222222222	(1)(3)(4)(5)(11)	注册失败(密码含有空格)	注册失败(密码含有空格)

编号	测试输入	覆盖等价类	期待输出	实际输出
T06	用户名：77 密码：qwerttt 确认密码：qwerttt 电话：222222222222	(1)(3)(4)(5)(12)	注册失败(含有少于2种不同类型的字符)	注册失败(含有少于2种不同类型的字符)
T07	用户名：张三 密码：zs12345678 确认密码：zs12345678 电话：11111111111	(1)(3)(4)(5)(13)	注册失败(用户名已存在于登录信息)	注册失败(用户名已存在于登录信息)
T08	用户名：77 密码：qwert123 确认密码：qwert123 电话：222222	(1)(2)(3)(5)(14)	注册失败(手机号位数不等于11位)	注册失败(手机号位数不等于11位)
T19	用户名：77 密码：qwert77 确认密码：qwert77 电话：22222222aaa	(1)(2)(3)(5)(15)	注册失败(手机号位数符合但含有非数字)	注册失败(手机号位数符合但含有非数字)
T10	用户名：777777777 密码：qwert123 确认密码：qwert123 电话：22222222222	(1)(2)(3)(4)(16)	注册失败(用户名字符个数超过8个)	注册失败(用户名字符个数超过8个)

登录界面测试用例

编号	测试输入	覆盖等价类	期待输出	实际输出
T11	用户名：张三 密码：zs12345678	(6)(7)	登录成功	登录成功
T12	（管理员登录） 用户名：sysu 密码：8888	(6)(7)	登录成功	登录成功
T13	用户名：777 密码：123456	(17)	登录失败(用户不存在)	登录失败(用户不存在)
T14	用户名：张三 密码：zs123456	(18)	登录失败(密码输入错误)	登录失败(密码输入错误)

(2) 管理员信息管理

- 管理员用户信息管理界面包括：会员名查询、添加新会员、用户信息管理（修改、删除、查看预约情况）。其中添加新会员界面包括：用户名、性别（选择）、年龄、联系电话、会员等级（选择）；修改会员信息界面可修改内容包括：性别（选择）、年龄、联系电话、会员等级（选择）。预约情况界面：课程名、课程时间、教练、预约时间。

- 管理员课程信息管理界面包括：课程名查询、添加新课、课程信息管理（修改、删除）。其中添加新课界面和修改课程信息界面可修改内容都包括：课程名称、上课时间、教练、价格。
- 其中已有输入要求与功能：添加新会员和添加新课程页面所有选项都是必填，必填项不输入则无法登入与注册；用户名超过8个字则无法输入；性别只能选择男女；密码可以显示输入；课程价格只能是数字。

新建用户与课程功能

据此划分为有效等价类和无效等价类。

输入条件	有效等价类	无效等价类
输入信息是否有效	新用户信息不存在于注册账号信息中(1) 12<=年龄<=99岁且为数字(2) 手机号 == 11位数字(3) 价格为非负数数字(4) 上课时间(HH:MM-HH:MM)规范(5)	新用户信息存在于注册账号信息中(6) 年龄<12岁(7) 年龄>99岁(8) 年龄不为数字(9) 手机号位数不等于11位(10) 手机号位数符合但含有非数字(11) 价格为负数(12) 价格为非数字字符(13) 上课持续时间为0(14) 上课时间存在小于0:00的情况(15) 上课时间存在大于24:00的情况(16)

添加新会员测试用例

编号	测试输入	覆盖等价类	期待输出	实际输出
T01	用户名：Jaimy 电话：12345123456 年龄：18 性别：女 会员等级：黄金会员	(1)(2)(3)	添加成功	添加成功
T03	用户名：张三 电话：11111111111 年龄：40 性别：男 会员等级：铂金会员	(2)(3)(6)	添加失败，该用户已存在	添加失败，该用户已存在

