Deja-Vu Plug-in Guidelines:

The Deja-Vu ZAP addon enables attackers to go back in time and find many remnants that may not have been deleted from the site. This addon makes use of WayBackMachine (more sources will be added in the future) to get the targeted domain snapshots and compare them with the original pages accessed by ZAP.

Throughout the content analyzing, Deja-Vu shows which links were visible on the cached pages and were not yet located in the original pages. This can help the attacker to export links (and later on other leads, such as parameters) and check if the original site still supports them. Those leads can be later exploited and used for leveraging different attacks.

In order to work with the Deja-Vu please follow the instructions:

1. Copy the addon (jar file) to the following directory:

%programfiles%\OWASP\Zed Attack Proxy\plugin

1. Open ZAP and go to "Tools > Deja-Vu – Config"
2. Define your targeted domain
   1. In order to refer all different sub-domains, please include the domain suffix (for example, for www.sample.com just use sample.com).
3. Press on the "Get Years" button to check whether valid snapshots exist for this domain. This may give you the entire snapshot's range of the targeted site.
4. In order to optimize the test, we suggest choosing short year ranges which are not too close or too far from the last domain snapshot.

For example, if the "Get Years" function shows that there are snapshots valid for 2000-2013 years, then you should probably use 2003-2005 or 2005-2008 as the range.

1. After manually crawling / spidering the web site, you will see notifications under the "Alert" tab, which include various links displayed with the following properties:
   1. Relevant URL changes (URLs that exist on the cached page but does not exist in the corresponded original link).
   2. The archive source (i.e. WayBackMachine)
   3. The specific year
2. By right clicking on one of the alerts, you can choose to use "Deja-Vu - Copy Links". This option will let you copy all the disclosed links, and run them via a fuzzer (use the Links2Proxy.pl script to send those links to an additional proxy).
3. In addition, you can press on one of the disclosed links and use the "Caching - Get Archive Page" to examine the WayBackMachine response on that specified year.

**Note:** The addon finds differences between specified years and categorize each link by its snapshot year. Nevertheless, if the link only exists in 2007 and does not exist in 2006, then you would find it under the 2007 category (although you didn't choose it). Using this information you can actually remove irrelevant / familiar links and copy the relevant ones.