StackOverFlow.

Saif Ezzat.

A picture containing text, screenshot, software, multimedia software

Description automatically generated

Using nano I was able to examine the code. Clearly we can see a vulnerability in the bad() function it allows user to input any number of items without checking the size of the input which makes the stack vulnerable to overflow.

I executed the program with the security flags disabled like canary and pie. And I passed a valid input and another time an invalid input and the program crashed.

A screenshot of a computer program

Description automatically generated with medium confidence

A screenshot of a computer screen

Description automatically generated with medium confidence

Using valgrind I checked for vulnerabilities and found spaced allocated without being freed after use.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

I changed the permission on the file using chmod and chown to have the file owned by root then I passed in some padding + addr in the memory for the pointer of the eip + some ‘/x90’ no operation slide then a shell code I was able to create using shellcraft.linux.i386

A screenshot of a computer program

Description automatically generated with medium confidence

A screenshot of a computer program

Description automatically generated with medium confidence