**Software Vulnerability Analysis**

Assignment 2

Sagar Wani (swani1@jhu.edu)

Prashanth Venkateswaran (pvenkat7@jhu.edu)

Chanakya Gaur ([cgaur1@jhu.edu](mailto:cgaur1@jhu.edu))

Reverse Engineering Deleverables

Header Dump

chanakya@chanakya-Aspire-E1-571:~$ objdump -h /usr/bin/konqueror  
  
/usr/bin/konqueror:     file format elf64-x86-64  
  
Sections:  
Idx Name          Size      VMA               LMA               File off  Algn  
  0 .interp       0000001c  0000000000400238  0000000000400238  00000238  2\*\*0  
                  CONTENTS, ALLOC, LOAD, READONLY, DATA  
  1 .note.ABI-tag 00000020  0000000000400254  0000000000400254  00000254  2\*\*2  
                  CONTENTS, ALLOC, LOAD, READONLY, DATA  
  2 .note.gnu.build-id 00000024  0000000000400274  0000000000400274  00000274  2\*\*2  
                  CONTENTS, ALLOC, LOAD, READONLY, DATA  
  3 .gnu.hash     00000050  0000000000400298  0000000000400298  00000298  2\*\*3  
                  CONTENTS, ALLOC, LOAD, READONLY, DATA  
  4 .dynsym       000001b0  00000000004002e8  00000000004002e8  000002e8  2\*\*3  
                  CONTENTS, ALLOC, LOAD, READONLY, DATA  
  5 .dynstr       00000141  0000000000400498  0000000000400498  00000498  2\*\*0  
                  CONTENTS, ALLOC, LOAD, READONLY, DATA  
  6 .gnu.version  00000024  00000000004005da  00000000004005da  000005da  2\*\*1  
                  CONTENTS, ALLOC, LOAD, READONLY, DATA  
  7 .gnu.version\_r 00000020  0000000000400600  0000000000400600  00000600  2\*\*3  
                  CONTENTS, ALLOC, LOAD, READONLY, DATA  
  8 .rela.dyn     00000018  0000000000400620  0000000000400620  00000620  2\*\*3  
                  CONTENTS, ALLOC, LOAD, READONLY, DATA  
  9 .rela.plt     00000030  0000000000400638  0000000000400638  00000638  2\*\*3  
                  CONTENTS, ALLOC, LOAD, READONLY, DATA  
 10 .init         0000001a  0000000000400668  0000000000400668  00000668  2\*\*2  
                  CONTENTS, ALLOC, LOAD, READONLY, CODE  
 11 .plt          00000030  0000000000400690  0000000000400690  00000690  2\*\*4  
                  CONTENTS, ALLOC, LOAD, READONLY, CODE  
 12 .plt.got      00000008  00000000004006c0  00000000004006c0  000006c0  2\*\*3  
                  CONTENTS, ALLOC, LOAD, READONLY, CODE  
 13 .text         00000192  00000000004006d0  00000000004006d0  000006d0  2\*\*4  
                  CONTENTS, ALLOC, LOAD, READONLY, CODE  
 14 .fini         00000009  0000000000400864  0000000000400864  00000864  2\*\*2  
                  CONTENTS, ALLOC, LOAD, READONLY, CODE  
 15 .rodata       00000004  0000000000400870  0000000000400870  00000870  2\*\*2  
                  CONTENTS, ALLOC, LOAD, READONLY, DATA  
 16 .eh\_frame\_hdr 0000003c  0000000000400874  0000000000400874  00000874  2\*\*2  
                  CONTENTS, ALLOC, LOAD, READONLY, DATA  
 17 .eh\_frame     00000104  00000000004008b0  00000000004008b0  000008b0  2\*\*3  
                  CONTENTS, ALLOC, LOAD, READONLY, DATA  
 18 .init\_array   00000008  0000000000600df0  0000000000600df0  00000df0  2\*\*3  
                  CONTENTS, ALLOC, LOAD, DATA  
 19 .fini\_array   00000008  0000000000600df8  0000000000600df8  00000df8  2\*\*3  
                  CONTENTS, ALLOC, LOAD, DATA  
 20 .jcr          00000008  0000000000600e00  0000000000600e00  00000e00  2\*\*3  
                  CONTENTS, ALLOC, LOAD, DATA  
 21 .dynamic      000001f0  0000000000600e08  0000000000600e08  00000e08  2\*\*3  
                  CONTENTS, ALLOC, LOAD, DATA  
 22 .got          00000008  0000000000600ff8  0000000000600ff8  00000ff8  2\*\*3  
                  CONTENTS, ALLOC, LOAD, DATA  
 23 .got.plt      00000028  0000000000601000  0000000000601000  00001000  2\*\*3  
                  CONTENTS, ALLOC, LOAD, DATA  
 24 .data         00000010  0000000000601028  0000000000601028  00001028  2\*\*3  
                  CONTENTS, ALLOC, LOAD, DATA  
 25 .bss          00000008  0000000000601038  0000000000601038  00001038  2\*\*0  
                  ALLOC  
 26 .gnu\_debuglink 00000034  0000000000000000  0000000000000000  00001038  2\*\*0  
                  CONTENTS, READONLY

Shared library dependencies

chanakya@chanakya-Aspire-E1-571:~$ ldd /usr/bin/konqueror  
    linux-vdso.so.1 =>  (0x00007ffc02fd7000)  
    libkdeinit4\_konqueror.so => /usr/lib/kde4/libkdeinit/libkdeinit4\_konqueror.so (0x00007fe3bc57b000)  
    libc.so.6 => /lib/x86\_64-linux-gnu/libc.so.6 (0x00007fe3bc192000)  
    libkonquerorprivate.so.4 => /usr/lib/libkonquerorprivate.so.4 (0x00007fe3bbf74000)  
    libkonq.so.5abi1 => /usr/lib/libkonq.so.5abi1 (0x00007fe3bbd3a000)  
    libkparts.so.4 => /usr/lib/libkparts.so.4 (0x00007fe3bbae3000)  
    libkcmutils.so.4 => /usr/lib/libkcmutils.so.4 (0x00007fe3bb8a0000)  
    libkfile.so.4 => /usr/lib/libkfile.so.4 (0x00007fe3bb5f3000)  
    libX11.so.6 => /usr/lib/x86\_64-linux-gnu/libX11.so.6 (0x00007fe3bb2b9000)  
    libkactivities.so.6 => /usr/lib/libkactivities.so.6 (0x00007fe3bb09c000)  
    libkio.so.5 => /usr/lib/libkio.so.5 (0x00007fe3babd3000)  
    libQtXml.so.4 => /usr/lib/x86\_64-linux-gnu/libQtXml.so.4 (0x00007fe3ba98d000)  
    libkdeui.so.5 => /usr/lib/libkdeui.so.5 (0x00007fe3ba311000)  
    libQtGui.so.4 => /usr/lib/x86\_64-linux-gnu/libQtGui.so.4 (0x00007fe3b961d000)  
    libkdecore.so.5 => /usr/lib/libkdecore.so.5 (0x00007fe3b913a000)  
    libQtCore.so.4 => /usr/lib/x86\_64-linux-gnu/libQtCore.so.4 (0x00007fe3b8c46000)  
    libQtDBus.so.4 => /usr/lib/x86\_64-linux-gnu/libQtDBus.so.4 (0x00007fe3b89c3000)  
    libstdc++.so.6 => /usr/lib/x86\_64-linux-gnu/libstdc++.so.6 (0x00007fe3b8641000)  
    libm.so.6 => /lib/x86\_64-linux-gnu/libm.so.6 (0x00007fe3b8337000)  
    /lib64/ld-linux-x86-64.so.2 (0x00005595f753c000)  
    libz.so.1 => /lib/x86\_64-linux-gnu/libz.so.1 (0x00007fe3b811d000)  
    libXrender.so.1 => /usr/lib/x86\_64-linux-gnu/libXrender.so.1 (0x00007fe3b7f12000)  
    libsolid.so.4 => /usr/lib/libsolid.so.4 (0x00007fe3b7c09000)  
    libxcb.so.1 => /usr/lib/x86\_64-linux-gnu/libxcb.so.1 (0x00007fe3b79e7000)  
    libdl.so.2 => /lib/x86\_64-linux-gnu/libdl.so.2 (0x00007fe3b77e2000)  
    libQtNetwork.so.4 => /usr/lib/x86\_64-linux-gnu/libQtNetwork.so.4 (0x00007fe3b748d000)  
    libQtSvg.so.4 => /usr/lib/x86\_64-linux-gnu/libQtSvg.so.4 (0x00007fe3b7234000)  
    libstreamanalyzer.so.0 => /usr/lib/libstreamanalyzer.so.0 (0x00007fe3b6fb6000)  
    libacl.so.1 => /lib/x86\_64-linux-gnu/libacl.so.1 (0x00007fe3b6dae000)  
    libattr.so.1 => /lib/x86\_64-linux-gnu/libattr.so.1 (0x00007fe3b6ba9000)  
    libgcc\_s.so.1 => /lib/x86\_64-linux-gnu/libgcc\_s.so.1 (0x00007fe3b6992000)  
    libSM.so.6 => /usr/lib/x86\_64-linux-gnu/libSM.so.6 (0x00007fe3b678a000)  
    libICE.so.6 => /usr/lib/x86\_64-linux-gnu/libICE.so.6 (0x00007fe3b6570000)  
    libattica.so.0.4 => /usr/lib/x86\_64-linux-gnu/libattica.so.0.4 (0x00007fe3b62b2000)  
    libdbusmenu-qt.so.2 => /usr/lib/x86\_64-linux-gnu/libdbusmenu-qt.so.2 (0x00007fe3b607e000)  
    libXfixes.so.3 => /usr/lib/x86\_64-linux-gnu/libXfixes.so.3 (0x00007fe3b5e78000)  
    libfontconfig.so.1 => /usr/lib/x86\_64-linux-gnu/libfontconfig.so.1 (0x00007fe3b5c34000)  
    libpthread.so.0 => /lib/x86\_64-linux-gnu/libpthread.so.0 (0x00007fe3b5a17000)  
    libaudio.so.2 => /usr/lib/x86\_64-linux-gnu/libaudio.so.2 (0x00007fe3b57fd000)  
    libglib-2.0.so.0 => /lib/x86\_64-linux-gnu/libglib-2.0.so.0 (0x00007fe3b54ec000)  
    libpng12.so.0 => /lib/x86\_64-linux-gnu/libpng12.so.0 (0x00007fe3b52c7000)  
    libfreetype.so.6 => /usr/lib/x86\_64-linux-gnu/libfreetype.so.6 (0x00007fe3b501d000)  
    libgobject-2.0.so.0 => /usr/lib/x86\_64-linux-gnu/libgobject-2.0.so.0 (0x00007fe3b4dc9000)  
    libXi.so.6 => /usr/lib/x86\_64-linux-gnu/libXi.so.6 (0x00007fe3b4bb9000)  
    libXext.so.6 => /usr/lib/x86\_64-linux-gnu/libXext.so.6 (0x00007fe3b49a7000)  
    libbz2.so.1.0 => /lib/x86\_64-linux-gnu/libbz2.so.1.0 (0x00007fe3b4796000)  
    liblzma.so.5 => /lib/x86\_64-linux-gnu/liblzma.so.5 (0x00007fe3b4574000)  
    libdlrestrictions.so.1 => /usr/lib/libdlrestrictions.so.1 (0x00007fe3b436e000)  
    librt.so.1 => /lib/x86\_64-linux-gnu/librt.so.1 (0x00007fe3b4166000)  
    libdbus-1.so.3 => /lib/x86\_64-linux-gnu/libdbus-1.so.3 (0x00007fe3b3f1a000)  
    libudev.so.1 => /lib/x86\_64-linux-gnu/libudev.so.1 (0x00007fe3b3ef9000)  
    libXau.so.6 => /usr/lib/x86\_64-linux-gnu/libXau.so.6 (0x00007fe3b3cf5000)  
    libXdmcp.so.6 => /usr/lib/x86\_64-linux-gnu/libXdmcp.so.6 (0x00007fe3b3aef000)  
    libstreams.so.0 => /usr/lib/libstreams.so.0 (0x00007fe3b38b6000)  
    libxml2.so.2 => /usr/lib/x86\_64-linux-gnu/libxml2.so.2 (0x00007fe3b34fb000)  
    libuuid.so.1 => /lib/x86\_64-linux-gnu/libuuid.so.1 (0x00007fe3b32f5000)  
    libexpat.so.1 => /lib/x86\_64-linux-gnu/libexpat.so.1 (0x00007fe3b30cc000)  
    libXt.so.6 => /usr/lib/x86\_64-linux-gnu/libXt.so.6 (0x00007fe3b2e62000)  
    libpcre.so.3 => /lib/x86\_64-linux-gnu/libpcre.so.3 (0x00007fe3b2bf2000)  
    libffi.so.6 => /usr/lib/x86\_64-linux-gnu/libffi.so.6 (0x00007fe3b29ea000)  
    libsystemd.so.0 => /lib/x86\_64-linux-gnu/libsystemd.so.0 (0x00007fe3b2964000)  
    libicuuc.so.55 => /usr/lib/x86\_64-linux-gnu/libicuuc.so.55 (0x00007fe3b25d0000)  
    libselinux.so.1 => /lib/x86\_64-linux-gnu/libselinux.so.1 (0x00007fe3b23ad000)  
    libgcrypt.so.20 => /lib/x86\_64-linux-gnu/libgcrypt.so.20 (0x00007fe3b20cc000)  
    libicudata.so.55 => /usr/lib/x86\_64-linux-gnu/libicudata.so.55 (0x00007fe3b0615000)  
    libgpg-error.so.0 => /lib/x86\_64-linux-gnu/libgpg-error.so.0 (0x00007fe3b0400000)

