信息安全保障人员（CISAW）认证考试大纲
渗透测试方向（基础级/专业级）

第一部分 考核目标与要求

依据《信息安全保障人员认证准则》，确定信息安全保障人员认证（CISAW）渗透测试方向的考试目标和要求。

信息安全保障人员认证（CISAW）渗透测试方向的考试主要考查考生对渗透测试基础知识、基本技能掌握程度和综合运用所学知识分析、解决问题的能力。

第二部分 对知识内容的要求层次

1.了解：要求对所列知识的含义有初步的、感性的认识，知道这一知识内容是什么，按照一定的程序和步骤照样模仿，并能(或会)在有关的问题中识别和认识它。

2.理解：要求对所列知识内容有较深刻的理性认识，知道知识间的逻辑关系，能够对所列知识做正确的描述说明并表达，能够利用所学的知识内容对有关问题进行比较、判别、讨论，具备利用所学知识解决简单问题的能力。

3.综合应用：要求能够对所列的知识内容进行推导证明，能够利用所学知识对问题进行分析、研究、讨论，并且加以解决。

第三部分 能力要求

本考试主要考查考生推理论证能力、实践操作能力和综合应用能力，具体能力要求如下：

1.推理论证能力：考生应具有渗透测试技术方案与实施方案的设计、漏洞修复方案的制定、人工智能安全等方面的综合能力。

2.实践操作能力：考生应具有渗透测试所需安全技能中的实际操作能力，例如信息收集工具的使用，Web 应用漏洞扫描器的使用，漏洞利用工具的使用及常见漏洞的挖掘等能力。

3.综合应用能力：考生应具有渗透测试前期交互、信息收集、漏洞扫描、漏洞挖掘、漏洞利用等几个阶段所需技能的综合应用与把控能力。例如，能够理解渗透测试流程与方法，具备综合利用管理措施和技术手段实施安全服务项目的能力。

第四部分 考试内容

知识内容		要求
渗透测试概述	渗透测试概念、流程与思路，渗透测试服务的基本介绍。	理解
	网络安全法与渗透测试职业道德规范。	理解
	Web 服务器运作原理。	理解
	Web 应用程序常见的编码方式。	理解
	HTTP 协议报文格式、请求方法、状态码。	理解
	本地攻击环境搭建的方法。	理解
	BurpSuite 与 Firefox 插件的使用。	理解
信息收集	信息收集工具使用，包括 Google Hacking、网络空间搜索引擎、Nmap。	理解
	域名信息收集的方法与手段。	综合应用
	服务器信息收集的方法与手段。	综合应用
	Web 应用信息收集收集的方法与手段。	综合应用
漏洞扫描	漏洞扫描流程与方法。	理解
	漏洞扫描工具的基本使用，包括 AWVS、Nessus。	综合应用
渗透测试技术	WebShell 原理与 WebShell 管理工具基本使用。	理解
	文件上传漏洞的原理、漏洞利用、防护和绕过的手段与方法。	综合应用

	XSS 漏洞的原理、漏洞利用、防护的手段与方法。	综合应用
	CSRF 漏洞的原理、漏洞利用、防护的手段与方法。	理解
	SQL 漏洞的原理、漏洞利用、防护的手段与方法。	综合应用
	SQLMAP 工具的基本使用。	理解
	代码执行漏洞的原理、漏洞利用、防护的手段与方法。	理解
	命令执行漏洞的原理、漏洞利用、防护的手段与方法。	理解
	反序列化漏洞的原理、漏洞利用、防护的手段与方法。	综合应用
	对常见身份认证场景的攻击手段与方法。	综合应用
	越权的原理、漏洞利用的手段与方法。	综合应用
	逻辑漏洞常见场景的漏洞挖掘、利用的手段与方法。	理解
	SSRF、XXE、文件包含等漏洞的原理、漏洞利用、防护的手段与方法。	综合应用
	常见中间件漏洞利用及检测方法。	理解
	主机与数据库漏洞利用及检测方法。	理解
人工智能安全	AI 大模型的身份安全、应用安全、模型安全、数据安全等风险。	了解
	LLM 的 top10 风险，包括提示注入、训练数据投毒、拒绝服务攻击等。	了解
	提示词攻击的多种手段与方法，包括角色扮演、指令篡改、场景设计、词语替换等。	了解
	人工智能在网络安全中的帮助和应用，智能体构建思路与方法。	了解