编号	测试输入	覆盖等价类	期待输出	实际输出
T04	用户名：Jaimy 电话：33333333333 年龄：1 性别：女 会员等级：白银会员	(1)(3)(7)	添加失败，年龄必须大于等于12岁	添加失败，年龄必须大于等于12岁
T05	用户名：Jaimy 电话：33333333333 年龄：100 性别：女 会员等级：白银会员	(1)(3)(8)	添加失败，年龄必须小于等于99岁	添加失败，年龄必须小于等于99岁
T06	用户名：Jaimy 电话：33333333333 年龄：aaa 性别：女 会员等级：白银会员	(1)(3)(9)	添加失败，请输入一个数字	添加失败，请输入一个数字
T07	用户名：Jaimy 电话：333 年龄：18 性别：女 会员等级：白银会员	(1)(2)(10)	添加失败，手机号位数不等于11位	添加失败，手机号位数不等于11位
T08	用户名：Jaimy 电话：33333333aaa 年龄：18 性别：女 会员等级：白银会员	(1)(2)(11)	添加失败，手机号含有非数字	添加失败，手机号含有非数字

添加新课程测试用例

编号	测试输入	覆盖等价类	期待输出	实际输出
T09	课程名称：瑜伽 上课时间：16:00-18:00 教练：yiyi 价格：80	(4)(5)	添加成功	添加成功
T10	课程名称：瑜伽 上课时间：16:00-18:00 教练：yiyi 价格：-80	(5)(12)	添加失败，价格为负数	添加失败，价格为负数
T11	课程名称：瑜伽 上课时间：16:00-18:00 教练：yiyi 价格：aa	(5)(13)	添加失败，价格为非数字字符	添加失败，价格为非数字字符
T12	课程名称：瑜伽 上课时间：16:00 教练：yiyi 价格：-40	(4)(14)	添加失败，请与请求的格式匹配	添加失败，请与请求的格式匹配
T13	课程名称：瑜伽 上课时间：-1:00-18:00 教练：yiyi 价格：80	(4)(15)	添加失败，请与请求的格式匹配	添加失败，请与请求的格式匹配
T14	课程名称：瑜伽 上课时间：16:00-28:00 教练：yiyi 价格：80	(4)(16)	添加失败，请与请求的格式匹配	添加失败，请与请求的格式匹配

查询功能(查询会员相关信息、查询课程相关信息)

编号	界面	测试输入	期待输出	实际输出
T15	用户信息管理	张三	张三用户信息	张三用户信息
T16	用户信息管理	李四	李四用户信息	李四用户信息
T17	用户信息管理	77	无用户信息	无用户信息
T18	用户信息管理	（空）	全部用户信息	全部用户信息
T19	课程信息管理	游泳	游泳课程信息	游泳课程信息
T20	课程信息管理	拳击	拳击课程信息	拳击课程信息

编号	界面	测试输入	期待输出	实际输出
T21	课程信息管理	瑜伽	无课程信息	无课程信息
T22	课程信息管理	（空）	全部课程信息	全部课程信息

修改功能(修改会员相关信息、修改课程相关信息)

输入条件	有效等价类	无效等价类
性别、年龄、联系电话、会员等级可更改，用户信息不允许更改； 课程名称、上课时间、教练可更改	12<=年龄<=99且为数字(1) 手机号 == 11位数字(2) 价格为数字(3) 上课时间(HH:MM-HH:MM)规范(4)	年龄<12岁(5) 年龄>99岁(6) 年龄存在非数字字符(7) 手机号位数不等于11位(8) 手机号位数符合但含有非数字(9) 价格为非数字字符(10) 价格为负数(11) 上课持续时间为0(12) 上课时间存在小于0:00的情况(13) 上课时间存在大于24:00的情况(14)

编号	测试输入	覆盖等价类	期待输出	实际输出
T23（在T01基础上）	年龄：-20	(2)(5)	修改失败，年龄必须大于等于12岁	修改失败，年龄必须大于等于12岁
T24（在T01基础上）	年龄：100	(2)(6)	修改失败，年龄必须小于等于99岁	修改失败，年龄必须小于等于99岁
T25（在T01基础上）	年龄：aa	(2)(7)	修改失败，年龄存在非数字字符	修改失败，年龄存在非数字字符
T26（在T01基础上）	联系电话：333	(1)(8)	修改失败，请与请求的格式匹配	修改失败，请与请求的格式匹配
T27（在T01基础上）	联系电话：33333333aaa	(1)(9)	修改失败，请与请求的格式匹配	修改失败，请与请求的格式匹配
T28（在T01基础上）	年龄：20 联系电话：55555555555	(1)(2)	修改成功	修改成功

编号	测试输入	覆盖等价类	期待输出	实际输出
T29（在T09基础上）	价格：！	(4)(10)	修改失败，请输入一个数字	修改失败，请输入一个数字
T30（在T09基础上）	价格：-200	(4)(11)	修改失败，请填写规范的价格（不能为负数）	修改失败，请填写规范的价格（不能为负数）
T30（在T09基础上）	上课时间：14:00	(3)(12)	修改失败，请与请求的格式匹配	修改失败，请与请求的格式匹配
T31（在T09基础上）	上课时间：-4:00-16:00	(3)(13)	修改失败，请与请求的格式匹配	修改失败，请与请求的格式匹配
T32（在T09基础上）	上课时间：14:00-26:00	(3)(14)	修改失败，请与请求的格式匹配	修改失败，请与请求的格式匹配
T33（在T09基础上）	价格：120 上课时间：14:00-16:00	(3)(4)	修改成功	修改成功

删除功能

在课程信息管理的删除功能中有一个机制，被会员预约的课程无法删除，在这里有四个课程“拳击”“游泳”：瑜伽”“健美操“，其中“游泳”和”健美操“被预约了

编号	界面	测试输入	期待输出	实际输出
T34	用户信息管理	删除11	11用户信息被删除	11用户信息被删除
T35	用户信息管理	删除jaimy	jaimy用户信息被删除	jaimy用户信息被删除
T36	课程信息管理	删除游泳	该课程已被预约，无法删除	该课程已被预约，无法删除
T37	课程信息管理	删除拳击	拳击课程信息被删除	拳击课程信息被删除
T38	课程信息管理	删除瑜伽	瑜伽课程信息被删除	瑜伽课程信息被删除
T39	课程信息管理	删除健美操	该课程已被预约，无法删除	该课程已被预约，无法删除

查看预约情况

编号	测试输入	期待输出	实际输出
T40	查看张三	游泳、健美操课程信息	游泳、健美操课程信息
T41	查看李四	无	无

（3）会员信息管理

- 会员课程查询界面包括：全部课程查询、课程预约和取消预约。
- 个人信息界面显示包括：用户名、性别、年龄、联系电话、会员等级、修改联系方式和密码，修改联系电话和密码界面：联系方式、新密码（选填），密码可以显示输入。
- 我的课程界面包括：课程名、上课时间、年龄、预约时间。此界面只可显示不可更改。
- 其中已有输入要求与功能：修改联系电话和密码界面联系方式为必填，输入要求为11位数字，新密码可选填，新密码不可与原密码相同。

查询功能

编号	界面	测试输入	期待输出	实际输出
T01	会员课程查询	游泳	游泳课程信息	游泳课程信息
T02	会员课程查询	拳击	拳击课程信息	拳击课程信息
T03	会员课程查询	瑜伽	无课程信息	无课程信息
T04	会员课程查询	（空）	全部课程信息	全部课程信息

预约和取消预约功能

会员课程查询界面可预约未预约的课程和取消预约已预约的课程，预约课程将在“我的课程”界面显示课程基本信息，取消预约则不再显示该课程信息。

编号	界面	测试输入	期待输出	实际输出
T05	会员课程查询	预约游泳	预约成功、我的课程显示游泳课条目	预约成功、我的课程显示游泳课条目
T06	会员课程查询	预约拳击	预约成功、我的课程显示拳击课条目	预约成功、我的课程显示拳击课条目
T07	会员课程查询	取消预约游泳	取消成功、我的课程不显示游泳课条目	取消成功、我的课程不显示游泳课条目
T08	会员课程查询	取消预约健美操	取消成功、我的课程不显示健美操课条目	取消成功、我的课程不显示健美操课条目

修改联系方式和密码功能

有效密码限制：密码长度为6-20位，包含大写字母、小写字母、数字和特殊符号中的至少两种。

输入条件	有效等价类	无效等价类
输入信息是否有效	手机号 == 11位数字(1) 新密码有效且不与原密码相同(2)	手机号位数不等于11位(3) 手机号满足11位但含非数字字符(4) 新密码与原密码相同(5) 新密码长度小于6(6) 新密码长度大于20(7) 新密码含有字符类型少于2种(8)

