Reviewer #1

Thank you for the reviewer's comments concerning our manuscript entitled "Program-PLATE: A Method for Identifying the Ability to Extract Vulnerability Features". Those comments are valuable and very helpful. We have read through comments carefully and have made corrections. Based on the instructions provided, we uploaded the file of the revised manuscript. The revisions in the manuscript are highlighted in yellow.

[Comment 1]

Expand Dataset: Include a broader range of CVE files to strengthen the generalizability of the findings.

[Reply 1]

Thank you for your insightful suggestion. We greatly appreciate your feedback, and upon receiving the review comments, we treated this issue as a top priority. We conducted extensive discussions and additional experiments to assess the feasibility and necessity of expanding the dataset. We elaborate on the following four points in detail.

1) Our dataset is already quite extensive, consisting of approximately 1,600 CVE entries. However, not all CVEs meet our selection criteria. Specifically, vulnerabilities that require cross-function interactions are excluded because they cannot be analyzed from a single-function perspective. Similarly, single-line vulnerabilities (where the vulnerability is triggered by a single line and later patched by modifying that single line) are also excluded, as our study focuses on inserting irrelevant code, which does not affect single-line features. Furthermore, loosely structured vulnerability-related code is not included, as it would significantly increase the dataset's complexity and volume. After careful manual selection, we identified 10 CVE files that meet our criteria, including the two CVEs analyzed in our paper.
2) Among these 10 selected CVEs, we conducted additional experiments on another CVE(CVE-2014-8543) that all tested models could correctly identify. The results are presented in the following figures. Since RCVD++ and Reveal successfully passed all test cases(which means that all data points in the figures are zero), we do not include their corresponding data here.

