

T10-17通达-OA-文件上传

漏洞描述:

通达OA“组织”->“管理员”->附件上传处存在任意文件上传漏洞，结合“系统管理”->“附件管理”->“添加存储目录”，修改附件上传后保存的路径，最终导致getshell。

网站图片:



网络测绘:

Hunter 语法:

app.name="通达 OA"

漏洞复现:



2、点击系统管理->系统参数设置->OA服务设置，找到网站根目录：D:\MYOA\webroot;

OFFICE ANYWHERE®

系统参数设置

OA服务设置

全文检索服务	IP地址: 127.0.0.1	端口: 2287	Web服务; 预览Office
Redis缓存数据库服务	IP地址: 127.0.0.1	端口: 2377	该端口仅
邮件服务	IP地址: 127.0.0.1	端口: 2597	Web服务; 邮件。修
	间隔: 10 分钟自动收取一次外部邮件, 超过 2 MB的邮件不自动收取		自动收取; 服务器带
POP3服务	POP3端口: 110		POP3端口
	邮件收取设置: <input checked="" type="radio"/> 收取最近多少天 <input type="radio"/> 收取某日期之后		POP3根提
	设置天数: 30		请根据实
	设置日期:		为当前前
监控服务	IP地址: 127.0.0.1	端口: 2753	Web服务; 其他服务, 监控服务
	检查间隔: 2 分钟		
默认附件路径	D:\MYOA\attach		邮件服务; 发送不能
Webroot目录	D:\MYOA\webroot		OA所有PI

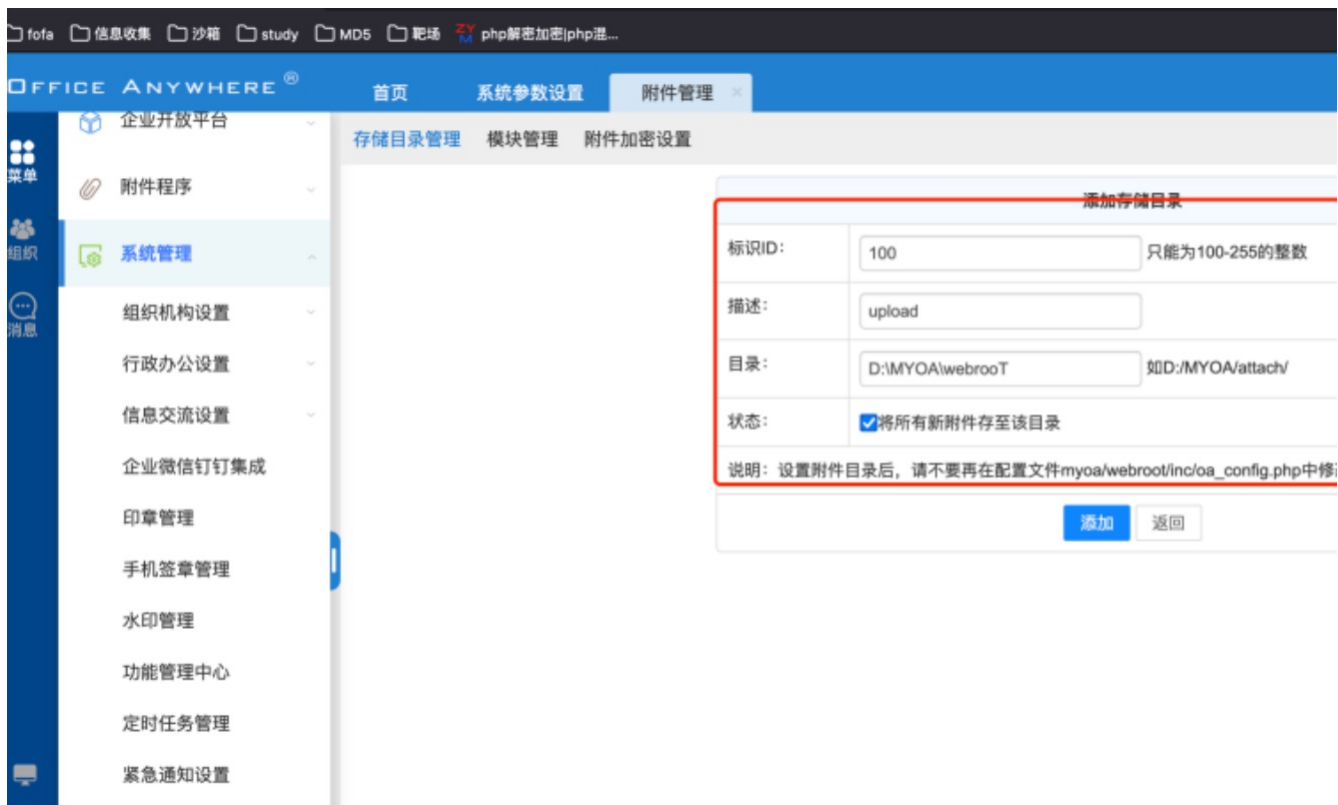
3、点击系统管理->附件管理->添加存储目录，设置附件上传目录为网站根目录；
存储目录设置为Webroot目录，标识id为100-255的整数，勾选将所有新附件存至该目录，描述随意；
□□注意：在11.2以上版本会检测存储目录是否包含webroot关键词检测，所以采用大小写绕过：D:\MYOA\webrootT；

