New issue

Jump to bottom

There is an arbitrary file upload vulnerability in the HYBBS upload plugin function #33

⊙ Open **shmilylty** opened this issue on Feb 7 · 1 comment

shmilylty commented on Feb 7

There is an arbitrary file upload vulnerability in the HYBBS upload plugin function

Vulnerability overview

There is an arbitrary file upload vulnerability in the upload plugin function of the HYBBS management background, which can lead to server permissions.

Vulnerability scope

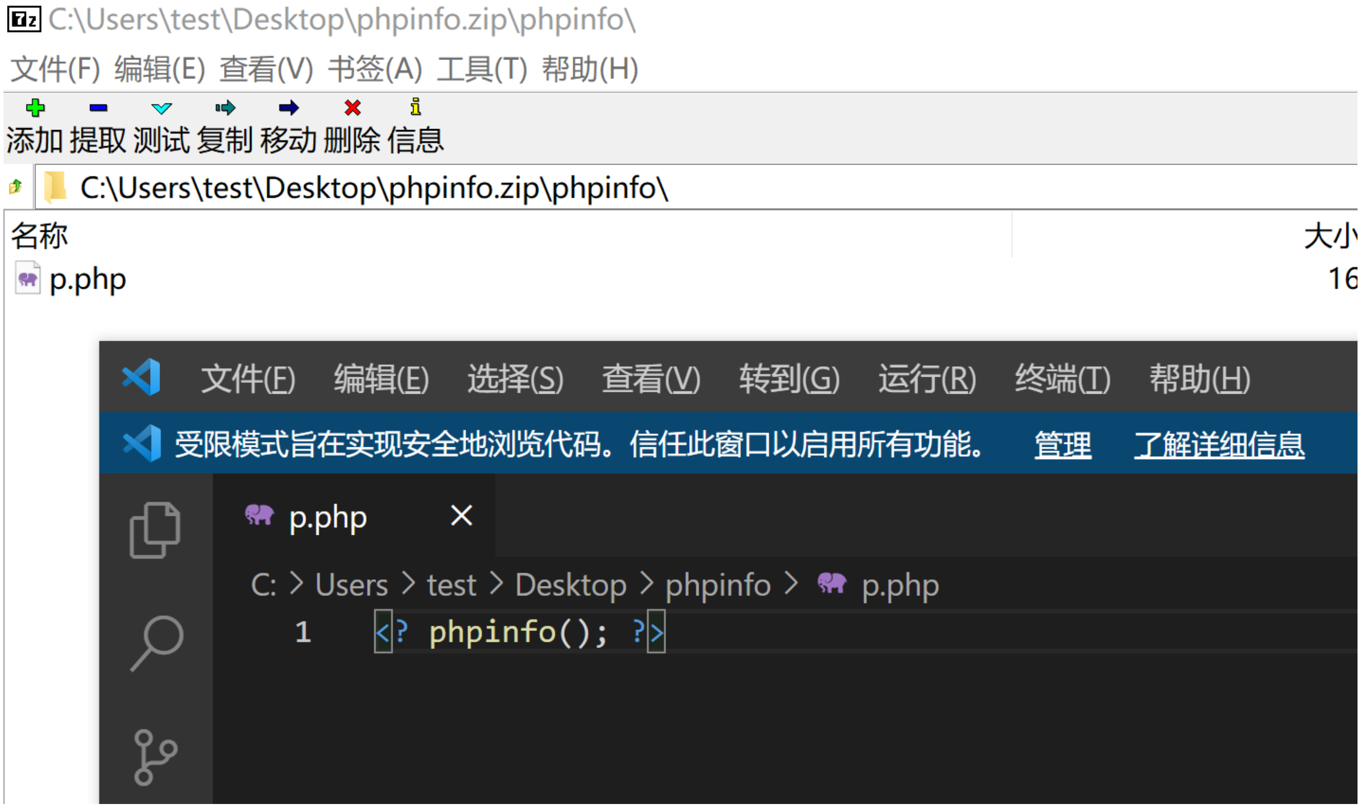
All versions prior to HYBBS 2.3.3

Vulnerability environment construction

Clone the latest code factory library of HYBBS to the local, and then use phpstudy to build HYBBS.