第五部分 试卷满分及考试时间

笔试试卷满分 70 分，上机实操考试满分 50 分，总分 120 分。考试时间为 2.5 小时，84 分（含）为合格分。如考生有作弊行为则该考生最终成绩为 0 分。

考生最终总考试成绩为“合格”的，可根据《信息安全保障人员认证准则》相关要求，被授予基础级或专业级认证证书。

第六部分 试卷内容结构

笔试试卷内容

知识类型	占比（%）
渗透测试概述	9%
信息收集	9%
漏洞扫描	3%
渗透测试技术	57%
人工智能安全	22%

上机实操内容

知识类型	占比（%）
信息收集	20%
漏洞扫描	10%
渗透测试技术	70%

渗透测试概述占比 9%，信息收集占比 9%，漏洞扫描占比 3%，渗透测试技术占比 57%，人工智能安全占比 22%。（按笔试机考填进去）

第七部分 答题方式

笔试加上机实操考试闭卷独立完成。

第八部分 试卷题型结构

单选题 30 题，每小题 1 分，共 30 分;

多选题 10 题，每小题 2 分，共 20 分;

简答题 2 题，每小题 10 分，共 20 分;

实操小题 6 题，每小题 5 分，共 30 分;

综合实操 2 题，每小题 10 分，共 20 分。

第九部分 例题

一、单选题

1、以下关于 SQLMap 描述正确的是？（B）

A. SQLMap 是一个自动化 WEB 漏洞扫描器，能够发现基本的 WEB 漏洞

B. SQLMap 是一个自动化 SQL 注入工具

C. SQLMap 是一个脚本语言

D. SQLMap 是基于 JAVA 的

说明：本题考查 SQLMap 工具基本知识，属于了解的知识。SQLMap 是一个开源的渗透测试工具，基于 Python 进行开发，可以用来进行自动化检测和利用 SQL 注入漏洞，获取数据库服务器的权限。

二、多选题

1、在 WEB 应用攻击中，（ABC）不是对客户端进行攻击的手段是？

A. 暴力破解

B. 代码执行漏洞

C. SQL 注入攻击

D. 跨站脚本攻击

说明：本题考查的是对于 Web 应用漏洞的原理理解，属于掌握的知识。跨站脚本攻击是通过利用网页开发时留下的漏洞，通过巧妙的方法注入恶意指令代码到网页，使用户加载并执行攻击者恶意制造的网页程序。

三、简答题：

1、发现 lpt.aspx?id=1 存在 SQL 注入，你有哪几种思路获取 webshell。

答：

(1)使用 xp_cmdshell 执行系统命令。

(2)使用差异备份拿 Shell。

(3)使用 log 备份拿 Shell。

(4)通过查询管理员的账户和密码，然后扫后台登录后台，再在后台通过等方法 getshell。

说明: 本题考察的是 SQL 注入漏洞的利用思路,属于综合应用的知识。渗透测试中极其容易发现 SQL Server 数据库的 SQL 注入漏洞，扩大攻击面就必须通过各种利用方式尝试获得 Shell。

四、实操小题:

