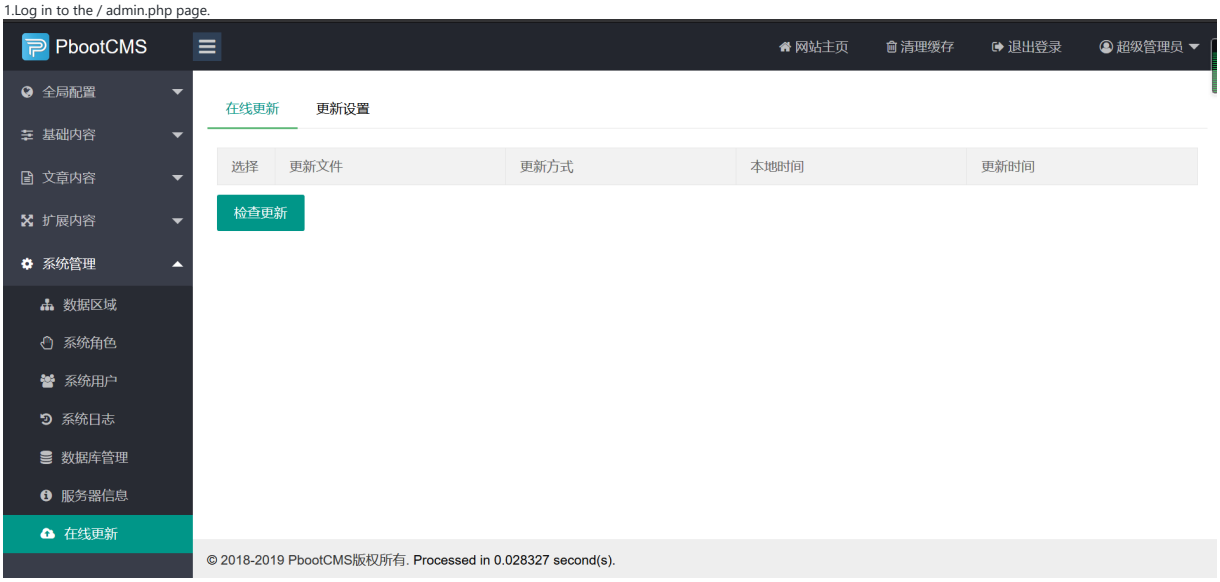
Pbootcms2.0.6 has a management background arbitrary file download vulnerability #5

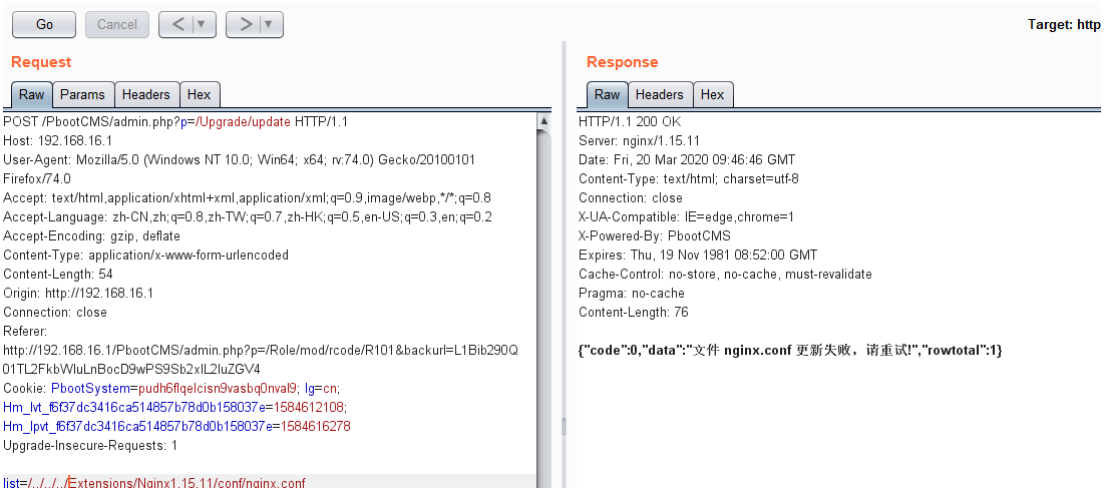
Open fKzhangsa opened this issue on Mar 20, 2020 · 0 comments

