The PHP is a very popular language which is used to write a server side part of web applications. The language is very simple to use and there are lots of small or more complex pages across the internet. But the great widespread of the PHP attracts the people which want to harm and compromise security of the web applications.

The weverca analyzer is the first tool which is able to perform complex security analysis of a full page written in the modern version of the PHP and give information about possible security risks in the application. But the performance of Weverca is limited by its time and memory complexity caused by inefficient inner representation of a PHP memory state.

The goal of this thesis is to find and solve main problems of the original memory representation. The output of this thesis is an implementation of the new memory representation which minimizes the complexity of the original solution.