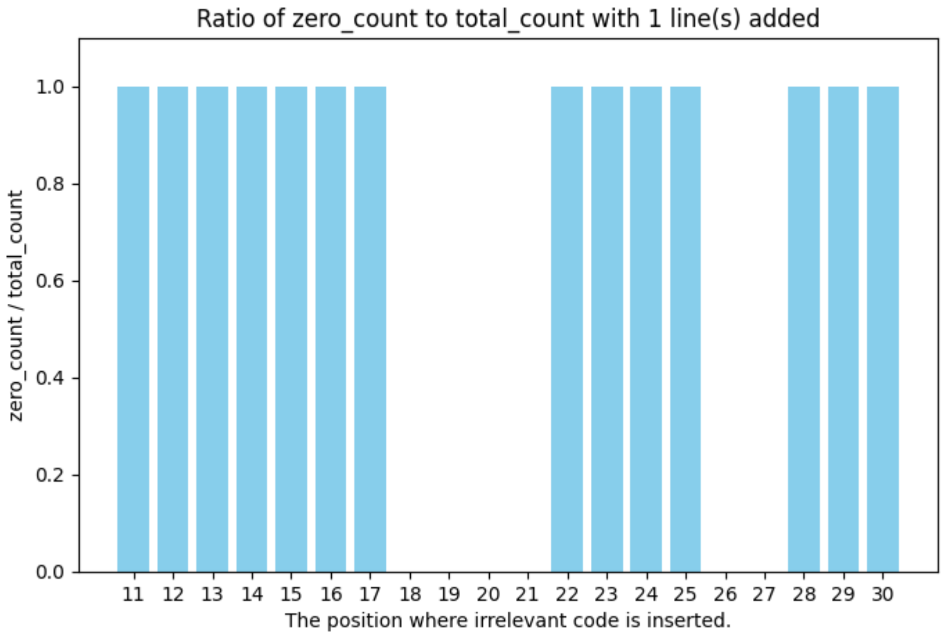

fig1: Devign's performance in a dataset with one irrelevant line of code added

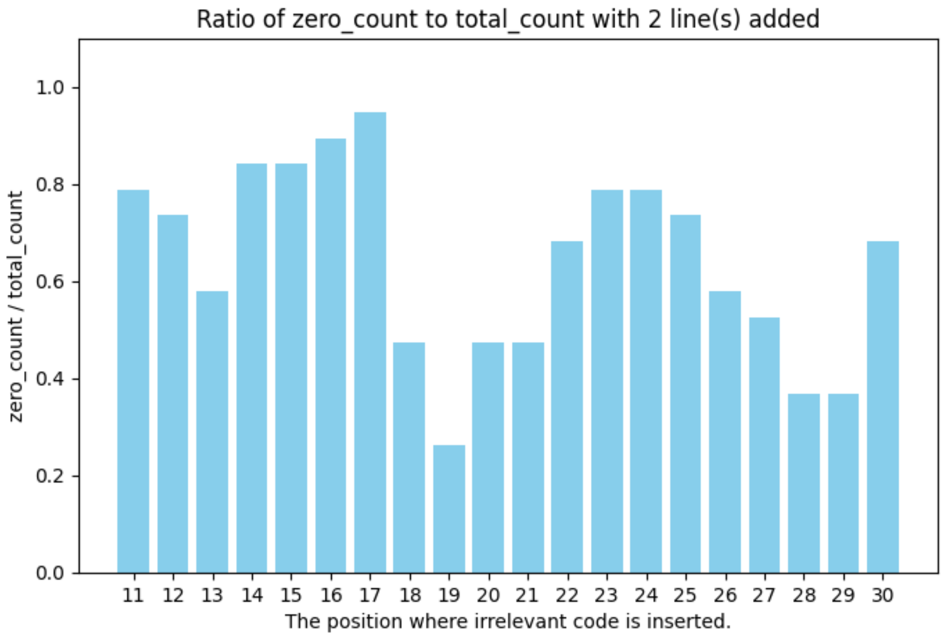

fig2: Devign's performance in a dataset with two irrelevant lines of code added

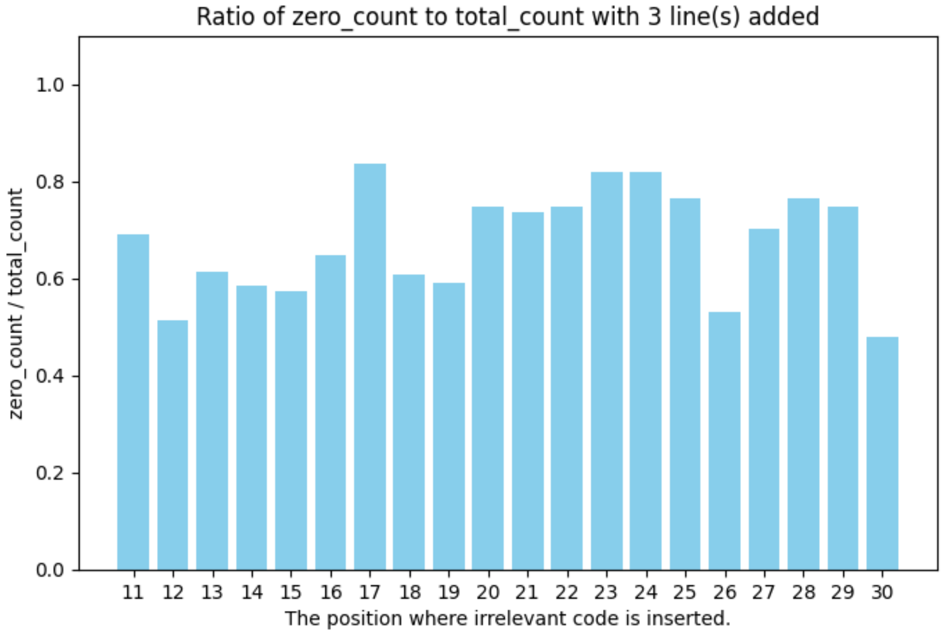

fig3: Devign's performance in a dataset with three irrelevant lines of code added