fKzhangsa commented on Mar 20, 2020

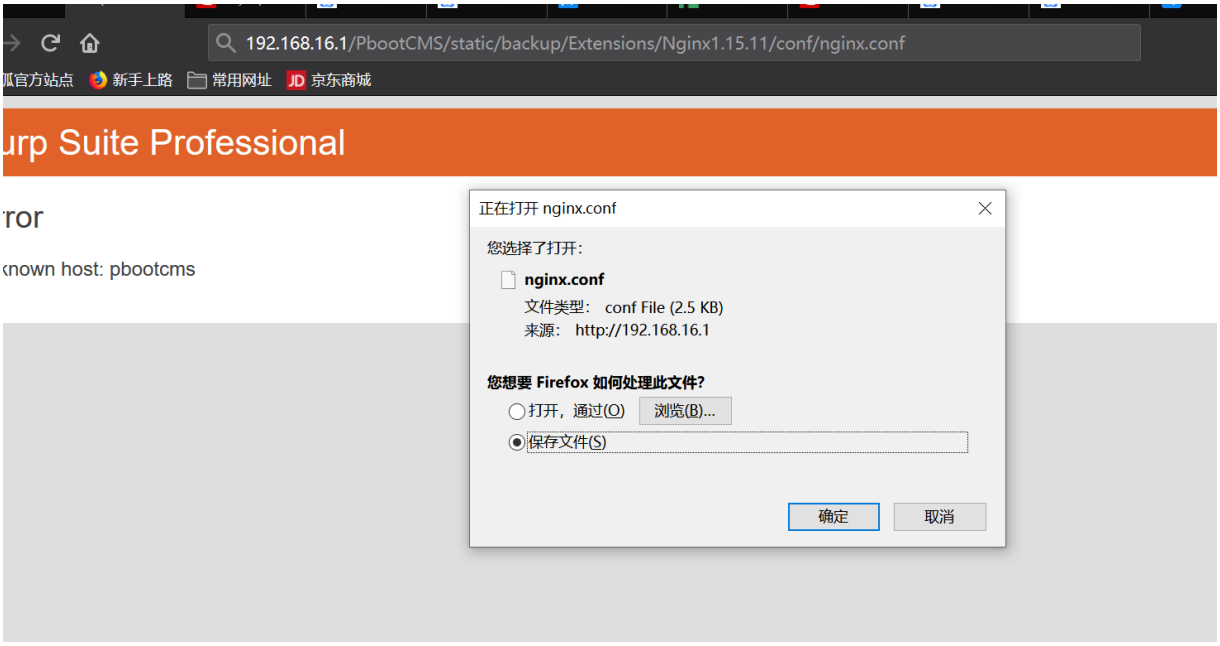
The vulnerability lies in the update function of the upgradecontroller.php file.
In this function, the 'list' variable is spliced into the path without filtering, so any file can be copied under the '/ backup / upgrade /' path, and then the file can be downloaded by directly accessing the file.
1.Log in to the / admin.php page.



2.Post the '/ pbootcms / Admin. PHP? P = / upgrade / update' to request that the contents of the list point to the file to be downloaded



3.Next, visit '\ pbootcms \ static \ backup \ extensions \ nginx1.15.11 \ conf \ nginx. Conf' to download to the file



code

```
($_POST) {
 if (! ! $list = post('list')) {
    $list = explode(',', $list);
    $backdir = date('YmdHis');

    // 分离文件
    foreach ($list as $value) {
        if (stripos($value, '/script/') !== false) {
            $sqls[] = $value;
        } else {
            $path = RUN_PATH . '/upgrade' . $value;
            $des_path = ROOT_PATH . $value;
            $back_path = DOC_PATH . STATIC_DIR . '/backup/upgrade/' . $bac
            if (! check_dir(dirname($des_path), true)) {
                json(0, '目录写入权限不足，无法正常升级！' . dirname($des_pat
            }
            if (file_exists($des_path)) { // 文件存在时执行备份
                check_dir(dirname($back_path), true);
                copy($des_path, $back_path);
            }

            // 如果后台入口文件修改过名字，则自动适配
            if (stripos($path, 'admin.php') !== false && stripos($_SERVER[
                if (file_exists($_SERVER['SCRIPT_FILENAME'])) {
```

The filtering of 'list' is not strict.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant