New issue

Jump to bottom

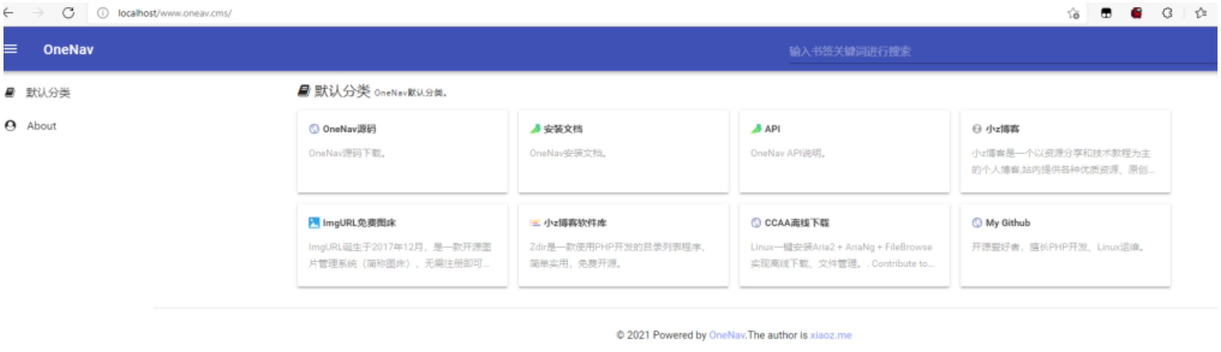
disclosure of information about sqlite #25

Closed **mcblog** opened this issue on Aug 4, 2021 · 1 comment

mcblog commented on Aug 4, 2021

disclosure of information about sqlite

I download this cms and i first install it .



OneNav源码下载。

OneNav安装文档。

OneNav API说明。

小z博客是一个以资源分享和技术教程为主的个人博客,站内提供各种优质资源、原创...

ImgURL诞生于2017年12月，是一款开源图片管理系统（简称图床），无需注册即可...

Zdir是一款使用PHP开发的目录列表程序，简单实用，免费开源。

Linux一键安装Aria2 + AriaNg + FileBrowse实现离线下载、文件管理。. Contribute to...

开源爱好者，擅长PHP开发、Linux运维。

© 2021 Powered by OneNav.The author is xiaoz.me

index.php:

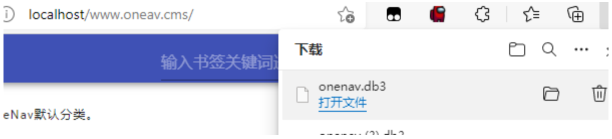
```
if( !file_exists('./data/config.php') ) {
        exit('<h3>配置文件不存在，请将站点目录下的config.simple.php复制为data/config.php</h3>');
}
//检查数据库是否存在，不存在则复制数据库
if( !file_exists('./data/onenav.db3') ) {
        copy('db/onenav.simple.db3','data/onenav.db3');
        // copy('db/.htaccess','data/.htaccess');
}

//载入配置文件
require("./data/config.php");

//根据不同的请求载入不同的方法
//如果没有请求控制器
if((!isset($c)) || ($c == '')){
        //载入主页
    include_once("./controller/index.php");

}

else{
        include_once("./controller/".$c.'.php');
}
```

bug code :

```
if( !file_exists('./data/onenav.db3') ) {
        copy('db/onenav.simple.db3','data/onenav.db3');
```

then i try to require "./data/onenav.db3" and "/data/.htaccess" http response status 200

it means i can download onenav.db3 and



can gets some privacy information

you can add some random code to document name or sqlite database name .

this cms has many users.

helloxz commented on Aug 4, 2021 Owner

hello,You can set things up to prevent the database from being downloaded.You can refer to this link: https://www.yuque.com/helloz/onenav/install#ImLOx

mcblog closed this as completed on Apr 2

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants