Author Details

- **Name:** Jaya Prakash Tirumalasetty , Abhitosh Kumar
- **Email:** jtirumalasetty@albany.edu akumar6@albany.edu
- **Team Number:** 2
- GitHub

Questions

Answer the following questions about your tool. Your answers should be thorough and fully answer the question. Answers should be grammatically correct and be full sentences.

(8 points) What is the goal of this tool? What purpose does it bring to the competitions?

The primary goal of our tool is it was designed to exploit the remote code vulnerability. We can accomplish this using specifically crafted Microsoft documents. For the catch the flag based on our strategies we can easily get into the targets computer through delivery and it will create an huge impact

(8 points) Did other tools influence your tool? If so, what are they? If not, what was your inspiration for the tool?

Our tool drew inspiration from CVE-2023-36884 because it works like If an email or instant message attack scenario, the attacker could send the targeted user a specially crafted file that is designed to exploit the remote code execution vulnerability. In any case an attacker would have no way to force a user to view attacker-controlled content.

(8 points) What is the feasibility of another team member quickly learning to use or contribute to your tool? What makes it easy or difficult to learn?

This code, while intriguing, might require some extra effort to learn and contribute to. While its core goal and function structure are understandable, hurdles await. You'll need to know external libraries like docx and win32com.client, and potentially dabble in os and sys. Integrating with Microsoft Word through COM adds another layer of complexity, especially for newbies. The existing error messages aren't the most beginner-friendly, and comprehensive documentation is missing. To top it off, the potential use for exploiting vulnerabilities raises ethical concerns that need careful consideration. While the code showcases interesting possibilities, mastering it

might require specific prior knowledge and navigating some roadblocks.
Overall, learnability depends on the team member's existing knowledge and experience.
Familiarity with Python, file manipulation, and basic COM concepts would be beneficial.
Understanding security implications is crucial when dealing with such functionalities.