**[[【原创】]](https://forum.90sec.org/forumdisplay.php?fid=10&filter=type&typeid=2) phpmywind多个鸡肋漏洞**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 本帖最后由 darkmoon 于 2012-8-24 13:49 编辑   phpmywind多个鸡肋漏洞 声明:额 不要看错是phpwind不然我受到各种诅咒 硬盘里面有个程序看看 不知道是不是最新的 套着看吧 Author:mOon site:[www.moonhack.org](http://www.moonhack.org) upload\_filemgr\_dir.php  鸡肋一 变量$dirname没进过滤 导致各种遍历  [预览源代码](https://forum.90sec.org/thread-3580-1-4.html#viewSource)    [打印](https://forum.90sec.org/thread-3580-1-4.html#printSource)[关于](https://forum.90sec.org/thread-3580-1-4.html#about)   |  |  | | --- | --- | | 01 | <?php | | 02 |  |  |  |  | | --- | --- | | 03 | if(empty($dirname) or $dirname=='uploads/') | | 04 | { |  |  |  | | --- | --- | | 05 | $dirname = 'uploads/'; | | 06 | $dirhigh = 'javascript:;'; |  |  |  | | --- | --- | | 07 | $dirtext = '上传根目录'; | | 08 | } |  |  |  | | --- | --- | | 09 | else | | 10 | { |  |  |  | | --- | --- | | 11 | $dirarr = explode('/', $dirname); | | 12 | $curnum = count($dirarr)-2; |  |  |  | | --- | --- | | 13 | $dirhigh = '?mode=dir&dirname='; | | 14 | $dirtext = '返回上一层'; |  |  |  | | --- | --- | | 15 |  | | 16 | for($i=0; $i<$curnum; $i++) |  |  |  | | --- | --- | | 17 | { | | 18 | $dirhigh .= $dirarr[$i].'/'; |  |  |  | | --- | --- | | 19 | } | | 20 | } |  |  |  | | --- | --- | | 21 | ?> |   登陆后台看看 https://forum.90sec.org/images/default/attachimg.gif图片1.jpg  [**下载**](https://forum.90sec.org/attachment.php?aid=NTI5NHwwNmVhZGIzM3wxMzUyOTk5OTk1fGZkZDFNWkZURHNXNkNwcUthNzhMdkcyYk9scEVVcTZMVVVoeXBVU2oxMjRuVHRN&nothumb=yes) (23.37 KB)  2012-8-24 13:36  鸡肋二 文件没进行权限验证 导致越权访问  https://forum.90sec.org/images/default/attachimg.gif图片2.jpg  [**下载**](https://forum.90sec.org/attachment.php?aid=NTI5NXw1NGJjZDE3NXwxMzUyOTk5OTk1fGZkZDFNWkZURHNXNkNwcUthNzhMdkcyYk9scEVVcTZMVVVoeXBVU2oxMjRuVHRN&nothumb=yes) (20.56 KB)  2012-8-24 13:39  鸡肋三 同样文件没有进行权限验证upload\_filemgr\_sql.php  [预览源代码](https://forum.90sec.org/thread-3580-1-4.html#viewSource)    [打印](https://forum.90sec.org/thread-3580-1-4.html#printSource)[关于](https://forum.90sec.org/thread-3580-1-4.html#about)   |  |  | | --- | --- | | 01 | if(!empty($keyword)) | | 02 | { |  |  |  | | --- | --- | | 03 | $sql = "SELECT \* FROM `#@\_\_uploads` WHERE name LIKE '%$keyword%'"; | | 04 | } |  |  |  | | --- | --- | | 05 | else | | 06 | { |  |  |  | | --- | --- | | 07 | $sql = "SELECT \* FROM `#@\_\_uploads`"; | | 08 | } |  |  |  | | --- | --- | | 09 |  | | 10 | $dopage->GetPage($sql, 50); |  |  |  | | --- | --- | | 11 | while($row = $dosql->GetArray()) | | 12 | { |  |  |  | | --- | --- | | 13 | ?