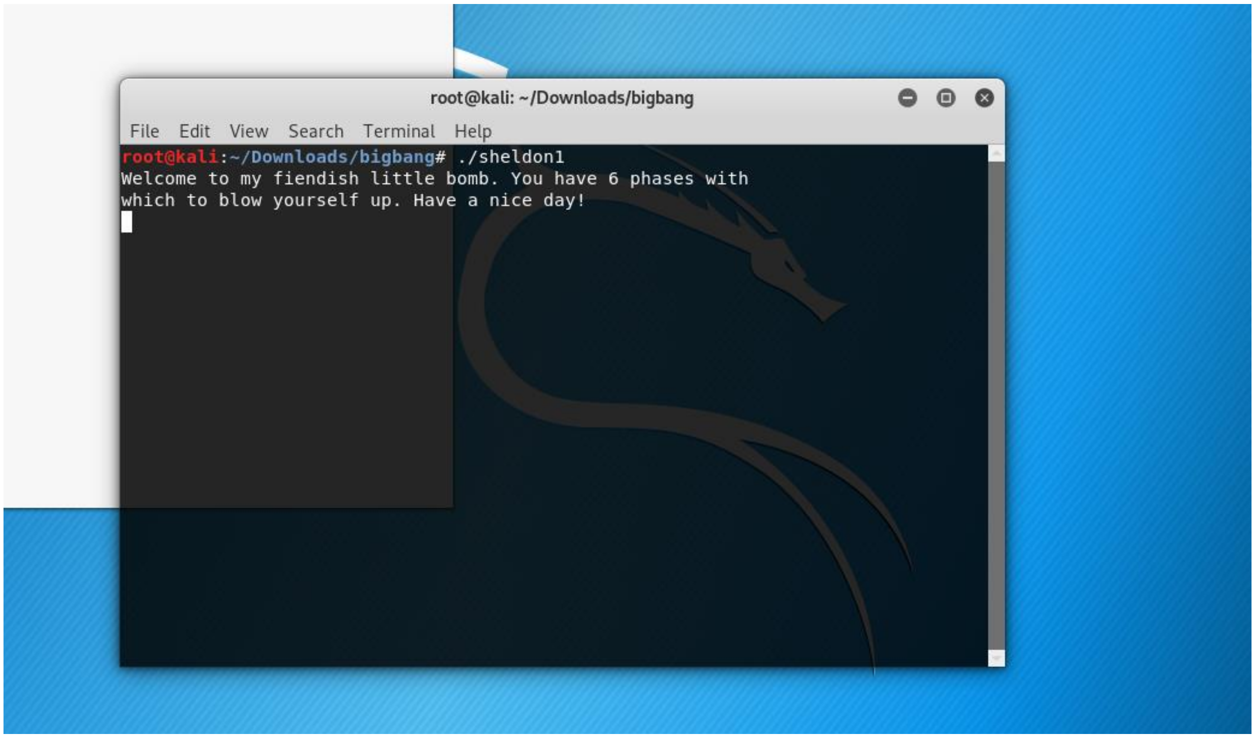
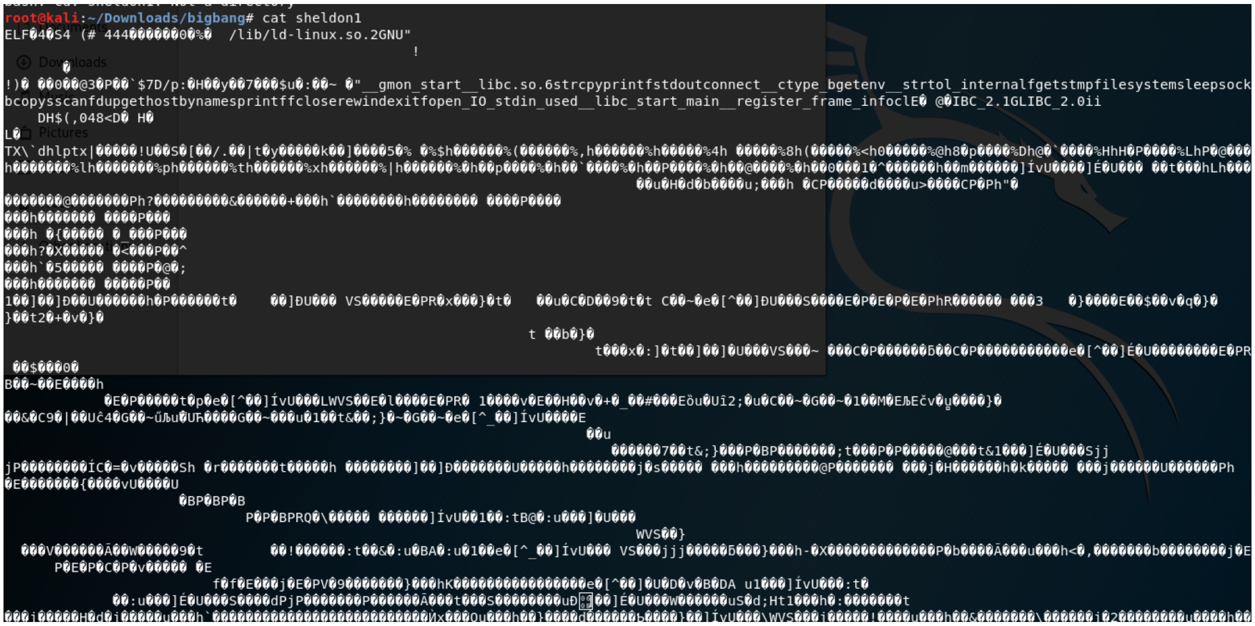
SHELDON1

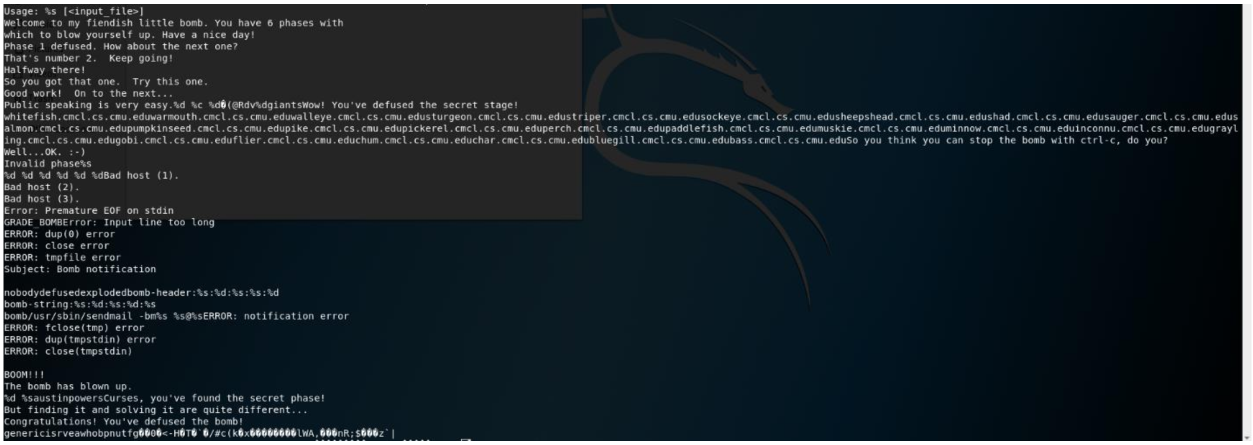


root@kali: ~/Downloads/bigbang
File Edit View Search Terminal Help

```
root@kali:~/Downloads/bigbang# ./sheldon1
Welcome to my fiendish little bomb. You have 6 phases with
which to blow yourself up. Have a nice day!
