Assignment 4

Vulnerabilities search in shark cage

IMT 3501 Software Security

Jan Kerkenhoff
(141628)
David Vierheilig
(140155)
Christian Neßlinger
(140153)

Task
Find security vulnerabilities in the Secure Desktop Application.

Solution
We tried to use several different types of software to make an automated vulnerability scan with the existing code in the repository.

We tried to use:

- Gprofile 2011
- ICARUS – Use List Analyzer for Delphi
- CodeHealer for Delphi
  - Doesn't work with the Delphi project files (.dpr), but we don't know why
- Embacadero Delphi XE7 to try to compile the code, but it was impossible because there are missing code files
- Larzarus IDE v1.2.4 to try to compile the code...
- Delphi Code Analyzer (http://sourceforge.net/projects/dca/)
  - was only useful to calculate the code metrics, but not for finding vulnerabilities
- Pascal Browser 2 (http://www.peganza.com/products_pab.htm)
  - seems to be not useful in our case
- ModelMaker 11 Pascal (http://www.modelmakertools.com/modelmaker/history/mm1100.html)
  - was not useful in our case
- Nexus Quality Suite – CoverageAnalyst (http://www.nexusdb.com/support/index.php)
  - can only use binaries
- SourceMonitor – Tracks Source Code Quality and Quantity (Version 3.5.0.306) (www.campwoodsw.com)
  - mainly for code metric analysis
- Pascal Analyzer (http://www.peganza.com/#PAL)
  - program showed a lot of code optimizations possibilities, but not no real vulnerabilities
  - we had only the free community edition from this tool, that's why the tool displayed only 2 items per section

After we tried to use these tools, we decided to inspect the code manually, in the hope of finding vulnerabilities. We found some vulnerabilities/bugs, which you can find summarized below.

In general
The libraries DataUtils, IniFiles, SysUtils, ShlObj, ActiveX, KnownFolder, AccCrl and AclApi are loaded.
Perhaps these libraries have known security gaps?

Perhaps a fault can appear through wtsapi32.dll
```
WTSAPIDLLNAME = 'wtsapi32.dll';
```

There are several external program calls for example:
```
"if SDCreateProcessWithTokenOnDesktop('C:\Windows\
system32\calc.exe', '', hNewToken, 'Default') then".
```

It's possible to manipulate the “calc.exe”. What happens, if calc.exe is manipulated ?

SDAppInfo.dpr
Delphi project file: no vulnerabilities found

SDCommon.pas
line 16: Config file is loaded (`SecureDesktop.ini`)
→ What is the content of this file? Is it possible to manipulate this file? Can you modify the start up parameters.

line 23: `BackroundBitmapFileName = 'Background.bmp'`
What does happen if we replace the file with a malicious file, e. g. what happens if we replace the background bitmap with a 4 GB file → does the program crash?

Line 111: BUG
Hardcoded path like this example is bad coding style.
`StrPCopy(pszAppDataPath, 'C:\Users\hannol\AppData\Roaming');`

line 334:
We think it is possible to change the displayed application logo, if the applications key is known.

SDInfoSecurity.pas

line 200: `“if (AProcessData.FileName = 'bds.exe') then”`

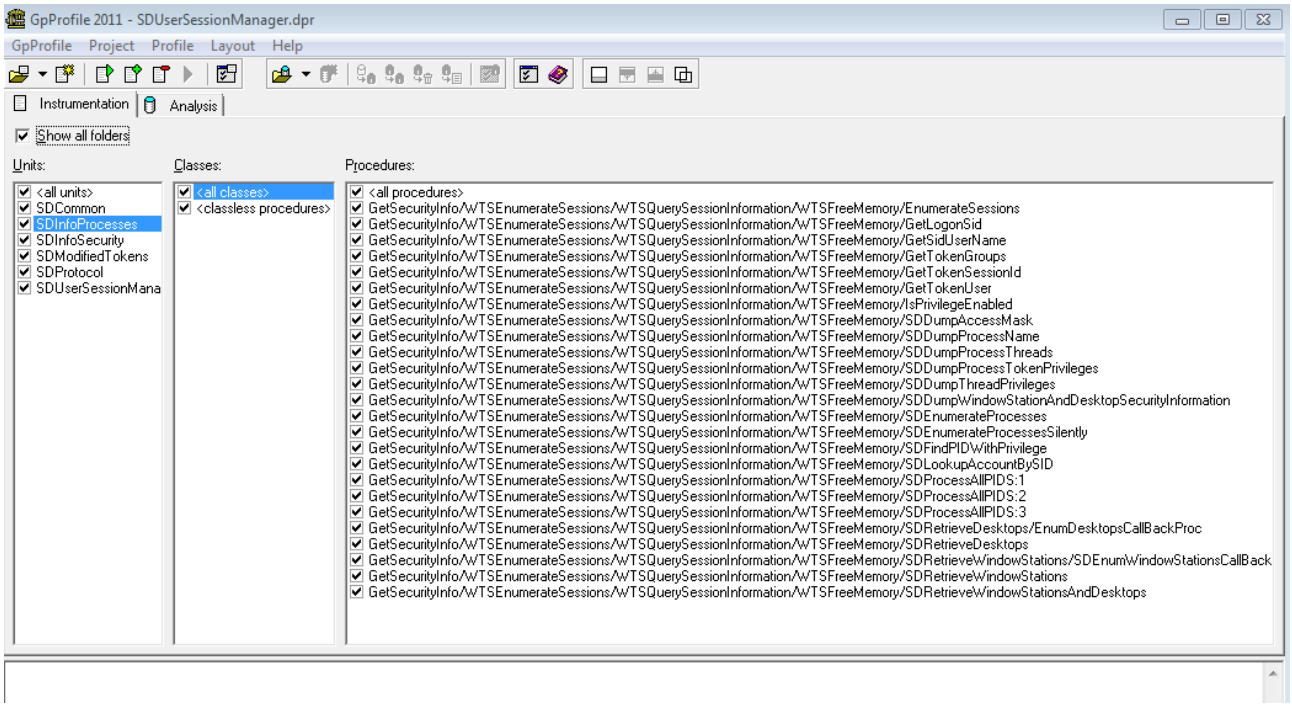
What is “bds.exe”, and why is this checked ?

Line 409: `“cbName := 2048 + 1”`
Use of global variable, if the value changes, everything has to modified manually.
Possible bugs could be created if this is ever refactored.