编号	测试输入	覆盖等价类	期待输出	实际输出
T09	联系电话：11111222222 新密码：（空）	(1)	修改成功	修改成功
T10	联系电话：333 新密码：（空）	(3)	修改失败，请与请求的格式匹配	修改失败，请与请求的格式匹配
T12	联系电话：1111111111a 新密码：（空）	(4)	修改失败，请与请求的格式匹配	修改失败，请与请求的格式匹配
T13	联系电话：11111222222 新密码：1234	(1) (6)	密码长度必须为6-20位	密码长度必须为6-20位
T14	联系电话：11111222222 新密码：12345123451234512345 6	(1) (7)	密码长度必须为6-20位	密码长度必须为6-20位
T15	联系电话：11111222222 新密码：123456	(1) (8)	密码必须包含大写字母、小写字母、数字和特殊符号中的至少两种	密码必须包含大写字母、小写字母、数字和特殊符号中的至少两种
T16	联系电话：11111222222 新密码：1234aa	(1) (2)	修改成功	修改成功
T17（基于T16）	联系电话：11111222222 新密码：1234aa	(1) (5)	该密码与原密码一致，请重新填写	该密码与原密码一致，请重新填写

2. 性能测试

我们使用工具k6对网页进行综合性能测试，安装好k6后运行以下脚本，模拟大量用户访问，监控系统性能：

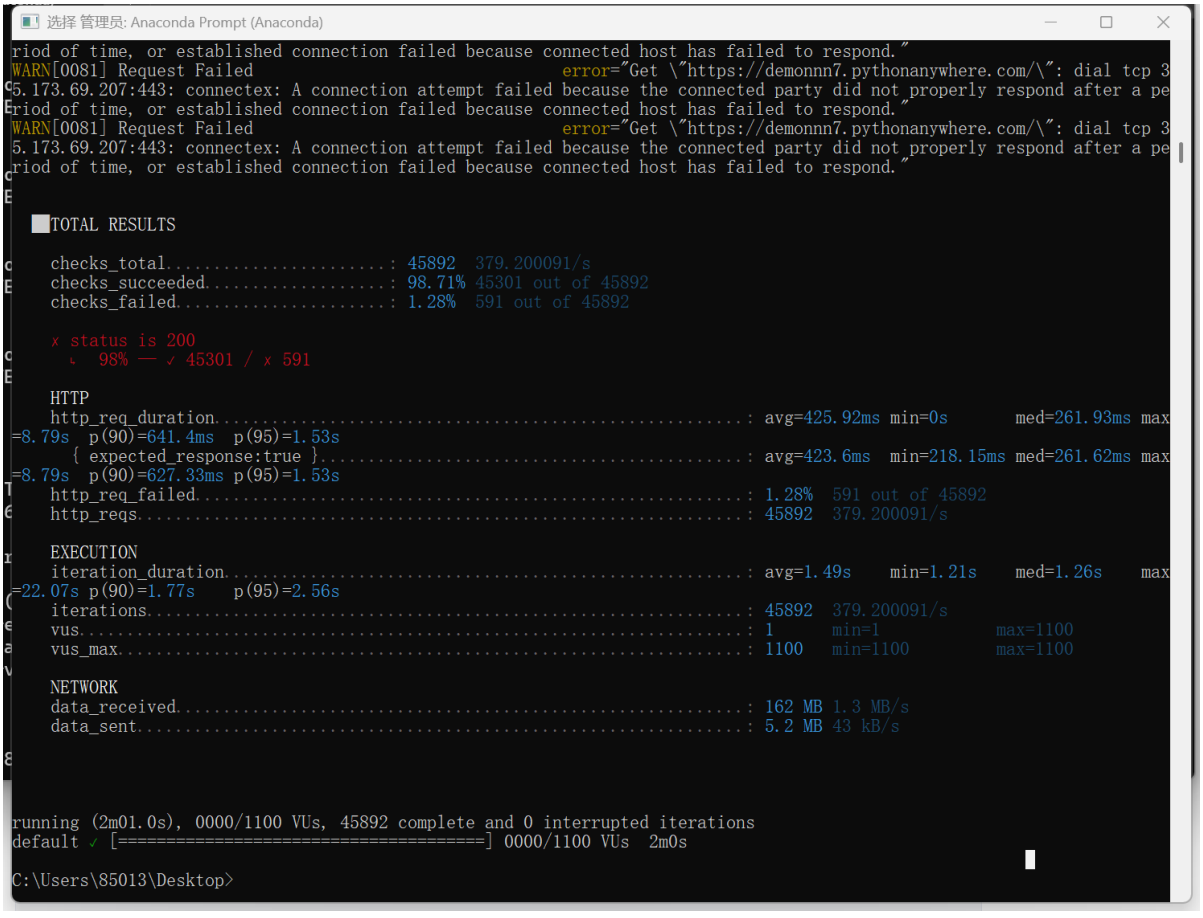
1分钟内访问用户逐渐增加到1000，之后1分钟内逐渐减少到0

```
import http from 'k6/http';
import { check, sleep } from 'k6';
```