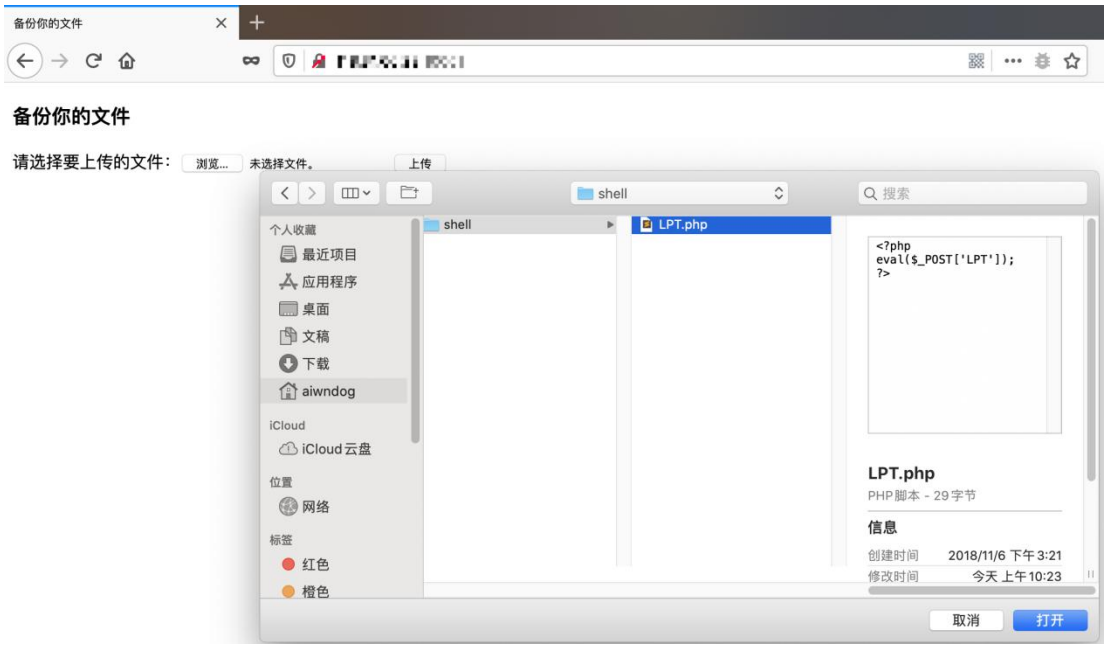
题目名称: 简单的上传

题目描述: 发现了一个文件上传点，不过这个上传点好像有缺陷。尝试利用这个上传功能拿下目标服务器权限，flag 信息就在服务器的根目录下。靶机地址: http://IP:PORT

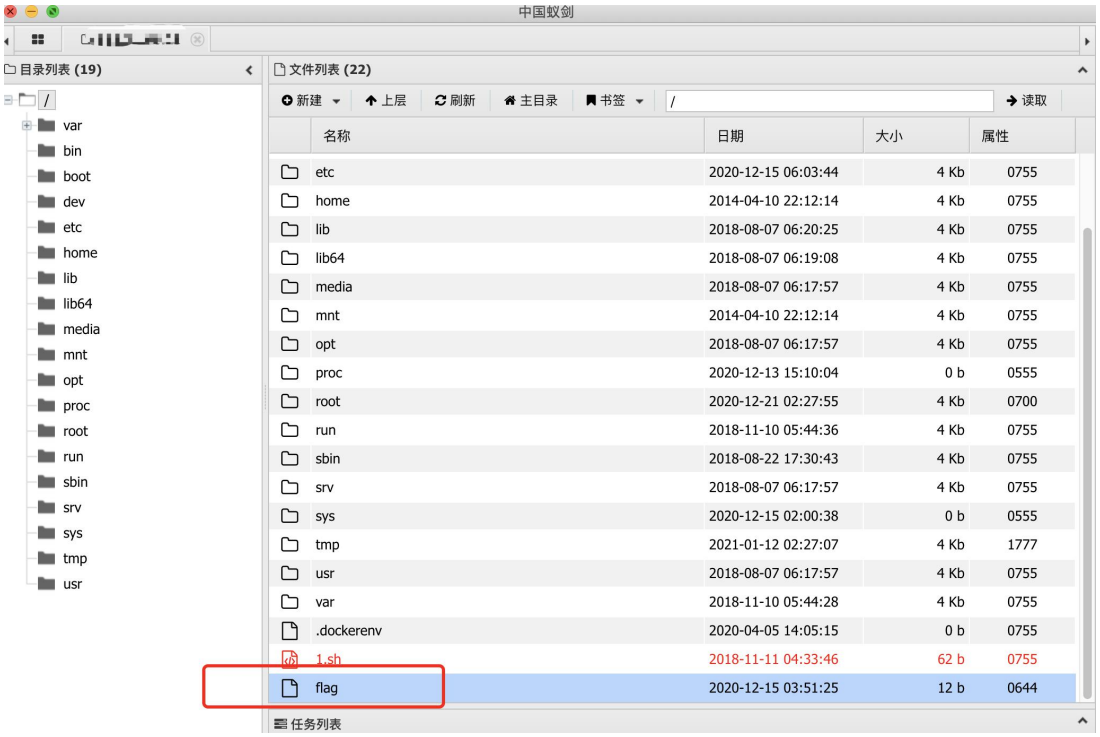
说明: 本题考察的是渗透测试技术中的文件上传漏洞的原理、漏洞利用、防护和绕过的手段与方法，属于综合应用的知识。文件上传漏洞是渗透测试中的常见漏洞，也是实际影响较大的漏洞，在渗透测试实施过程中对该类型的漏洞发现与利用是渗透测试人员应具备的基本能力。