Symbol List

chanakya@chanakya-Aspire-E1-571:~$ nm -D /usr/bin/konqueror  
0000000000601038 B \_\_bss\_start  
0000000000601028 D \_\_data\_start  
0000000000601028 W data\_start  
0000000000601038 D \_edata  
0000000000601040 B \_end  
0000000000400864 T \_fini  
                 w \_\_gmon\_start\_\_  
0000000000400668 T \_init  
0000000000400870 R \_IO\_stdin\_used  
                 w \_ITM\_deregisterTMCloneTable  
                 w \_ITM\_registerTMCloneTable  
                 w \_Jv\_RegisterClasses  
                 U kdemain  
0000000000400860 T \_\_libc\_csu\_fini  
00000000004007f0 T \_\_libc\_csu\_init  
                 U \_\_libc\_start\_main  
00000000004006e0 T \_start

Virtual Memory Table

Strace

Strace is an amazing widely known unix tool to trace system calls and signals. It might not be a good idea to run this command in production environments without meticoulously considering it's consiquences. It uses the arcane ptrace() debugging interface to debug the system calls. In reality strace might be pausing the application at least two times for each syscall to actually debug each call. If the speed isn't much of a concern of in a test case environment, this might prove to be an excellent debugging tool. The most used syscalls or the key syscalls are read, write, open, close, fork, exec, connect, accept, stat, ioctl, nmap, brk.

The read call will read the bytes from the file provided and write would, as the name suggests, write to those files. Open opens a file, essentially returns a file descriptor. While fork creates a new process, current porcess is forked to do it. Exec executes a new program. Close is used to close the file descriptor. To connect to a network host, connect is used. Accept to accept a connection and stat to read the file statistics. IOCTL will set the input output properties and other miscellanous functions. Nmap maps a file to the process memory address space and BRK is used to extend the heap pointer.

Some interesting facts on Strace:

* It is banned in france because it is classified as a cracking tool since it can trace the plain text input/output.
* The first starce is in display at Computer History Museum at San Jose which was made in 1961 using wire wrapped circuits and core memory and could trace upto 12 system calls a second.
* "The largest strace is the Soviet "Tacti-call" class, which can remain at syscall depth for over 120 days, and has a maximum crew of 160. It is nuclear powered, and has 4 forward and 2 aft signal tubes, each typically armed with type 9 signals."

Because of the above reasons it is highly relevant debugging tool that can be used for various other purposes as well. It provides us with important info about various issues, for example, which configuration files the program is reading at a given point of time, last file or library read by the program that led to its crashing. We can also save the output of strace and use it for offline debugging. Even for tracing out the performance issues strace proves to be of most use to understand how often a system call is executed, how much time does a kernel call is consuming, how much of the computing time is being used by program between two consequent kernel calls. As already discussed, complete input/output history of the program can be fetched using strace in case of in depth forensics.