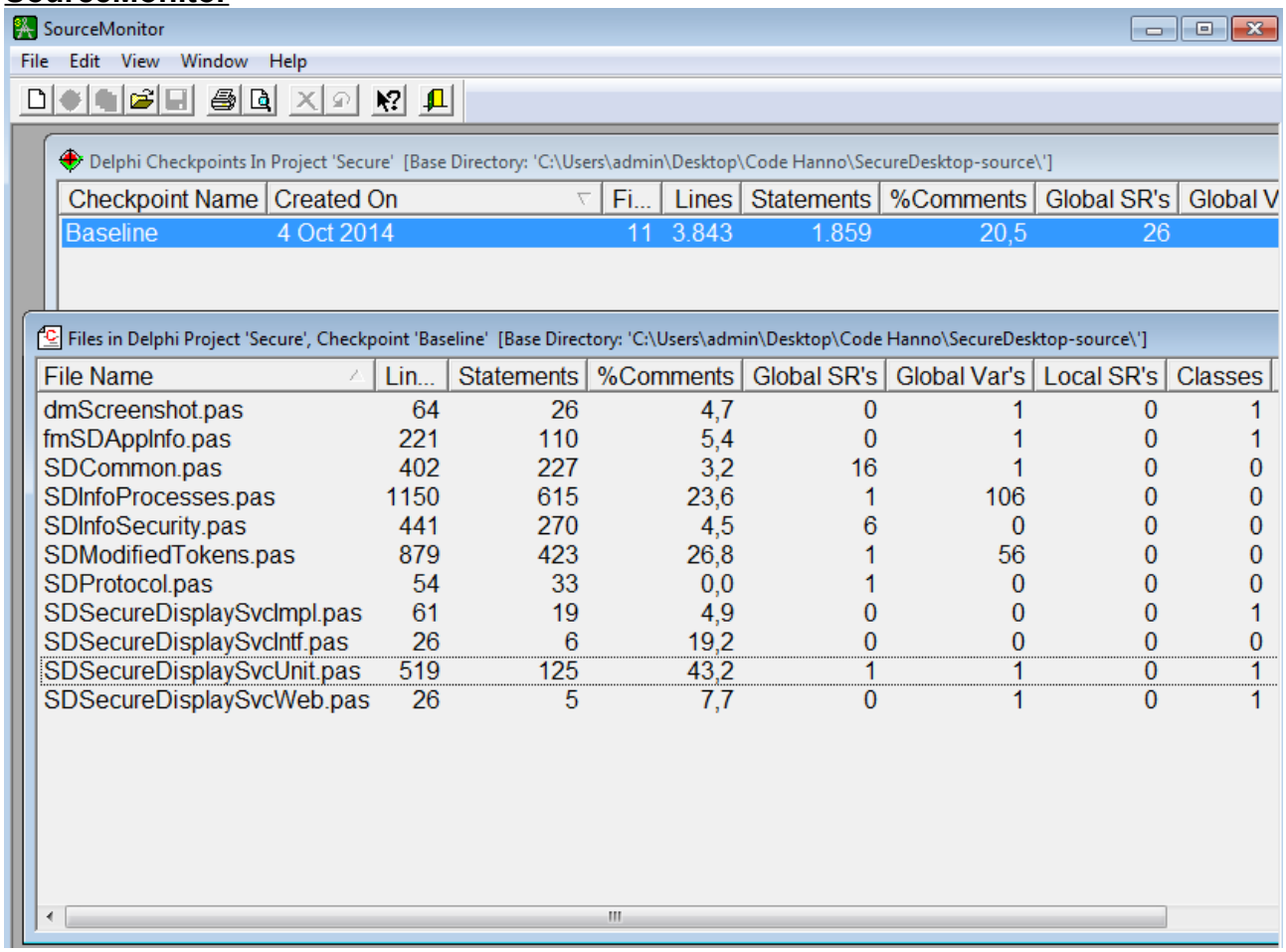
We found no other vulnerabilities, one reason is that the code is not well documented.
We think that the biggest vulnerability is that everything is logged very detailed.
As an attacker the first target should be reading the log file.

In the following pages are some screen shots of the used applications.