Vulnerability reproduction steps

Make a malicious zip archive as shown below

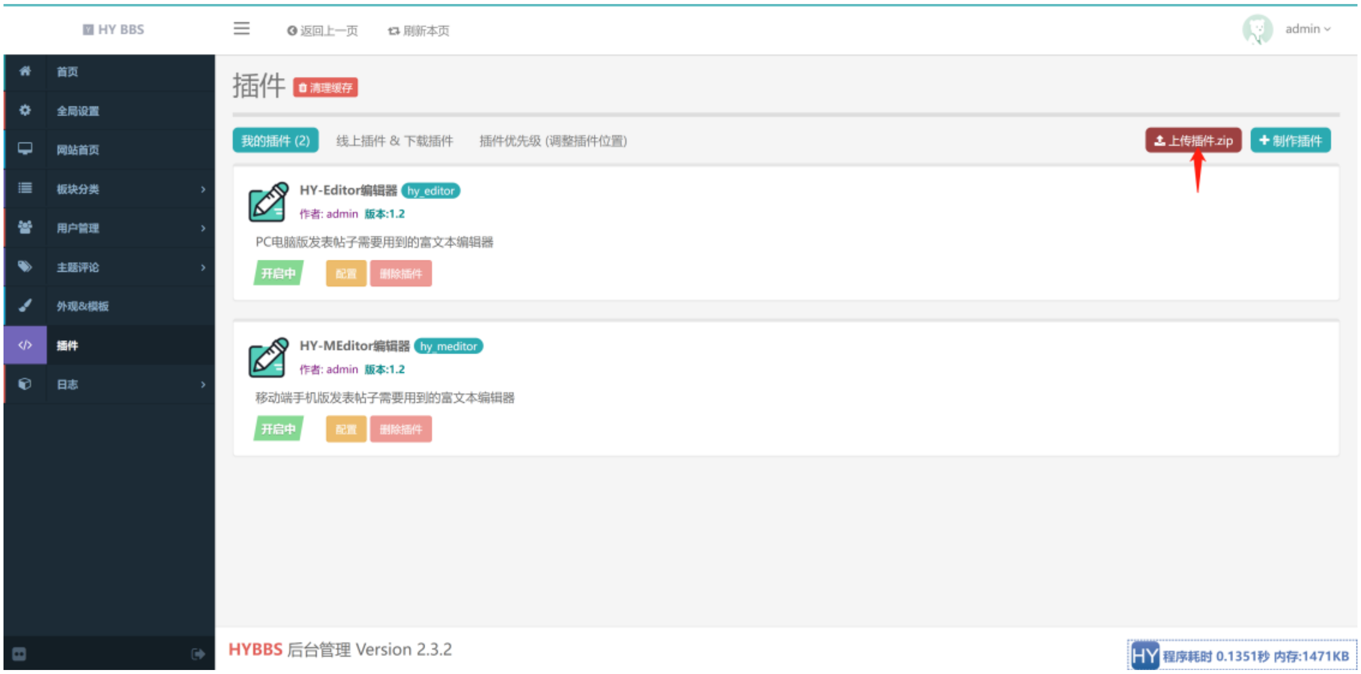

C:\Users\test\Desktop\phpinfo.zip\phpinfo\
文件(F) 编辑(E) 查看(V) 书签(A) 工具(T) 帮助(H)
添加 提取 测试 复制 移动 删除 信息
C:\Users\test\Desktop\phpinfo.zip\phpinfo\
名称
大小
p.php
16
文件(F) 编辑(E) 选择(S) 查看(V) 转到(G) 运行(R) 终端(T) 帮助(H)

