phpok任意文件上传(CVE-2018-12491)

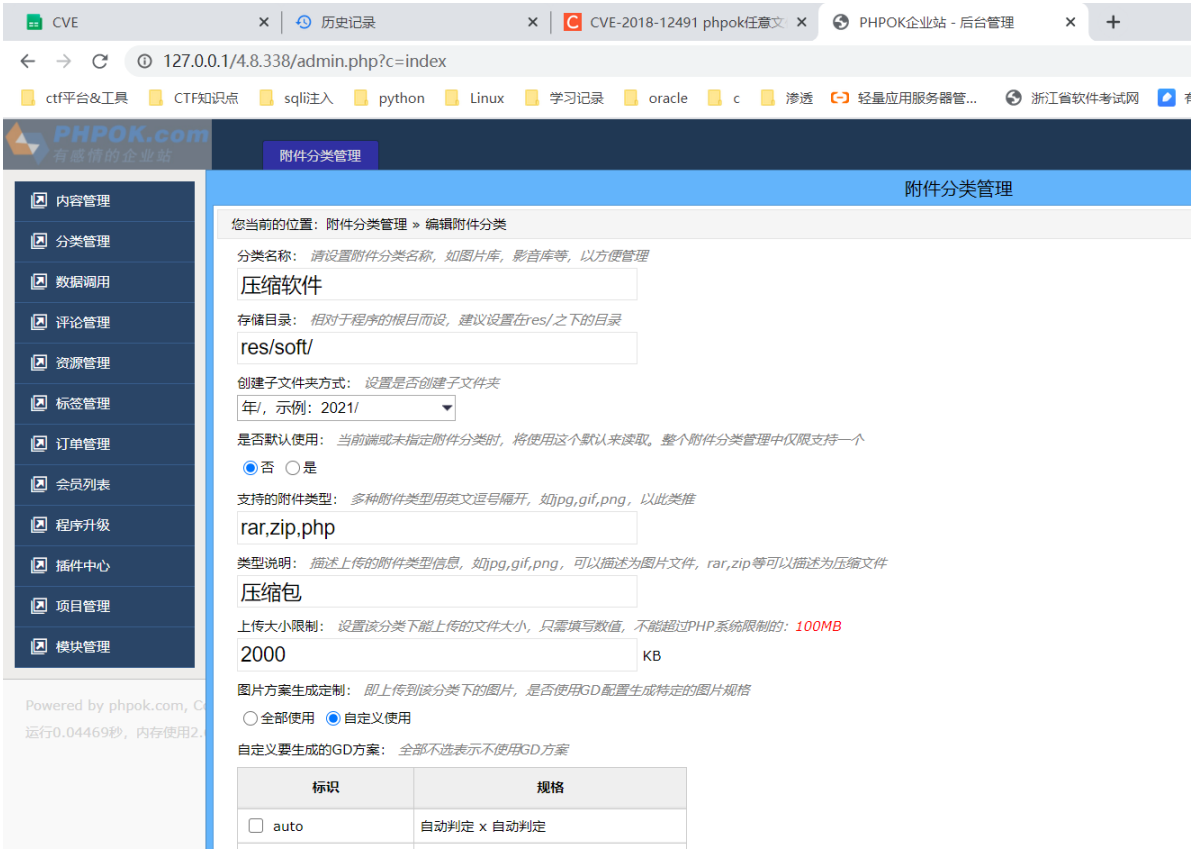
漏洞简介

phpok是一套采用PHP+MySQL开发的企业网站系统，其4.8.338及4.9.015版本存在任意文件上传漏洞，攻击者可利用漏洞上传任意文件，获取网站权限。

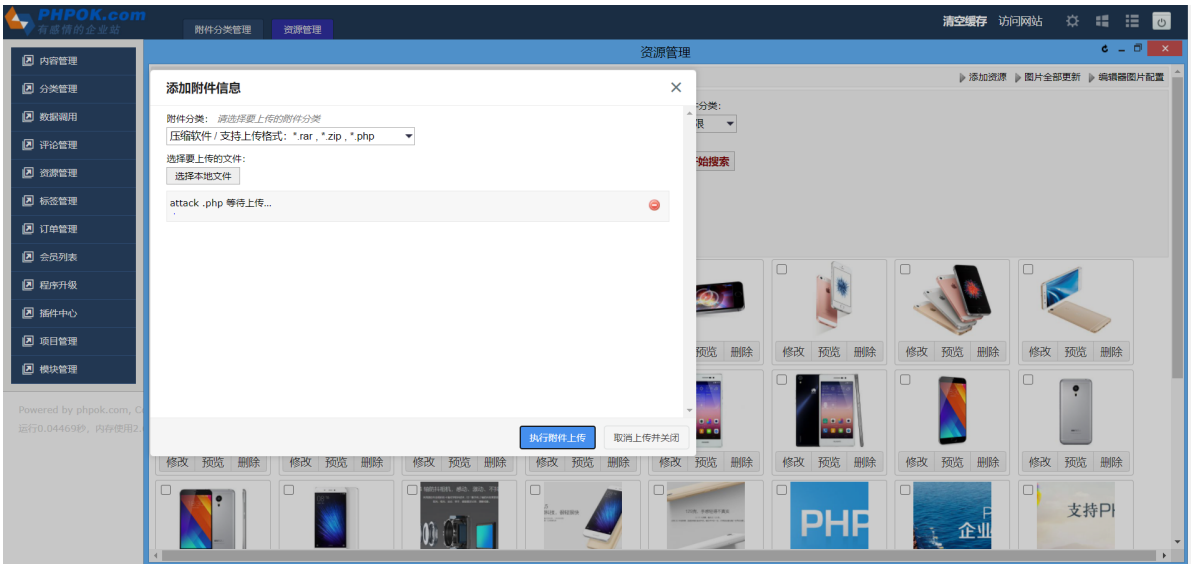
漏洞复现

访问 https://download.phpok.com/4.8.338.zip 下载源码，将其解压到phpstudy的网站根目录中。根据提示安装，安装完成后，访问管理员登录页面 http://127.0.0.1/4.8.338/admin.php?c=login

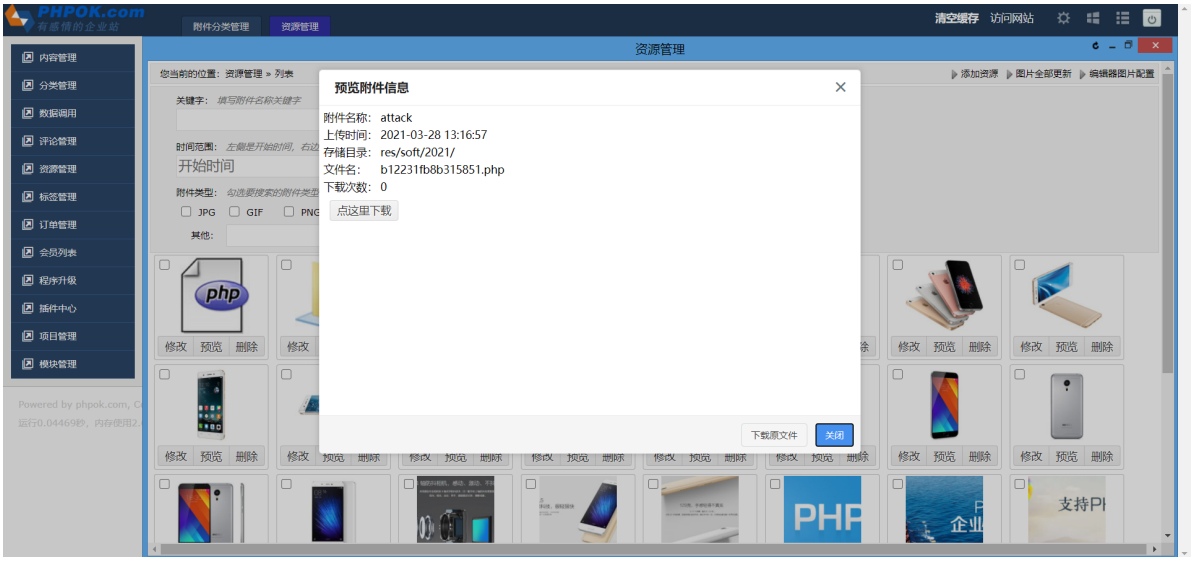
管理员登录后，可以在附件分类管理工具中编辑压缩软件，将.php添加为支持的附件类型。



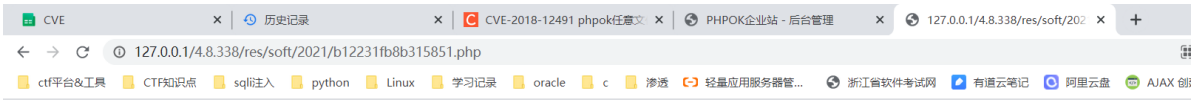
点击提交按钮，成功修改后，就可以在资源管理模块中添加资源，选择附件类型为压缩软件这时就可以上传php木马了。



可以看到php木马文件成功被上传了，可以点击预览查看其详细信息，获得其文件路径与文件名。



访问 http://127.0.0.1/4.8.338/res/soft/2021/b12231fb8b315851.php ，访问成功。



利用蚁剑进行连接，成功获得WebShell。