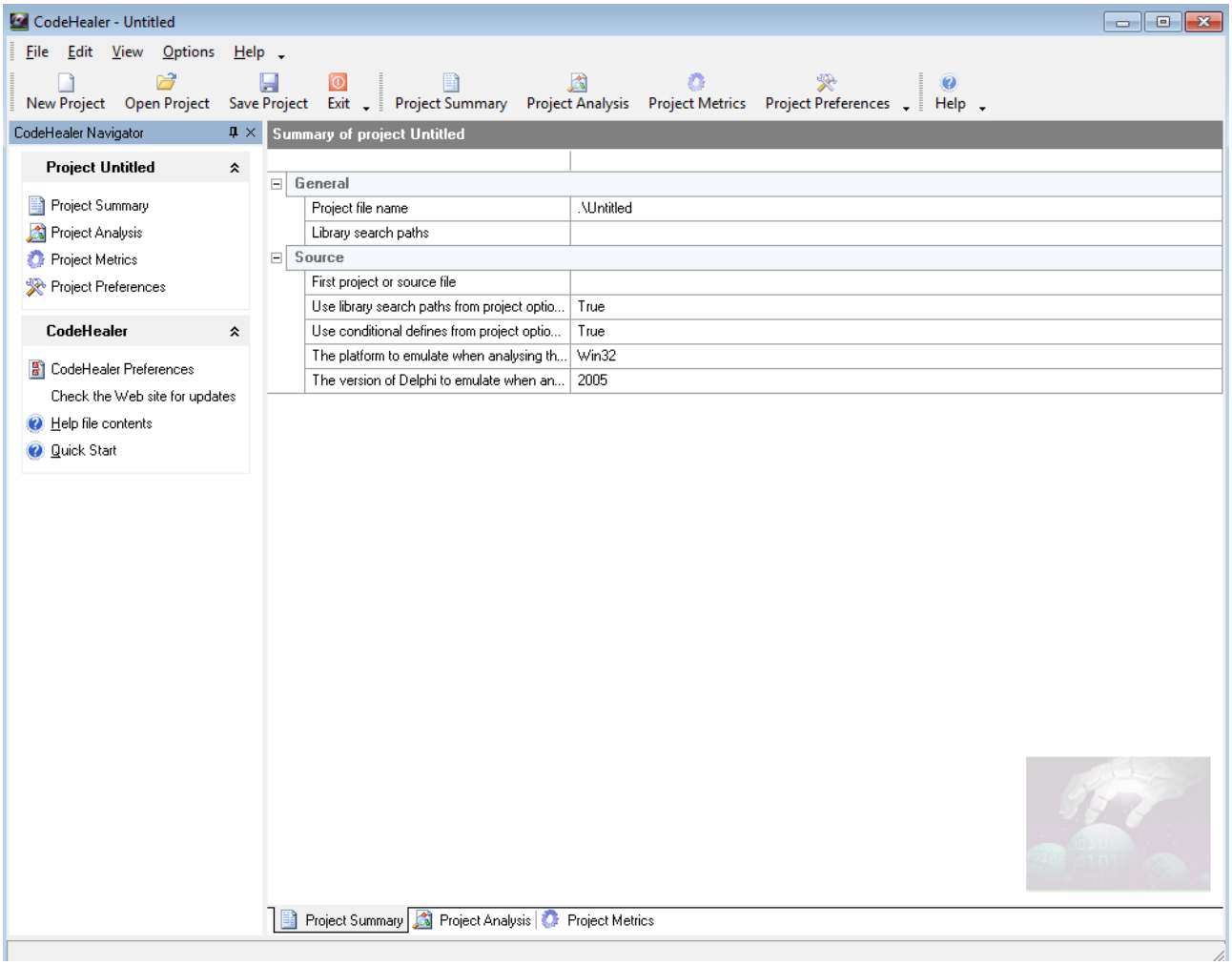
GpProfile 2011



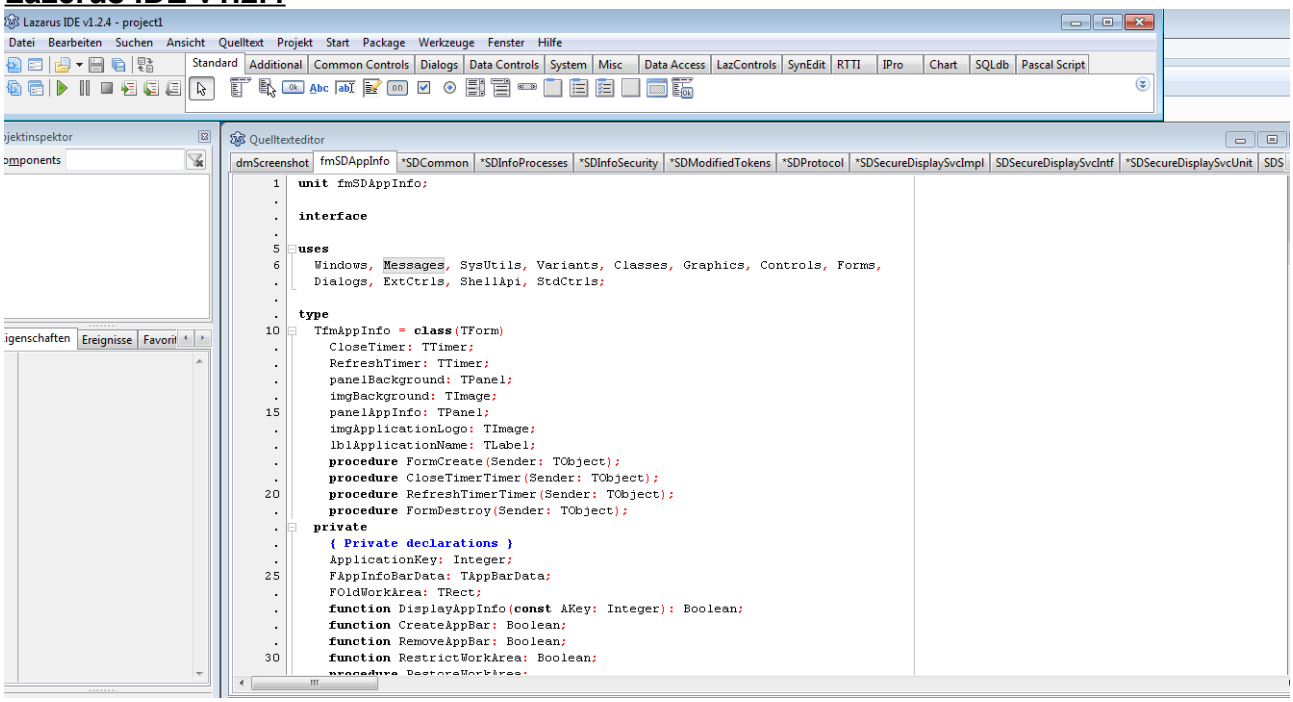
SourceMonitor



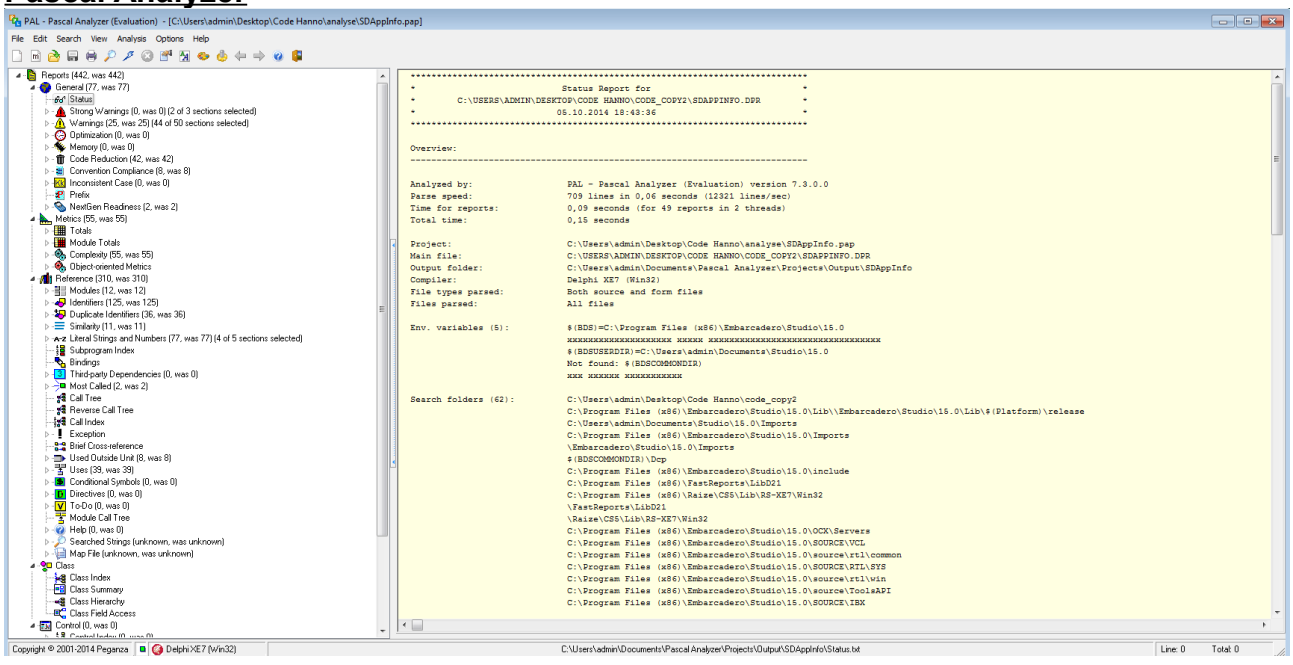
CodeHealer


CodeHealer - Untitled
File Edit View Options Help
New Project
Open Project
Save Project
Exit
Project Summary
Project Analysis
Project Metrics
Project Preferences
Help
CodeHealer Navigator
Project Untitled
Project Summary
Project Analysis
Project Metrics
Project Preferences
CodeHealer
CodeHealer Preferences
Check the Web site for updates
Help file contents
Quick Start
Summary of project Untitled
General
Project file name
.\Untitled
Library search paths
Source
First project or source file
Use library search paths from project optio...
True
Use conditional defines from project optio...
True
The platform to emulate when analysing th...
Win32
The version of Delphi to emulate when an...
2005
Project Summary
Project Analysis
Project Metrics

Lazerus IDE v1.2.4



Pascal Analyzer



Embacadero Delphi EX7