受限模式旨在实现安全地浏览代码。信任此窗口以启用所有功能。 管理 了解详细信息

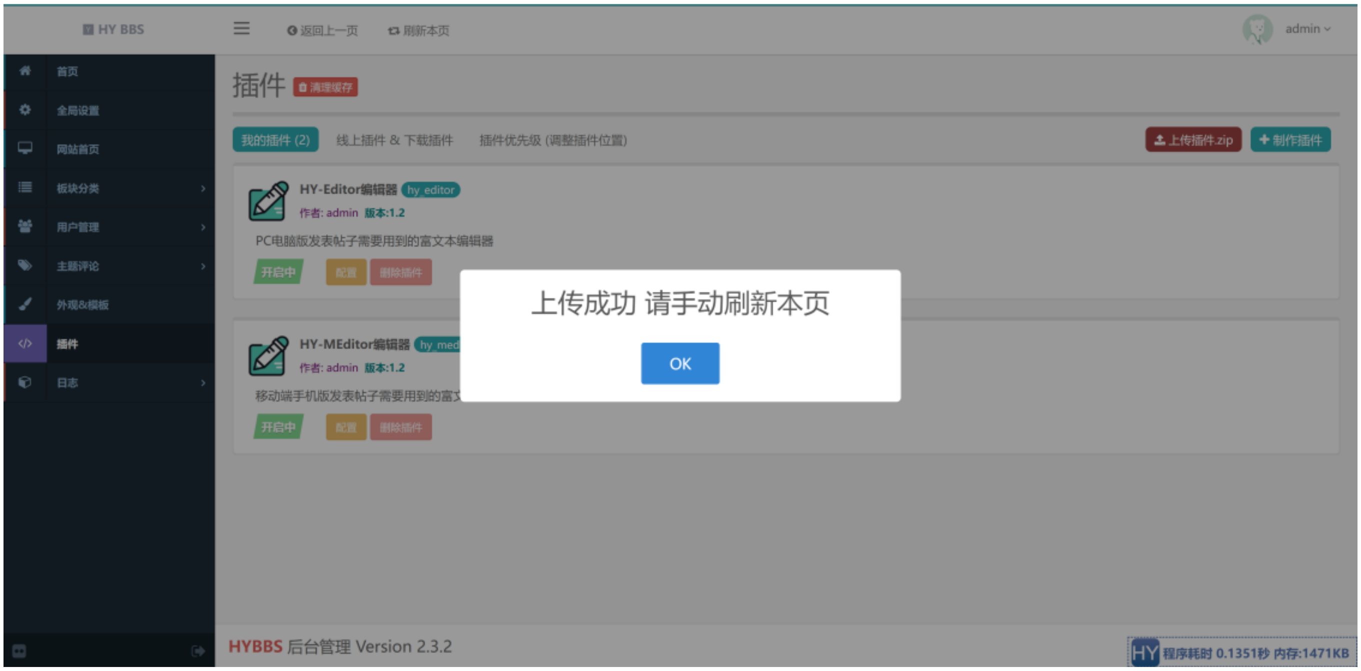
p.php
C: > Users > test > Desktop > phpinfo > p.php

```
<? phpinfo(); ?>
```

Upload malicious zip archives in the management background upload plugin function



