**Lab: Reflected DOM XSS**

Problem: Reflected DOM vulnerabilities occur when the server-side application processes data from a request and echoes the data in the response. A script on the page then processes the reflected data in an unsafe way, ultimately writing it to a dangerous sink.

Goal: create an injection that calls the alert() function.

Solve:

1-A screenshot of a computer

Description automatically generated

2-

A screenshot of a computer screen

Description automatically generated

3-

A screen shot of a computer

Description automatically generated

4-

A screenshot of a computer screen

Description automatically generated

5-An arithmetic operator (in this case the subtraction operator) is then used to separate the expressions before the alert() function is called. Finally, a closing curly bracket and two forward slashes close the JSON object early and comment out what would have been the rest of the object.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated