jizhiCMS's background has arbitrary file reading vulnerabilities

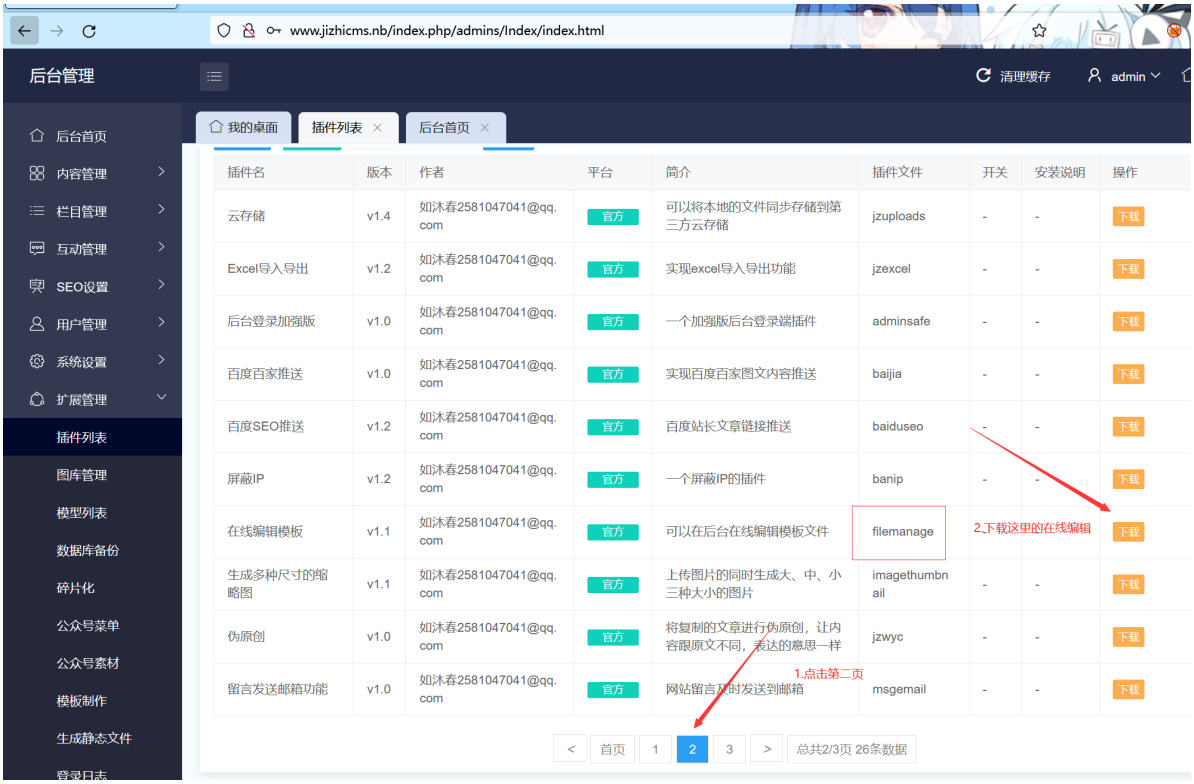
Environment and CMS download address

windows11 | Apache2.4.39 | MySQL5.7.26 | phpstudy2020 | php7.3.4nts

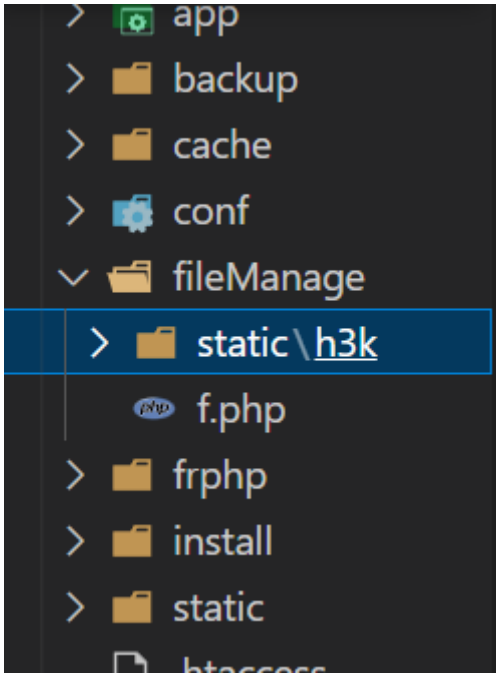
Official website：https://www.jizhicms.cn/ github：https://github.com/Cherry-toto/jizhicms

Description of the vulnerability

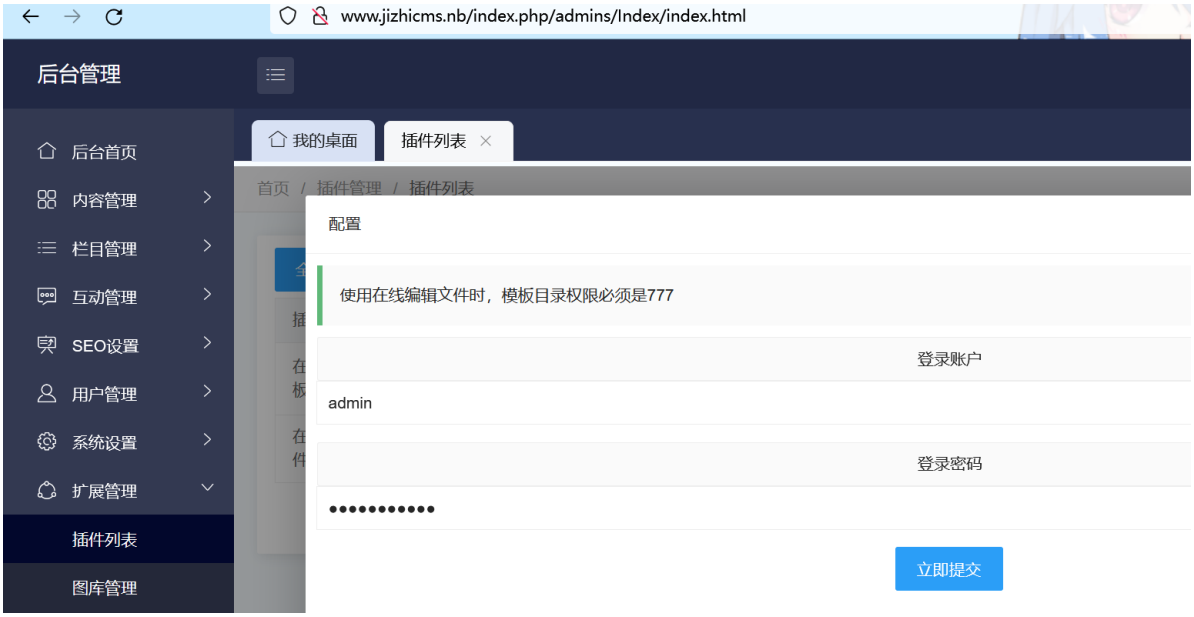
After registering an account, enter the background (admin|123456 is used here), click the second page of the plugin list, and download the online editing template