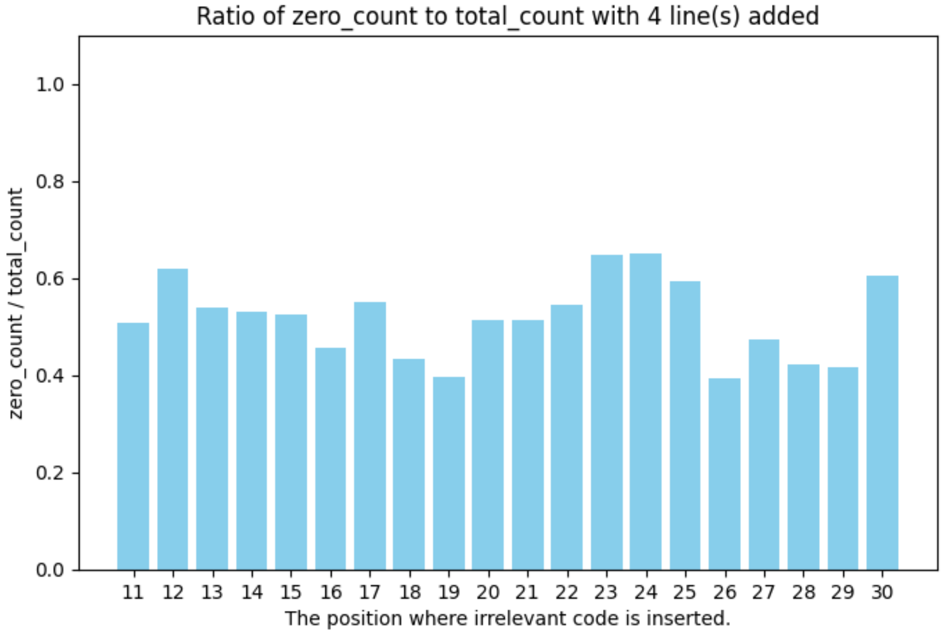

fig4: Devign's performance in a dataset with four irrelevant lines of code added

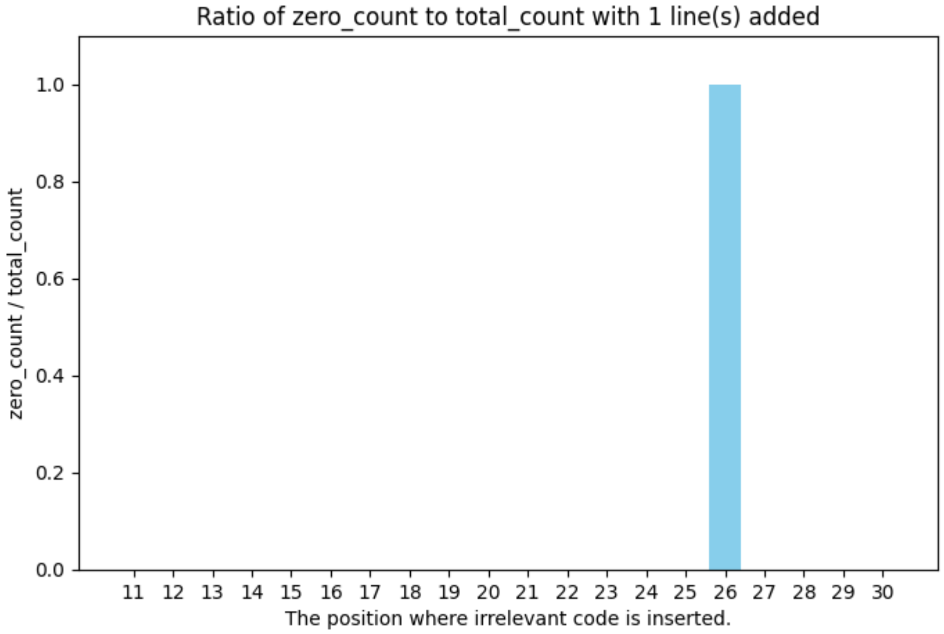

fig5: LineVD’s performance in a dataset with one irrelevant line of code added

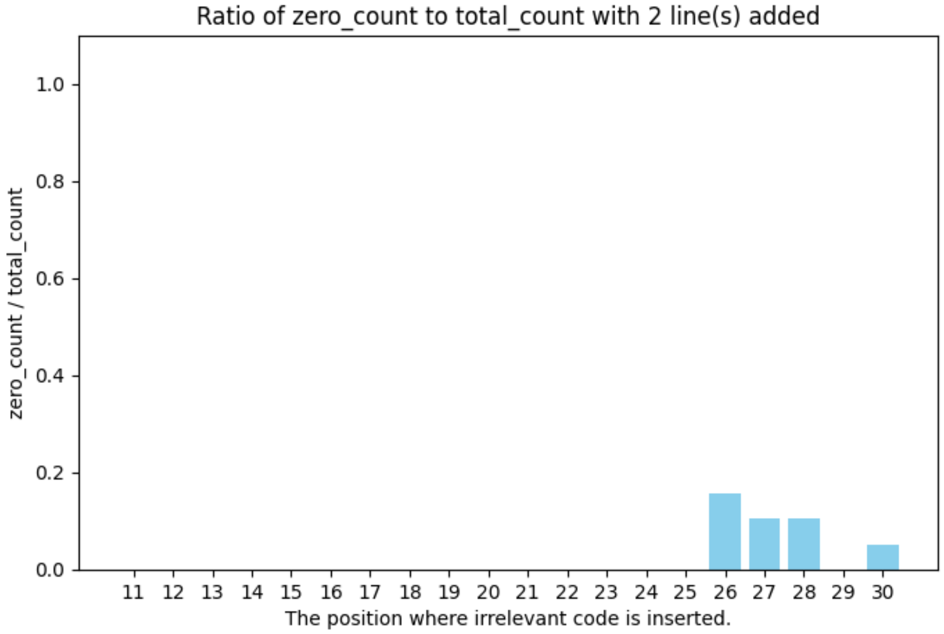

fig6: LineVD’s performance in a dataset with two irrelevant lines of code added

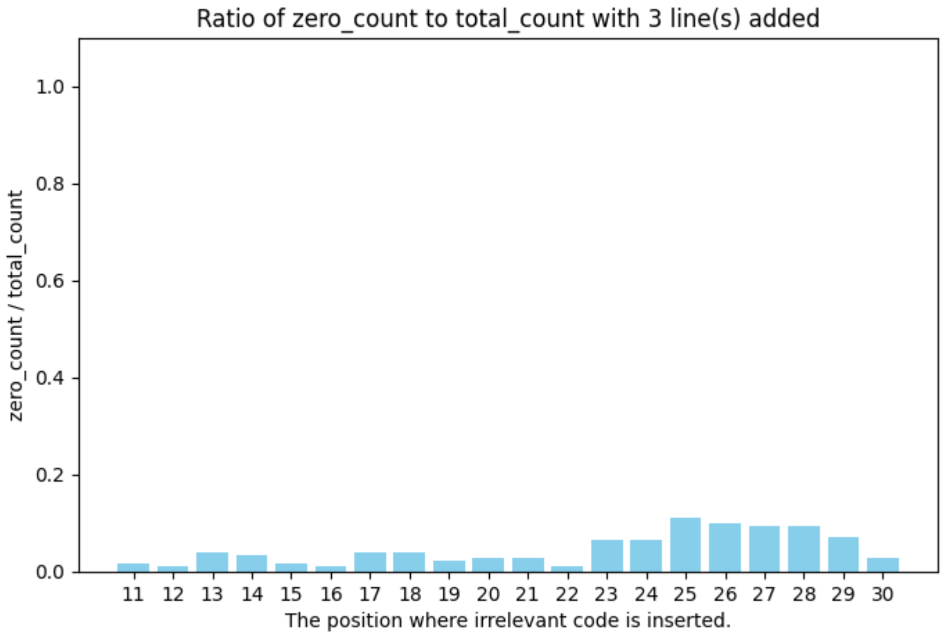

fig7: LineVD's performance in a dataset with three irrelevant lines of code added

