

User Manual**Created by hjerold & gaber52****Table of Contents**


• Introduction	2
• Program Development Environment	3
• GUI Program Development Environment	4
• Installing the Web Shell Detector	5
• Running and Using the Web Shell Detector	7-13

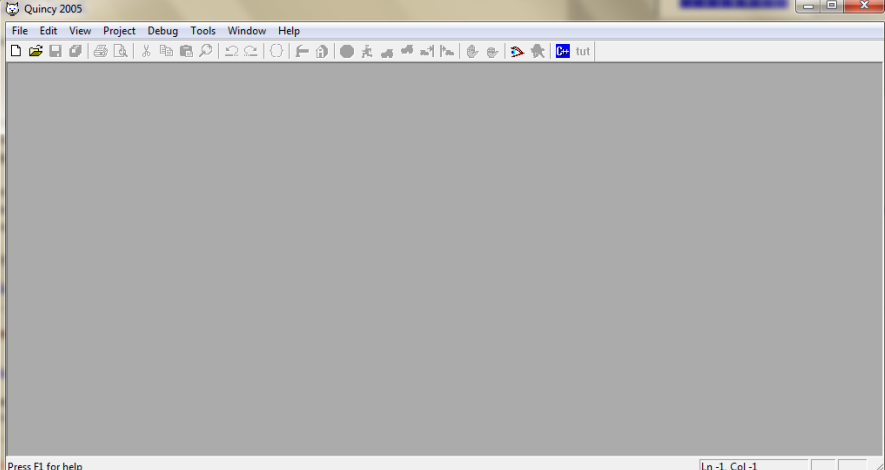
Introduction

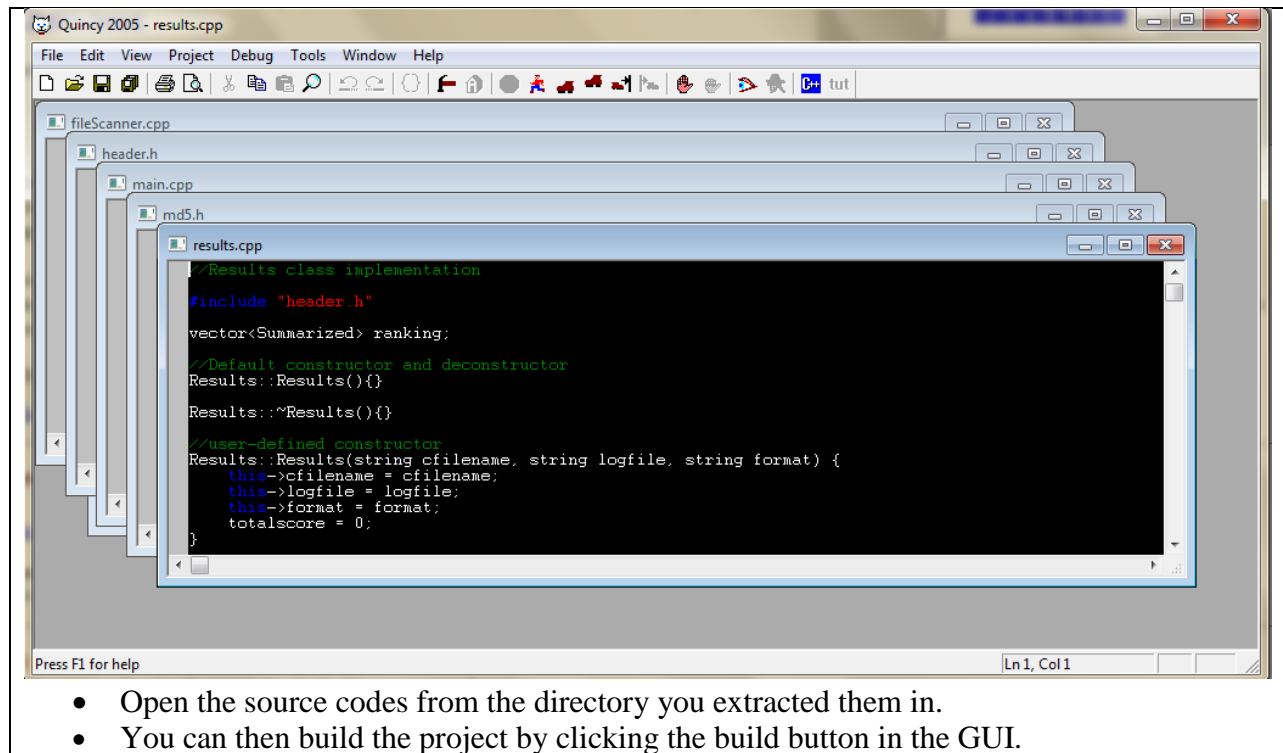
This user manual highlights and introduces the key features of the program and provides detailed step-by-step instructions on using the program efficiently. It also states the environment in which the program is developed in and compilation instructions for the GUI.