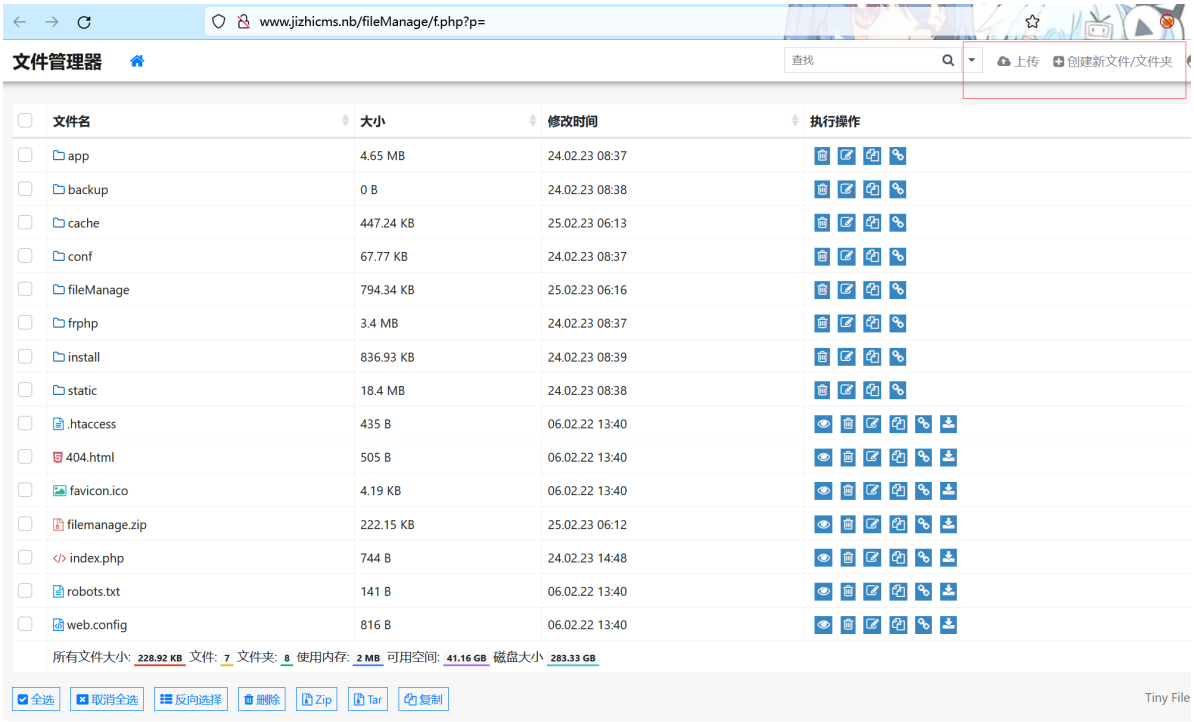
After the download is completed, select the local plugin (add a filemanage folder under the following directory)



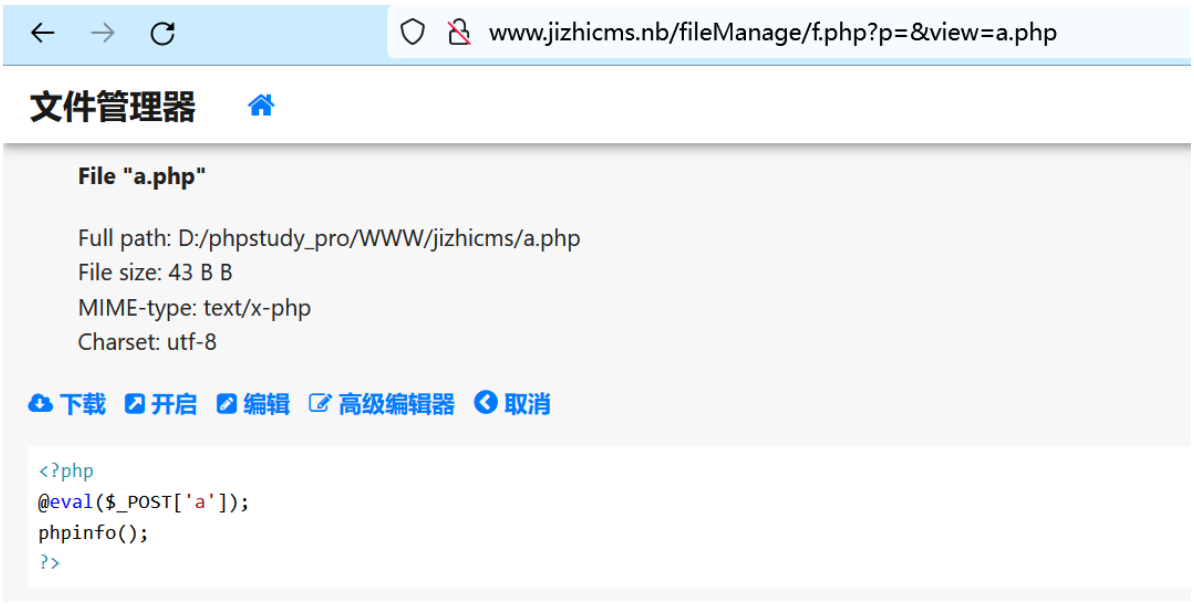
Here it is configured as (admin|admin123456)

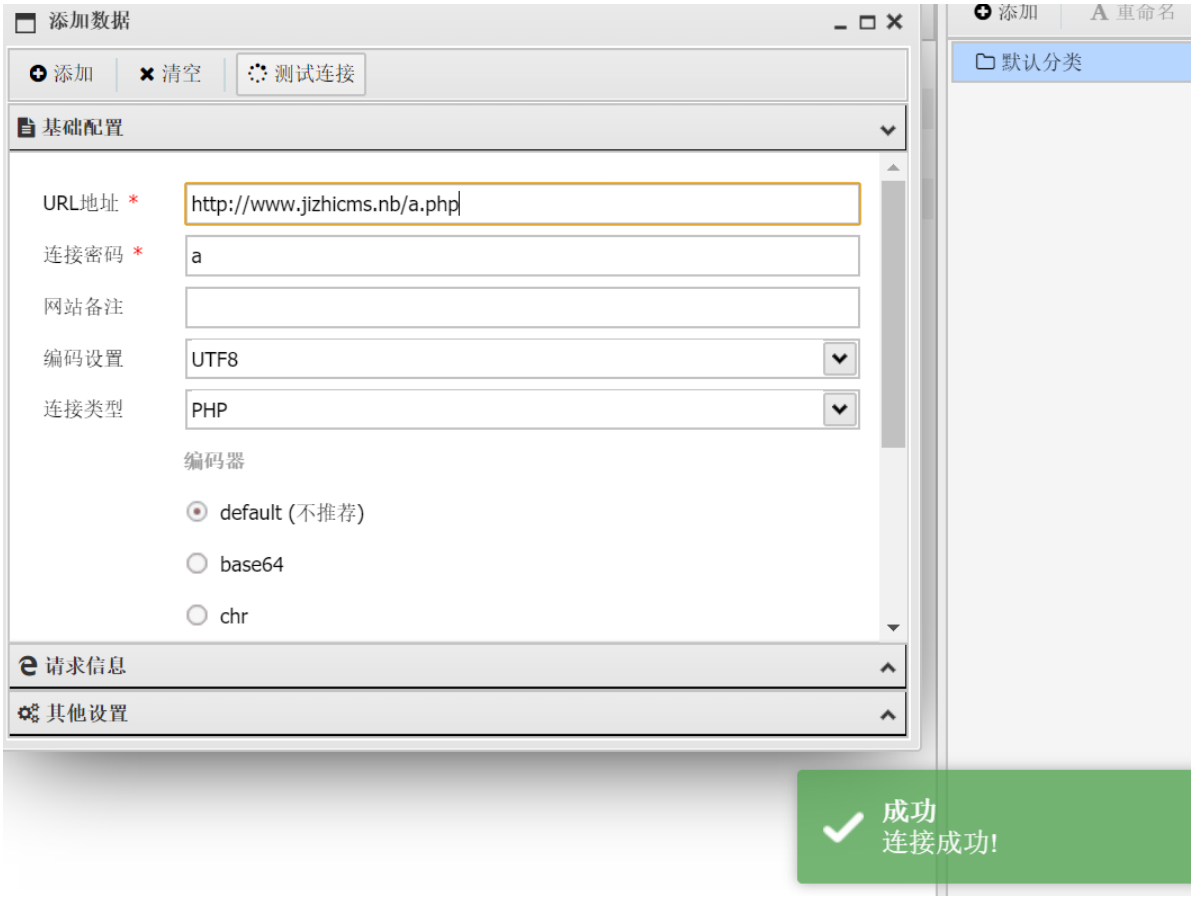


Click Submit Now, there are any files uploaded/modified/downloaded(The Chinese in the upper right corner means uploading and creating files/folders)