存储目录管理 模块管理 附件加密设置

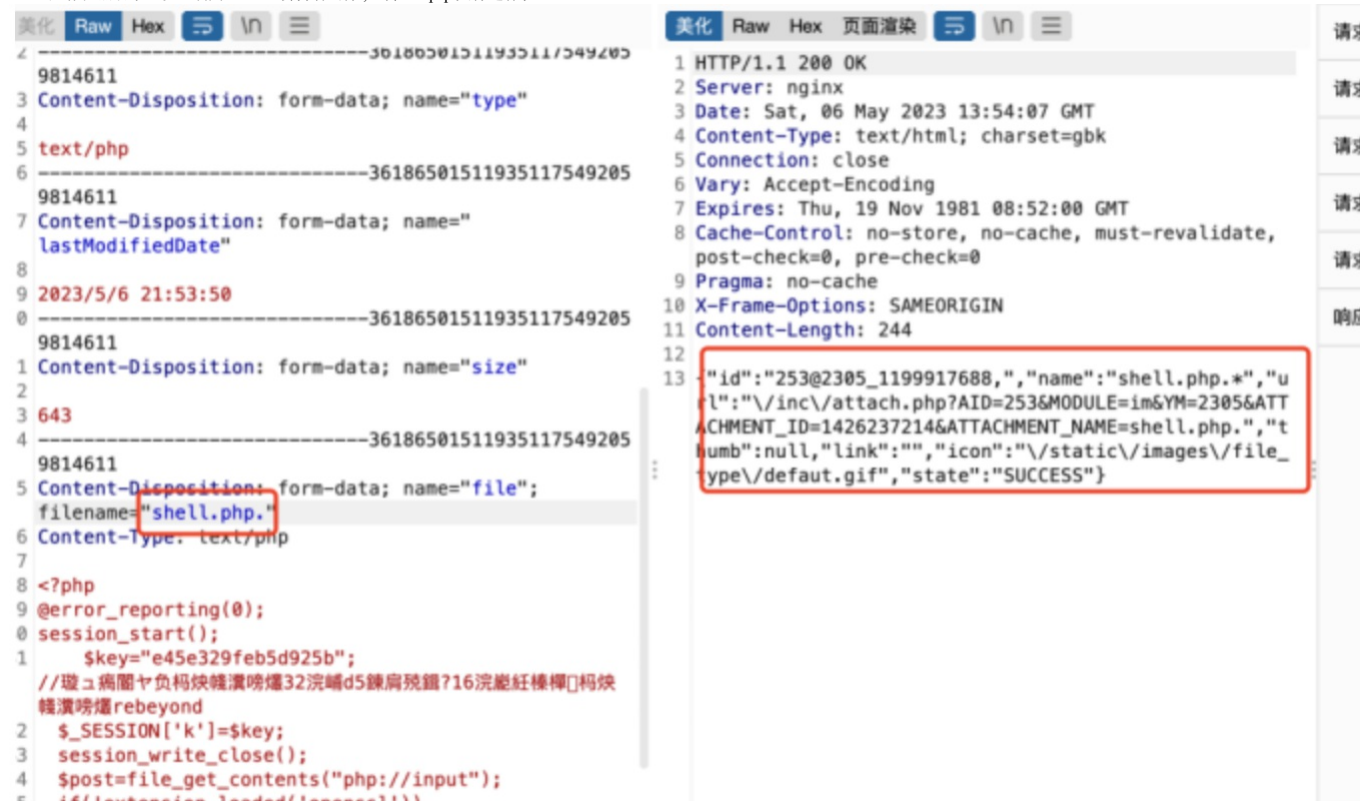


错误

目录[D:\MYOA\webroot]不能



4、选择组织->系统管理员->附件上传, 上传webshell:
□□此处存在黑名单过滤, 利用windows会自动去掉, 上传shell.php文件进行绕过



5、根据响应, 拼接webshell地址: <http://ip/m/2305/1199917688.shell.php> 冰蝎连接成功getshell:

目录结构

C:/

D:/

\$RECYCLE.BIN

MYOA

MyAdmin

attach

bin

data5

logs

mysql5

nginx

tmp

webroot

帮助文档

System Volume Information

nps

M:/

路径：D:/MYOA/

名称	大小	修改时间
.	4096	2023-05-06 16:24:23
..	4096	2023-05-06 16:26:22
MyAdmin	0	2023-05-06 16:24:23
attach	4096	2023-05-06 16:24:23
bin	12288	2023-05-06 16:24:23
data5	4096	2023-05-06 16:26:25
logs	4096	2023-05-06 16:55:14
mysql5	0	2023-05-06 16:24:20
nginx	4096	2023-05-06 16:26:31
readme.txt	3606	2016-09-08 17:32:00
tmp	4096	2023-05-06 22:22:23
webroot	4096	2023-05-06 16:30:57
帮助文档	0	2023-05-06 16:24:20