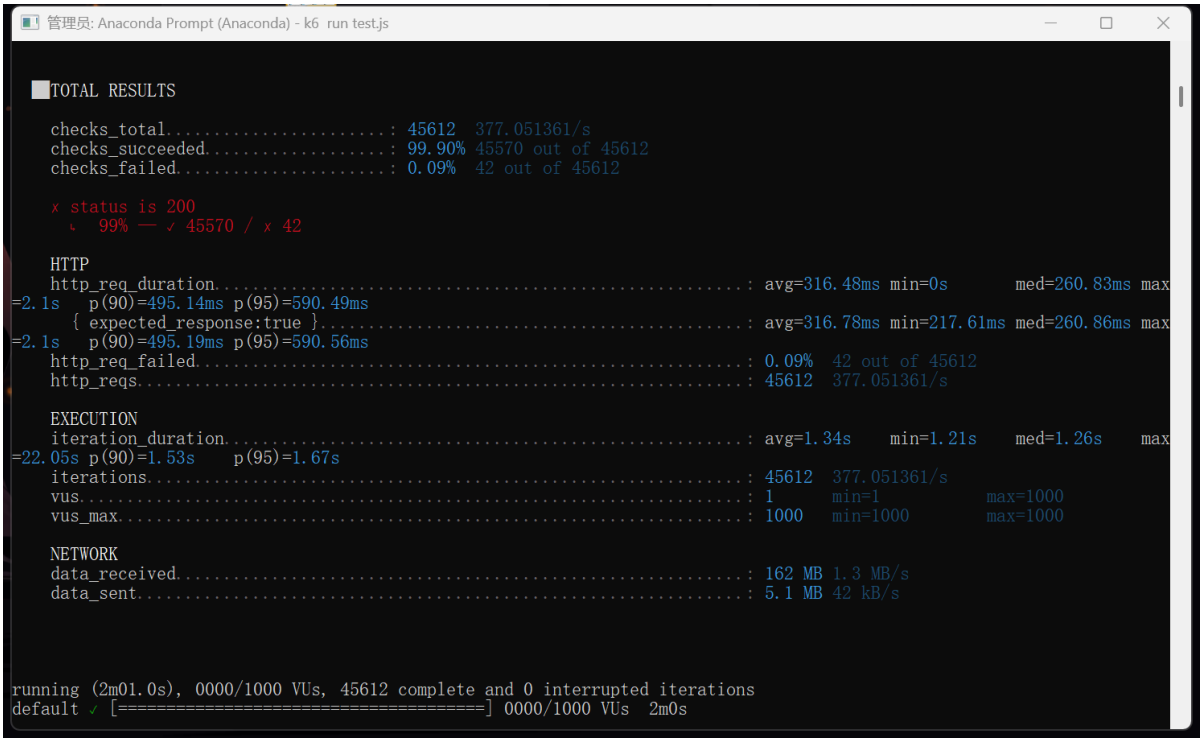
```
export let options = {
  stages: [
   { duration: '1m', target: 1000 },
   { duration: '1m', target: 0 },
 ],
};
export default function () {
  let res = http.get('https://demonnn7.pythonanywhere.com/');
  check(res, {
    'status is 200': (r) => r.status === 200,
 });
  sleep(1);
}
```

多次运行，我们发现请求成功占比平均约为98%-99.9%。且我们运行了用户分别为800、900、1100作为对比，800、900的所有请求均正常完成（避免篇幅过长这边不做展示），1100个用户请求完成率为98.71%，591条请求被拒绝。所以我们猜测网页并发上限约为950-1000。

