Author Details

- **Name:** Tarun,Abhitosh
- **Email:** akumar6@albany.edu
tkattasreenivasulu@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 my script is to execute system commands based on user input provided through the 'cmd' parameter. Specifically, the script runs these commands on the server and displays the output within HTML 'pre' tags. However, it's essential to acknowledge that this script introduces a significant security risk due to its vulnerability to command injection. Unintentionally, it could potentially serve as a gateway for malicious actors to execute arbitrary commands on the server, posing severe risks to the organization's security during competitions.

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

While specific tools may not have directly influenced this script, the inspiration likely stems from the general concept of command execution within web applications. However, it's crucial to emphasize that executing system commands based on user input without proper validation and sanitization is inherently risky. The script serves as a reminder to follow secure coding practices, avoiding direct command execution with user input. Proper input validation and sanitization are critical measures to mitigate potential risks and enhance overall security.

(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?

The feasibility for another team member to swiftly learn and contribute to this script is relatively high due to its simplicity. However, this simplicity also exposes the script to inherent security vulnerabilities. While the straightforward nature makes it easy to understand, it lacks fundamental security measures. To improve feasibility, comprehensive documentation could be provided, outlining the script's purpose, associated risks, and secure coding practices for handling user input. Additionally, educating team members on secure coding principles, particularly the risks associated with command injection, would enhance their understanding and ability to contribute safely.