root@kali:/usr/bin# strace -p 15698  
strace: Process 15698 attached  
restart\_syscall(<... resuming interrupted poll ...>) = 0  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(8, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
poll([{fd=3, events=POLLIN}, {fd=6, events=POLLIN}, {fd=7, events=POLLIN}, {fd=8, events=POLLIN}, {fd=9, events=POLLIN}, {fd=11, events=POLLIN}, {fd=12, events=POLLIN}, {fd=14, events=POLLIN}, {fd=26, events=POLLIN}], 9, 0) = 0 (Timeout)  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
poll([{fd=6, events=POLLIN|POLLOUT}], 1, -1) = 1 ([{fd=6, revents=POLLOUT}])  
writev(6, [{iov\_base="\24\0\6\0\31\0\0\4\211\1\0\0\211\1\0\0\0\0\0\0\1\0\0\0", iov\_len=24}, {iov\_base=NULL, iov\_len=0}, {iov\_base="", iov\_len=0}], 3) = 24  
poll([{fd=6, events=POLLIN}], 1, -1)    = 1 ([{fd=6, revents=POLLIN}])  
recvmsg(6, {msg\_name=NULL, msg\_namelen=0, msg\_iov=[{iov\_base="\1 \3419\1\0\0\0\211\1\0\0\4\0\0\0\1\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0"..., iov\_len=4096}], msg\_iovlen=1, msg\_controllen=0, msg\_flags=0}, 0) = 36  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
poll([{fd=6, events=POLLIN|POLLOUT}], 1, -1) = 1 ([{fd=6, revents=POLLOUT}])  
writev(6, [{iov\_base="\24\0\6\0\31\0\0\4P\1\0\0\4\0\0\0\0\0\0\0\0\10\0\0", iov\_len=24}, {iov\_base=NULL, iov\_len=0}, {iov\_base="", iov\_len=0}], 3) = 24  
poll([{fd=6, events=POLLIN}], 1, -1)    = 1 ([{fd=6, revents=POLLIN}])  
recvmsg(6, {msg\_name=NULL, msg\_namelen=0, msg\_iov=[{iov\_base="\1 \3429\0\0\0\0\4\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0", iov\_len=4096}], msg\_iovlen=1, msg\_controllen=0, msg\_flags=0}, 0) = 32  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(8, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
poll([{fd=3, events=POLLIN}, {fd=6, events=POLLIN}, {fd=7, events=POLLIN}, {fd=8, events=POLLIN}, {fd=9, events=POLLIN}, {fd=11, events=POLLIN}, {fd=12, events=POLLIN}, {fd=14, events=POLLIN}, {fd=26, events=POLLIN}], 9, 9999) = 2 ([{fd=6, revents=POLLIN}, {fd=8, revents=POLLIN}])  
recvmsg(6, {msg\_name=NULL, msg\_namelen=0, msg\_iov=[{iov\_base="W\0\3429\311\1\0\0\2\0\340\2\1\0\0\0~\373\307\2|\373\307\2\0\0\0\0\0\0\0\0", iov\_len=4096}], msg\_iovlen=1, msg\_controllen=0, msg\_flags=0}, 0) = 32  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(8, {msg\_name=NULL, msg\_namelen=0, msg\_iov=[{iov\_base="W\0i\24\1\0 \4\2\0\340\2\1\0\0\0~\373\307\2|\373\307\2\0\0\0\0\0\0\0\0", iov\_len=4096}], msg\_iovlen=1, msg\_controllen=0, msg\_flags=0}, 0) = 32  
recvmsg(8, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(8, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
poll([{fd=3, events=POLLIN}, {fd=6, events=POLLIN}, {fd=7, events=POLLIN}, {fd=8, events=POLLIN}, {fd=9, events=POLLIN}, {fd=11, events=POLLIN}, {fd=12, events=POLLIN}, {fd=14, events=POLLIN}, {fd=26, events=POLLIN}], 9, 4558) = 2 ([{fd=6, revents=POLLIN}, {fd=8, revents=POLLIN}])  
recvmsg(6, {msg\_name=NULL, msg\_namelen=0, msg\_iov=[{iov\_base="W\0\3429\311\1\0\0\2\0\340\2\1\0\0\0\1\r\310\2\0\r\310\2\0\0\0\0\0\0\0\0", iov\_len=4096}], msg\_iovlen=1, msg\_controllen=0, msg\_flags=0}, 0) = 32  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(8, {msg\_name=NULL, msg\_namelen=0, msg\_iov=[{iov\_base="W\0i\24\1\0 \4\2\0\340\2\1\0\0\0\1\r\310\2\0\r\310\2\0\0\0\0\0\0\0\0", iov\_len=4096}], msg\_iovlen=1, msg\_controllen=0, msg\_flags=0}, 0) = 32  
recvmsg(8, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(8, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
poll([{fd=3, events=POLLIN}, {fd=6, events=POLLIN}, {fd=7, events=POLLIN}, {fd=8, events=POLLIN}, {fd=9, events=POLLIN}, {fd=11, events=POLLIN}, {fd=12, events=POLLIN}, {fd=14, events=POLLIN}, {fd=26, events=POLLIN}], 9, 75) = 1 ([{fd=26, revents=POLLIN}])  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(26, {msg\_name=NULL, msg\_namelen=0, msg\_iov=[{iov\_base="l\4\1\1\31\0\0\0b\35\2\0\265\0\0\0\10\1g\0\5a{sv}\0\0\0\0\0\0"..., iov\_len=2048}], msg\_iovlen=1, msg\_controllen=0, msg\_flags=MSG\_CMSG\_CLOEXEC}, MSG\_CMSG\_CLOEXEC) = 225  
recvmsg(26, {msg\_namelen=0}, MSG\_CMSG\_CLOEXEC) = -1 EAGAIN (Resource temporarily unavailable)  
write(3, "\1\0\0\0\0\0\0\0", 8)         = 8  
write(25, "\1\0\0\0\0\0\0\0", 8)        = 8  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(8, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
poll([{fd=3, events=POLLIN}, {fd=6, events=POLLIN}, {fd=7, events=POLLIN}, {fd=8, events=POLLIN}, {fd=9, events=POLLIN}, {fd=11, events=POLLIN}, {fd=12, events=POLLIN}, {fd=14, events=POLLIN}, {fd=26, events=POLLIN}], 9, 0) = 1 ([{fd=3, revents=POLLIN}])  
read(3, "\1\0\0\0\0\0\0\0", 16)         = 8  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(8, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
poll([{fd=3, events=POLLIN}, {fd=6, events=POLLIN}, {fd=7, events=POLLIN}, {fd=8, events=POLLIN}, {fd=9, events=POLLIN}, {fd=11, events=POLLIN}, {fd=12, events=POLLIN}, {fd=14, events=POLLIN}, {fd=26, events=POLLIN}], 9, 25) = 0 (Timeout)  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(8, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
poll([{fd=3, events=POLLIN}, {fd=6, events=POLLIN}, {fd=7, events=POLLIN}, {fd=8, events=POLLIN}, {fd=9, events=POLLIN}, {fd=11, events=POLLIN}, {fd=12, events=POLLIN}, {fd=14, events=POLLIN}, {fd=26, events=POLLIN}], 9, 0) = 0 (Timeout)  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
poll([{fd=6, events=POLLIN|POLLOUT}], 1, -1) = 1 ([{fd=6, revents=POLLOUT}])  
writev(6, [{iov\_base="\24\0\6\0\31\0\0\4\211\1\0\0\211\1\0\0\0\0\0\0\1\0\0\0", iov\_len=24}, {iov\_base=NULL, iov\_len=0}, {iov\_base="", iov\_len=0}], 3) = 24  
poll([{fd=6, events=POLLIN}], 1, -1)    = 1 ([{fd=6, revents=POLLIN}])  
recvmsg(6, {msg\_name=NULL, msg\_namelen=0, msg\_iov=[{iov\_base="\1 \3439\1\0\0\0\211\1\0\0\4\0\0\0\1\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0"..., iov\_len=4096}], msg\_iovlen=1, msg\_controllen=0, msg\_flags=0}, 0) = 36  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
poll([{fd=6, events=POLLIN|POLLOUT}], 1, -1) = 1 ([{fd=6, revents=POLLOUT}])  
writev(6, [{iov\_base="\24\0\6\0\31\0\0\4P\1\0\0\4\0\0\0\0\0\0\0\0\10\0\0", iov\_len=24}, {iov\_base=NULL, iov\_len=0}, {iov\_base="", iov\_len=0}], 3) = 24  
poll([{fd=6, events=POLLIN}], 1, -1)    = 1 ([{fd=6, revents=POLLIN}])  
recvmsg(6, {msg\_name=NULL, msg\_namelen=0, msg\_iov=[{iov\_base="\1 \3449\0\0\0\0\4\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0", iov\_len=4096}], msg\_iovlen=1, msg\_controllen=0, msg\_flags=0}, 0) = 32  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(8, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
poll([{fd=3, events=POLLIN}, {fd=6, events=POLLIN}, {fd=7, events=POLLIN}, {fd=8, events=POLLIN}, {fd=9, events=POLLIN}, {fd=11, events=POLLIN}, {fd=12, events=POLLIN}, {fd=14, events=POLLIN}, {fd=26, events=POLLIN}], 9, 9999) = 2 ([{fd=6, revents=POLLIN}, {fd=8, revents=POLLIN}])  
recvmsg(6, {msg\_name=NULL, msg\_namelen=0, msg\_iov=[{iov\_base="W\0\3449\311\1\0\0\2\0\340\2\1\0\0\0(\"\310\2&\"\310\2\0\0\0\0\0\0\0\0", iov\_len=4096}], msg\_iovlen=1, msg\_controllen=0, msg\_flags=0}, 0) = 32  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(8, {msg\_name=NULL, msg\_namelen=0, msg\_iov=[{iov\_base="W\0i\24\1\0 \4\2\0\340\2\1\0\0\0(\"\310\2&\"\310\2\0\0\0\0\0\0\0\0", iov\_len=4096}], msg\_iovlen=1, msg\_controllen=0, msg\_flags=0}, 0) = 32  
recvmsg(8, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(8, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
poll([{fd=3, events=POLLIN}, {fd=6, events=POLLIN}, {fd=7, events=POLLIN}, {fd=8, events=POLLIN}, {fd=9, events=POLLIN}, {fd=11, events=POLLIN}, {fd=12, events=POLLIN}, {fd=14, events=POLLIN}, {fd=26, events=POLLIN}], 9, 4661) = 2 ([{fd=6, revents=POLLIN}, {fd=8, revents=POLLIN}])  
recvmsg(6, {msg\_name=NULL, msg\_namelen=0, msg\_iov=[{iov\_base="W\0\3449\311\1\0\0\2\0\340\2\1\0\0\0l+\310\2R+\310\2\0\0\0\0\0\0\0\0", iov\_len=4096}], msg\_iovlen=1, msg\_controllen=0, msg\_flags=0}, 0) = 32  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(8, {msg\_name=NULL, msg\_namelen=0, msg\_iov=[{iov\_base="W\0i\24\1\0 \4\2\0\340\2\1\0\0\0l+\310\2R+\310\2\0\0\0\0\0\0\0\0", iov\_len=4096}], msg\_iovlen=1, msg\_controllen=0, msg\_flags=0}, 0) = 32  
recvmsg(8, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(8, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
poll([{fd=3, events=POLLIN}, {fd=6, events=POLLIN}, {fd=7, events=POLLIN}, {fd=8, events=POLLIN}, {fd=9, events=POLLIN}, {fd=11, events=POLLIN}, {fd=12, events=POLLIN}, {fd=14, events=POLLIN}, {fd=26, events=POLLIN}], 9, 2289) = 0 (Timeout)  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
poll([{fd=6, events=POLLIN|POLLOUT}], 1, -1) = 1 ([{fd=6, revents=POLLOUT}])  
writev(6, [{iov\_base="\24\0\6\0\31\0\0\4\211\1\0\0\211\1\0\0\0\0\0\0\1\0\0\0", iov\_len=24}, {iov\_base=NULL, iov\_len=0}, {iov\_base="", iov\_len=0}], 3) = 24  
poll([{fd=6, events=POLLIN}], 1, -1)    = 1 ([{fd=6, revents=POLLIN}])  
recvmsg(6, {msg\_name=NULL, msg\_namelen=0, msg\_iov=[{iov\_base="\1 \3459\1\0\0\0\211\1\0\0\4\0\0\0\1\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0"..., iov\_len=4096}], msg\_iovlen=1, msg\_controllen=0, msg\_flags=0}, 0) = 36  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
poll([{fd=6, events=POLLIN|POLLOUT}], 1, -1) = 1 ([{fd=6, revents=POLLOUT}])  
writev(6, [{iov\_base="\24\0\6\0\31\0\0\4P\1\0\0\4\0\0\0\0\0\0\0\0\10\0\0", iov\_len=24}, {iov\_base=NULL, iov\_len=0}, {iov\_base="", iov\_len=0}], 3) = 24  
poll([{fd=6, events=POLLIN}], 1, -1)    = 1 ([{fd=6, revents=POLLIN}])  
recvmsg(6, {msg\_name=NULL, msg\_namelen=0, msg\_iov=[{iov\_base="\1 \3469\0\0\0\0\4\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0", iov\_len=4096}], msg\_iovlen=1, msg\_controllen=0, msg\_flags=0}, 0) = 32  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(8, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
poll([{fd=3, events=POLLIN}, {fd=6, events=POLLIN}, {fd=7, events=POLLIN}, {fd=8, events=POLLIN}, {fd=9, events=POLLIN}, {fd=11, events=POLLIN}, {fd=12, events=POLLIN}, {fd=14, events=POLLIN}, {fd=26, events=POLLIN}], 9, 9999) = 2 ([{fd=6, revents=POLLIN}, {fd=8, revents=POLLIN}])  
recvmsg(6, {msg\_name=NULL, msg\_namelen=0, msg\_iov=[{iov\_base="W\0\3469\311\1\0\0\2\0\340\2\1\0\0\0\372>\310\2\371>\310\2\0\0\0\0\0\0\0\0", iov\_len=4096}], msg\_iovlen=1, msg\_controllen=0, msg\_flags=0}, 0) = 32  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(8, {msg\_name=NULL, msg\_namelen=0, msg\_iov=[{iov\_base="W\0i\24\1\0 \4\2\0\340\2\1\0\0\0\372>\310\2\371>\310\2\0\0\0\0\0\0\0\0", iov\_len=4096}], msg\_iovlen=1, msg\_controllen=0, msg\_flags=0}, 0) = 32  
recvmsg(8, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(6, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
recvmsg(8, {msg\_namelen=0}, 0)          = -1 EAGAIN (Resource temporarily unavailable)  
poll([{fd=3, events=POLLIN}, {fd=6, events=POLLIN}, {fd=7, events=POLLIN}, {fd=8, events=POLLIN}, {fd=9, events=POLLIN}, {fd=11, events=POLLIN}, {fd=12, events=POLLIN}, {fd=14, events=POLLIN}, {fd=26, events=POLLIN}], 9, 7285^Cstrace: Process 15698 detached  
 <detached ...>

Functionality

Konqueror is a web browsing application that consist of several embedded parts. Each of these parts is present inside a view, such as, icon views, tree views, html views etc. The user input is taken and parsed by the URI handler to browse the web as well as file management capabilities. The main() of the application that initiates all the necessary parts is present in the Konqmain.cpp. The main window has several kinds of views that show several URL's at once.

Each of the view present is a Konqview. The Konqview has its child parts, also called as KParts which are opened in read only mode. For example,

* DolphinPart is one of them that helps providing a directory view.
* KHTMLPart is responsible for providing the HTML view.

The KHTMLPart is responsible for storing/saving the whole structure of the website (all frames, and their URL) in the history buffer (saveState/restoreState). Every time a URL is changed in a frame, the new contents are immediately stored in the history buffer. In the code, saveState() is invoked every time a URL is opened in the frame to perform the same. Similarly, restoreState() is called while restoring the specific items out of the history list.

System-level Functions

Here is a quick overview of places to find the right classes at:

src/\* : This is where konqueror is.

konqrun.\* : Re-implementation of KRun (see libkio) for konqueror.

Responsible for finding appropriate view<->mimetype bindings.

konqview.\* : KonqView, class used by KonqMainView to handle child views

konqframe.\* : KonqFrame and KonqFrameHeader (handles view-statusbar).

konqmain.\* : The main()

konqmainwindow.\* : KonqMainWindow, the main window :)

konqviewmanager.\*: View manager. Handles view creation, activation, splitters etc.

about/\* : The about part, shows the about page on startup

client/\* : kfmclient, for talking to running konqueror processes

sidebar/\* : The konqueror sidebar (framework+plugins)

Following are the libs used by konqueror:

From kdelibs:

kdecore - mimetypes, services

kdeui - widgets

kparts - component model

khtml - HTML rendering

kio - I/O stuff, bookmarks, properties dial

From kdebase:

libkonq - templates ("new") menu, RMB popup menu, file operations

Figure below explains how the konqueror helps to process the user input and open up the websites:

KonqMainWindow:

openFilteredURL or slotOpenURLRequest

|

|

-----openUrl----

| | |

| | |

| KonqRun KRun

| |

| |

openView

| \----- splitView to create a new one

KonqView: |

changeViewMode

|

[switchView if different mode required]

|

openUrl [emits openURLEvent (after calling openURL)]

Part: |

|

openUrl [emits started, progress info, completed]

...

Buildspy

The SciTools Understand is primarily a tool for static analysis and visualizing source code architecture to optimize software design. It helps perform impact analysis for changes made in the code. It is also used to comprehend and maintain poorly documented legacy code with excellent visualizations and metrics. It is also an excellent code editor combined with static analysis tools for impressive ease of code management etc.

Compiling using Buildspy:

We planned on using CMake to help compile the Konqueror source code. CMake is a cross-platform alternative to Linux Makefiles and make. CMake is controlled by writing instructions in CMakeLists.txt files. Each directory in your project should have a CMakeLists.txt file. What is nice about CMake is that CMakeLists.txt files in a sub-directory inherit properties set in the parent directory, reducing the amount of code duplication. The konqueror has built-in CmakeList.txt built into the code that we pulled from GitHub. The Konqueror web browser is primarily C++.

Metrics Summary

Metrics are immensely essential to any code review or security assessment. Here some basic set of metrics which helps in managing a product:-

(white paper- https://www.sans.org/reading-room/whitepapers/analyst/metrics-manage-application-security-program-36822)

1. Technical Metrics

* Number of vulnerabilities found
* Density of vulnerabilities = number of vulnerabilities/lines of code
* Severity of the vulnerabilities
* Type of vulnerabilities
* Process of discovery
* Number of fixed vulnerabilities
* Time to Repair

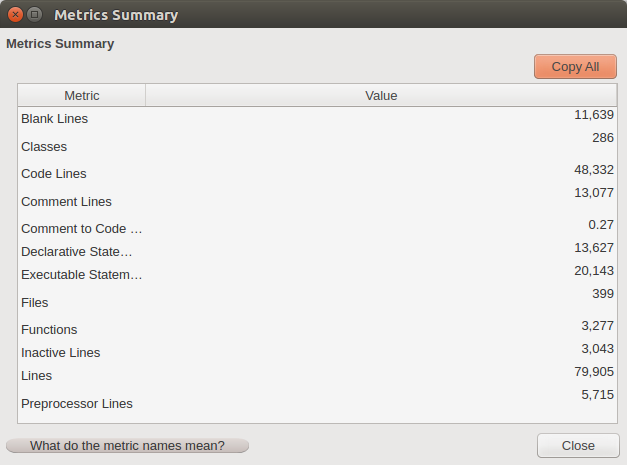
Apart from these we also have two very important metrics.

Complexity Eg:- Cyclomatic Complexity

Size (or volume):- Length or lines of code

Lines of code or complexity and chance of vulnerability are more or less directly proportional to each other.

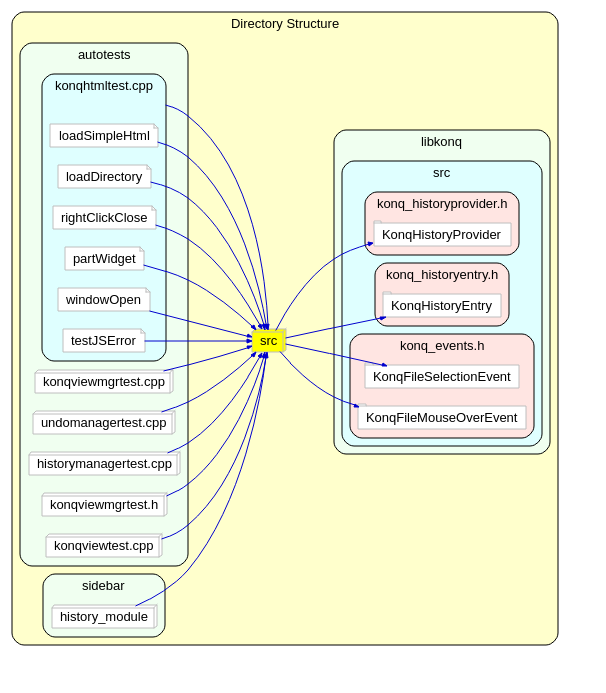
As the complexity or the number of lines increase, the chance of a possible mistake or vulnerability in the code increases.

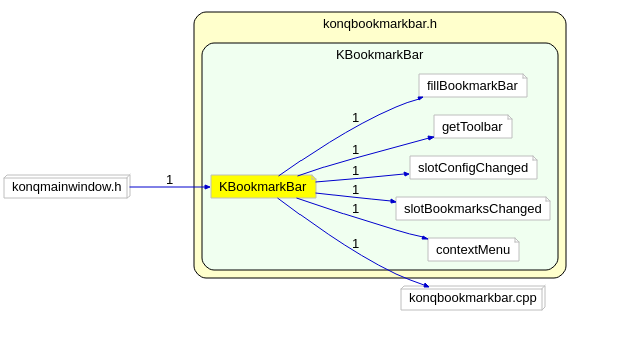


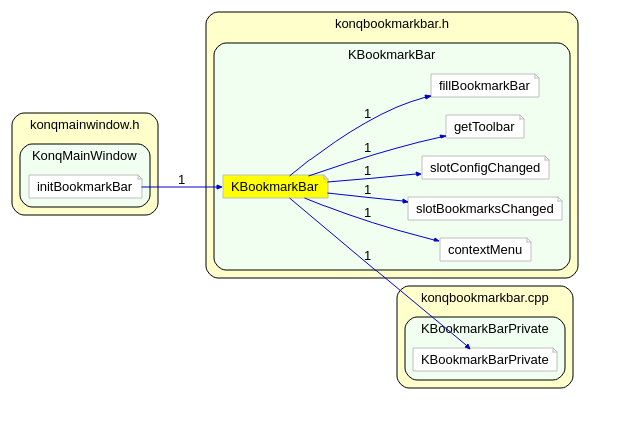
Cluster Call Butterfly Graph

Cluster graphs are a special type of hierarchy view. They provide a more interactive view of call relationships than other hierarchy views. The Cluster Call, Cluster Callby, Cluster Call Butterfly, Cluster Call Internal, and Cluster Control Flow variants are available, and can be accessed from the function, class, file, or architecture level.

<https://scitools.com/clustered-call-graphs/>

Cluster Call Butterfly Graph of KBookmark



A Cluster call butterfly graph is a vital piece of static analysis tool where the relationships between the class and their linked functions. This also gives a holistic approach about the class and its dependencies. It is necessary or rather simplifies the understanding of the code to easily recognize the dependencies. Once the dependencies are realized, the analyzer will be able to make the necessary decisions for a correct, easy and accurate security assessment, also proper code reviews.

The overall visualization of the modules involved in the code will give the code reviewer a structured approach. Ultimately, helping to find out various attack surfaces or attack vectors in code. Since time is always of essence since if vulnerable codes are in production, risk of hacker to exploit a potential vulnerability is always a fear. Having an idea or threat modeling is imperative any product in any position is a software development life cycle.

Control Flow Graph

Control Flow Graph of Kbookmark

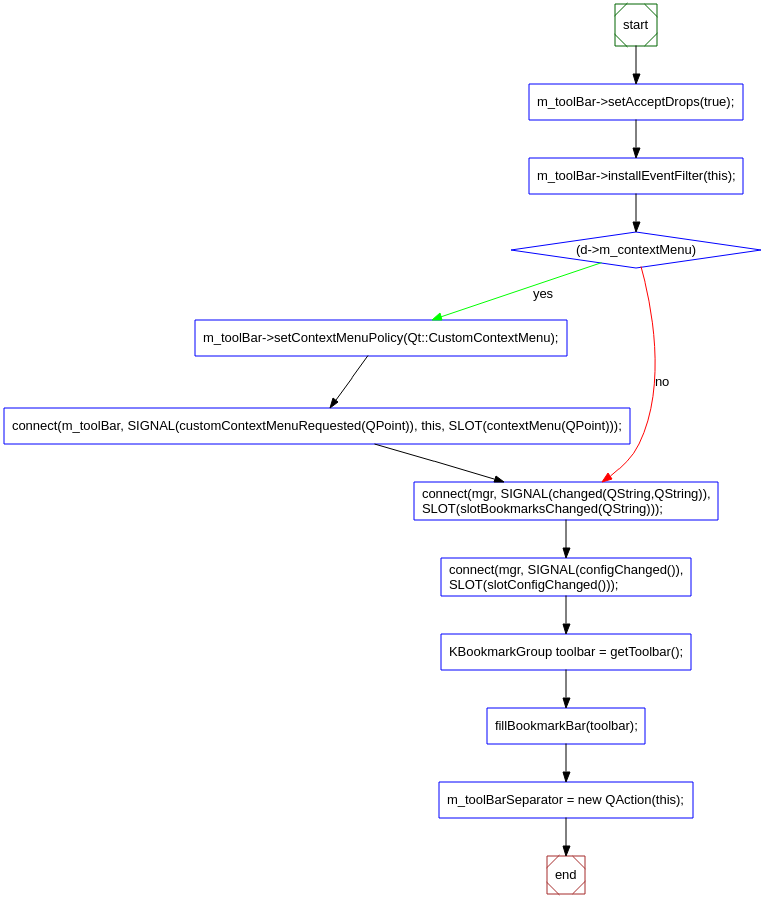
A control flow is a mechanism used to step through the logical modules and conditions in the code. It helps examine a function and determine each branch condition. Namely, all the loops, if-else statements, switch statements, try/catch blocks etc. This also helps us to understand the conditions under which each block will execute.

The control flow path gives us a complete path from the Start to End of a designated class.

Control flow graphs also treats calls to a functions like any other sequential statement that is executed without the possibility of termination.

A control flow graph consists of a basic block, path, path vector (lines), entry point s and exist points as well.

This a unmatchable tool or graph to conduct code reviews as a code reviewer or a security analyst performing a security assessment. Understanding the flow of control might give the analyzer an idea or an avenue for a possible exploit and help mitigate the issue before any major harm.



prashanth@prashanth-GL502VMK:~$ grep -rnw '/home/prashanth/konqueror/' -e 'printf'

/home/prashanth/konqueror/plugins/fsview/tests/scantest.cpp:30: printf("Started Scan on %s\n", qPrintable(d->name()));

/home/prashanth/konqueror/plugins/fsview/tests/scantest.cpp:35: printf("Change in %s: Dirs %d, Files %d",

/home/prashanth/konqueror/plugins/fsview/tests/scantest.cpp:38: printf("Size %llu\n", (unsigned long long int)d->size());

/home/prashanth/konqueror/plugins/fsview/tests/scantest.cpp:43: printf("Finished Scan on %s\n", qPrintable(d->name()));

/home/prashanth/konqueror/src/konqviewmanager.cpp:1314: printf("Parent sizes %s :", msg);

/home/prashanth/konqueror/src/konqviewmanager.cpp:1316: printf(" %d", i);

/home/prashanth/konqueror/src/konqviewmanager.cpp:1318: printf("\n");

/home/prashanth/konqueror/src/konqmain.cpp:54: printf("%s\n", Qfile::encodeName(fileInfo.baseName()).constData());

Input Function Analyses for Vulnerabilities

The function that processes user input is URI Handler of the browser. The URL is taken as args in urlList object of type QList which further uses KonqMisc::konqFilteredURL takes the input and filters the URI with invalid characters. Now this happens to be in the latest version of the konqueror, however, if the client if running an older version this filtering was not present as a result it opens up a wide variety of options of exploit the application on the basis of user input. Based on the malicious intent, the exploitation should be given a specific direction. For example, we tried browsing the below URL:

https://events.mozilla.org/portal/events/

and tried running a simple javascript that takes the user input on client end, parses it and displays the output on screen in the form of alert.

"><script>alert("This is a test parsing string")</script>

Malicious intent 1: From our research of possible attacks on web browsers, if we fill this alert string with large number of characters that are considard invalid by the browser, can lead to the crash of application possible leading to denial of service attack on the client end.

Malicious intent 2: Invoking of the javascript can also lead to XSS attacks although, that would be on the webpage rather than the specific application.

Malicious intent 3: The specific regular expressions that are used to check for the long patterns, for example /(.)\*/., can be used in bulk to cause the application to crash causing denial of service attack.

In our opinion, the central idea that makes attacker realize that these attack surfaces are even problems is the intent to manipulate the browser functionality that can not ideally be manipulated/controlled by the user. In other words, to mess with the actual functions of the application causing it to perform and execute something else than what it was originally intended to do. It can be either in terms of return memory address, processing of sql queries, input validation etc.