1100用户输出如下：



1000用户输出如下：



针对上图的数据分析如下：

- 用户：1000；吞吐量：377.05请求/秒。系统能够支持高达 1000 个并发用户，且在高并发下仍能保持较高的迭代速率，说明系统在并发处理能力上表现良好。
- 总请求量(checks_total) 45612 次；成功请求(checks_succeeded) 45570 次（99.90%）；失败请求(checks_failed) 42 次（0.09%）。大部分请求成功返回，表明网页系统在高并发情况下能够稳定响应大部分请求，但有小部分响应会被拒绝，可能是因为达到并发用户上限的问题。
- 平均响应时间较短（316.48ms），90% 和 95% 响应时间均在 1 秒以内，说明大部分用户的体验较好，系统在高负载下仍能保持较好的性能，能够快速响应。最大响应时间为 2.1 秒，可能是由于个别请求的异常导致，说明网页负载有限，可能存在资源竞争或网络波动的问题。
- 数据流量：接收162MB（1.3MB/s），发送5.1MB（42kB/s）。数据传输量在合理范围内，表明网页系统在高并发下没有出现数据传输瓶颈。平均数据接收和发送速率表明系统能够高效处理请求和响应数据。
- 错误集中在测试后期（约63秒后），可能因服务器资源耗尽或网络拥塞导致连接超时。

3. 跨平台兼容性测试

PC端浏览器兼容性

- Windows 11系统：
  - Firefox (版本 116.0.3)：功能完整运行
  - Microsoft Edge (版本 136.0.3240.92)：功能完整运行
  - Google Chrome (版本 137.0.7151.69)：功能完整运行

移动端兼容性

- Android系统：
  - QQ浏览器 (版本 19.0.7.7031)：功能完整运行
  - 系统浏览器：功能完整运行
- iOS系统：

- Safari浏览器：功能完整运行
- 第三方浏览器(如Chrome for iOS)：功能完整运行

PC端测试详情

设备类型	操作系统	浏览器	运行效果
ROG Strix G513RM	Windows 11	Microsoft Edge	功能完整运行
XiaoxinAir 14ITL 2021	Windows 11	Google Chrome	功能完整运行

移动端测试详情

设备类型	操作系统	浏览器	运行效果
荣耀Magic4	Android 15	系统浏览器	功能完整运行
iPad Air5	iPadOS 18	Safari	功能完整运行
vivo S15	Android 14	系统浏览器	功能完整运行
HUAWEI P40	Harmony 4.2.0	系统浏览器	功能完整运行

4. 安全测试

1. 使用测试工具
   - 工具名称：OWASP ZAP (Zed Attack Proxy)
   - 版本号：[ZAP 2.16.1]
   - 测试时间：[2025.6.9]
2. 测试结果摘要

漏洞类型	风险等级	数量
Content Security Policy (CSP) Header未设置	Medium	6
缺少Anti-clickjacking Header	Medium	4
缺少反CSRF令牌	Medium	4
Cookie未设置SameSite属性	Low	1
X-Content-Type-Options Header缺失	Low	5
会话管理问题	Informational	2
身份验证问题	Informational	1

3. 测试结果分析
   - 中等风险漏洞14个（占比60.9%）
   - 低风险问题6个（占比26.1%）
   - 信息类提示3个（占比13%）

系统存在多个Web应用常见安全配置缺陷，虽无直接高危漏洞，但中等风险问题组合利用可能造成实质性危害。

4. 手工测试

    1. 登录界面测试（http://demonnn7.pythonanywhere.com/login）

    测试点：用户名输入框

测试用例	输入内容	系统反馈	测试结果
基础注入	`admin' --`	显示"用户名不存在"	防御成功
永真条件	`' OR '1'='1`	显示"用户名不存在"	防御成功
联合查询	`' UNION SELECT username, password FROM users --`	显示"用户名不存在"	防御成功
时间盲注	`admin' AND (SELECT pg_sleep(5)) --`	显示"用户名不存在"	防御成功

    2. 管理员用户信息管理界面测试（http://demonnn7.pythonanywhere.com/members）

测试点：会员名搜索框

测试用例	输入内容	系统反馈	测试结果
基础注入	`admin' --`	返回空结果集	防御成功
错误注入	`1 AND 1=CONVERT(int,(SELECT table_name FROM information_schema.tables)) --`	返回空结果集	防御成功
布尔盲注	`李四' AND (SELECT SUBSTRING(password,1,1) FROM users WHERE username='admin')='a' --`	返回空结果集	防御成功

