

COMPLIANCE WORKING RECORD

Formula injection checker

Fictional sample. Requires tailoring and responsible review.

Document control

Field	Value
Organization	Fictional Example Company
Document type	Formula injection checker
Document reference	39-formula-injection-checker
Jurisdiction	United States
Version	2026-10-06.export-safety.1
Status	Supported checks found review items
Prepared by	Fictional reviewer
Prepared on	October 6, 2026
Sources reviewed	October 6, 2026
Generated	October 6, 2026

Review source and method

Tool	Method	Source rows	Source columns
39-formula-injection-checker	2026-10-06.export-safety.1	5	2

Purpose and boundary

Inspect every supplied header and cell for formula-triggering prefixes, hidden leading characters and previously escaped values. Inspect saved XLSX formulas without executing them.

A flagged value is a potential spreadsheet interpretation risk, not proof of a malicious payload. Negative numbers can be flagged. No universal CSV escaping method is guaranteed across spreadsheet applications or repeated save and reopen operations. Macros, links and destination application behavior require separate review.

Result

12 headers and cells inspected. 4 review items recorded.

- A flagged value is a potential spreadsheet interpretation risk, not proof of a malicious payload. Negative numbers can be flagged. No universal CSV escaping method is guaranteed across spreadsheet applications or repeated save and reopen operations. Macros, links and destination application behavior require separate review.

- Escaped previews show whitespace and non-ASCII characters explicitly and are abridged after 400 characters. The structured source backup preserves every original parsed value.

- The source file was not changed. No date, formula or filename was executed or silently repaired.

Measure	Value
Source rows	5
Source columns	2
Inspected values	12
Review items	4

Detailed checks

The report shows the first 100 findings or row assessments. Escaped previews are abridged after 400 characters. Excel, CSV and JSON retain every result. JSON preserves the complete parsed source, including column positions and duplicate headings.

Row	Result	Preview	Finding
3, column 2	Potential interpretation risk	"=1+2"	A formula-triggering prefix remains after compatibility normalization and removal of leading whitespace or invisible controls.
4, column 2	Potential interpretation risk	"\t=1+2"	The original cell begins with tab, carriage return or line feed. A formula-triggering prefix remains after compatibility normalization and removal of leading whitespace or invisible controls.
5, column 2	Potential interpretation risk	"\uff1d1+2"	A formula-triggering prefix remains after compatibility normalization and removal of leading whitespace or invisible controls.
6, column 2	Potential interpretation risk	"'=1+2"	The value appears previously escaped. Saving and reopening or downstream transformations may remove that protection.

Responsible review

- Row 3, column 2. Potential interpretation risk. A formula-triggering prefix remains after compatibility normalization and removal of leading whitespace or invisible controls.
- Row 4, column 2. Potential interpretation risk. The original cell begins with tab, carriage return or line feed. A formula-triggering prefix remains after compatibility normalization and removal of leading whitespace or invisible controls.
- Row 5, column 2. Potential interpretation risk. A formula-triggering prefix remains after compatibility normalization and removal of leading whitespace or invisible controls.
- Row 6, column 2. Potential interpretation risk. The value appears previously escaped. Saving and reopening or downstream transformations may remove that protection.

Assumptions

- The source format and approved destination require responsible review. No source value was silently repaired.

Limitations

- A flagged value is a potential spreadsheet interpretation risk, not proof of a malicious payload. Negative numbers can be flagged. No universal CSV escaping method is guaranteed across spreadsheet applications or repeated save and reopen operations. Macros, links and destination application behavior require separate review.

Official sources

Source	Provision	Date	Link
OWASP Foundation: CSV Injection	Formula injection checker. Spreadsheet interpretation prefixes and escaping limitations. A detected prefix is a review item, not a malicious-payload conclusion.	October 6, 2026	https://community.owasp.org/attacks/CSV_Injection
MITRE: CWE-1236, Improper Neutralization of Formula Elements in a CSV File	Formula injection checker. Formula interpretation weakness and destination-dependent mitigation. The tool inspects supplied values without executing or universally sanitizing them.	October 6, 2026	https://cwe.mitre.org/data/definitions/1236.html