CSV Excel 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

```
DDE ("cmd";"/C calc";"!A0")A0
@SUM(1+1)*cmd|' /C calc'!A0
```

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) !Ao 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

```
=
+
-
@
```

Thanks to

- OWASP - CSV Excel Macro Injection (https://owasp.org/index.php/CSV_Excel_Macro_Injection)
- Google Bug Hunter University - CSV Excel formula injection (https://sites.google.com/site/bughunteruniversity/nonvuln/csv-excel-formula-injection)
- Comma Separated Vulnerabilities - James Kettle (https://www.contextis.com/resources/blog/comma-separated-vulnerabilities/)