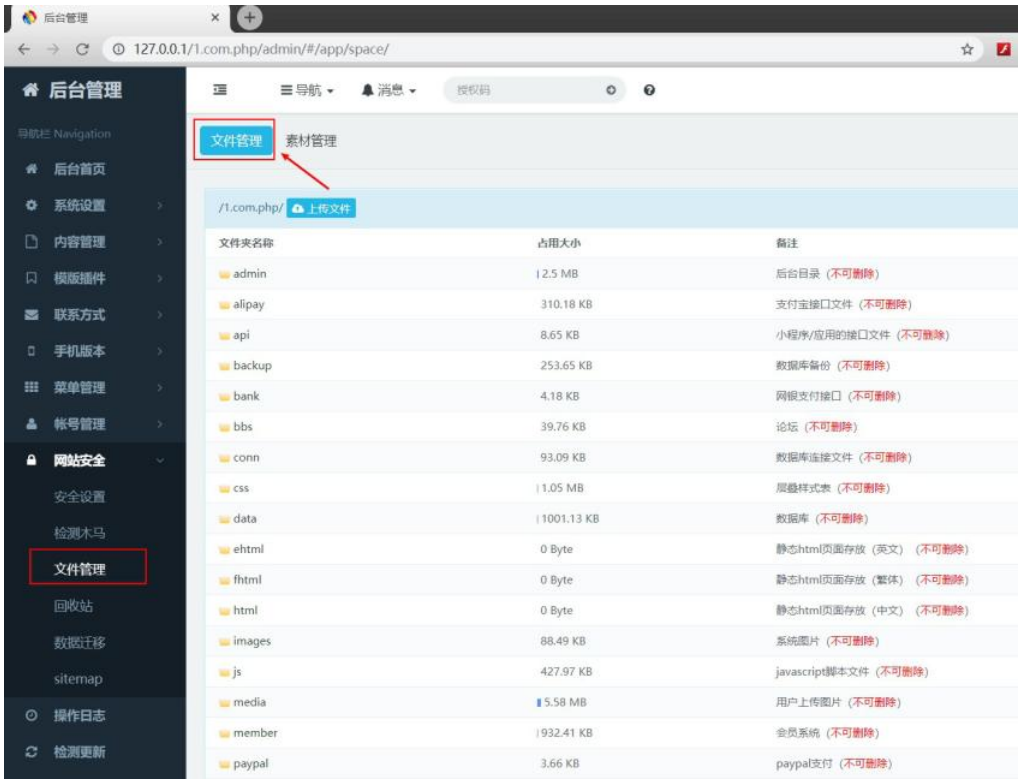
S-CMS(PHP enterprise edition)v3.0 backstage getshell

S-CMS PHP v3.0 Remote code execution vulnerability

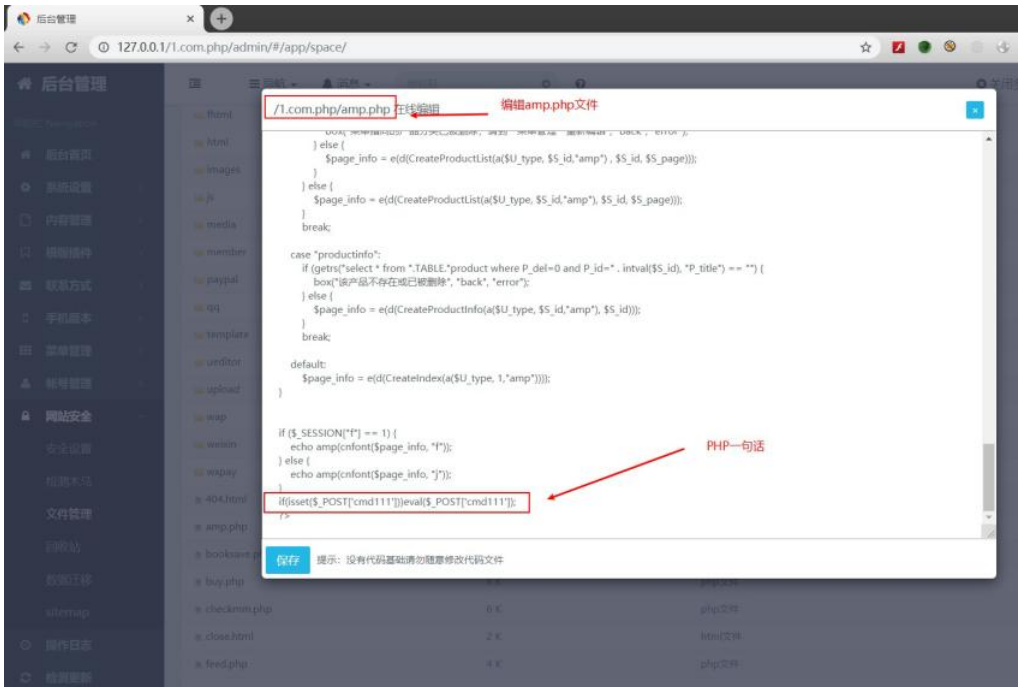
The attacker login to the system backstage management page, can attack the server through the PHP one-sentence Trojan horse, obtain the control authority of the server, seriously threaten the security of server assets, and this CMS belongs to the commercial, the influence range is very wide.

exploit

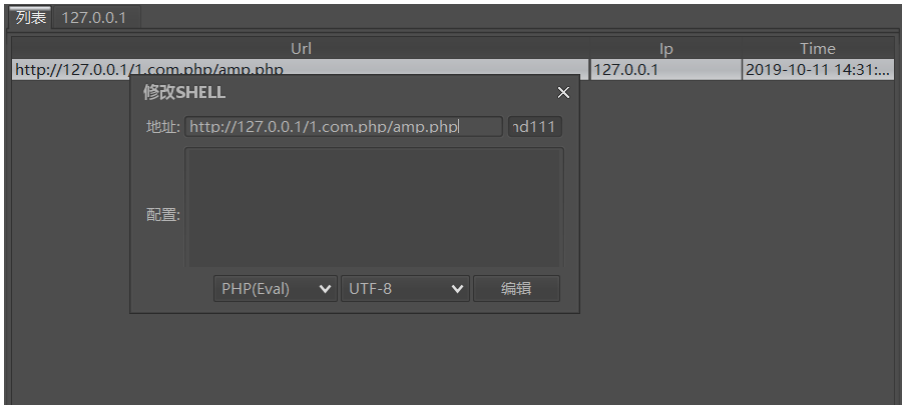
1.When using an administrator's account to entry the backstage web page, users could modify any documents of Document Management in the program of Website Safety，lead to Remote code execution vulnerability. (as shown in illustration)

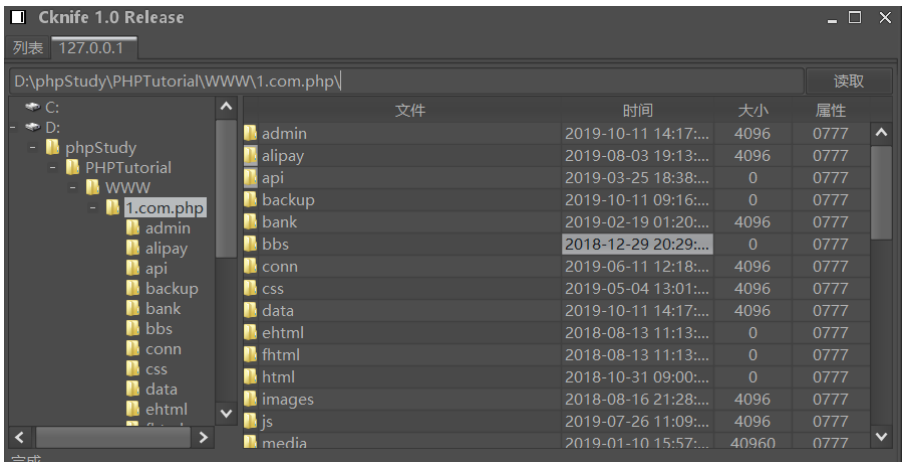


2. Try to unfold any one of PHP documents, modify it, input a line code of PHP and then save it.



3. Connecting with Cknife, the password is cmd111(as shown in illustration), enabling to getshell directly.





4. vulnerability code download(click the link)--Software download.


s-cms.cn/download.html?code=php
S-CMS
企业建站系统
闪灵网络 旗下产品
产品
下载 免费
介绍
帮助
新闻
购买
案例
加盟 特惠
企业建站 · 首选S-CMS
PC、手机、微信网站一建三屏，不会技术，你也牛！
环境支持：IIS(6/7/8)或Apache
操作系统：Windows或Linux
数据库：MYSQL
说明：免费版仅供学习、测试、个人建站，不可用于商业用途
政府单位、教育机构、协会团体、企业用户请购买 授权版 使用
购买授权
如何安装
企业建站系统
版本：PHP版 v3.0
大小：12.19M
含115套模板 / 预览
免费下载
电子商城系统
版本：PHP版 v1.5
大小：12.28M
含3套模板 / 预览
免费下载
学校建站系统
版本：PHP版 v1.0
大小：13.26M
含3套模板 / 预览
免费下载
医院建站系统
版本：PHP版 v1.0
大小：14.30M
含1套模板 / 预览
免费下载