For this second assignment, we were assigned to create a vulnerable web app based on the different types of vulnerabilities that an application can be subject to with two security issues.

For my assignment, the two intentional vulnerabilities I decided to include were the following:

1. Reflected XSS
2. Command Injection

I wrote my simple webapp using Flask for the first time and I must credit a lot of the design work and knowledge from the video series “Python Flask Tutorial”[1]. Using some of the template for the design, and the understanding of the know-how of creating a flask web app, I created two simple tools that were vulnerable to user input.

The first tool was to turn whatever text you input as red, but I purposely turned off the autoescape feature of Jinja2/Flask so that a user could inject javascript into the textfield and output the code.

The second tool was to find the ip address of a domain name using the nslookup tool that runs off the servers of these webapps (in our case, whatever local machine that we use to run the program). I purposely did not scrub the input to only accept domain names and no other pipelining, therefore attackers could inject OS commands into the textfield and get the output, allowing for exfiltration or an understanding of the web server itself.

References:

[1] <https://www.youtube.com/watch?v=MwZwr5Tvyxo>