> | | 14 | <tr align="center" class="mgr\_tr"> |  |  |  | | --- | --- | | 15 | <td height="30"><input type="checkbox" name="checkid[]" id="checkid[]" value="<?php echo $row['path']; ?>" /></td> | | 16 | <td><?php echo $row['name']; ?></td> |  |  |  | | --- | --- | | 17 | <td><?php echo $row['type']; ?></td> | | 18 | <td class="number"><span><?php echo GetDateTime($row['posttime']); ?></span></td> |  |  |  | | --- | --- | | 19 | <td><?php echo GetRealSize($row['size']); ?></td> | | 20 | <td class="action"><span>[<a href="../<?php echo $row['path']; ?>" target="\_blank">预览</a>]</span><span>[<a href="upload\_filemgr\_save.php?mode=sql&action=del&id=<?php echo $row['id']; ?>&path=<?php echo $row['path']; ?>" onclick="return ConfDel(0);">删除</a>]</span></td> |  |  |  | | --- | --- | | 21 | </tr> | | 22 | <?php |  |  |  | | --- | --- | | 23 | } | | 24 | ?> |   $keyword 木有进行过滤 导致注入  直接访问 木有找到GetPage函数导致出错 注入变成鸡肋 https://forum.90sec.org/images/default/attachimg.gif图片3.jpg  [**下载**](https://forum.90sec.org/attachment.php?aid=NTI5NnxjM2RhMDU5Y3wxMzUyOTk5OTk1fGZkZDFNWkZURHNXNkNwcUthNzhMdkcyYk9scEVVcTZMVVVoeXBVU2oxMjRuVHRN&nothumb=yes) (19.21 KB)  2012-8-24 13:40  后台拿webshell 默认模板 找到php文件 直接插入一句话 https://forum.90sec.org/images/default/attachimg.gif图片4.jpg  [**下载**](https://forum.90sec.org/attachment.php?aid=NTI5OHxkZDRjNGEzMHwxMzUyOTk5OTk1fGZkZDFNWkZURHNXNkNwcUthNzhMdkcyYk9scEVVcTZMVVVoeXBVU2oxMjRuVHRN&nothumb=yes) (27.1 KB)  2012-8-24 13:41  再送一个找后台方法  [预览源代码](https://forum.90sec.org/thread-3580-1-4.html#viewSource)    [打印](https://forum.90sec.org/thread-3580-1-4.html#printSource)[关于](https://forum.90sec.org/thread-3580-1-4.html#about)   |  |  | | --- | --- | | 01 | function DisplayError($msg) | | 02 | { |  |  |  | | --- | --- | | 03 | $emsg = ''; | | 04 | $emsg .= '<div><h3 style="color:red;line-height:30px;">请检查执行语句是否正确或录入内容是否正确!</h3>'; |  |  |  | | --- | --- | | 05 | $emsg .= '<strong>错误文件</strong>：'.GetCurUrl().''; | | 06 | $emsg .= '<strong>错误信息</strong>：'.$msg.''; |  |  |  | | --- | --- | | 07 | $emsg .= '</div>'; | | 08 |  |  |  |  | | --- | --- | | 09 | echo $emsg; | | 10 |  |  |  |  | | --- | --- | | 11 | //保存MySql错误日志 | | 12 | $savemsg = 'Page: '.GetCurUrl()."\r\nError: ".$msg; |  |  |  | | --- | --- | | 13 | $fp = @fopen(dirname(\_\_FILE\_\_).'/../data/error/mysql\_error\_trace.txt', 'a'); | | 14 | @fwrite($fp, "{$savemsg}\r\n\r\n\r\n"); |  |  |  | | --- | --- | | 15 | @fclose($fp); | | 16 | } |   网址加 data/error/mysql\_error\_trace.txt 找后台 https://forum.90sec.org/images/default/attachimg.gif图片5.jpg |