Severe XSS in Google and Others Due To The JAR Protocol Issues

Severe XSS in Google and Others Due To The JAR Protocol Issues - pdp, gnucitizen.org.

- Published: date not stated
- Original: <https://www.gnucitizen.org/blog/severe-xss-in-google-and-others-due-to-the-jar-protocol-issues>
- Current location: <https://www.gnucitizen.org/blog/severe-xss-in-google-and-others-due-to-the-jar-protocol-issues/>
- Preserved from: https://www.gnucitizen.org/blog/severe-xss-in-google-and-others-due-to-the-jar-protocol-issues/ (stored) on 2026-08-11
- Licence: unknown

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.

Severe XSS in Google and Others Due To The JAR Protocol Issues

Sat, 10 Nov 2007 11:39:16 GMT

by pdp

After publishing my findings on the `jar:` URL protocol security issue for Firefox, I was contacted by MichaÅ, Zalewski regarding the possibilities for exploiting the vulnerability on the Google domain. I did not have much time to get back to him at the time, but I had a few ideas about how it could work. Of course, I was planning to silently release any of my findings to Michal and Google in order to prevent any attacks that may occur before Mozilla's scheduled update. The guys from Mozilla are currently busy with Firefox3, so I knew that it may take some time to properly patch the issue.

I had a few ideas in my mind about how the problem can be exploited in terms of Google. The first one was related to uploading a JAR archive on a public Google URL (docs, groups, etc). The second idea that I had was related to tricking the browser into believing that an external archive is located on the Google domain, possibly related to some kind of redirect. I was not aware of any redirect issues at Google at the time. I kind of remembered that the mobile GMail interface had one but I forget where I've put my notes regarding it.

So, I was scratching my head this morning on the problem. Meanwhile, beford was light-years ahead of me. He managed to prove that open redirects on Google could lead to domain wide XSS.

"Suddenly, it feels that the sky is falling." This means that attackers can get to any place on Google and do whatever they want with your profile and your online presence (i.e. backdoor Google service, snoop onto your searches, read your emails, etc).

Unfortunately, the issue is public so Google needs to make sure that they close all their open redirects (which are far too many) or Firefox should release an update **now**. Untill then, no one is safe! I repeat, the same technique can be applied to any other Web application out there. This is what I would like to refer to as **Web-wide Cross-site Scripting** vulnerabilities. There is more research coming very soon. Let's catch up at OWASP San Jose.
