

main

...

bug_report / UCMS-1.6 / UCMS-RCE1.md



debug601 Create UCMS-RCE1.md

History

1 contributor

23 lines (13 sloc) 1.09 KB

There is an arbitrary file upload vulnerability (RCE) in the file management module in UCMS 1.6.

vendor: <http://uuu.la/>

UCMS 1.6 installation package: http://uuu.la/uploadfile/file/ucms_1.6.zip

After installation, log in to the background

Click File Management

站点设置

后台管理 > 文件管理

文件管理 /ucms_1.6/

根目录 最近修改 返回

| 文件名 | 文件大小 | 创建时间 | 修改时间 | 操作 |
|------------|------|---------------------|---------------------|-----------|
| cache | | 2021-05-20 00:00:00 | 2022-04-02 19:37:36 | 打开文件夹 重命名 |
| inc | | 2021-05-20 00:00:00 | 2022-04-02 19:25:27 | 打开文件夹 重命名 |
| index.php | 72 B | 2021-05-20 00:00:00 | 2021-05-20 00:00:00 | 编辑 重命名 删除 |
| install | | 2021-05-20 00:00:00 | 2022-04-02 19:23:31 | 打开文件夹 重命名 |
| shell.php | 17 B | 2022-04-02 19:30:18 | 2022-04-02 19:32:03 | 编辑 重命名 删除 |
| template | | 2021-05-20 00:00:00 | 2022-04-02 19:23:31 | 打开文件夹 重命名 |
| ucms | | 2021-05-20 00:00:00 | 2022-04-02 19:23:31 | 打开文件夹 重命名 |
| uploadfile | | 2021-05-20 00:00:00 | 2022-04-02 19:34:52 | 打开文件夹 重命名 |

新建文件夹: 提交

新建文件: 提交

上传文件:

选择文件 未选择任何文件 上传

总数:8

Click uploadfile

文件管理 /ucms_1.6/

[根目录](#)[最近修改](#)[返回](#)

| 文件名 | 文件大小 | 创建时间 | 修改时间 | 操作 |
|--|------|---------------------|---------------------|---|
|  cache | | 2021-05-20 00:00:00 | 2022-04-02 19:37:36 | 打开文件夹 重命名 |
|  inc | | 2021-05-20 00:00:00 | 2022-04-02 19:25:27 | 打开文件夹 重命名 |
|  index.php | 72 B | 2021-05-20 00:00:00 | 2021-05-20 00:00:00 | 编辑 重命名 删除 |
|  install | | 2021-05-20 00:00:00 | 2022-04-02 19:23:31 | 打开文件夹 重命名 |
|  shell.php | 17 B | 2022-04-02 19:30:18 | 2022-04-02 19:32:03 | 编辑 重命名 删除 |
|  template | | 2021-05-20 00:00:00 | 2022-04-02 19:23:31 | 打开文件夹 重命名 |
|  ucms | | 2021-05-20 00:00:00 | 2022-04-02 19:23:31 | 打开文件夹 重命名 |
|  uploadfile | | 2021-05-20 00:00:00 | 2022-04-02 19:34:52 | 打开文件夹 重命名 |
| 新建文件夹: <input type="text"/> 提交 新建文件: <input type="text"/> 提交 上传文件: | | | | 总数:8 |
| 选择文件 未选择任何文件 上传 | | | | |

Click to select the file, and after selecting the file ---> Click upload to upload to the "uploadfile directory"

| | | | | |
|--|------|------|------|------|
| 后台管理 > 文件管理 | | | | |
| 文件管理 /ucms_1.6/uploadfile/ | | | | |
| | | | | |
| 文件名 | 文件大小 | 创建时间 | 修改时间 | 操作 |
| 新建文件夹: <input type="text"/> 提交 新建文件: <input type="text"/> 提交 上传文件: | | | | 总数:0 |
| 选择文件 shell.php 上传 | | | | |

| | | | | |
|--|------|---------------------|---------------------|---|
| 后台管理 > 文件管理 | | | | |
| 文件管理 /ucms_1.6/uploadfile/ | | | | |
| | | | | |
| 文件名 | 文件大小 | 创建时间 | 修改时间 | 操作 |
|  shell.php | 24 B | 2022-04-02 20:05:29 | 2022-04-02 20:05:29 | 编辑 重命名 删除 |
| 新建文件夹: <input type="text"/> 提交 新建文件: <input type="text"/> 提交 上传文件: | | | | 总数:1 |
| 选择文件 未选择任何文件 上传 | | | | |

We visit the shell.php file from the browser and upload it to the uploadfile directory of the website, and we find that the code has been executed

JFJF

PHP 版本 5.2.17

| | |
|-------------------|---|
| 系统 | Windows NT 桌面-EVF2JTB 6.2 构建 9200 |
| 建造日期 | 2011年1月6日17:26:08 |
| 配置命令 | cscrip /nologo configure.js "--enable-snapshot-build" "--en: snapshot-template=d:\php-sdk\snap_5_2\vc6\x86\template" sdk\snap_5_2\vc6\x86\php_build" "--with-pdo-oci=D:\php-sdk\oracle\instantclient10\sdk,shared" "--with -oci8=D:\php-sdk\oracle\instantclient10\sdk,shared" "--without-pi3web" |
| 服务器 API | Apache 2.4 处理程序 - Apache Lounge |
| 虚拟目录支持 | 启用 |
| 配置文件 (php.ini) 路径 | C:\Windows |