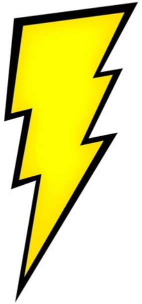
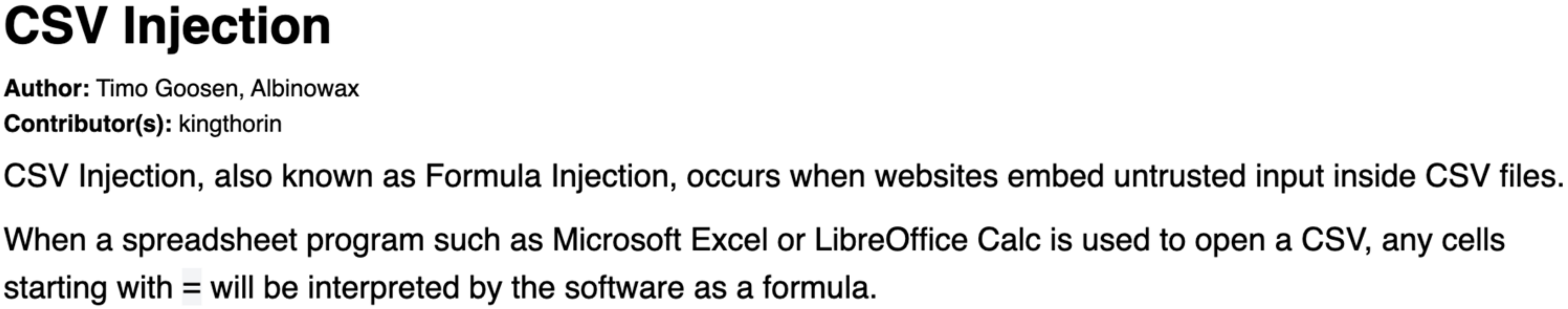
Should We Care About Formula Injection?



=CONCATENATE(“Austin”, “ “, “Turecek”)

What Is Formula Injection?



CSV Injection

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

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.

https://owasp.org/www-community/attacks/CSV_Injection

Potential Impact

- Data Exfiltration
- Remote Code Execution
  - Leverage Known Exploits (CVE-2014-3524)
  - DDE
- Data Manipulation

https://owasp.org/www-community/attacks/CSV_Injection

Should We Care About These Vulnerabilities?

- Yes

Excuses I’ve Seen (And Why I Don’t Think They’re Good)

- “I really see this as Excel flaw” - https://hackerone.com/reports/223344
- “is effectively something that can be duplicated by emailing someone a malicious CSV or modifying the export CSV after it's created” - https://hackerone.com/reports/216243
- “Clients reading a CSV and interpreting the content as commands are misinterpreting the file format in my opinion.” - https://github.com/splitbrain/dokuwiki/issues/2450
- “Any mitigation on our end would have a limited effectiveness and would force us to modify the data. This would break the workflow of users manipulating the CSV files with "safe" software.” - https://huntr.dev/bounties/eef8273d-207c-4be2-ab4a-694f1e824881/

Mitigations

- Simplest (Remove Highest Severity Issues)
    - Remove/Escape “=”, “DDE”, and “@”
- More Thorough (https://owasp.org/www-community/attacks/CSV_Injection)
    - Wrap each cell field in double quotes
    - Prepend each cell field with a single quote
    - Escape every double quote using an additional double quote
- Raise Awareness
    - If a Fix Isn’t Possible/Decided Against Warn Users

Question/Comments/Concerns

- LinkedIn - https://www.linkedin.com/in/austin-turecek
- Twitter - @I_Am_Galapag0s
- Github - https://github.com/Galapag0s
- Hunter.dev - https://huntr.dev/users/galapag0s/