After uploading, it prompts that the upload was successful

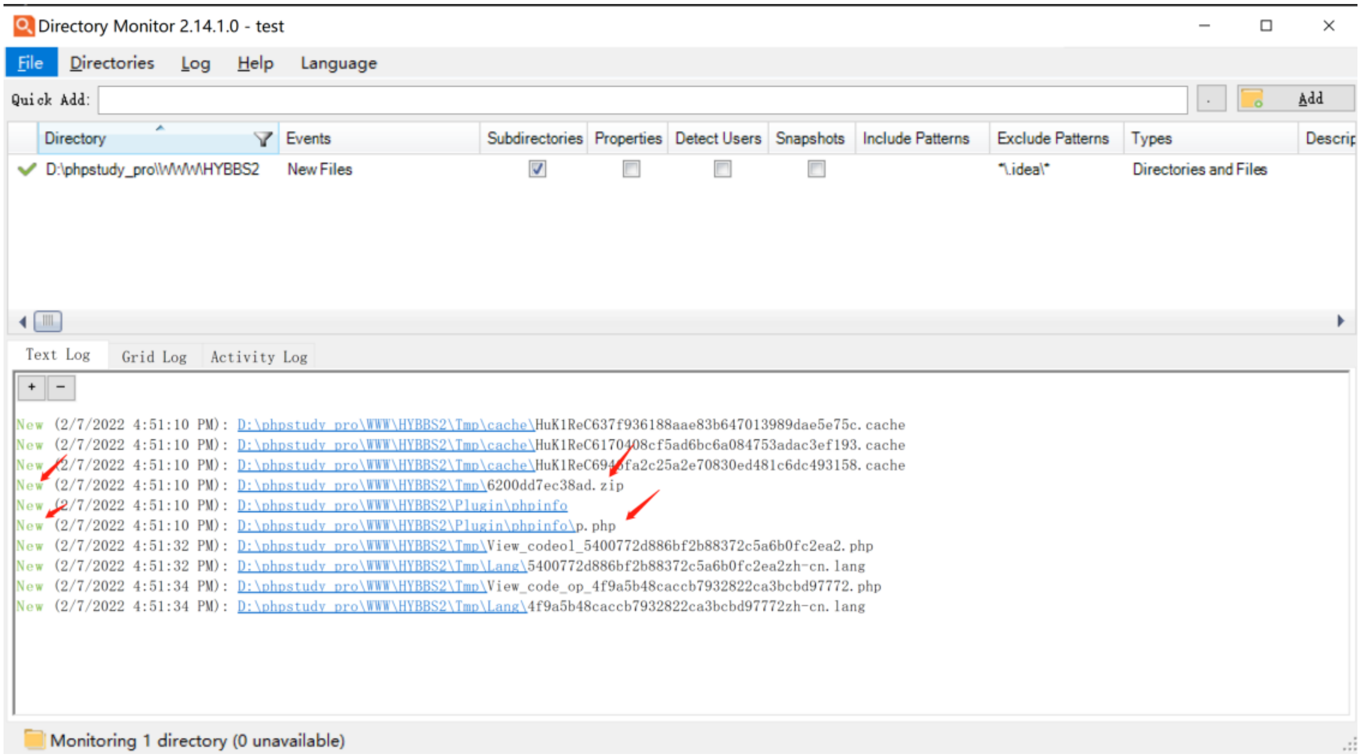


PC电脑版发表帖子需要用到的富文本编辑器

移动端手机版发表帖子需要用到的富文

上传成功 请手动刷新本页

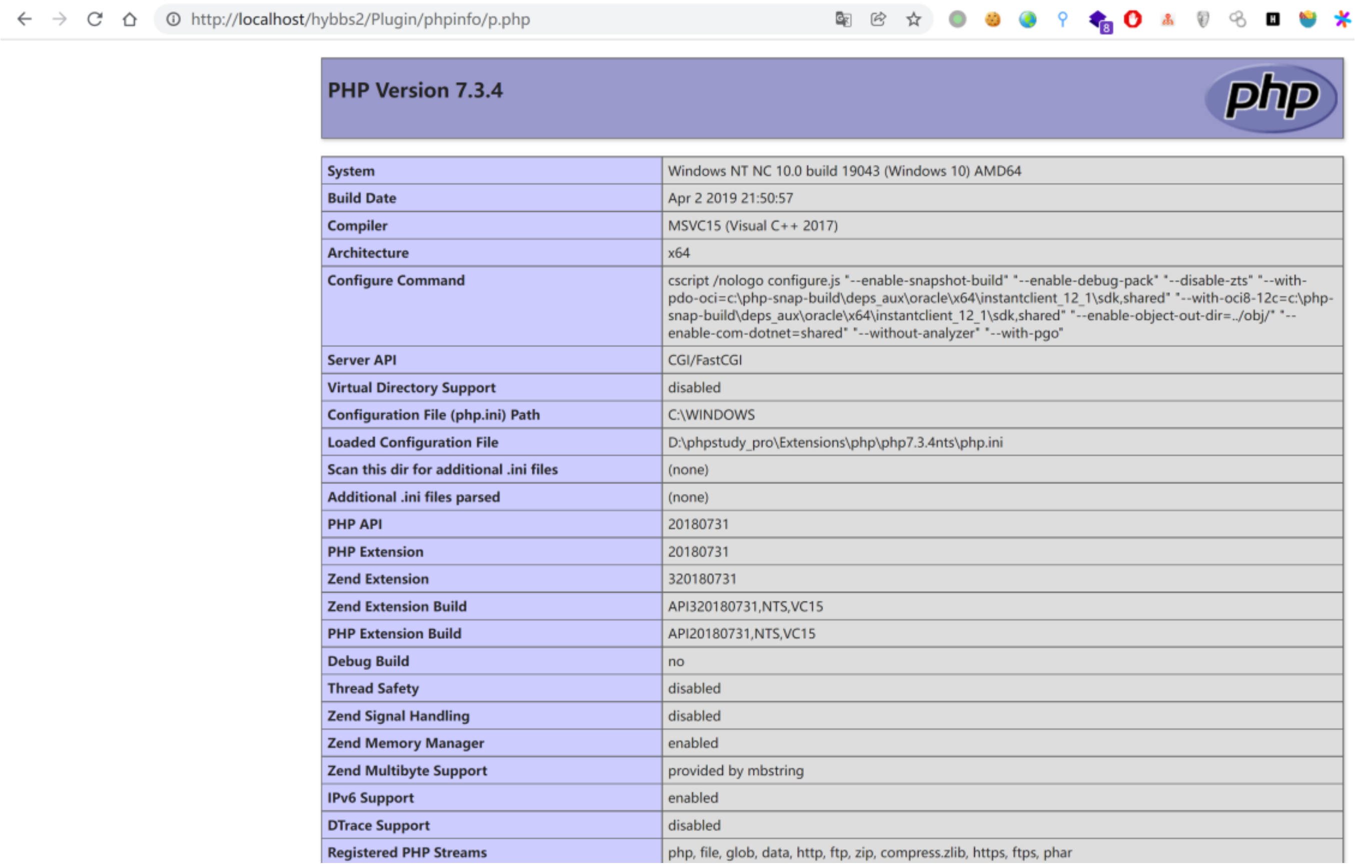
It can be seen from the log of the folder monitoring software that HYBBS renamed the malicious compressed package and extracted it to the Plugin directory



Directory	Events	Subdirectories	Properties	Detect Users	Snapshots	Include Patterns	Exclude Patterns	Types	Descrip
✓ D:\phpstudy_pro\WWW\HYBBS2	New Files	☑	□	□	□		*\.idea*	Directories and Files	

```
New (2/7/2022 4:51:10 PM): D:\phpstudy_pro\WWW\HYBBS2\Tmp\cache\HuK1ReC637f936188aae83b647013989dae5e75c.cache
New (2/7/2022 4:51:10 PM): D:\phpstudy_pro\WWW\HYBBS2\Tmp\cache\HuK1ReC6170408cf5ad6bc6a084753adac3ef193.cache
New (2/7/2022 4:51:10 PM): D:\phpstudy_pro\WWW\HYBBS2\Tmp\cache\HuK1ReC694[illegible]fa2c25a2e70830ed481c6dc493158.cache
New (2/7/2022 4:51:10 PM): D:\phpstudy_pro\WWW\HYBBS2\Tmp\6200dd7ec38ad.zip
New (2/7/2022 4:51:10 PM): D:\phpstudy_pro\WWW\HYBBS2\Plugin\phpinfo
New (2/7/2022 4:51:10 PM): D:\phpstudy_pro\WWW\HYBBS2\Plugin\phpinfo\p.php
New (2/7/2022 4:51:32 PM): D:\phpstudy_pro\WWW\HYBBS2\Tmp\View_codeol_5400772d886bf2b88372c5a6b0fc2ea2.php
New (2/7/2022 4:51:32 PM): D:\phpstudy_pro\WWW\HYBBS2\Tmp\Lang\5400772d886bf2b88372c5a6b0fc2ea2zh-cn.lang
New (2/7/2022 4:51:34 PM): D:\phpstudy_pro\WWW\HYBBS2\Tmp\View_code_op_4f9a5b48caccb7932822ca3bcbd97772.php
New (2/7/2022 4:51:34 PM): D:\phpstudy_pro\WWW\HYBBS2\Tmp\Lang\4f9a5b48caccb7932822ca3bcbd97772zh-cn.lang
```

Monitoring 1 directory (0 unavailable)

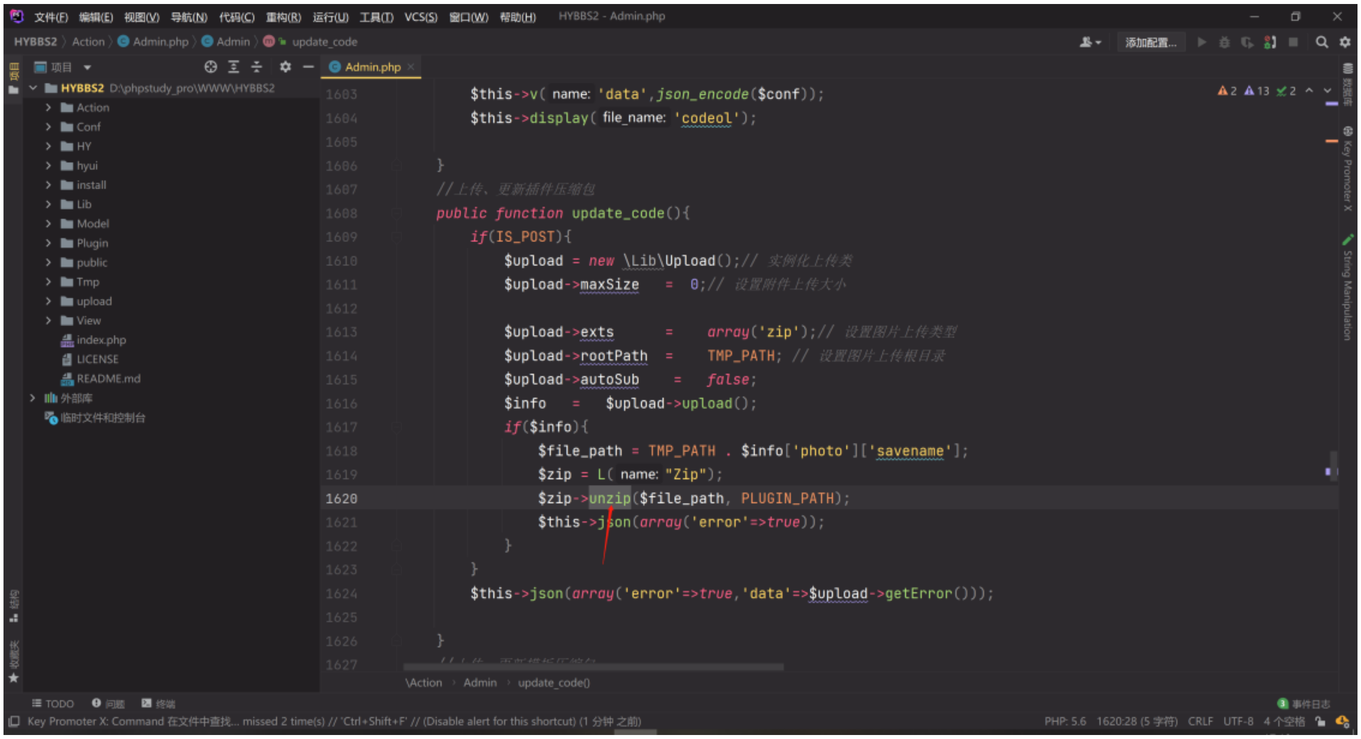


PHP Version 7.3.4

System	Windows NT NC 10.0 build 19043 (Windows 10) AMD64
Build Date	Apr 2 2019 21:50:57
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	D:\phpstudy_pro\Extensions\php\php7.3.4nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731,NTS,VC15
PHP Extension Build	API20180731,NTS,VC15
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	php, file, glob, data, http, ftp, zip, compress.zlib, https, ftps, phar