    3. 会员个人信息修改界面测试（http://demonnn7.pythonanywhere.com/edit_profile）

测试点：联系方式修改框

测试用例	输入内容	系统反馈	测试结果
反射型XSS	`<script>alert(1)</script>`	提示请与请求格式匹配	防御成功
存储型XSS	`<img src=x onerror=alert(document.cookie)>`	提示请与请求格式匹配	防御成功
DOM型XSS	`javascript:alert(1)`	提示请与请求格式匹配	防御成功

4. 会员课程搜索界面测试（http://demonnn7.pythonanywhere.com/members）

测试点：课程搜索框

测试用例	输入内容	系统反馈	测试结果
基础注入	`' OR 1=1 --`	返回空结果集	防御成功
联合查询	`' UNION SELECT username, password FROM users --`	返回空结果集	防御成功
时间盲注	`游泳' AND (SELECT SLEEP(5)) --`	返回空结果集	防御成功

5. 管理员课程信息管理测试（http://demonnn7.pythonanywhere.com/view_courses）

测试点：课程名搜索框

测试用例	输入内容	系统反馈	测试结果
基础注入	`admin' --`	返回空结果集	防御成功
错误注入	`1 AND 1=CONVERT(int,(SELECT table_name FROM information_schema.tables)) --`	返回空结果集	防御成功
布尔盲注	`游泳' AND (SELECT SUBSTRING(password,1,1) FROM users WHERE username='admin')='a' --`	返回空结果集	防御成功

五、缺陷跟踪

缺陷编号	00001
标题	会员登录时出现报错页面
描述	在会员登录时，若输出不存在的用户或者输入错误密码，会出现报错页面“Internal Server Error”。应该改为出现密码错误或用户不存在提示。
优先级	高
报告人	谢宇桐
状态	已解决
解决人	余佳丽

缺陷编号	00002
标题	添加课程的时间、价格没有约束
描述	在添加课程的页面里，时间和价格可输入任何字符也可以为负，这不太符合规定，建议加入约束
优先级	中
报告人	谢宇桐
状态	已解决
解决人	余佳丽

缺陷编号	00003
标题	添加会员的年龄没有约束
描述	在添加会员的页面里，年龄可输入任何字符，不太符合逻辑，建议加入约束
优先级	中
报告人	谢宇桐
状态	已解决
解决人	余佳丽

缺陷编号	00004
标题	查询会员时会出现报错页面
描述	在查询会员课程的页面里，若查询不在会员列表里的其它用户名字，则会出现报错页面“Internal Server Error”。应该改为出现没有用户提示或者显示为空。
优先级	高
报告人	谢宇桐
状态	已解决
解决人	余佳丽

缺陷编号	00005
标题	删除课程时出现报错页面

缺陷编号	00005
描述	在删除被预约的课程时，因其被预约过所以有约束无法删除，但删除后出现报错页面“Failed to delete a course from the database”。应该改为出现课程已被预约无法删除提示。
优先级	高
报告人	谢宇桐
状态	已解决
解决人	余佳丽

缺陷编号	00006
标题	预约时间错误
描述	会员预约课程后显示预约时间与电脑时间相差八小时
优先级	高
报告人	许璟梵
状态	已解决
解决人	余佳丽

六、质量保证方法

为确保系统质量，本次测试采用了以下质量保证（QA）方法：

（1）测试驱动开发（TDD）

- 在开发关键功能模块时，先编写测试用例，再基于测试用例进行开发，确保代码逻辑符合预期。
- 通过自动化测试脚本k6持续验证系统稳定性。

（2）代码审查

- 使用静态代码分析工具检查代码质量，识别潜在的安全漏洞、代码冗余或性能瓶颈。
- 开发组进行代码审查，确保代码符合最佳实践，减少逻辑错误。

（3）缺陷管理与回归测试

- 使用缺陷跟踪系统记录、分类和跟踪所有发现的缺陷，确保每个问题都有明确的优先级、状态和修复责任人。
- 在修复缺陷后，执行回归测试验证修复效果，并确保新修改不会引入新的问题。

（4）用户验收测试（UAT）

- 在测试环境完成核心测试后，邀请其他同学（如管理员、普通会员）进行UAT测试，确保系统符合实际业务需求。
- 收集用户反馈，优化交互体验和功能逻辑。