```



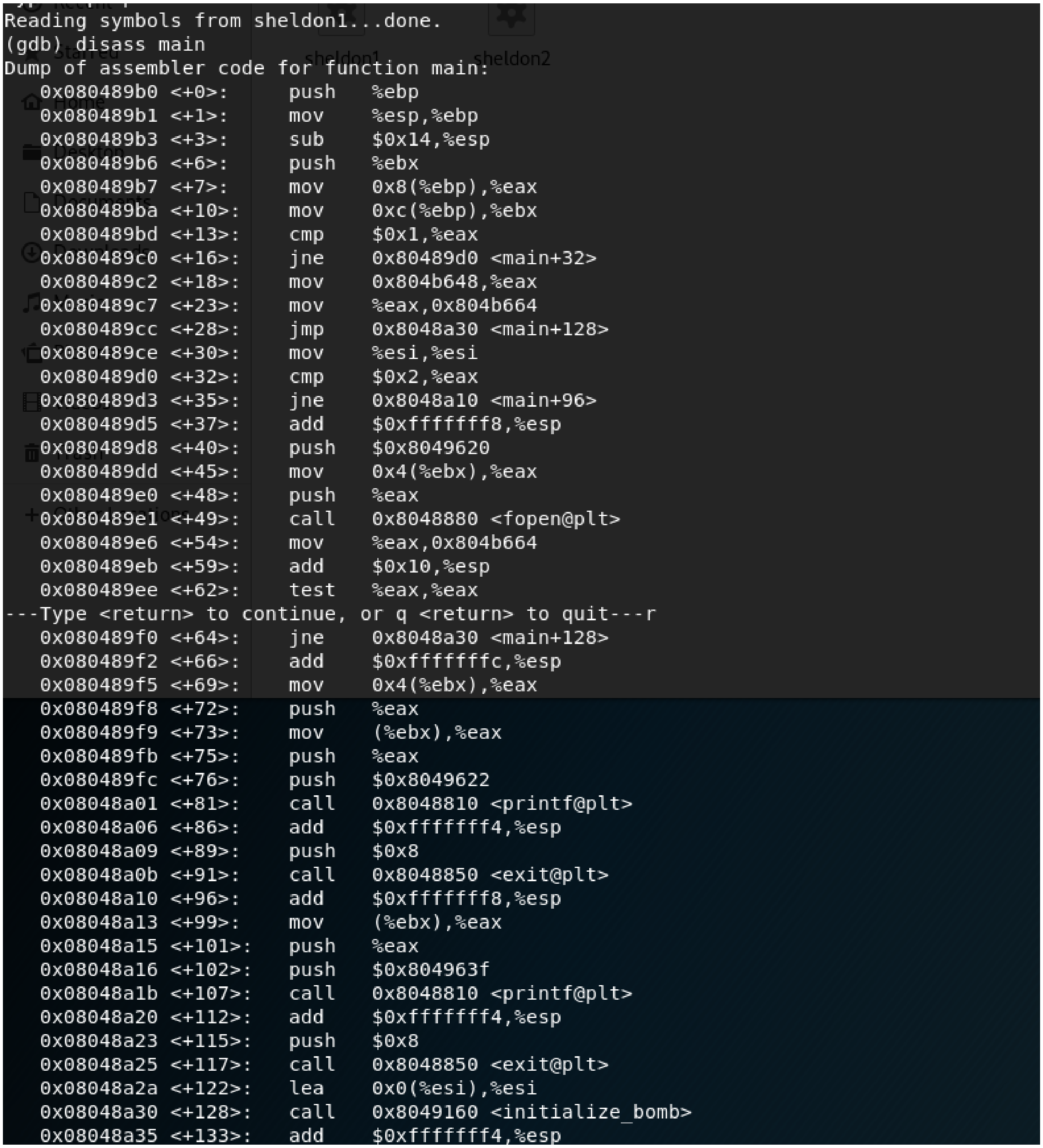
```
root@kali:~/Downloads/bigbang# cat sheldon1
ELF�4�S4 (# 444��������0�%�  /lib/ld-linux.so.2GNU"
                                                  !
       �
!)� ��0��@3�P��`$7D/p:�H��y��7���$u�:��~ �"__gmon_start__libc.so.6strcpyprintfstdoutconnect__ctype_bgetenv__strtol_internalfgetstmpfilesystemsleepsock
bcopysscanfdupgethostbynamesprintffcloserewindexitfopen_IO_stdin_used__libc_start_main__register_frame_infoclE� @�IBC_2.1GLIBC_2.0ii
    DH$(,048<D� H�
L�
TX\`dhlptx|�����!U��S�[��/.��|t�y�����k��]����5�% �%$h������%(������%,h������%h�����%4h �����%8h(�����%<h0�����%@h8�p����%Dh@�`����%HhH�P����%LhP�@���
h�������%lh�������%ph������%th������%xh������%|h������%�h��p����%�h��`����%�h��P����%�h��@����%�h��0����1�^������h��m������]ÍvU����]É�U��� ��t���hLh���
                                                                            ��u�H�d�b����u;���h �CP�����d����u>����CP�Ph"�
�������@�������Ph?���������&������+���h`��������h�������� ����P����
���h������� ����P���
���h �{����� �_���P���
���h?�X����� �<���P��^
���h`�5����� ����P�@�;
���h������� �����P��
1��]��]Đ��U������h�P������t�    ��]ĐU��� VS�����E�PR�x���}�t�   ��u�C�D��9�t�t C��~�e�[^��]ĐU���S����E�P�E�P�E�PhR������ ���3   �}����E��$��v�q�}�
}��t2�+�v�}�
                                                               t ��b�}�
                                                                       t���x�:]�t��]��]�U���VS���~ ���C�P������Б��C�P�����������e�[^��]É�U���������E�PR
 ��$����0�
B��~��E����h
            �E�P������t�p�e�[^��]ÍvU���LWVS��E�l����E�PR� 1����v�E��H��v�+�_��#���Eȍu�Uî2;�u�C��~�G��~�1��M�EЉEčv�ų����}�
��&�C9�|��Uĉ4�G��~űЉu�UЋ����G��~���u�1��t&��;}�~�G��~�e�[^_��]ÍvU����E
                                                                         ��u
                                                                            ������7��t&;}���P�BP�������;t���P�P�����@���t&1���]É�U���Sjj
jP��������ÍC�=�v�����Sh �r�������t�����h ��������]��]Đ�������U�����h��������j�s����� ���h���������@P������� ���j�H������h�k����� ���j������U������Ph
�E�������{����vU�����U
                     �BP�BP�B
                             P�P�BPRQ�\����� ������]ÍvU��1��:tB@�:u���]�U���
                                                                            WVS��}
  ���V�������Ā��W������9�t        ��!������:t��&�:u�BA�:u�1��e�[^_��]ÍvU��� VS���jjj�����Б���}���h-�X��������������P�b����Ā���u���h<�,�������b��������j�E
      P�E�P�C�P�v����� �E
                         f�f�E���j�E�PV�9��������}���hK����������������e�[^��]�U�D�v�B�DA u1���]ÍvU���:t�
             ��:u���]É�U���S����dPjP��������P�������Ā���t���S���������uĐ▯��]É�U���W������uS�d;Ht1���h�:�������t
���j�����H�d�j������u���h`����������������������������Йx���Ou���h��}����d�������ь����}��]ÍvU���\WVS���j�����!����u���h��&�������\������j�2��������u����h��
```



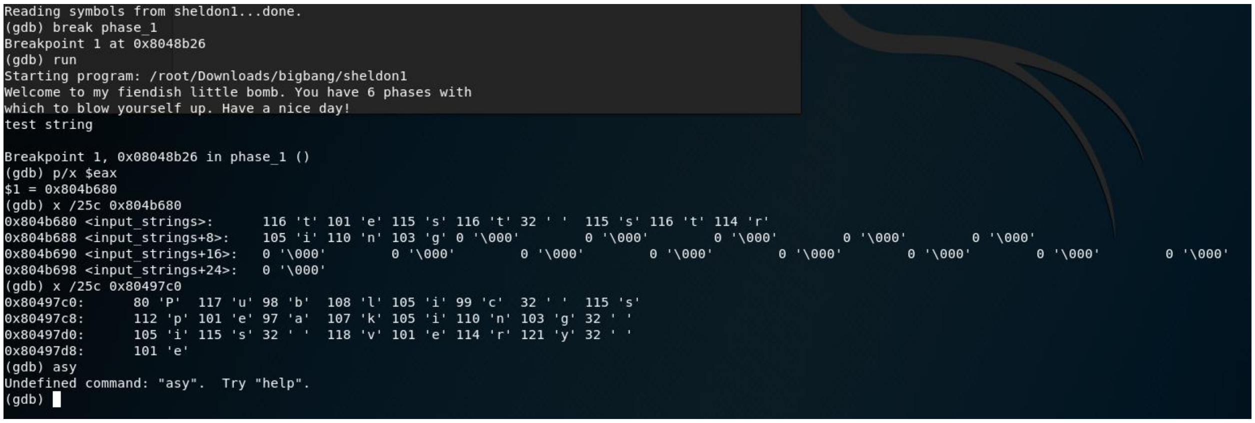
```
Usage: %s [<input_file>]
Welcome to my fiendish little bomb. You have 6 phases with
which to blow yourself up. Have a nice day!