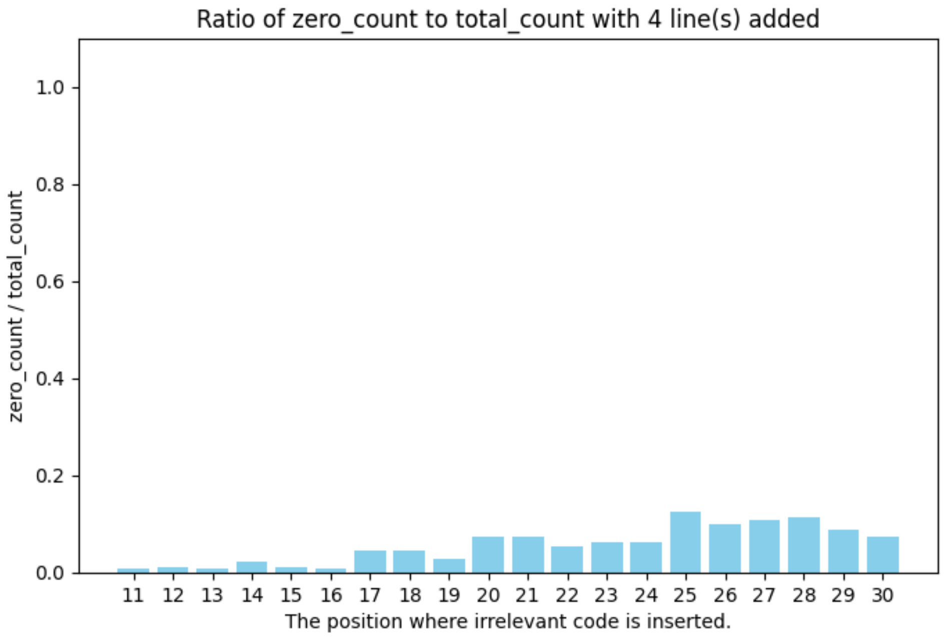

fig8: LineVD's performance in a dataset with four irrelevant lines of code added

As observed, the inclusion of these additional experiments would take up substantial space in the paper while providing limited added value in terms of generalizing our findings. The experimental results align with our original conclusions: **RCVD++** can correctly distinguish all data in this PLATE-dataset, leading to the same conclusion as in Section 4.2.1 (The method proved highly effective in accurately identifying vulnerabilities in PLATE-datasets, with minimal interference from irrelevant code changes). **Devign** performs poorly, exhibiting a high error rate, and the most frequently identified line is far from the actual vulnerability at line 27, consistent with the conclusion in Section 4.2.2 (Devign struggles to extract meaningful features from the actual vulnerability. The model seems to focus on irrelevant features or nearby code segments rather than the true vulnerability). **Reveal** can correctly distinguish all data in this PLATE-dataset, leading to the same conclusion as in Section 4.2.3 (Reveal successfully demonstrating its capability as a model that can effectively extract features of vulnerable code). **LineVD** performs reasonably well but is affected by irrelevant code. However, its most frequently identified line is close to the actual vulnerability at line 27, aligning with the conclusion in Section 4.2.4 (LineVD demonstrates promising results in detecting vulnerabilities. Additionally, although the model performs well with small modifications, it is sensitive to larger disruptions in code. These findings indicate that while LineVD is effective in certain contexts, there is room for further improvement in its robustness and generalization ability to handle a wider range of vulnerability types and code perturbations). To ensure transparency, we have made these 10 CVE files publicly available as part of our open-source materials.

3) The reason additional CVEs do not enhance the diversity of our findings is that our work focuses on identifying the limitations of existing methods. In other words, even a single poorly performing CVE example is sufficient to demonstrate a model's shortcomings in extracting vulnerability-related features (e.g., any of the test results for Devign indicate that it lacks the capability to extract features correctly). Conversely, a model that correctly classifies all irrelevant-code-added programs in a PLATE-dataset can be confidently recognized for its robustness against irrelevant code, as the PLATE-dataset is expanded from a CVE vulnerability file into over 1,000 samples, providing strong evidence for this conclusion (as seen with RCVD++ and Reveal). For models that perform moderately well on individual cases, we can only infer that they likely have feature extraction capabilities but weak resistance to interference (such as LineVD). Identifying a few fully correct examples for such models would not alter our overall assessment.
4) As such, incorporating more CVEs into the paper does not strengthen the general applicability of our conclusions.
5) If the reviewer’s concern is related to the dataset size, we would like to highlight that we have already open-sourced our tool in Section 3.3.1, which allows users to expand a single CVE into a PLATE-dataset. This tool is a core contribution of our work—it enables users to specify the statement location and insertion range to generate a dataset automatically, facilitating further experiments. This approach not only ensures reproducibility but also allows researchers to conduct experiments on vulnerabilities of their own interest, addressing potential concerns regarding dataset diversity.

In summary, increasing the diversity of CVEs does not enhance the diversity of our conclusions. To address this concern, we have made the following modifications to our paper:

1) We have added descriptions of these ten vulnerabilities in the introductory part of Section 4.1 and provided the open-source repository . This allows readers to analyze and determine the applicable scenarios of our study.
2) We have provided the open-source repository for the dataset expansion tool in

Section 3.3.5, which enable users to replicate our experiments easily and conduct further research on vulnerabilities of interest.

3) We have systematically revised the descriptions of Figures 5 to 10 to more clearly convey the experimental results and conclusions.

We appreciate the reviewer's valuable feedback and believe that our modifications help clarify our approach while maintaining the paper's core focus.

[Comment 2]

Simplify Technical Sections: Break down complex methodologies and results for wider accessibility.

[Reply 2]

Thank you for your valuable suggestion. We acknowledge that the methodology section in the original manuscript was overly dense and lacked sufficient structural clarity, which may have hindered readability. We sincerely apologize for any difficulty this may have caused. To improve accessibility and readability, we have made the following modifications in Section 3:

1) We have introduced a more structured organization by dividing each subsection into well-defined subsubsections. This systematic restructuring clarifies our thought process and methodology.
2) In Section 3.2, we have broken down the previously long and dense descriptions into distinct, logically organized components. This refinement enhances readability and presents the conceptual framework of Program-PLATE in a more structured manner.

These improvements can be found in the revised version of Section 3. We hope that these modifications address your concerns and significantly enhance the clarity of our methodology.

[Comment 3]

Enhance Visuals: Improve figure clarity and provide more detailed captions and discussions.

[Reply 3]

Thank you for your valuable suggestion. We acknowledge that some figures in the original manuscript had issues that made comparisons less intuitive and introduced challenges in interpretation. To address these concerns, we have made the following modifications: For all the figures with data values, we have standardized the upper limit of the y-axis to 1.0. This adjustment ensures consistency across figures and facilitates direct comparisons.

In addition to improving figure clarity, we have also refined the experimental discussions:

1) In Section 4.2, we have reorganized the content using a modular structure. Each

subsection now follows a consistent format: **analysis of CVE-2011 (if applicable), analysis of CVE-2013 (if applicable), and conclusion**. This structured approach enhances readability and logical flow.

2) We have ensured formatting consistency across subsections in Section 4.2 to provide a more coherent reading experience.

These modifications can be found in the revised version of Section 4.2. We sincerely appreciate your feedback, which has helped us improve the clarity and presentation of our results.

[Comment 4]

Explore Hybrid Methods: Further develop hybrid detection approaches combining rule-based and learning-based techniques.

[Reply 4]

Thank you for your insightful suggestion. We appreciate the importance of hybrid detection approaches and would like to highlight that we have already conducted research in this area, which has been submitted as a separate paper. Therefore, we have chosen not to expand on this topic within the current manuscript to maintain focus.
However, to strengthen the experimental section, we have re-evaluated this aspect using RCVD++ and updated the corresponding results in our paper. The revised experimental findings have replaced the original results in Section 4.2.1.

[Comment 5]

Overall, the paper demonstrates a strong contribution to the field of software vulnerability detection, with room for improvements in presentation and dataset scope.

[Reply 5]

Thank you for your positive evaluation of our work. We sincerely appreciate your recognition of our contribution to software vulnerability detection, as well as your constructive feedback on areas for improvement. In response to your suggestions, we have made corresponding revisions and enhancements to the manuscript. We hope that these modifications align with your expectations and further improve the clarity and comprehensiveness of our study.

Reviewer 2

Thank you for the reviewer's comments concerning our manuscript entitled "Program-PLATE: A Method for Identifying the Ability to Extract Vulnerability Features". Those comments are valuable and very helpful. We have read through comments carefully and have made corrections. Based on the instructions provided, we uploaded the file of the revised manuscript. The revisions in the manuscript are highlighted in yellow.

[Comment 1]

The motivations should be further highlighted in the manuscript, e.g., what problems did the previous works exist? How to solve these problems? The authors may consider analyzing the problems of the previous works and how to address these problems with the proposed method.

[Reply 1]

Thank you for your insightful suggestion. We acknowledge that the original manuscript did not clearly articulate the limitations of existing approaches and how our method addresses these challenges. To improve clarity and completeness, we have reorganized the **Related Work** section and provided a more detailed discussion. The specific modifications are as follows:

1) For each category of existing methods, we have structured the discussion into two distinct components: **Existing Approaches** and **Advantages and Limitations.** This modular structure enhances readability and facilitates a clearer comparison with our proposed method.
2) We have expanded the coverage of vulnerability detection techniques by incorporating a broader range of related works, including recent advancements in large language model (LLM)-based approaches. This ensures a more comprehensive and up-to-date discussion.

These revisions can be found in the updated **Related Work** section. We appreciate your valuable feedback, which has helped us strengthen the motivation and contextualization of our work.

[Comment 2]

The Related Work section could be further extended and incorporates additional discussions on background, challenges, literature review of this manuscript.

[Reply 2]

Thank you for your valuable suggestion. We have addressed these concerns through the modifications described in **Reply 1**, where we have reorganized and expanded the **Related Work** section. These revisions include a more structured discussion of background, challenges, and relevant literature to provide a clearer context for our study.

[Comment 3]

The author should provide a more detailed explanation of the design process of the Program-PLATE.

[Reply 3]

Thank you for your valuable suggestion. We acknowledge that the methodology section in the original manuscript was overly dense and lacked sufficient structural clarity, which may have hindered readability. We sincerely apologize for any difficulty this may have caused. To improve accessibility and readability, we have made the following modifications in Section 3:

1) We have introduced a more structured organization by dividing each subsection into well-defined subsubsections. This systematic restructuring clarifies our thought process and methodology.
2) In Section 3.2, we have broken down the previously long and dense descriptions into distinct, logically organized components. This refinement enhances readability and presents the conceptual framework of Program-PLATE in a more structured manner.

These improvements can be found in the revised version of Section 3. We hope that these modifications address your concerns and significantly enhance the clarity of our methodology.

[Comment 4]

The citation format of references needs to be standardized.

[Reply 4]

Thank you for your careful review and valuable suggestion. We acknowledge that the citation format in the original manuscript was not fully standardized. To address this issue, we have revised all citations based on the formatting conventions observed in previously published papers in **CyberSecurity**. The specific modifications are as follows:

1) In the **Related Work** section, citations have been consistently placed immediately after the author names.
2) In other sections, citations now appear directly after the mention of the corresponding work.

3) For references to multiple works, citations have been grouped following the term **works** in the sentence.

These adjustments ensure a more consistent and professional citation format throughout the manuscript.

[Comment 5]

The quality of language needs significant improvement, and professional editing may be necessary.

[Reply 5]

Thank you for your valuable suggestion. We acknowledge that the original manuscript had issues with language clarity and readability. To improve the overall quality of the writing, we have conducted a thorough revision, focusing on the following aspects:

1) Refining imprecise descriptions to enhance clarity and precision.
2) Rewriting informal or colloquial expressions to ensure a more academic tone.
3) Structuring explanations in a modular and segmented manner rather than presenting lengthy, dense paragraphs.

In particular, **Section 3 and Section 4** have undergone substantial revisions to improve readability and coherence. We believe these modifications significantly enhance the linguistic quality of the manuscript.

[Summary]

Thank you for your evaluation of our work. We sincerely appreciate your recognition of our contribution to software vulnerability detection, as well as your constructive feedback on areas for improvement. In response to your suggestions, we have made corresponding revisions and enhancements to the manuscript. We hope that these modifications align with your expectations and further improve the clarity and comprehensiveness of our study.