解题步骤

1、访问目标站点，利用上传功能上传 Webshell



2、根目录下找到 flag，确认相关格式为正确答案后提交



五、综合实操题

题目名称：博客站点实战

题目描述：发现了博客站点，不过这个站点拥有大量缺陷。尝试组合利用各种漏洞拿下目标服务器权限，flag 信息就在服务器的根目录下

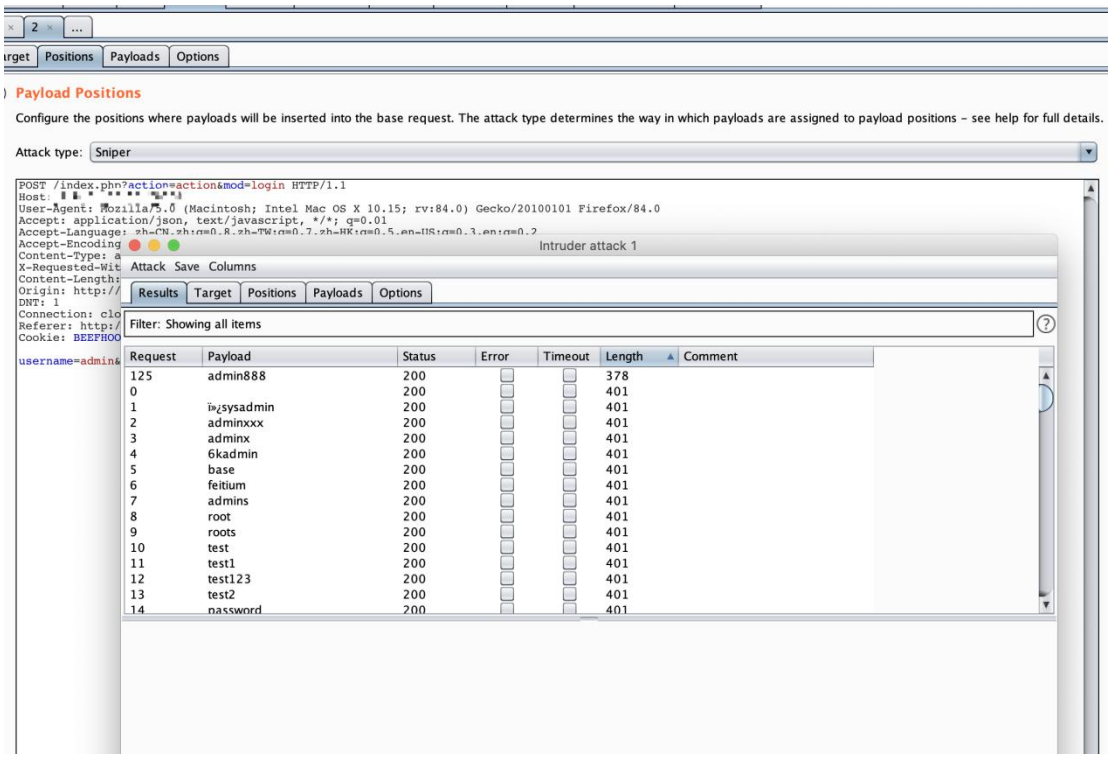
靶机地址：http://IP:PORT

说明：本题考综合考察了信息收集与渗透测试技术中的多个知识点，包括属于需要能够综合应用的信息收集工具使用，包括 Google Hacking、网络空间搜索引擎、Nmap；Web 应用信息收集收集的方法与手段；对常见身份认证场景的攻击手段与方法；文件上传漏洞的原理、漏洞利用、防护和绕过的手段与方法。在实际渗透环境中，除了单点漏洞的利用外，很多时候还需要渗透测试人员针对不同的业务场景能够思考不同的渗透思路，收集更多的信息进行多样化利用，利用各种综合手段完成渗透测试工作。