Phase 1 defused. How about the next one?
That's number 2.  Keep going!
Halfway there!
So you got that one.  Try this one.
Good work!  On to the next...
Public speaking is very easy.%d %c %d�(@Rdv%dgiantsWow! You've defused the secret stage!
whitefish.cmcl.cs.cmu.eduwarmouth.cmcl.cs.cmu.eduwalleye.cmcl.cs.cmu.edusturgeon.cmcl.cs.cmu.edustriper.cmcl.cs.cmu.edusockeye.cmcl.cs.cmu.edusheepshead.cmcl.cs.cmu.edushad.cmcl.cs.cmu.edusauger.cmcl.cs.cmu.edus
almon.cmcl.cs.cmu.edupumpkinseed.cmcl.cs.cmu.edupike.cmcl.cs.cmu.edupickerel.cmcl.cs.cmu.eduperch.cmcl.cs.cmu.edupaddlefish.cmcl.cs.cmu.edumuskie.cmcl.cs.cmu.eduminnow.cmcl.cs.cmu.eduinconnu.cmcl.cs.cmu.edugrayl
ing.cmcl.cs.cmu.edugobi.cmcl.cs.cmu.eduflier.cmcl.cs.cmu.educhum.cmcl.cs.cmu.educhar.cmcl.cs.cmu.edubluegill.cmcl.cs.cmu.edubass.cmcl.cs.cmu.eduSo you think you can stop the bomb with ctrl-c, do you?
Well...OK. :-)
Invalid phase%s
%d %d %d %d %d %dBad host (1).
Bad host (2).
Bad host (3).
Error: Premature EOF on stdin
GRADE_BOMBError: Input line too long
ERROR: dup(0) error
ERROR: close error
ERROR: tmpfile error
Subject: Bomb notification

nobodydefusedexplodedbomb-header:%s:%d:%s:%s:%d
bomb-string:%s:%d:%s:%d:%s
bomb/usr/sbin/sendmail -bm%s %s@%sERROR: notification error
ERROR: fclose(tmp) error
ERROR: dup(tmpstdin) error
ERROR: close(tmpstdin)

BOOM!!!
The bomb has blown up.
%d %saustinpowersCurses, you've found the secret phase!
But finding it and solving it are quite different...
Congratulations! You've defused the bomb!
genericisrveawhobpnutfg���0�<-H�T�`�/#c(k�x��������lWA,���nR;$���z`|
```

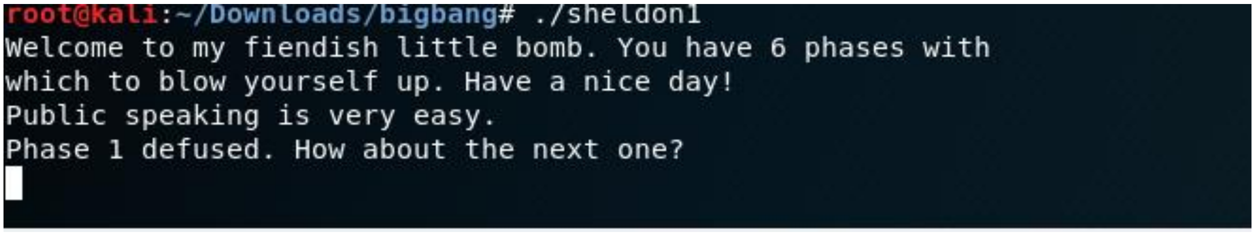


```
Reading symbols from sheldon1...done.
(gdb) disass main
Dump of assembler code for function main:
   0x080489b0 <+0>:     push   %ebp
   0x080489b1 <+1>:     mov    %esp,%ebp
   0x080489b3 <+3>:     sub    $0x14,%esp
   0x080489b6 <+6>:     push   %ebx
   0x080489b7 <+7>:     mov    0x8(%ebp),%eax
   0x080489ba <+10>:    mov    0xc(%ebp),%ebx
   0x080489bd <+13>:    cmp    $0x1,%eax
   0x080489c0 <+16>:    jne    0x80489d0 <main+32>
   0x080489c2 <+18>:    mov    0x804b648,%eax
   0x080489c7 <+23>:    mov    %eax,0x804b664
   0x080489cc <+28>:    jmp    0x8048a30 <main+128>
   0x080489ce <+30>:    mov    %esi,%esi
   0x080489d0 <+32>:    cmp    $0x2,%eax
   0x080489d3 <+35>:    jne    0x8048a10 <main+96>
   0x080489d5 <+37>:    add    $0xfffffff8,%esp
   0x080489d8 <+40>:    push   $0x8049620
   0x080489dd <+45>:    mov    0x4(%ebx),%eax
   0x080489e0 <+48>:    push   %eax
   0x080489e1 <+49>:    call   0x8048880 <fopen@plt>
   0x080489e6 <+54>:    mov    %eax,0x804b664
   0x080489eb <+59>:    add    $0x10,%esp
   0x080489ee <+62>:    test   %eax,%eax
---Type <return> to continue, or q <return> to quit---r
   0x080489f0 <+64>:    jne    0x8048a30 <main+128>
   0x080489f2 <+66>:    add    $0xfffffffc,%esp
   0x080489f5 <+69>:    mov    0x4(%ebx),%eax
   0x080489f8 <+72>:    push   %eax
   0x080489f9 <+73>:    mov    (%ebx),%eax
   0x080489fb <+75>:    push   %eax
   0x080489fc <+76>:    push   $0x8049622
   0x08048a01 <+81>:    call   0x8048810 <printf@plt>
   0x08048a06 <+86>:    add    $0xfffffff4,%esp
   0x08048a09 <+89>:    push   $0x8
   0x08048a0b <+91>:    call   0x8048850 <exit@plt>
   0x08048a10 <+96>:    add    $0xfffffff8,%esp
   0x08048a13 <+99>:    mov    (%ebx),%eax
   0x08048a15 <+101>:   push   %eax
   0x08048a16 <+102>:   push   $0x804963f
   0x08048a1b <+107>:   call   0x8048810 <printf@plt>
   0x08048a20 <+112>:   add    $0xfffffff4,%esp
   0x08048a23 <+115>:   push   $0x8
   0x08048a25 <+117>:   call   0x8048850 <exit@plt>
   0x08048a2a <+122>:   lea    0x0(%esi),%esi
   0x08048a30 <+128>:   call   0x8049160 <initialize_bomb>
   0x08048a35 <+133>:   add    $0xfffffff4,%esp
```



```
Reading symbols from sheldon1...done.
(gdb) break phase_1
Breakpoint 1 at 0x8048b26
(gdb) run
Starting program: /root/Downloads/bigbang/sheldon1
Welcome to my fiendish little bomb. You have 6 phases with
which to blow yourself up. Have a nice day!
test string

Breakpoint 1, 0x08048b26 in phase_1 ()
(gdb) p/x $eax
$1 = 0x804b680
(gdb) x /25c 0x804b680
0x804b680 <input_strings>:      116 't' 101 'e' 115 's' 116 't' 32 ' '  115 's' 116 't' 114 'r'
0x804b688 <input_strings+8>:    105 'i' 110 'n' 103 'g' 0 '\000'        0 '\000'        0 '\000'        0 '\000'        0 '\000'
0x804b690 <input_strings+16>:   0 '\000'        0 '\000'        0 '\000'        0 '\000'        0 '\000'        0 '\000'        0 '\000'        0 '\000'
0x804b698 <input_strings+24>:   0 '\000'
(gdb) x /25c 0x80497c0
0x80497c0:      80 'P'  117 'u' 98 'b'  108 'l' 105 'i' 99 'c'  32 ' '  115 's'
0x80497c8:      112 'p' 101 'e' 97 'a'  107 'k' 105 'i' 110 'n' 103 'g' 32 ' '
0x80497d0:      105 'i' 115 's' 32 ' '  118 'v' 101 'e' 114 'r' 121 'y' 32 ' '
0x80497d8:      101 'e'
(gdb) asy
Undefined command: "asy".  Try "help".
(gdb) 
```



```
root@kali:~/Downloads/bigbang# ./sheldon1
Welcome to my fiendish little bomb. You have 6 phases with
which to blow yourself up. Have a nice day!
Public speaking is very easy.
Phase 1 defused. How about the next one?
```