

The Center for Cyber Defenders

Expanding computer security knowledge

Snippet

Loic Guegan, University of Colorado Boulder;
Nathan Pitchaikani, University of Illinois Urbana-Champaign



Project Mentor: Danny Loffredo, 5638

Problem Statement:

There is currently no standard tool suite for source code auditors. As software become increasingly complex, we need tools that help researchers navigate, annotate, and collaborate to assess the security of large code bases. To solve this, Snippet is being developed as a custom source code auditing framework used internally at Sandia.

Approach:

Our goal for the summer was to implement new features in order to improve Snippet's functionality. We accomplished this through the use of Python, Qt, and Rtags.

1. **Qt**: an cross-platform application frame work used for developing application software with graphical user interfaces
2. **Rtags**: a client/server application that indexes C/C++ code and keeps a persistent file-based database of references, declaration, definitions, etc...

New Features:

1. Multi-highlighting functionality:
 - Highlight multiple words
 - Toggle highlights
 - Remove selected highlights
 - Options to transfer current highlights when user changes files.
2. Hyperlinked Comments:
 - Double clicking comments of format "filename:linenumber" take you to the specified location in the chosen file
 - Double clicking comments of format ":linenumber" take you to the specified line in current file
3. Undo Close Tab:
 - If a user accidently closes a tab it can be undone by clicking ctrl-z
4. Rtags Backend:
 - Integrated definitions, references, and references/virtuals searches
 - Useful for C++ code bases
5. Welcome page on new tab:
 - displays information about the project and helps users who haven't opened a project

```
File Edit View Navigate Annotate Help
bdfest1.c x
16 You should have received a copy of the GNU General Public License
17 along with this program; if not, write to the Free Software
18 Foundation, Inc., 51 Franklin Street - Fifth Floor, Boston,
19 MA 02110-1301, USA. */
20
21 #include "sysdep.h"
22 #include "bfd.h"
23
24 static void
25 die (const char *s)
26 {
27     printf ("oops: %s\n", s);
28     exit (1);
29 }
30
31 int
32 main (int argc, char **argv)
33 {
34     bfd_archive;
35     bfd_last, *next;
36
37     if (argc != 2)
38         die ("usage: bdfest1 <archive>");
39
40     archive = bfd_openr (argv[1], NULL);
41     if (archive == NULL)
42         die ("no such archive");
43
44     if (!bfd_check_format (archive, bfd_archive))
45     {
46         bfd_close (archive);
47         die ("bfd_check_format");
48     }
49
50     for (last = bfd_openr_next_archived_file (archive, NULL);
51          last;
52          last = next)
53     {
54         next = bfd_openr_next_archived_file (archive, last);
55         bfd_close (last);
56     }
57
58     for (last = bfd_openr_next_archived_file (archive, NULL);
59          last;
60          last = next)
61     {
62         next = bfd_openr_next_archived_file (archive, last);
63         bfd_close (last);
64     }
65
66     if (!bfd_close (archive))
```

Code Source: GNU Binutils (Open source project)

Impact and Benefits:

Snippet enables collaborative source code auditing in order to handle the most complex vulnerability assessment tasks. The newly added features listed in the previous section make Snippet more powerful by improving the existing user interface and experience as well as adding an improved C++ backend.