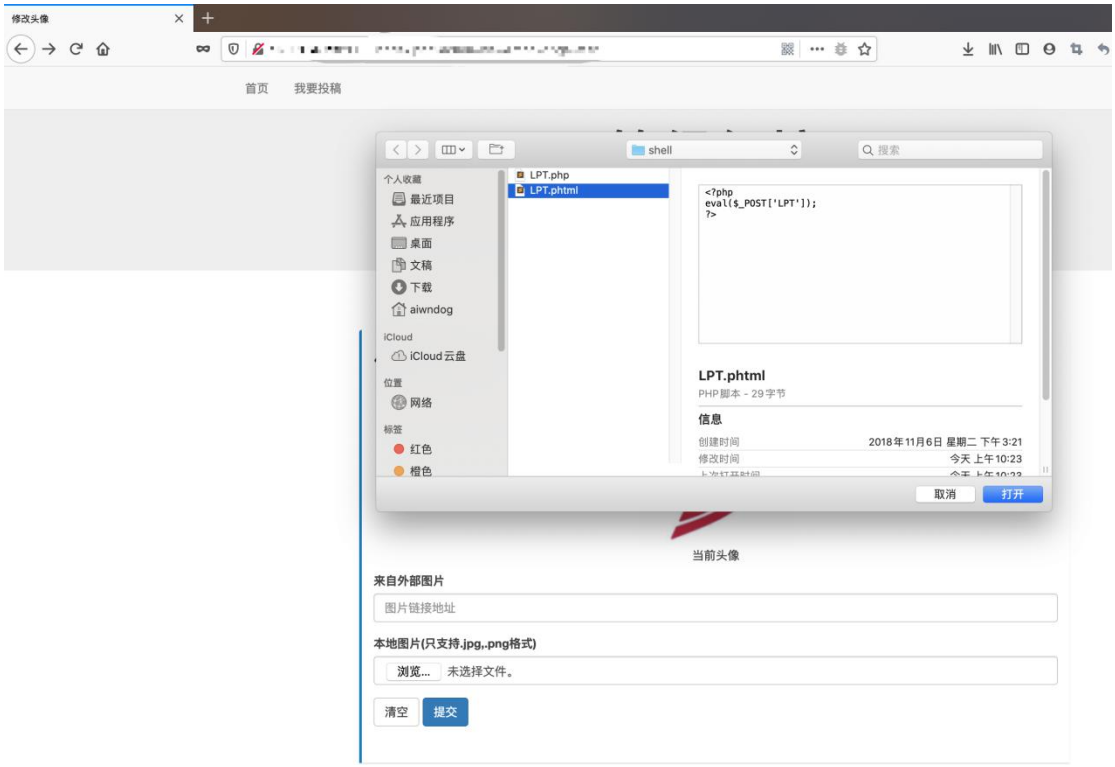
1、 访问目标站点进行信息收集，通过发现文章作者为 admin

2、通过后台扫描发现除了 phpinfo 的泄漏，暂时没有发现有用信息

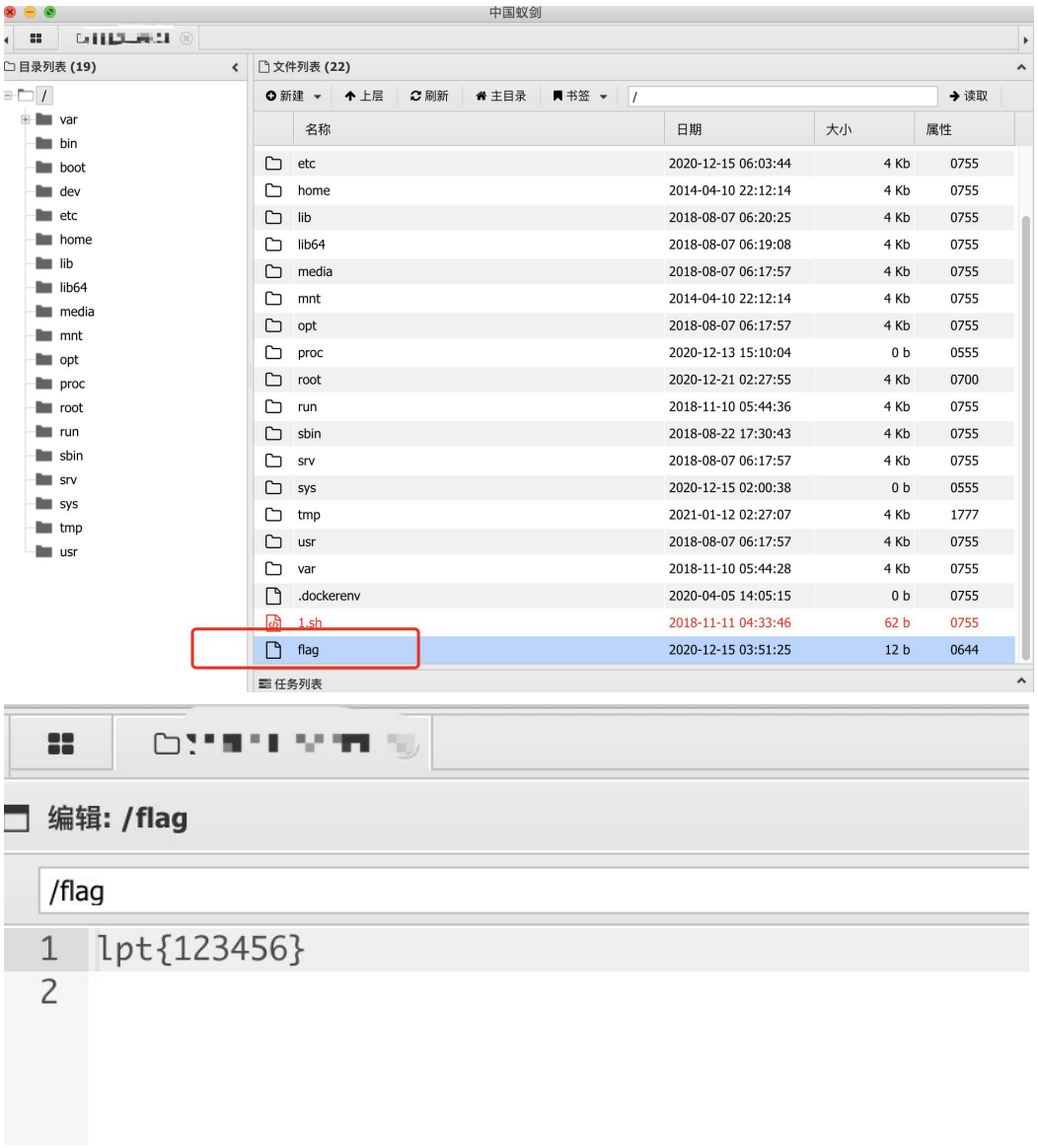
3、基于之前的管理员账号，使用 Burp Suite 尝试登录入口爆破，找到管理员密码



4、登录后台，使用头像修改处，使用特殊后缀绕过限制拿到 Webshell



5、根目录下找到 flag，确认相关格式为正确答案后提交


中国蚁剑
目录列表 (19)
/
var
bin
boot
dev
etc
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
文件列表 (22)
新建
上层
刷新
主目录
书签
/
读取
名称
日期
大小
属性
etc 2020-12-15 06:03:44 4 Kb 0755
home 2014-04-10 22:12:14 4 Kb 0755
lib 2018-08-07 06:20:25 4 Kb 0755
lib64 2018-08-07 06:19:08 4 Kb 0755
media 2018-08-07 06:17:57 4 Kb 0755
mnt 2014-04-10 22:12:14 4 Kb 0755
opt 2018-08-07 06:17:57 4 Kb 0755
proc 2020-12-13 15:10:04 0 b 0555
root 2020-12-21 02:27:55 4 Kb 0700
run 2018-11-10 05:44:36 4 Kb 0755
sbin 2018-08-22 17:30:43 4 Kb 0755
srv 2018-08-07 06:17:57 4 Kb 0755
sys 2020-12-15 02:00:38 0 b 0555
tmp 2021-01-12 02:27:07 4 Kb 1777
usr 2018-08-07 06:17:57 4 Kb 0755
var 2018-11-10 05:44:28 4 Kb 0755
.dockerenv 2020-04-05 14:05:15 0 b 0755
1.sh 2018-11-11 04:33:46 62 b 0755
flag 2020-12-15 03:51:25 12 b 0644
任务列表

编辑: /flag
/flag
1 lpt{123456}
2