CSV Injection | OWASP Foundation

Archived: 2026-04-06 00:23:24 UTC

Author: Timo Goosen, Albinowax
Contributor(s): kingthorin, Prasun Srivastav

CSV Injection, also known as Formula Injection, occurs when websites embed untrusted input inside CSV files.

When a spreadsheet program such as Microsoft Excel or LibreOffice Calc is used to open a CSV, any cells starting with `=` will be interpreted by the software as a formula. Maliciously crafted formulas can be used for three key attacks:

- Hijacking the user's computer by exploiting vulnerabilities in the spreadsheet software, such as CVE-2014-3524.
- Hijacking the user's computer by exploiting the user's tendency to ignore security warnings in spreadsheets that they downloaded from their own website.
- Exfiltrating contents from the spreadsheet, or other open spreadsheets.

This attack is difficult to mitigate, and explicitly disallowed from quite a few bug bounty programs. To remediate it, ensure that no cells begin with any of the following characters:

⚠️ Important (Microsoft Excel behavior)

Microsoft Excel may remove quotes or escape characters from CSV cells when a file is saved and re-opened. As a result, commonly suggested CSV injection mitigations may fail and previously escaped formulas may become active again.

- Equals to (`=`)
- Plus (`+`)
- Minus (`-`)
- At (`@`)
- Tab (`0x09`)
- Carriage return (`0x0D`)
- Line feed (`0x0A`)
- Full-width (double-byte) variants of formula-initiating characters such as `＝`, `＋`, `－`, and `＠`, which may be interpreted as formulas in some locales (e.g., Japanese environments).

Keep in mind that it is not sufficient to make sure that the untrusted user input does not start with these characters. You also need to take care of the field separator (e.g., `,`, `;`) and quotes (e.g., `"`, `'`), as attackers could use this to start a new cell and then have the dangerous character in the middle of the user input, but at the beginning of a cell.

Alternatively, apply the following sanitization to each field of the CSV, so that their content will be read as text by the spreadsheet editor:

- Wrap each cell field in double quotes
- Prepend each cell field with a single quote
- Escape every double quote using an additional double quote

Note: The above techniques are not reliable in Microsoft Excel after saving and re-opening the CSV file.

Two examples:

Input	Escaped Output
`=1+2";=1+2`	`"'=1+2"";=1+2"`
`=1+2'" ;,=1+2`	`"'=1+2'"" ;,=1+2"`

Excel-resistant mitigation

To reliably prevent formula execution in Microsoft Excel, prefix any cell starting with `=`, `+`, `-`, or `@` with a **tab character (`0x09`) inside the quoted field**.

This behavior has been observed in Microsoft Excel and may differ in other spreadsheet applications.

Input	Escaped Output
`=1+2`	`"\t=1+2"`

⚠️ Trade-off

The tab character remains part of the underlying data and may affect downstream processing if the CSV is later imported programmatically. This mitigation is best suited for CSV files intended for human viewing in spreadsheet applications.

There is no universal CSV sanitization strategy that is safe for all spreadsheet applications and all downstream consumers.

For further information, please refer to the following articles:

- Stealing Google Docs via CSV Injection
