# 场景说明

| 场景名称 | LeptonCMS 安全部署与数据保护 |
| --- | --- |

## 1. 场景描述

在数字世界的阴影中，一个名为“LeptonCMS”的网站曾经是万众瞩目的焦点，其稳固的外表隐藏了无法忽视的数字风险。

一天，当数据安全团队正在分析检查网站时，他们发现了网站公布的数据未进行数据脱敏。导致用户的个人信息和敏感数据如同城墙崩溃般被窃取，并成为了黑客攻击的目标，大量客户信息，包括姓名、身份证号、邮箱等。这些数据被迅速传播到黑市上，成为了其他犯罪活动的工具。企业的声誉受到了严重损害，客户们的信任也遭受了沉重打击。

与此同时，企业网站遭受了来自黑客的持续攻击，导致服务器负载剧增。由于未经优化的 Apache 配置，服务器在处理大量并发请求时陷入了困境，网站响应速度急剧下降。这给黑客提供了进一步渗透系统的机会。

在数据安全团队的持续监控下，他们发现了一些潜在的网站漏洞。黑客们利用这些漏洞成功地获取了服务器的 shell 权限，进而对企业系统进行了全面的入侵。他们窃取了更多的数据，甚至篡改了网站的内容，给企业带来了巨大的损失和混乱。

最终，企业不得不关闭了受到严重攻击的网站，并要求数据安全团队进行了全面的系统重建和加固。这次事件给企业带来了沉重的教训，也让网络安全团队深刻意识到了安全防护的重要性。他们深入分析了事件的起因，并采取了一系列措施来加强企业的网络安全，以防止类似事件再次发生。

要求搭建服务的相关组件及版本如下：

| | | |
|---|---|---|
| 基本信息 | 操作系统 | Ubuntu20.04 |
| | 中间件 | Apache/2.4.41 |
| | 数据库 | mysql5.7 |
| | 应用名称 | Leptoncms（附件提供，通过平台附件下载） |
| | 应用语言 | PHP 8.1 |

注意:（

1、禁止使用集成化搭建平台，包括但不限于：lmap、lmnp、小皮、宝塔等。

2、SSH 服务用户 root 的密码不允许修改，保证提供的默认用户名密码能够登录，否则将无法检测。）

## 2. 场景

### 考题 1

请选手在当前提供的 Ubuntu 系统上安装部署 LeptonCMS。

1、要求服务端口设置为 8081，并确保当前应用正常访问(默认路径)、功能正常使用。

2、 要求设置当前 cms 后台登录用户名为：admin、密码为：SSH 登录密码。

### 考题 2

在搭建当前网站时，运维人员突然收到业务部门通知，发现默认 Apache 的并发不足以满足业务要求，因此需要将 Apache 的最大并发进程数设置为 300。

要求：使用 Prefork MPM 模块

### 考题 3

数据脱敏是一种对敏感信息进行保护的重要方法。通过应用特定规则，脱敏

可以对个人隐私、金融财务、商业机密等敏感信息进行变形处理，以确保数据安全和隐私保护。运维人员在官网公布招聘人员信息时未经脱敏导致大量人员信息泄露。为了解决这一问题，您需要按照以下脱敏规则进行数据脱敏。请将脱敏后的数据结果输出到 page 目录下的文件中，并将文件名称设置为 md.txt。（该文件正确脱敏后的最终 md5 值：9184**********71c9，该值为脱敏正确的判断依据，供选手校验）

- 页面展示文件 http://IP/page/gonggao.php
- 脱敏规则如下：

对于姓名、身份证号和邮箱的脱敏规则如下：

- **姓名**：如果姓名是三个字符长，则保留第一个字符和最后一个字符，中间用一个星号替换。否则，保留第一个字符，其他字符用星号替换。
- **身份证号**：保留前六位和最后两位字符，中间的字符用星号替换。
- **邮箱**：保留邮箱用户名的第一个字符以及@符号前的字符，其他字符用星号替换。
- 请将脱敏的 10000 条数据按照以下格式进行拼接,所有拼接数据不要有换行符（每条脱敏后的数据以管道符“|”进行拼接）。样例如下：

姓名: 焦*梅, 身份证号码: 411600**********35, 邮箱: q**n@example.net|姓名: 张*, 身份证号码: 422802**********84, 邮箱: f*****n@example.net|姓名: 昝*强, 身份证号码: 532532**********37, 邮箱: y****e@example.net

## 考题 4

通过企业内部安全审计的结果表明该 cms 存在任意文件上传漏洞，请选手通过技术手段发现该 cms 存在的漏洞并修复（修复过程确保所有功能点正常）。