SERVER SECURITY CHECKLIST

服务器安全防护清单

面向公网的三站点部署 · 个人网站 / 宣传部工作台 / 西联素材库 · 复核日期 2026-11-08

> 本清单已脱敏：不包含服务器地址、管理入口、账号与密码等可被利用的信息。

3	3	4	14
公网站点	公网开放端口	fail2ban 防护层	天备份保留

01 网络边界

措施	实际配置
CDN 前置代理	主站接入 Cloudflare：DDoS 流量清洗、WAF 规则、隐藏源站地址、边缘缓存；两个实时工具站直连以保证低延迟。
主机防火墙	UFW 默认拒绝所有入站，公网仅放行 SSH / 80 / 443；SSH 连接启用频率限制。
管理面板隔离	运维面板不对公网开放，只能通过 SSH 隧道访问，并叠加自定义安全入口与 User-Agent 校验。
默认拒绝	nginx 默认站点返回 444：直接访问 IP、扫描 `.env` / `.git` / `*.php` 等路径一律断开连接（已实测）。
SSH 加固	仅允许密钥登录，密码登录已关闭，单次连接最多 3 次认证尝试。
入侵防护	fail2ban 四层 jail：SSH 爆破、目录扫描（封 24 小时）、接口限流触发（封 1 小时）、惯犯累进封禁。

02 传输加密

措施	实际配置
全站 HTTPS	三个域名全部启用 HTTPS，HTTP 请求 301 跳转；仅保留 TLS 1.2 / 1.3。
证书管理	Let's Encrypt 证书，覆盖全部子域，certbot 定时器每日自动续期；当前有效期剩余 89 天。
回源校验	CDN 回源采用 Full (strict) 模式，强制校验源站证书，防止中间人冒充。
HSTS	`max-age=31536000; includeSubDomains`，杜绝协议降级攻击。
安全响应头	`X-Content-Type-Options`、`X-Frame-Options`、`Referrer-Policy`、`Permissions-Policy`、`Content-Security-Policy` 全部下发。

03 账号与会话

项目	实现方式
密码哈希	Node 端 **scrypt**（N=16384, r=8, p=1，64 字节）；Python 端 **PBKDF2-HMAC-SHA256**，12 万轮迭代。
独立加盐	每个账号 16 字节随机盐，同一密码在不同账号下的哈希完全不同。
存储内容	数据库仅保存「盐 + 哈希」，不存在任何明文密码字段。
登录凭证	32 字节随机 token；服务端只保存其 SHA256；7 天有效期并支持滑动续期。
会话 Cookie	`HttpOnly` + `Secure` + `SameSite=Lax`。
暴力破解防护	登录接口 6 次/分钟限流；同一来源 10 分钟内失败 8 次即锁定，叠加 fail2ban 封禁。
未授权访问	所有数据接口强制登录，未登录统一返回 401，无法列举目录或下载文件（已实测）。

04 应用层防护

措施	实际配置
接口鉴权	素材列表、原文件、缩略图、下载、打包接口全部要求有效会话。
SSRF 防护	外链素材仅允许 http / https 且必须是公网地址；重定向逐跳校验，超时 10 秒，单图上限 20MB。内网段、回环、link-local、`file://`、`gopher://` 均实测拦截。
上传限制	素材分片上传单文件上限 2GB，JSON 请求体 4MB，头像仅限 png/jpg/gif/webp 且 ≤4MB，文件名统一清洗。
路径穿越	静态文件与存储路径均校验绝对路径前缀，阻断 `../` 穿越。
脚本注入	全站 `nosniff`；SVG 不内联预览；用户内容输出前统一转义；CSP 限制脚本仅同源。
限流与并发	普通 API 每 IP 20 次/秒（burst 40），登录单独 6 次/分钟；单 IP 并发 30，分片上传不受限流影响。
外链素材	仅缓存缩略图与播放副本，原文件由网盘直链提供；地址插入页面前统一转义。

05 主机与数据

措施	实际配置
文件权限	配置文件、数据库、密钥环境文件均为 600，仅 root 可读；备份目录 700。
自动补丁	unattended-upgrades 自动安装安全更新，已启用开机自启。
入侵检测	rkhunter 每周扫描 rootkit；数据库完整性检查结果为 **ok**。
自动备份	每日 03:30 增量快照（硬链接去重，保留 14 天）；03:40 单独备份数据库；每小时检查磁盘使用率。
维护任务	每日清理过期会话、邀请码、临时上传与到期回收站内容；每 6 小时巡检残留账号。
日志与告警	访问日志与错误日志分离，fail2ban 实时读取认证日志；磁盘使用率超过 85% 写入告警日志。

06 本次复核结果

- ✓ **接口鉴权** 未登录访问素材接口返回 401
- ✓ **扫描路径** .env / .git / .php 均直接断开
- ✓ **数据隔离** 未登录读取业务数据被拒绝
- ✓ **限流** 连续 50 次正常请求未被误伤
- ✓ **防火墙** UFW 与 SSH 加固策略生效
- ✓ **证书** 剩余 89 天，自动续期正常
- ✓ **IP 直连** 直接访问服务器地址被拒绝
- ✓ **SSRF** 五类内网与非法协议全部拦截
- ✓ **登录防护** 错误密码 401 并触发限流
- ✓ **响应头** 六个安全响应头全部齐全
- ✓ **fail2ban** 4 个 jail 正常，当前封禁 0
- ✓ **备份** 脚本执行成功，快照可读取

07 持续改进

- 应用进程目前以 root 运行，后续计划降权到专用系统用户，进一步缩小被利用后的影响面。
- 备份与源数据位于同一块磁盘，后续计划增加异地或对象存储副本，避免单盘故障导致数据同时丢失。
- 运维面板保持不对公网开放，如需使用仍走 SSH 隧道。
- 投稿入口当前对外开放，如出现滥用可随时在配置中关闭匿名投稿。