Review of: 02_140155_Vierheilig
Reviewed by: Ole Eivind Parken

Goals:

- Is the case chosen an electronic id solution/contains electronic id?
- Are two or more race possible conditions presented? Are these really race conditions? Do you find simultaneous operations on the same resource where the outcome depends on which operation is executed earlier/faster than the other? Does the outcome violate a security goal?
- Are countermeasures presented? Do the countermeasures address the race conditions?
- Is the overall presentation of the case specific or is it too abstract to be of value?
- Bonus: Is there at least one reference that is not just a URL, but refers to a scientific article?

Review:

- You are using sessions as an electronic ID in your first example one, but I can't say it's obvious, what you're using as ID in example two.
- Yes, there are two race possible conditions presented here, one based on sessions. And I think you, are using your second example based on this. Because the end result of the sessions depends on load time. This violates with the principle of data integrity.
- As countermeasures for the session there is the flock() system call, SQL transaction statement. In the other example you have open(), read() and symlink().
- The presentation was a bit messy to understand with in the beginning, but with the pictures, it got more easy to understand.

Comment:

I like the figures you have chosen to illustrate the race condition

Mark: **PASS**