Program Development Environment

The program main source codes are developed in Quincy, which can be downloaded for free from the internet.

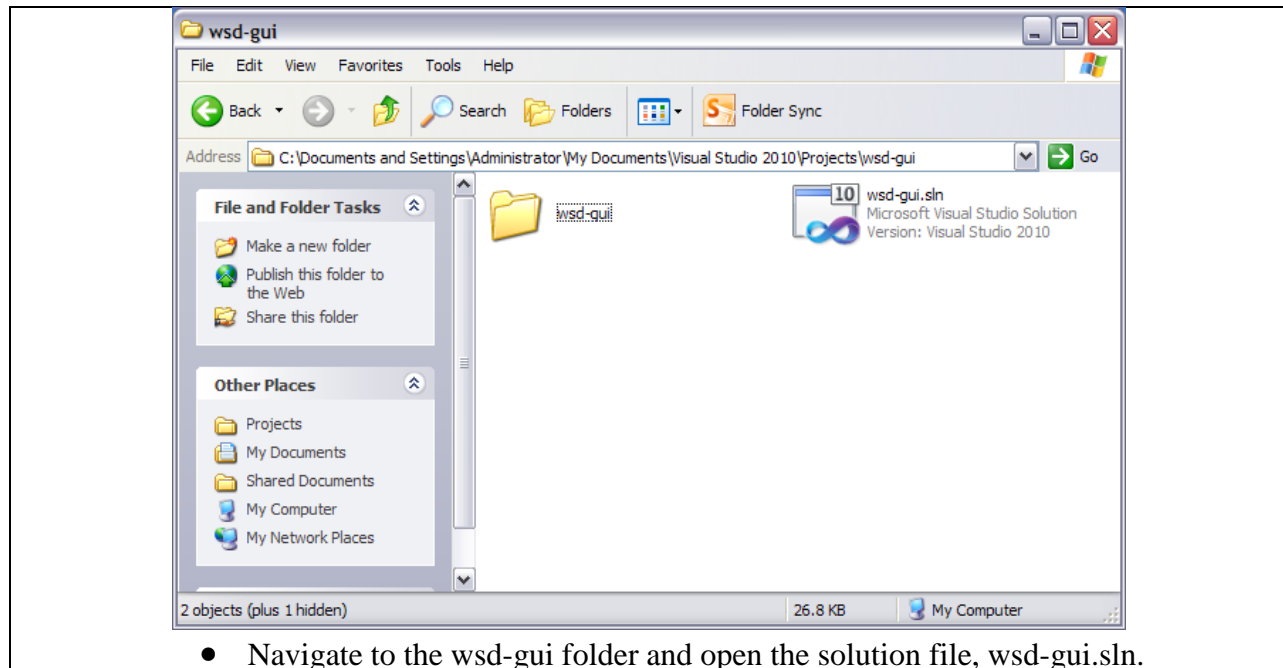
	<ul style="list-style-type: none">• Proceed to download Quincy 2005 and install it.
--	---

