Table 3: The selected heuristics guidelines.

<table>
<tr><td colspan="5">Please select on of the following SAST tools which you have a previous experience with to evaluate:
○ Fortify SCA
○ Sparrow SAST
○ PVS-Studio</td></tr>
<tr><td>No.</td><td>Heuristic</td><td>Description</td><td>Yes/No</td><td>Issues if "Yes"</td></tr>
<tr><td>1</td><td>Visibility of System Status</td><td>The system should always keep the user informed about what is going on through appropriate feedback within a reasonable time.</td><td></td><td></td></tr>
<tr><td>2</td><td>Match Between System and the Real World</td><td>The system should speak the user’s language, with words, phrases and concepts familiar to the user, rather than system-oriented terms. Follow realworld conventions, making information appear in a natural and logical order.</td><td></td><td></td></tr>
<tr><td>3</td><td>Help and Documentation</td><td>Even though it is better if the system can be used without documentation, it may be necessary to provide help and documentation. Any such information should be easy to search, focused on the user’s task, list concrete steps to be carried out, and not be too large.</td><td></td><td></td></tr>
<tr><td>4</td><td>Flexibility and efficiency of use</td><td>Accelerators — unseen by the novice user — may often speed up the interaction for the expert user such that the system can cater to both inexperienced and experienced users. Allow users to tailor frequent actions.</td><td></td><td></td></tr>
<tr><td>5</td><td>Understanding Alternative Fixes & Approaches</td><td>Information about alternative ways to achieve the same functionality securely.</td><td></td><td></td></tr>
<tr><td>6</td><td>Relationship Between Vulnerabilities</td><td>Information about how co-occurring vulnerabilities relate to each other.</td><td></td><td></td></tr>
<tr><td>7</td><td>Locating Information</td><td>Information that satisfies "where" questions. Searching for information in the code.</td><td></td><td></td></tr>
<tr><td>8</td><td>Code Background & Functionality</td><td>Information about the history and the functionality of the potentially vulnerable code.</td><td></td><td></td></tr>
<tr><td>9</td><td>End-User Interaction</td><td>Information about sanitization/validation and input coming from users. Does the tool help show where input to the application is coming from?</td><td></td><td></td></tr>
<tr><td>10</td><td>Understanding Concepts</td><td>Information about unfamiliar concepts that appear in the code or in the tool.</td><td></td><td></td></tr>
<tr><td>11</td><td>Notification Text</td><td>Textual information that an analysis tool provides and how that text relates to the potentially vulnerable code.</td><td></td><td></td></tr>
<tr><td>12</td><td>Vulnerability Severity &amp; Rank</td><td>Information about the potential impact of vulnerabilities, including which vulnerabilities are potentially most impactful.</td><td></td><td></td></tr>
<tr><td>13</td><td>Confirming Expectations</td><td>Does the tool behave as expected?</td><td></td><td></td></tr>
</table>