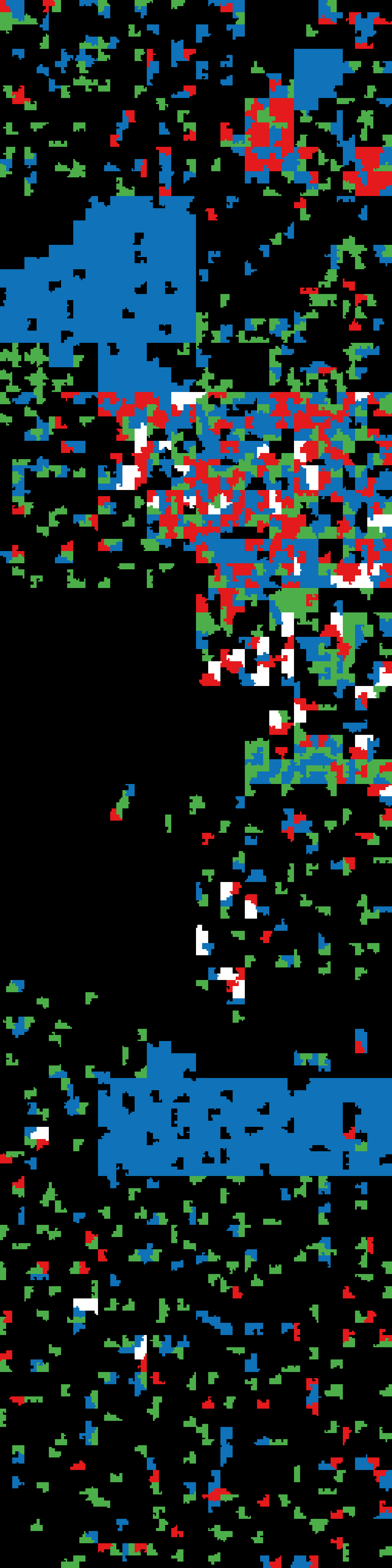
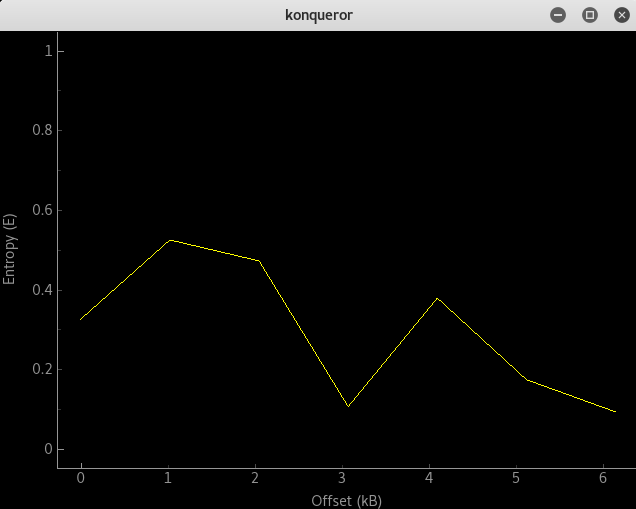
We also tried to find another approach by searching for the functions that can ready values from the memory directly such as printf. It has not been used much in the program except for once location:

printf("%s\n", QFile::encodeName(fileInfo.baseName()).constData());

however, based on the above code, the user cannot control what it is written inside the quotes so it would be difficult to exploit this while the application is running.

Entropy

Here entropy is termed as the extent or the degree upto which the chuck of a data is disordered. Above figure shows the visualization of the binary files using the space filling curves. This technique proves very useful to get a quick overview of the broader structure of file. For example, if we contain some data sets in which all the elements are having the same value, the entropy of this kind of data set would be zero or nil. Similarly, for the entropy to be maximum the values of the data sets has to be in the maximum amount of heteroginity which will also imply maximum amount of disordered chunk of data.  
  
For Reverse engineering, two most common kinds of high entropy data sets are:  
1. Compression Data  
2. Cryptographic Data  
The compression data is a part of various security audits for the process of finding and extracting. Cryptographic data is the encrypted portion of the data and is the heart of all kinds of security research areas.   
  
The colors in the picture, black as in instancce indicates zero entropy. As it goes into the shades of blue, the entropy increases, until hot pink which indicates maximum entropy.

Reverse Engineering

The file was used and tried in hexinator and binwalk and following hexdump was noted:

OFFSET konqueror

--------------------------------------------------------------------------------

0x00000000 7F 45 4C 46 02 01 01 00 00 00 00 00 00 00 00 00 |.ELF............|

0x00000010 03 00 3E 00 01 00 00 00 90 07 00 00 00 00 00 00 |..>.............|

0x00000020 40 00 00 00 00 00 00 00 68 11 00 00 00 00 00 00 |@.......h.......|

0x00000030 00 00 00 00 40 00 38 00 09 00 40 00 1D 00 1C 00 |....@.8...@.....|

0x00000040 06 00 00 00 05 00 00 00 40 00 00 00 00 00 00 00 |........@.......|

0x00000050 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 |@.......@.......|

0x00000060 F8 01 00 00 00 00 00 00 F8 01 00 00 00 00 00 00 |................|

0x00000070 08 00 00 00 00 00 00 00 03 00 00 00 04 00 00 00 |................|

0x00000080 38 02 00 00 00 00 00 00 38 02 00 00 00 00 00 00 |8.......8.......|

0x00000090 38 02 00 00 00 00 00 00 1C 00 00 00 00 00 00 00 |8...............|

0x000000A0 1C 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 |................|

0x000000B0 01 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 |................|

0x000000C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x000000D0 94 0A 00 00 00 00 00 00 94 0A 00 00 00 00 00 00 |................|

0x000000E0 00 00 20 00 00 00 00 00 01 00 00 00 06 00 00 00 |................|

0x000000F0 B8 0D 00 00 00 00 00 00 B8 0D 20 00 00 00 00 00 |................|

0x00000100 B8 0D 20 00 00 00 00 00 78 02 00 00 00 00 00 00 |........x.......|

0x00000110 80 02 00 00 00 00 00 00 00 00 20 00 00 00 00 00 |................|

0x00000120 02 00 00 00 06 00 00 00 D0 0D 00 00 00 00 00 00 |................|

0x00000130 D0 0D 20 00 00 00 00 00 D0 0D 20 00 00 00 00 00 |................|

0x00000140 00 02 00 00 00 00 00 00 00 02 00 00 00 00 00 00 |................|

0x00000150 08 00 00 00 00 00 00 00 04 00 00 00 04 00 00 00 |................|

0x00000160 54 02 00 00 00 00 00 00 54 02 00 00 00 00 00 00 |T.......T.......|

0x00000170 54 02 00 00 00 00 00 00 44 00 00 00 00 00 00 00 |T.......D.......|

0x00000180 44 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 |D...............|

0x00000190 50 E5 74 64 04 00 00 00 54 09 00 00 00 00 00 00 |P.td....T.......|

0x000001A0 54 09 00 00 00 00 00 00 54 09 00 00 00 00 00 00 |T.......T.......|

0x000001B0 3C 00 00 00 00 00 00 00 3C 00 00 00 00 00 00 00 |<.......<.......|

0x000001C0 04 00 00 00 00 00 00 00 51 E5 74 64 06 00 00 00 |........Q.td....|

0x000001D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x000001E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x000001F0 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 |................|

0x00000200 52 E5 74 64 04 00 00 00 B8 0D 00 00 00 00 00 00 |R.td............|

0x00000210 B8 0D 20 00 00 00 00 00 B8 0D 20 00 00 00 00 00 |................|

0x00000220 48 02 00 00 00 00 00 00 48 02 00 00 00 00 00 00 |H.......H.......|

0x00000230 01 00 00 00 00 00 00 00 2F 6C 69 62 36 34 2F 6C |......../lib64/l|

0x00000240 64 2D 6C 69 6E 75 78 2D 78 38 36 2D 36 34 2E 73 |d-linux-x86-64.s|

0x00000250 6F 2E 32 00 04 00 00 00 10 00 00 00 01 00 00 00 |o.2.............|

0x00000260 47 4E 55 00 00 00 00 00 02 00 00 00 06 00 00 00 |GNU.............|

0x00000270 20 00 00 00 04 00 00 00 14 00 00 00 03 00 00 00 |................|

0x00000280 47 4E 55 00 66 F8 C4 FA 9D 7D 5A 1E 8E ED E6 87 |GNU.f....}Z.....|

0x00000290 D1 72 CE B8 8F 27 BE 90 03 00 00 00 08 00 00 00 |.r...'..........|

0x000002A0 01 00 00 00 06 00 00 00 88 D1 21 05 20 65 C4 09 |..........!..e..|

0x000002B0 08 00 00 00 0B 00 00 00 11 00 00 00 6A 09 43 D6 |............j.C.|

0x000002C0 BA E3 92 7C 43 45 D5 EC 32 62 DB ED D8 71 58 1C |...|CE..2b...qX.|

0x000002D0 DA CD E3 9E B8 8D F1 0E 0C 3A 97 0B AD 4B E3 C0 |.........:...K..|

0x000002E0 EA D3 EF 0E 0D 14 E2 9E 00 00 00 00 00 00 00 00 |................|

0x000002F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000300 1A 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000310 00 00 00 00 00 00 00 00 85 00 00 00 22 00 00 00 |............"...|

0x00000320 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000330 36 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 |6...............|

0x00000340 00 00 00 00 00 00 00 00 45 00 00 00 20 00 00 00 |........E.......|

0x00000350 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000360 73 00 00 00 12 00 00 00 00 00 00 00 00 00 00 00 |s...............|

0x00000370 00 00 00 00 00 00 00 00 94 00 00 00 12 00 00 00 |................|

0x00000380 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000390 59 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 |Y...............|

0x000003A0 00 00 00 00 00 00 00 00 18 01 00 00 10 00 19 00 |................|

0x000003B0 20 10 20 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x000003C0 B9 00 00 00 10 00 1A 00 38 10 20 00 00 00 00 00 |........8.......|

0x000003D0 00 00 00 00 00 00 00 00 A6 00 00 00 10 00 19 00 |................|

0x000003E0 30 10 20 00 00 00 00 00 00 00 00 00 00 00 00 00 |0...............|

0x000003F0 1E 01 00 00 12 00 0E 00 90 07 00 00 00 00 00 00 |................|

0x00000400 2B 00 00 00 00 00 00 00 AD 00 00 00 10 00 1A 00 |+...............|

0x00000410 30 10 20 00 00 00 00 00 00 00 00 00 00 00 00 00 |0...............|

0x00000420 25 01 00 00 12 00 0E 00 D0 08 00 00 00 00 00 00 |%...............|

0x00000430 65 00 00 00 00 00 00 00 2F 01 00 00 12 00 0B 00 |e......./.......|

0x00000440 38 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |8...............|

0x00000450 1A 01 00 00 20 00 19 00 20 10 20 00 00 00 00 00 |................|

0x00000460 00 00 00 00 00 00 00 00 35 01 00 00 11 00 10 00 |........5.......|

0x00000470 50 09 00 00 00 00 00 00 04 00 00 00 00 00 00 00 |P...............|

0x00000480 12 01 00 00 12 00 0F 00 44 09 00 00 00 00 00 00 |........D.......|

0x00000490 00 00 00 00 00 00 00 00 08 01 00 00 12 00 0E 00 |................|

0x000004A0 40 09 00 00 00 00 00 00 02 00 00 00 00 00 00 00 |@...............|

0x000004B0 00 6C 69 62 6B 64 65 69 6E 69 74 34 5F 6B 6F 6E |.libkdeinit4\_kon|

0x000004C0 71 75 65 72 6F 72 2E 73 6F 00 5F 49 54 4D 5F 64 |queror.so.\_ITM\_d|

0x000004D0 65 72 65 67 69 73 74 65 72 54 4D 43 6C 6F 6E 65 |eregisterTMClone|

0x000004E0 54 61 62 6C 65 00 5F 5F 67 6D 6F 6E 5F 73 74 61 |Table.\_\_gmon\_sta|

0x000004F0 72 74 5F 5F 00 5F 4A 76 5F 52 65 67 69 73 74 65 |rt\_\_.\_Jv\_Registe|

0x00000500 72 43 6C 61 73 73 65 73 00 5F 49 54 4D 5F 72 65 |rClasses.\_ITM\_re|

0x00000510 67 69 73 74 65 72 54 4D 43 6C 6F 6E 65 54 61 62 |gisterTMCloneTab|

0x00000520 6C 65 00 6B 64 65 6D 61 69 6E 00 6C 69 62 63 2E |le.kdemain.libc.|

0x00000530 73 6F 2E 36 00 5F 5F 63 78 61 5F 66 69 6E 61 6C |so.6.\_\_cxa\_final|

0x00000540 69 7A 65 00 5F 5F 6C 69 62 63 5F 73 74 61 72 74 |ize.\_\_libc\_start|

0x00000550 5F 6D 61 69 6E 00 5F 65 64 61 74 61 00 5F 5F 62 |\_main.\_edata.\_\_b|

0x00000560 73 73 5F 73 74 61 72 74 00 5F 65 6E 64 00 2F 75 |ss\_start.\_end./u|

0x00000570 73 72 2F 6C 69 62 2F 6B 64 65 34 2F 6C 69 62 6B |sr/lib/kde4/libk|

0x00000580 64 65 69 6E 69 74 00 00 00 00 00 00 00 00 00 00 |deinit..........|

0x00000590 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x000005A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x000005B0 00 00 00 00 00 00 00 00 5F 5F 6C 69 62 63 5F 63 |........\_\_libc\_c|

0x000005C0 73 75 5F 66 69 6E 69 00 5F 5F 64 61 74 61 5F 73 |su\_fini.\_\_data\_s|

0x000005D0 74 61 72 74 00 5F 5F 6C 69 62 63 5F 63 73 75 5F |tart.\_\_libc\_csu\_|

0x000005E0 69 6E 69 74 00 5F 49 4F 5F 73 74 64 69 6E 5F 75 |init.\_IO\_stdin\_u|

0x000005F0 73 65 64 00 47 4C 49 42 43 5F 32 2E 32 2E 35 00 |sed.GLIBC\_2.2.5.|

0x00000600 00 00 00 00 02 00 00 00 00 00 00 00 02 00 00 00 |................|

0x00000610 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 |................|

0x00000620 01 00 01 00 01 00 00 00 01 00 01 00 7B 00 00 00 |............{...|

0x00000630 10 00 00 00 00 00 00 00 75 1A 69 09 00 00 02 00 |........u.i.....|

0x00000640 44 01 00 00 00 00 00 00 B8 0D 20 00 00 00 00 00 |D...............|

0x00000650 08 00 00 00 00 00 00 00 90 08 00 00 00 00 00 00 |................|

0x00000660 C0 0D 20 00 00 00 00 00 08 00 00 00 00 00 00 00 |................|

0x00000670 50 08 00 00 00 00 00 00 28 10 20 00 00 00 00 00 |P.......(.......|

0x00000680 08 00 00 00 00 00 00 00 28 10 20 00 00 00 00 00 |........(.......|

0x00000690 D0 0F 20 00 00 00 00 00 06 00 00 00 01 00 00 00 |................|

0x000006A0 00 00 00 00 00 00 00 00 D8 0F 20 00 00 00 00 00 |................|

0x000006B0 06 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 |................|

0x000006C0 E0 0F 20 00 00 00 00 00 06 00 00 00 03 00 00 00 |................|

0x000006D0 00 00 00 00 00 00 00 00 E8 0F 20 00 00 00 00 00 |................|

0x000006E0 06 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 |................|

0x000006F0 F0 0F 20 00 00 00 00 00 06 00 00 00 06 00 00 00 |................|

0x00000700 00 00 00 00 00 00 00 00 F8 0F 20 00 00 00 00 00 |................|

0x00000710 06 00 00 00 07 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000720 18 10 20 00 00 00 00 00 07 00 00 00 05 00 00 00 |................|

0x00000730 00 00 00 00 00 00 00 00 48 83 EC 08 48 8B 05 9D |........H...H...|

0x00000740 08 20 00 48 85 C0 74 02 FF D0 48 83 C4 08 C3 00 |...H..t...H.....|

0x00000750 FF 35 B2 08 20 00 FF 25 B4 08 20 00 0F 1F 40 00 |.5.....%......@.|

0x00000760 FF 25 B2 08 20 00 68 00 00 00 00 E9 E0 FF FF FF |.%....h.........|

0x00000770 FF 25 62 08 20 00 66 90 00 00 00 00 00 00 00 00 |.%b...f.........|

0x00000780 E9 DB FF FF FF 66 2E 0F 1F 84 00 00 00 00 00 90 |.....f..........|

0x00000790 31 ED 49 89 D1 5E 48 89 E2 48 83 E4 F0 50 54 4C |1.I..^H..H...PTL|

0x000007A0 8D 05 9A 01 00 00 48 8D 0D 23 01 00 00 48 8D 3D |......H..#...H.=|

0x000007B0 CC FF FF FF FF 15 36 08 20 00 F4 0F 1F 44 00 00 |......6......D..|

0x000007C0 48 8D 3D 69 08 20 00 48 8D 05 69 08 20 00 55 48 |H.=i...H..i...UH|

0x000007D0 29 F8 48 89 E5 48 83 F8 0E 76 15 48 8B 05 EE 07 |).H..H...v.H....|

0x000007E0 20 00 48 85 C0 74 09 5D FF E0 66 0F 1F 44 00 00 |..H..t.]..f..D..|

0x000007F0 5D C3 0F 1F 40 00 66 2E 0F 1F 84 00 00 00 00 00 |]...@.f.........|

0x00000800 48 8D 3D 29 08 20 00 48 8D 35 22 08 20 00 55 48 |H.=)...H.5"...UH|

0x00000810 29 FE 48 89 E5 48 C1 FE 03 48 89 F0 48 C1 E8 3F |).H..H...H..H..?|

0x00000820 48 01 C6 48 D1 FE 74 18 48 8B 05 C9 07 20 00 48 |H..H..t.H......H|

0x00000830 85 C0 74 0C 5D FF E0 66 0F 1F 84 00 00 00 00 00 |..t.]..f........|

0x00000840 5D C3 0F 1F 40 00 66 2E 0F 1F 84 00 00 00 00 00 |]...@.f.........|

0x00000850 80 3D D9 07 20 00 00 75 27 48 83 3D 77 07 20 00 |.=.....u'H.=w...|

0x00000860 00 55 48 89 E5 74 0C 48 8B 3D BA 07 20 00 E8 FD |.UH..t.H.=......|

0x00000870 FE FF FF E8 48 FF FF FF 5D C6 05 B0 07 20 00 01 |....H...].......|

0x00000880 F3 C3 0F 1F 40 00 66 2E 0F 1F 84 00 00 00 00 00 |....@.f.........|

0x00000890 48 8D 3D 31 05 20 00 48 83 3F 00 75 0B E9 5E FF |H.=1...H.?.u..^.|

0x000008A0 FF FF 66 0F 1F 44 00 00 48 8B 05 39 07 20 00 48 |..f..D..H..9...H|

0x000008B0 85 C0 74 E9 55 48 89 E5 FF D0 5D E9 40 FF FF FF |..t.UH....].@...|

0x000008C0 E9 9B FE FF FF 66 2E 0F 1F 84 00 00 00 00 00 90 |.....f..........|

0x000008D0 41 57 41 56 41 89 FF 41 55 41 54 4C 8D 25 D6 04 |AWAVA..AUATL.%..|

0x000008E0 20 00 55 48 8D 2D D6 04 20 00 53 49 89 F6 49 89 |..UH.-....SI..I.|

0x000008F0 D5 4C 29 E5 48 83 EC 08 48 C1 FD 03 E8 37 FE FF |.L).H...H....7..|

0x00000900 FF 48 85 ED 74 20 31 DB 0F 1F 84 00 00 00 00 00 |.H..t.1.........|

0x00000910 4C 89 EA 4C 89 F6 44 89 FF 41 FF 14 DC 48 83 C3 |L..L..D..A...H..|

0x00000920 01 48 39 DD 75 EA 48 83 C4 08 5B 5D 41 5C 41 5D |.H9.u.H...[]A\A]|

0x00000930 41 5E 41 5F C3 90 66 2E 0F 1F 84 00 00 00 00 00 |A^A\_..f.........|

0x00000940 F3 C3 00 00 48 83 EC 08 48 83 C4 08 C3 00 00 00 |....H...H.......|

0x00000950 01 00 02 00 01 1B 03 3B 38 00 00 00 06 00 00 00 |.......;8.......|

0x00000960 FC FD FF FF 84 00 00 00 2C FE FF FF C4 00 00 00 |........,.......|

0x00000970 3C FE FF FF 54 00 00 00 6C FF FF FF AC 00 00 00 |<...T...l.......|

0x00000980 7C FF FF FF DC 00 00 00 EC FF FF FF 24 01 00 00 ||...........$...|

0x00000990 14 00 00 00 00 00 00 00 01 7A 52 00 01 78 10 01 |.........zR..x..|

0x000009A0 1B 0C 07 08 90 01 07 10 14 00 00 00 1C 00 00 00 |................|

0x000009B0 E0 FD FF FF 2B 00 00 00 00 00 00 00 00 00 00 00 |....+...........|

0x000009C0 14 00 00 00 00 00 00 00 01 7A 52 00 01 78 10 01 |.........zR..x..|

0x000009D0 1B 0C 07 08 90 01 00 00 24 00 00 00 1C 00 00 00 |........$.......|

0x000009E0 70 FD FF FF 20 00 00 00 00 0E 10 46 0E 18 4A 0F |p..........F..J.|

0x000009F0 0B 77 08 80 00 3F 1A 3B 2A 33 24 22 00 00 00 00 |.w...?.;\*3$"....|

0x00000A00 14 00 00 00 44 00 00 00 B8 FE FF FF 05 00 00 00 |....D...........|

0x00000A10 00 00 00 00 00 00 00 00 14 00 00 00 5C 00 00 00 |............\...|

0x00000A20 60 FD FF FF 05 00 00 00 00 00 00 00 00 00 00 00 |`...............|

0x00000A30 44 00 00 00 74 00 00 00 98 FE FF FF 65 00 00 00 |D...t.......e...|

0x00000A40 00 42 0E 10 8F 02 42 0E 18 8E 03 45 0E 20 8D 04 |.B....B....E....|

0x00000A50 42 0E 28 8C 05 48 0E 30 86 06 48 0E 38 83 07 4D |B.(..H.0..H.8..M|

0x00000A60 0E 40 72 0E 38 41 0E 30 41 0E 28 42 0E 20 42 0E |.@r.8A.0A.(B..B.|

0x00000A70 18 42 0E 10 42 0E 08 00 14 00 00 00 BC 00 00 00 |.B..B...........|

0x00000A80 C0 FE FF FF 02 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000A90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000AA0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000AB0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000AC0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000AD0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000AE0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000AF0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000B00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000B10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000B20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000B30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000B40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000B50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000B60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000B70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000B80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000B90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000BA0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000BB0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000BC0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000BD0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000BE0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000BF0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000C00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000C10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000C20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000C30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000C40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000C50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000C60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000C70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000C80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000C90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000CA0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000CB0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000CC0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000CD0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000CE0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000CF0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000D00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000D10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000D20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000D30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000D40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000D50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000D60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000D70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000D80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000D90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000DA0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000DB0 00 00 00 00 00 00 00 00 90 08 00 00 00 00 00 00 |................|

0x00000DC0 50 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |P...............|

0x00000DD0 01 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 |................|

0x00000DE0 01 00 00 00 00 00 00 00 7B 00 00 00 00 00 00 00 |........{.......|

0x00000DF0 1D 00 00 00 00 00 00 00 BE 00 00 00 00 00 00 00 |................|

0x00000E00 0C 00 00 00 00 00 00 00 38 07 00 00 00 00 00 00 |........8.......|

0x00000E10 0D 00 00 00 00 00 00 00 44 09 00 00 00 00 00 00 |........D.......|

0x00000E20 19 00 00 00 00 00 00 00 B8 0D 20 00 00 00 00 00 |................|

0x00000E30 1B 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 |................|

0x00000E40 1A 00 00 00 00 00 00 00 C0 0D 20 00 00 00 00 00 |................|

0x00000E50 1C 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 |................|

0x00000E60 F5 FE FF 6F 00 00 00 00 98 02 00 00 00 00 00 00 |...o............|

0x00000E70 05 00 00 00 00 00 00 00 B0 04 00 00 00 00 00 00 |................|

0x00000E80 06 00 00 00 00 00 00 00 E8 02 00 00 00 00 00 00 |................|

0x00000E90 0A 00 00 00 00 00 00 00 50 01 00 00 00 00 00 00 |........P.......|

0x00000EA0 0B 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 |................|

0x00000EB0 15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000EC0 03 00 00 00 00 00 00 00 00 10 20 00 00 00 00 00 |................|

0x00000ED0 02 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 |................|

0x00000EE0 14 00 00 00 00 00 00 00 07 00 00 00 00 00 00 00 |................|

0x00000EF0 17 00 00 00 00 00 00 00 20 07 00 00 00 00 00 00 |................|

0x00000F00 07 00 00 00 00 00 00 00 48 06 00 00 00 00 00 00 |........H.......|

0x00000F10 08 00 00 00 00 00 00 00 D8 00 00 00 00 00 00 00 |................|

0x00000F20 09 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 |................|

0x00000F30 FB FF FF 6F 00 00 00 00 00 00 00 08 00 00 00 00 |...o............|

0x00000F40 FE FF FF 6F 00 00 00 00 28 06 00 00 00 00 00 00 |...o....(.......|

0x00000F50 FF FF FF 6F 00 00 00 00 01 00 00 00 00 00 00 00 |...o............|

0x00000F60 F0 FF FF 6F 00 00 00 00 00 06 00 00 00 00 00 00 |...o............|

0x00000F70 F9 FF FF 6F 00 00 00 00 03 00 00 00 00 00 00 00 |...o............|

0x00000F80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000F90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000FA0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000FB0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000FC0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000FD0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000FE0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00000FF0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00001000 D0 0D 20 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00001010 00 00 00 00 00 00 00 00 66 07 00 00 00 00 00 00 |........f.......|

0x00001020 00 00 00 00 00 00 00 00 28 10 20 00 00 00 00 00 |........(.......|

0x00001030 66 38 63 34 66 61 39 64 37 64 35 61 31 65 38 65 |f8c4fa9d7d5a1e8e|

0x00001040 65 64 65 36 38 37 64 31 37 32 63 65 62 38 38 66 |ede687d172ceb88f|

0x00001050 32 37 62 65 39 30 2E 64 65 62 75 67 00 00 00 00 |27be90.debug....|

0x00001060 CF 27 62 12 00 2E 73 68 73 74 72 74 61 62 00 2E |.'b...shstrtab..|

0x00001070 69 6E 74 65 72 70 00 2E 6E 6F 74 65 2E 41 42 49 |interp..note.ABI|

0x00001080 2D 74 61 67 00 2E 6E 6F 74 65 2E 67 6E 75 2E 62 |-tag..note.gnu.b|

0x00001090 75 69 6C 64 2D 69 64 00 2E 67 6E 75 2E 68 61 73 |uild-id..gnu.has|

0x000010A0 68 00 2E 64 79 6E 73 79 6D 00 2E 64 79 6E 73 74 |h..dynsym..dynst|

0x000010B0 72 00 2E 67 6E 75 2E 76 65 72 73 69 6F 6E 00 2E |r..gnu.version..|

0x000010C0 67 6E 75 2E 76 65 72 73 69 6F 6E 5F 72 00 2E 72 |gnu.version\_r..r|

0x000010D0 65 6C 61 2E 64 79 6E 00 2E 72 65 6C 61 2E 70 6C |ela.dyn..rela.pl|

0x000010E0 74 00 2E 69 6E 69 74 00 2E 70 6C 74 2E 67 6F 74 |t..init..plt.got|

0x000010F0 00 2E 74 65 78 74 00 2E 66 69 6E 69 00 2E 72 6F |..text..fini..ro|

0x00001100 64 61 74 61 00 2E 65 68 5F 66 72 61 6D 65 5F 68 |data..eh\_frame\_h|

0x00001110 64 72 00 2E 65 68 5F 66 72 61 6D 65 00 2E 69 6E |dr..eh\_frame..in|

0x00001120 69 74 5F 61 72 72 61 79 00 2E 66 69 6E 69 5F 61 |it\_array..fini\_a|

0x00001130 72 72 61 79 00 2E 6A 63 72 00 2E 64 79 6E 61 6D |rray..jcr..dynam|

0x00001140 69 63 00 2E 67 6F 74 2E 70 6C 74 00 2E 64 61 74 |ic..got.plt..dat|

0x00001150 61 00 2E 62 73 73 00 2E 67 6E 75 5F 64 65 62 75 |a..bss..gnu\_debu|

0x00001160 67 6C 69 6E 6B 00 00 00 00 00 00 00 00 00 00 00 |glink...........|

0x00001170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00001180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00001190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x000011A0 00 00 00 00 00 00 00 00 0B 00 00 00 01 00 00 00 |................|

0x000011B0 02 00 00 00 00 00 00 00 38 02 00 00 00 00 00 00 |........8.......|

0x000011C0 38 02 00 00 00 00 00 00 1C 00 00 00 00 00 00 00 |8...............|

0x000011D0 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 |................|

0x000011E0 00 00 00 00 00 00 00 00 13 00 00 00 07 00 00 00 |................|

0x000011F0 02 00 00 00 00 00 00 00 54 02 00 00 00 00 00 00 |........T.......|

0x00001200 54 02 00 00 00 00 00 00 20 00 00 00 00 00 00 00 |T...............|

0x00001210 00 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 |................|

0x00001220 00 00 00 00 00 00 00 00 21 00 00 00 07 00 00 00 |........!.......|

0x00001230 02 00 00 00 00 00 00 00 74 02 00 00 00 00 00 00 |........t.......|

0x00001240 74 02 00 00 00 00 00 00 24 00 00 00 00 00 00 00 |t.......$.......|

0x00001250 00 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 |................|

0x00001260 00 00 00 00 00 00 00 00 34 00 00 00 F6 FF FF 6F |........4......o|

0x00001270 02 00 00 00 00 00 00 00 98 02 00 00 00 00 00 00 |................|

0x00001280 98 02 00 00 00 00 00 00 50 00 00 00 00 00 00 00 |........P.......|

0x00001290 05 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 |................|

0x000012A0 00 00 00 00 00 00 00 00 3E 00 00 00 0B 00 00 00 |........>.......|

0x000012B0 02 00 00 00 00 00 00 00 E8 02 00 00 00 00 00 00 |................|

0x000012C0 E8 02 00 00 00 00 00 00 C8 01 00 00 00 00 00 00 |................|

0x000012D0 06 00 00 00 01 00 00 00 08 00 00 00 00 00 00 00 |................|

0x000012E0 18 00 00 00 00 00 00 00 46 00 00 00 03 00 00 00 |........F.......|

0x000012F0 02 00 00 00 00 00 00 00 B0 04 00 00 00 00 00 00 |................|

0x00001300 B0 04 00 00 00 00 00 00 50 01 00 00 00 00 00 00 |........P.......|

0x00001310 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 |................|

0x00001320 00 00 00 00 00 00 00 00 4E 00 00 00 FF FF FF 6F |........N......o|

0x00001330 02 00 00 00 00 00 00 00 00 06 00 00 00 00 00 00 |................|

0x00001340 00 06 00 00 00 00 00 00 26 00 00 00 00 00 00 00 |........&.......|

0x00001350 05 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 |................|

0x00001360 02 00 00 00 00 00 00 00 5B 00 00 00 FE FF FF 6F |........[......o|

0x00001370 02 00 00 00 00 00 00 00 28 06 00 00 00 00 00 00 |........(.......|

0x00001380 28 06 00 00 00 00 00 00 20 00 00 00 00 00 00 00 |(...............|

0x00001390 06 00 00 00 01 00 00 00 08 00 00 00 00 00 00 00 |................|

0x000013A0 00 00 00 00 00 00 00 00 6A 00 00 00 04 00 00 00 |........j.......|

0x000013B0 02 00 00 00 00 00 00 00 48 06 00 00 00 00 00 00 |........H.......|

0x000013C0 48 06 00 00 00 00 00 00 D8 00 00 00 00 00 00 00 |H...............|

0x000013D0 05 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 |................|

0x000013E0 18 00 00 00 00 00 00 00 74 00 00 00 04 00 00 00 |........t.......|

0x000013F0 42 00 00 00 00 00 00 00 20 07 00 00 00 00 00 00 |B...............|

0x00001400 20 07 00 00 00 00 00 00 18 00 00 00 00 00 00 00 |................|

0x00001410 05 00 00 00 18 00 00 00 08 00 00 00 00 00 00 00 |................|

0x00001420 18 00 00 00 00 00 00 00 7E 00 00 00 01 00 00 00 |........~.......|

0x00001430 06 00 00 00 00 00 00 00 38 07 00 00 00 00 00 00 |........8.......|

0x00001440 38 07 00 00 00 00 00 00 17 00 00 00 00 00 00 00 |8...............|

0x00001450 00 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 |................|

0x00001460 00 00 00 00 00 00 00 00 79 00 00 00 01 00 00 00 |........y.......|

0x00001470 06 00 00 00 00 00 00 00 50 07 00 00 00 00 00 00 |........P.......|

0x00001480 50 07 00 00 00 00 00 00 20 00 00 00 00 00 00 00 |P...............|

0x00001490 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 |................|

0x000014A0 10 00 00 00 00 00 00 00 84 00 00 00 01 00 00 00 |................|

0x000014B0 06 00 00 00 00 00 00 00 70 07 00 00 00 00 00 00 |........p.......|

0x000014C0 70 07 00 00 00 00 00 00 08 00 00 00 00 00 00 00 |p...............|

0x000014D0 00 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 |................|

0x000014E0 00 00 00 00 00 00 00 00 8D 00 00 00 01 00 00 00 |................|

0x000014F0 06 00 00 00 00 00 00 00 80 07 00 00 00 00 00 00 |................|

0x00001500 80 07 00 00 00 00 00 00 C2 01 00 00 00 00 00 00 |................|

0x00001510 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 |................|

0x00001520 00 00 00 00 00 00 00 00 93 00 00 00 01 00 00 00 |................|

0x00001530 06 00 00 00 00 00 00 00 44 09 00 00 00 00 00 00 |........D.......|

0x00001540 44 09 00 00 00 00 00 00 09 00 00 00 00 00 00 00 |D...............|

0x00001550 00 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 |................|

0x00001560 00 00 00 00 00 00 00 00 99 00 00 00 01 00 00 00 |................|

0x00001570 12 00 00 00 00 00 00 00 50 09 00 00 00 00 00 00 |........P.......|

0x00001580 50 09 00 00 00 00 00 00 04 00 00 00 00 00 00 00 |P...............|

0x00001590 00 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 |................|

0x000015A0 04 00 00 00 00 00 00 00 A1 00 00 00 01 00 00 00 |................|

0x000015B0 02 00 00 00 00 00 00 00 54 09 00 00 00 00 00 00 |........T.......|

0x000015C0 54 09 00 00 00 00 00 00 3C 00 00 00 00 00 00 00 |T.......<.......|

0x000015D0 00 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 |................|

0x000015E0 00 00 00 00 00 00 00 00 AF 00 00 00 01 00 00 00 |................|

0x000015F0 02 00 00 00 00 00 00 00 90 09 00 00 00 00 00 00 |................|

0x00001600 90 09 00 00 00 00 00 00 04 01 00 00 00 00 00 00 |................|

0x00001610 00 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 |................|

0x00001620 00 00 00 00 00 00 00 00 B9 00 00 00 0E 00 00 00 |................|

0x00001630 03 00 00 00 00 00 00 00 B8 0D 20 00 00 00 00 00 |................|

0x00001640 B8 0D 00 00 00 00 00 00 08 00 00 00 00 00 00 00 |................|

0x00001650 00 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 |................|

0x00001660 08 00 00 00 00 00 00 00 C5 00 00 00 0F 00 00 00 |................|

0x00001670 03 00 00 00 00 00 00 00 C0 0D 20 00 00 00 00 00 |................|

0x00001680 C0 0D 00 00 00 00 00 00 08 00 00 00 00 00 00 00 |................|

0x00001690 00 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 |................|

0x000016A0 08 00 00 00 00 00 00 00 D1 00 00 00 01 00 00 00 |................|

0x000016B0 03 00 00 00 00 00 00 00 C8 0D 20 00 00 00 00 00 |................|

0x000016C0 C8 0D 00 00 00 00 00 00 08 00 00 00 00 00 00 00 |................|

0x000016D0 00 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 |................|

0x000016E0 00 00 00 00 00 00 00 00 D6 00 00 00 06 00 00 00 |................|

0x000016F0 03 00 00 00 00 00 00 00 D0 0D 20 00 00 00 00 00 |................|

0x00001700 D0 0D 00 00 00 00 00 00 00 02 00 00 00 00 00 00 |................|

0x00001710 06 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 |................|

0x00001720 10 00 00 00 00 00 00 00 88 00 00 00 01 00 00 00 |................|

0x00001730 03 00 00 00 00 00 00 00 D0 0F 20 00 00 00 00 00 |................|

0x00001740 D0 0F 00 00 00 00 00 00 30 00 00 00 00 00 00 00 |........0.......|

0x00001750 00 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 |................|

0x00001760 08 00 00 00 00 00 00 00 DF 00 00 00 01 00 00 00 |................|

0x00001770 03 00 00 00 00 00 00 00 00 10 20 00 00 00 00 00 |................|

0x00001780 00 10 00 00 00 00 00 00 20 00 00 00 00 00 00 00 |................|

0x00001790 00 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 |................|

0x000017A0 08 00 00 00 00 00 00 00 E8 00 00 00 01 00 00 00 |................|

0x000017B0 03 00 00 00 00 00 00 00 20 10 20 00 00 00 00 00 |................|

0x000017C0 20 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 |................|

0x000017D0 00 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 |................|

0x000017E0 00 00 00 00 00 00 00 00 EE 00 00 00 08 00 00 00 |................|

0x000017F0 03 00 00 00 00 00 00 00 30 10 20 00 00 00 00 00 |........0.......|

0x00001800 30 10 00 00 00 00 00 00 08 00 00 00 00 00 00 00 |0...............|

0x00001810 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 |................|

0x00001820 00 00 00 00 00 00 00 00 F3 00 00 00 01 00 00 00 |................|

0x00001830 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00001840 30 10 00 00 00 00 00 00 34 00 00 00 00 00 00 00 |0.......4.......|

0x00001850 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 |................|

0x00001860 00 00 00 00 00 00 00 00 01 00 00 00 03 00 00 00 |................|

0x00001870 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

0x00001880 64 10 00 00 00 00 00 00 02 01 00 00 00 00 00 00 |d...............|

0x00001890 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 |................|

0x000018A0 00 00 00 00 00 00 00 00 XX XX XX XX XX XX XX XX |................|

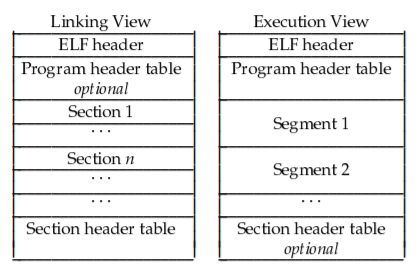
Following are the headers present in this file:

|  |  |  |
| --- | --- | --- |
| Position (32 bit) | Position (64 bit) | Value |
| 0-3 | 0-3 | Magic number - 0x7F, then 'ELF' in ASCII |
| 4 | 4 | 1 = 32 bit, 2 = 64 bit |
| 5 | 5 | 1 = little endian, 2 = big endian |
| 6 | 6 | ELF Version |
| 7 | 7 | OS ABI - usually 0 for System V |
| 8-15 | 8-15 | Unused/padding |
| 16-17 | 16-17 | 1 = relocatable, 2 = executable, 3 = shared, 4 = core |
| 18-19 | 18-19 | Instruction set - see table below |
| 20-23 | 20-23 | ELF Version |
| 24-27 | 24-31 | Program entry position |
| 28-31 | 32-39 | Program header table position |
| 32-35 | 40-47 | Section header table position |
| 36-39 | 48-51 | Flags - architecture dependent; see note below |
| 40-41 | 52-53 | Header size |
| 42-43 | 54-55 | Size of an entry in the program header table |
| 44-45 | 56-57 | Number of entries in the program header table |
| 46-47 | 58-59 | Size of an entry in the section header table |
| 48-49 | 60-61 | Number of entries in the section header table |
| 50-51 | 62-63 | Index in section header table with the section names |

Following is the program header of an ELF file:

|  |  |
| --- | --- |
| Position | Value |
| 0-3 | Type of segment (see below) |
| 4-7 | Flags (see below) |
| 8-15 | The offset in the file that the data for this segment can be found (p\_offset) |
| 16-23 | Where you should start to put this segment in virtual memory (p\_vaddr) |
| 24-31 | Undefined for the System V ABI |
| 32-39 | Size of the segment in the file (p\_filesz) |
| 40-47 | Size of the segment in memory (p\_memsz) |
| 48-55 | The required alignment for this section (must be a power of 2) |

Here is a generic format for the file specifications for an ELF file:



A little bit of reverse engineering we tried, took a few hex digits from the hex dump, for example, “7F 45 4C 46” which represent the file format in ASCII ELF = “45 4C 46” along with an extra hex bit of 7F. “02” hex digits that are placed immediately after the file format are indicating the version of ELF file. E.g. in our file the digit was 2 which indicates the 64 bit file format. “01” hex digits that are placed after the file format name are the ones representing kind of data present in the binary file along with the appropriate format to enable them for parsing. For example, in our file we observed the format to be in the 2’s compliment with little endian layout. The hex digits occurring after 16 bytes of parsing as indicated in the file format are the ones indicating the type of file that was provided to the parser. Different kinds of elf are Relocatable file, Executable file, Shared object file, Core file, Processor-specific, Processor-specific. For example, in the conqueror we found that the bits indicating file type were set as “00 03” which implies the shared object file. The next four bytes as per the specification are the machine type which were set as “00 3E” for the conqueror browser which implies the architecture of the machine was AMD x86-64 architecture. Hence the process of reverse engineering the file goes in a very similar fashion for rest of the file specifications and headers.

Goal: To steal cookies from the victim’s browser

Precondition: Cross Site scripting protection should fail to initialize the domains on sub-(i)frames correctly

Attack: JavaScript can access any foreign subframe which is defined in the HTML source

Postcondition: Cookies should be stored in the victim’s browser

Script

|  |  |  |  |
| --- | --- | --- | --- |
| Property | Threat Definition | Examples | Mitigation |
| Denial of Service | The attacker or a group of attackers take an action to make the browser application inaccessible | - the attackers can change the property parameters of the window/frame objects that reserve memory to increase upto infinite consumption. e.g. CVE-2009-2537  - invalid use of document.load methods that trigger the use of deleted objects can also result in such condition. e.g. CVE-2008-5698  - the adversary can also trigger this condition while invoking the javascript alert containin URL encoded with large number of invalid characters. e.g. CVE-2008-4382 | - Variable/Parameter integrity validation.  - Defining access privileges to access the internal methods of program.  - Network/Application based access control mechanism.  - Traffic rate limiting. |

|  |  |  |
| --- | --- | --- |
| **Name** | **Description** | **Countermeasures** |
| **Denial of Services**   * using large HTTP Cookies Parameters * of the HTML Parser | Major aim in this case is not to gain access or data from the victim but more along lines of breaking the application such that it cannot be used by the victim.  For Example: - The browsers can be DoSed by attacking various modules such as sending extra-large HTTP cookies. Or by sending a COLOR attribute that it is too large for the HTML Parser to understand. | * Extensive Input/Parameter/Attribute verification needs to be performed before product release. * By using session protection. * Extensive testing of the product by validating various modules in the code. |

Goal: Cause Denial of Service via large HTTP cookie parameters.

Precondition: Attacker should be able to send a cookie to the browser

Attack:  Send an argument containing an over long cookie causing the browser of the victim to crash.

Postcondition: Victim’s browser must accept cookies from attacker

# **document the threats**

|  |  |
| --- | --- |
| **Threat Description** | **Attacker spoofs the URL address bar** |
| Threat Target | Konqueror’s URI Handler |
| Risk | **Low** |
| Attack techniques | http URI altering with large amount of whitespace in username/password portion. |
| Countermeasures | User must use SSL all the times to encrypt the communication over channel along with certificate validation techniques for all connections over SSL. |

|  |  |
| --- | --- |
| **Threat Description** | **Attacker tempers javascript alert function with large number of invalid characters** |
| Threat Target | Konqueror’s Javascript Parser |
| Risk | **Medium** |
| Attack techniques | Use of JavaScript alert function |
| Countermeasures | Effective input validation along with parameter integrity validation. |

|  |  |
| --- | --- |
| **Threat Description** | **Attacker exploits browser extensions to execute arbitrary code with the privileges of the browser on a system.** |
| Threat Target | Konqueror’s extensions |
| Risk | **High** |
| Attack techniques | Use trusted third party extensions and show warnings before any kind of change. |
| Countermeasures | Sanitize and validate all user inputs |
| **Threat Description** | **Attacker tries to steal cookies from victims browser** |
| Threat Target | Konqueror’s JavaScript Parser |
| Risk | **High** |
| Attack techniques | Idea is to use the JavaScript to steam cookie as it can access any foreign subframe which is defined in the HTML source. |
| Countermeasures | Use of SSL and VPN is recommended for 100% protection from such attacks. |

|  |  |
| --- | --- |
| **Threat Description** | **Attacker tries to cause denial of service** |
| Threat Target | Konqueror’s handling of HTTP Cookies |
| Risk | **Medium** |
| Attack techniques | To send an argument containing an over long cookie causing the browser of the victim to crash. |
| Countermeasures | Use of SSL. Network/Application based Access Control along with Parameter integrity check would be able to counter such attacks. |

Thank you!