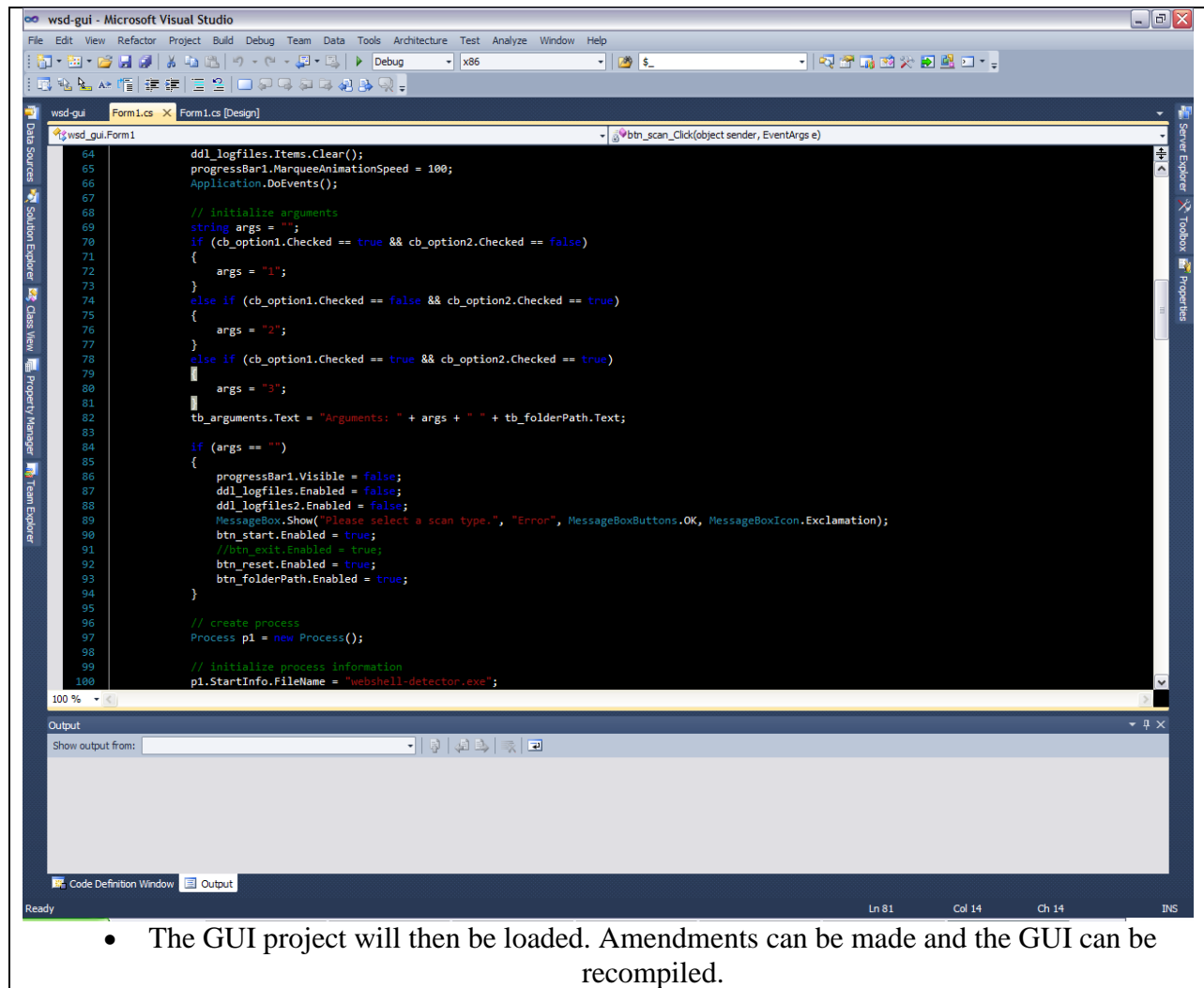
	<ul style="list-style-type: none">• Quincy Development UI
--	---