Vulnerability code analysis

Locate the code of the plugin upload function

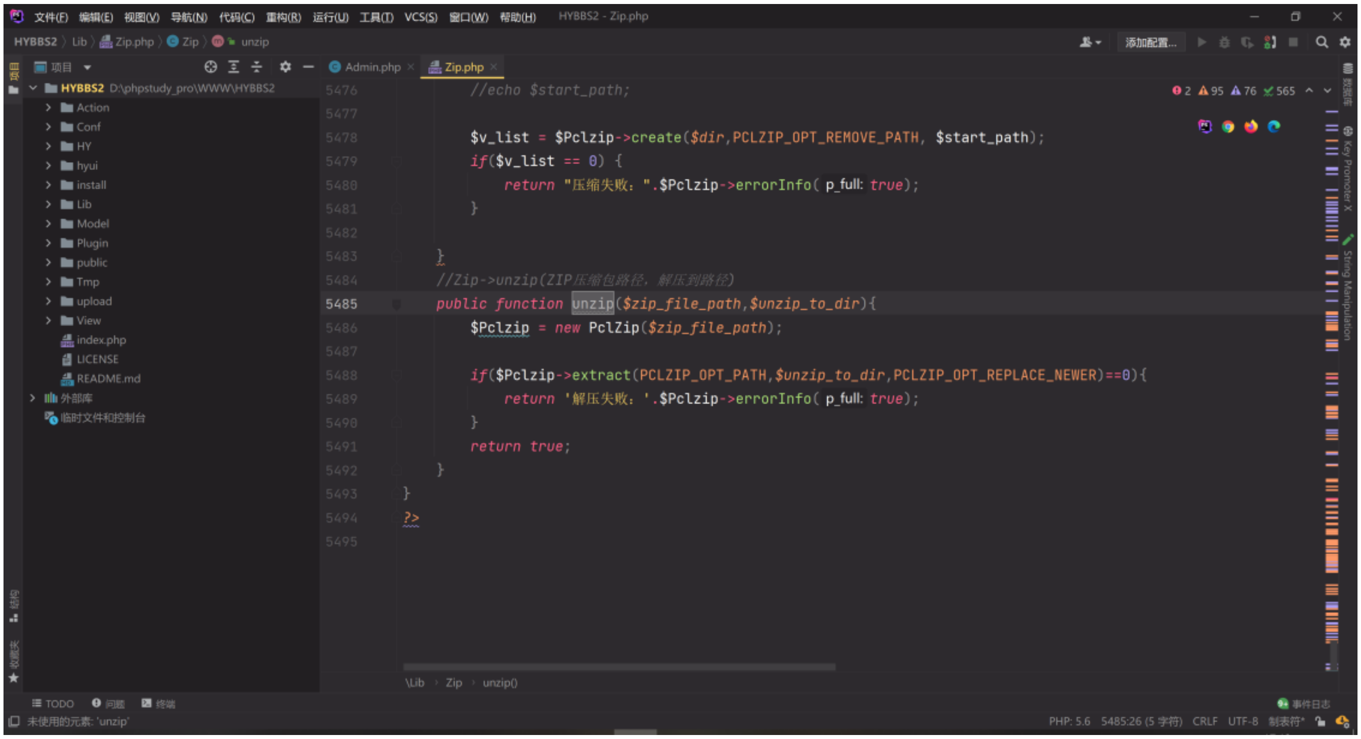

文件(F) 编辑(E) 视图(V) 导航(N) 代码(C) 重构(R) 运行(U) 工具(T) VCS(S) 窗口(W) 帮助(H) HYBBS2 - Admin.php
HYBBS2 〉 Action 〉 Admin.php 〉 Admin 〉 update_code
添加配置...
项目
HYBBS2 D:\phpstudy_pro\WWW\HYBBS2
Action
Conf
HY
hyui
install
Lib
Model
Plugin
public
Tmp
upload
View
index.php
LICENSE
README.md
外部库
临时文件和控制台
Admin.php
\Action 〉 Admin 〉 update_code()
TODO
问题
终端
事件日志
Key Promoter X: Command 在文件中查找... missed 2 time(s) // 'Ctrl+Shift+F' // (Disable alert for this shortcut) (1 分钟 之前)
PHP: 5.6 1620:28 (5 字符) CRLF UTF-8 4 个空格

```php
        $this->v( name: 'data',json_encode($conf));
        $this->display( file_name: 'codeol');

    }
    //上传、更新插件压缩包
    public function update_code(){
        if(IS_POST){
            $upload = new \Lib\Upload();// 实例化上传类
            $upload->maxSize   =  0;// 设置附件上传大小

            $upload->exts      =    array('zip');// 设置图片上传类型
            $upload->rootPath  =    TMP_PATH; // 设置图片上传根目录
            $upload->autoSub    =   false;
            $info   =   $upload->upload();
            if($info){
                $file_path = TMP_PATH . $info['photo']['savename'];
                $zip = L( name: "Zip");
                $zip->unzip($file_path, PLUGIN_PATH);
                $this->json(array('error'=>true));
            }
        }
        $this->json(array('error'=>true,'data'=>$upload->getError()));

    }
```



```
        //echo $start_path;

        $v_list = $Pclzip->create($dir,PCLZIP_OPT_REMOVE_PATH, $start_path);
        if($v_list == 0) {
            return "压缩失败：".$Pclzip->errorInfo( p_full: true);
        }

    }
    //Zip->unzip(ZIP压缩包路径，解压到路径)
    public function unzip($zip_file_path,$unzip_to_dir){
        $Pclzip = new PclZip($zip_file_path);

        if($Pclzip->extract(PCLZIP_OPT_PATH,$unzip_to_dir,PCLZIP_OPT_REPLACE_NEWER)==0){
            return '解压失败：'.$Pclzip->errorInfo( p_full: true);
        }
        return true;
    }
}
?>
```

HYBBS directly decompresses the compressed package and does not check the content of the compressed package, resulting in an arbitrary file upload vulnerability.

daniuwo commented on Feb 26

Contributor

需要管理员才能在后台上传，普通用户没有权限的。

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants