Preventing session fixation attacks in Aleph's OPAC

- **Article Type:** Q&A
- **Product:** Aleph
- **Product Version:** 21

Question

How can session fixation attacks in Aleph's OPAC be prevented?

Answer

Since the session ID is add, by default, to the OPAC URL, a session fixation attack could happen, in one of the following 2 scenarios:

1. Scenario 1:
- Person A logs in into OPAC and performs a search.
- Now he sends a complete URL (with session ID) to person B.
- When person B calls up this URL he is immediately logged in as person A and can see loans of person A etc.

The first scenario could be avoided by modifying $alephe_root/www_server.conf from
setenv server_f "&server_httpd/F/&session"
to:
setenv server_f "&server_httpd/F/"

This will remove the session ID from the URL.

2. Scenario 2:
- Person A is not logged in OPAC and sends a complete URL (including session-ID) to person B asking him to check something in Aleph OPAC and to log in.
- Person B calls up this URL and logs in.
- In parallel person A still is online in OPAC with the same session ID and now has taken over control about account information of person B.

The second scenario could be avoided by setting SESSION-FIXATION=Y in $alephe_tab/tab100 (available from Aleph 21). Setting this parameter will change the session ID one person B logs in.

Additional Information

If you are using Aleph version before 21, it is recommended to modify server_f, as this will help with both scenarios.

Note that removing the session ID from the URL, will prevent users who disabled cookies in their browsers from creating a session. However, nowadays, disabling cookies is not a common practice.

Category: Web OPAC (500)

- **Article last edited:** 10/8/2013