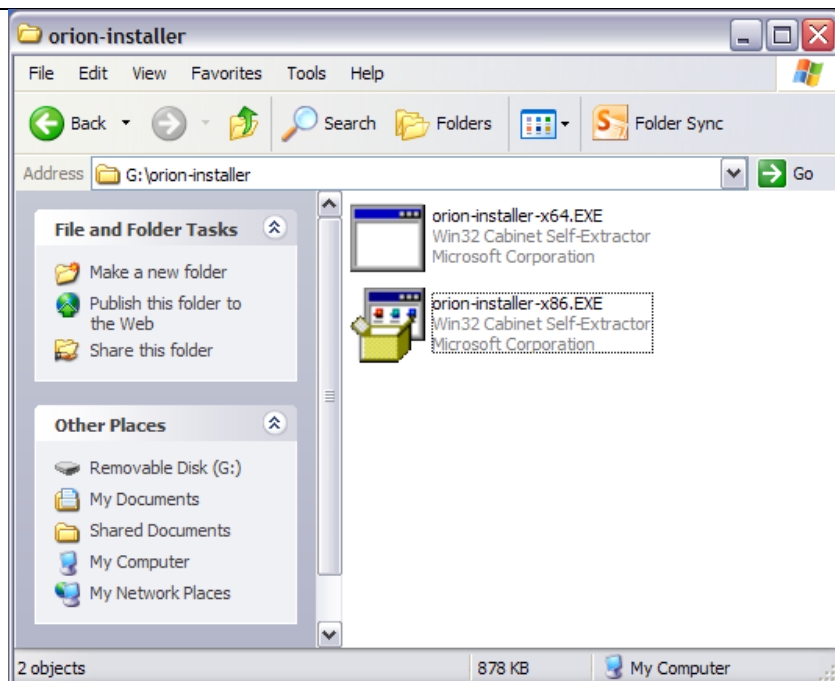
GUI Program Development Environment

The GUI is developed using Microsoft Visual Studio 2010. To make amendments to the GUI, Microsoft Visual Studio 2010 is required. To open the GUI project:

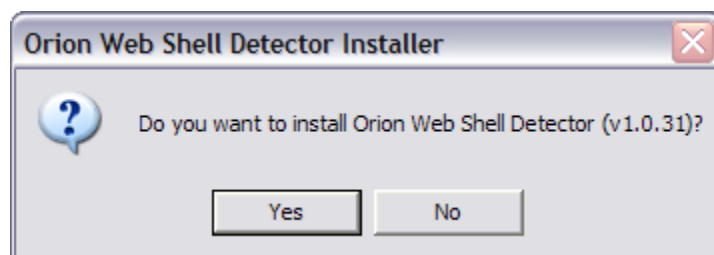




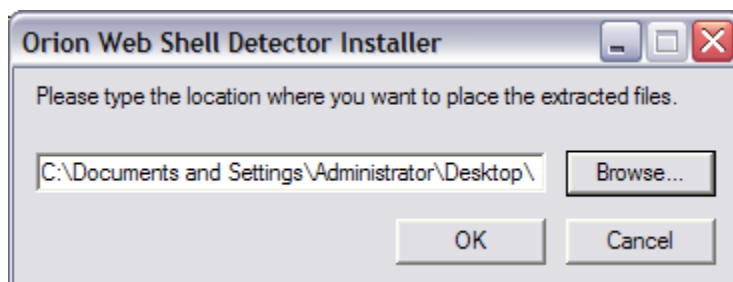
Installing the Web Shell Detector



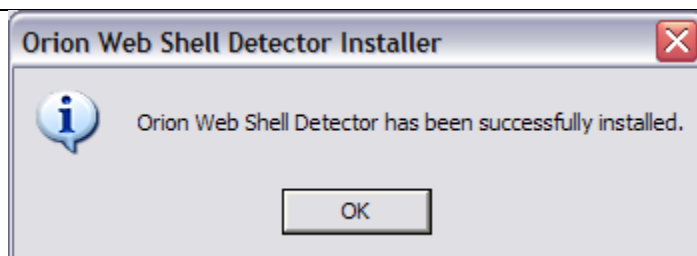
- Navigate to the installer folder and choose an appropriate installer for your operating system. (32 bit / 64 bit)