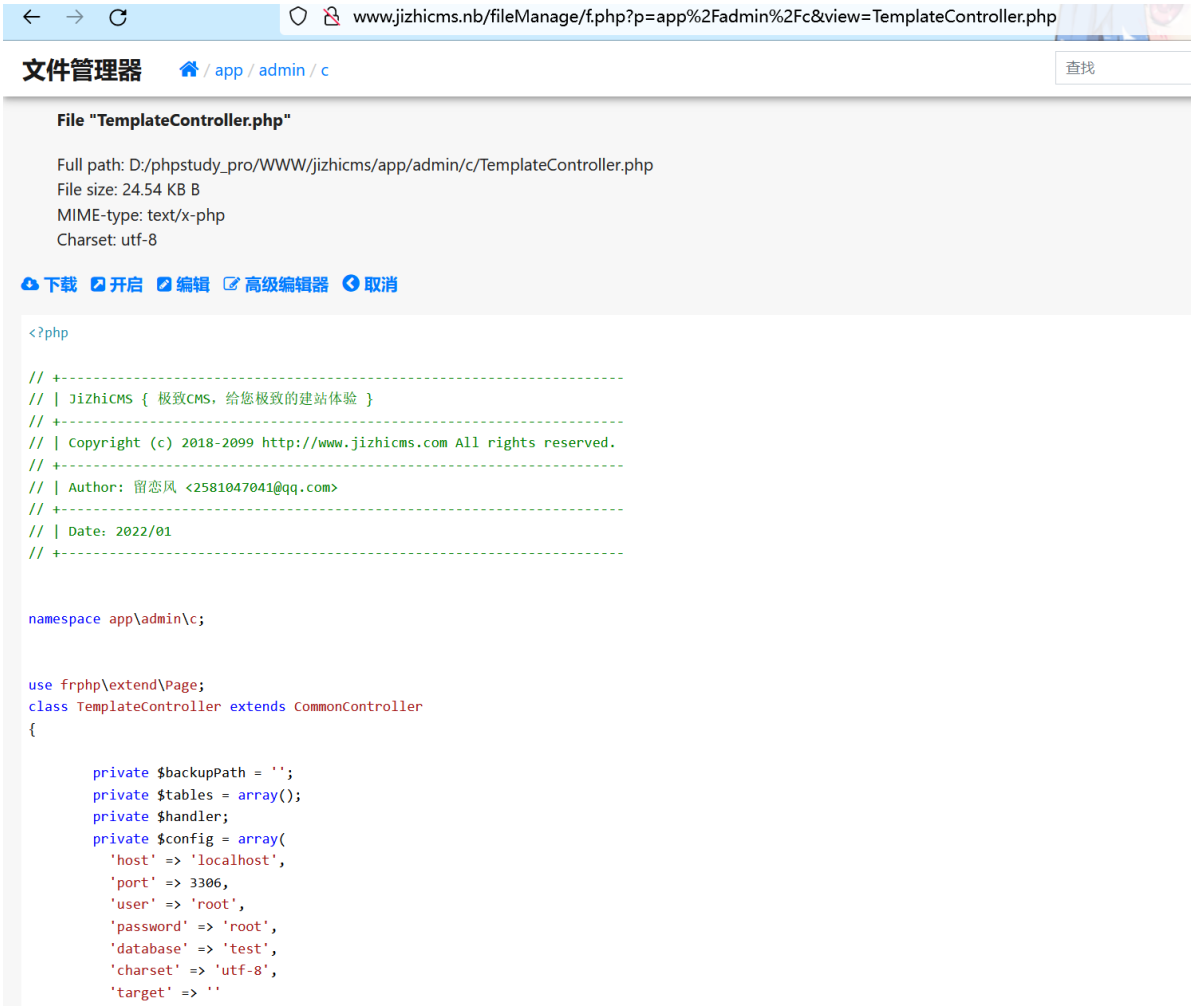


Upload a trojan to the root directory and connect(The green part Chinese means that the connection was successful)





Obtain the password of the database account

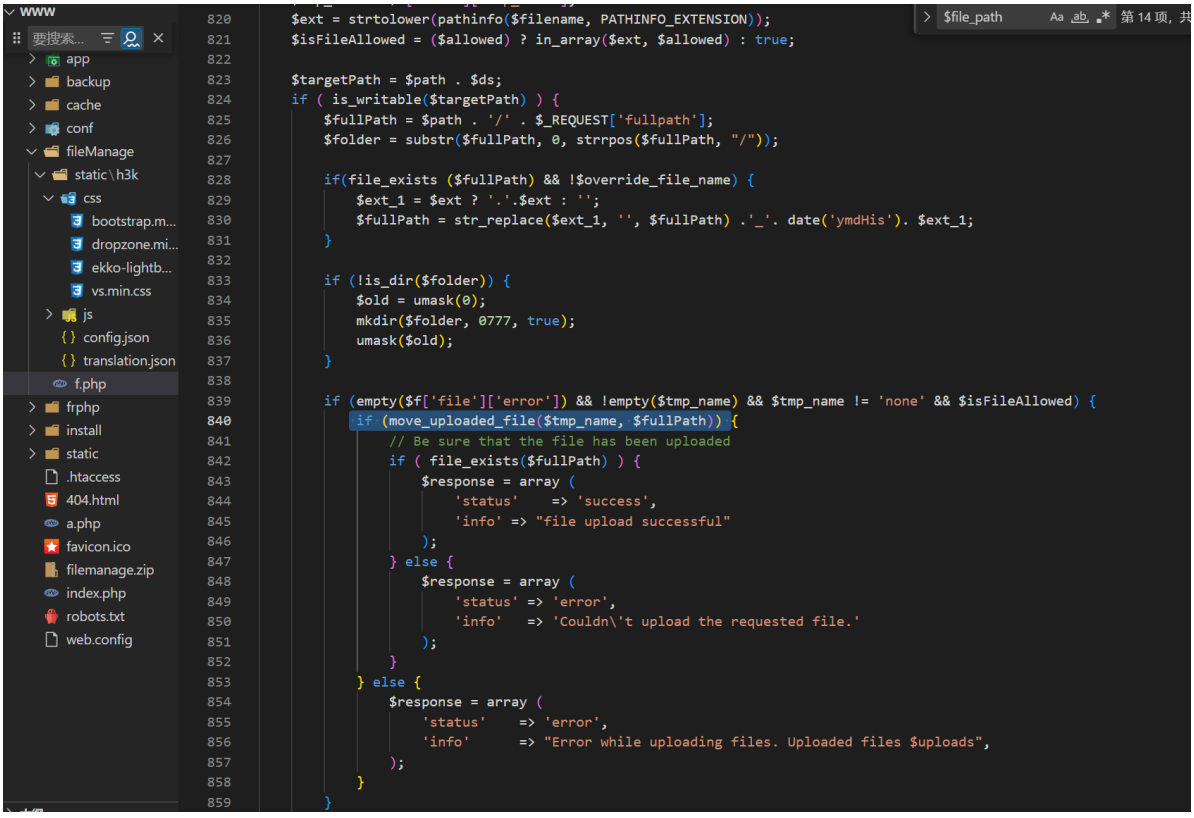


Vulnerability analysis

The `$fm_file` in the plugin `fileManage/f .php` is controllable, causing arbitrary file reads

```
3081    function save()
3082    {
3083        global $root_path;
3084        $fm_file = $root_path.$_SERVER["PHP_SELF"];
3085        $var_name = '$CONFIG';
3086        $var_value = var_export(json_encode($this->data), true);
3087        $config_string = "<?php" . chr(13) . chr(10) . "// Default Configuration".chr(13) . chr(10)."$var_name = $var_value;" . chr(13) .
3088        if (file_exists($fm_file)) {
3089            $lines = file($fm_file);
3090            if ($fh = @fopen($fm_file, "w")) {
3091                @fputs($fh, $config_string, strlen($config_string));
3092                for ($x = 3; $x < count($lines); $x++) {
3093                    @fputs($fh, $lines[$x], strlen($lines[$x]));
3094                }
3095                @fclose($fh);
3096            }
3097        }
3098    }
3099 }
```

Line 840: File uploads are not filtered here, resulting in arbitrary file uploads



Fix suggestions

1. Cancel the online editor plugin
2. When installing CMS, force the installation of online plug-ins and set different passwords (not weak passwords)