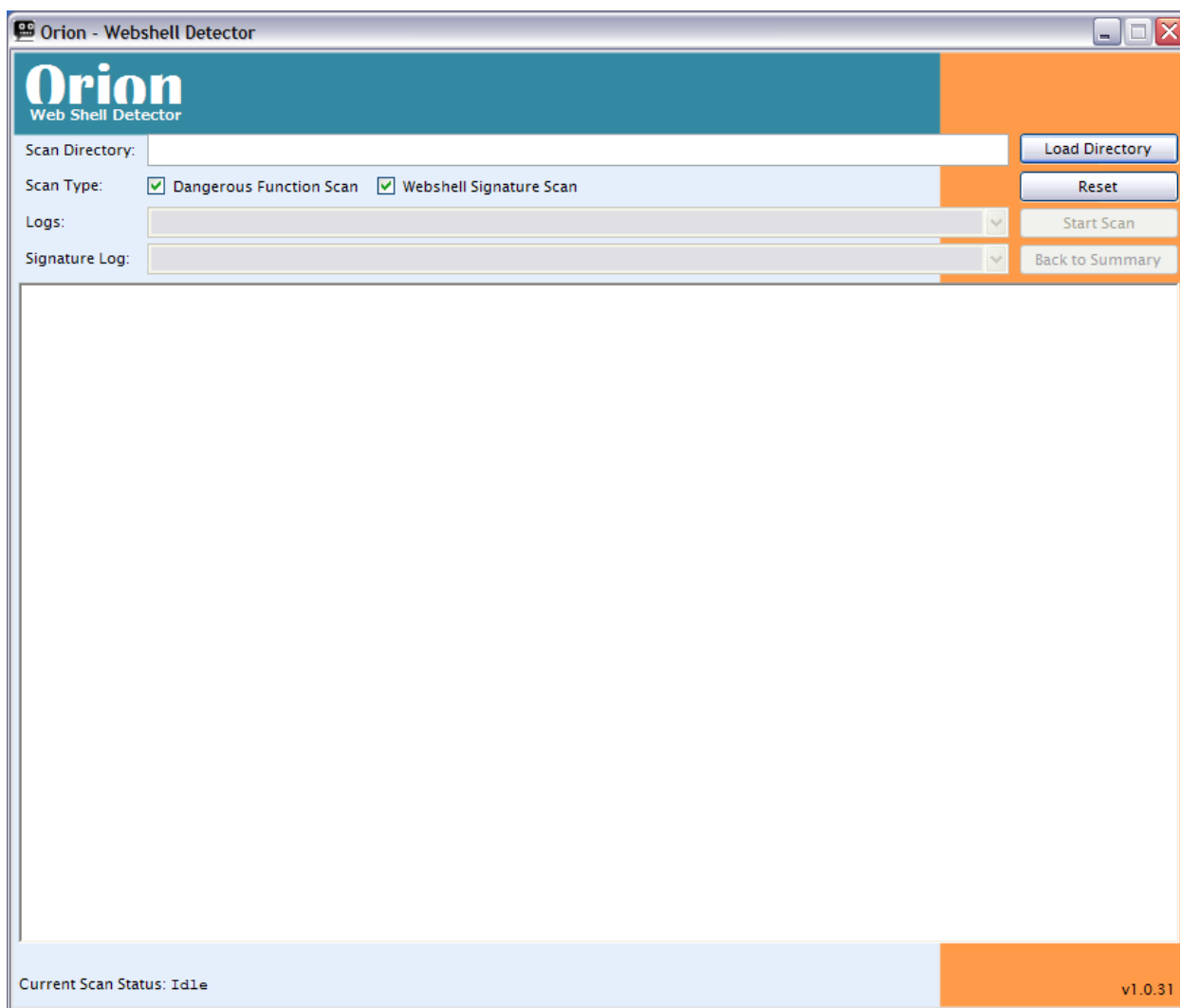
- To install, click Yes.



- Choose your installation directory.



- The installation is complete when the above message is displayed.
- Navigate to the installation folder and open wsd-gui.exe to run the web shell detector.



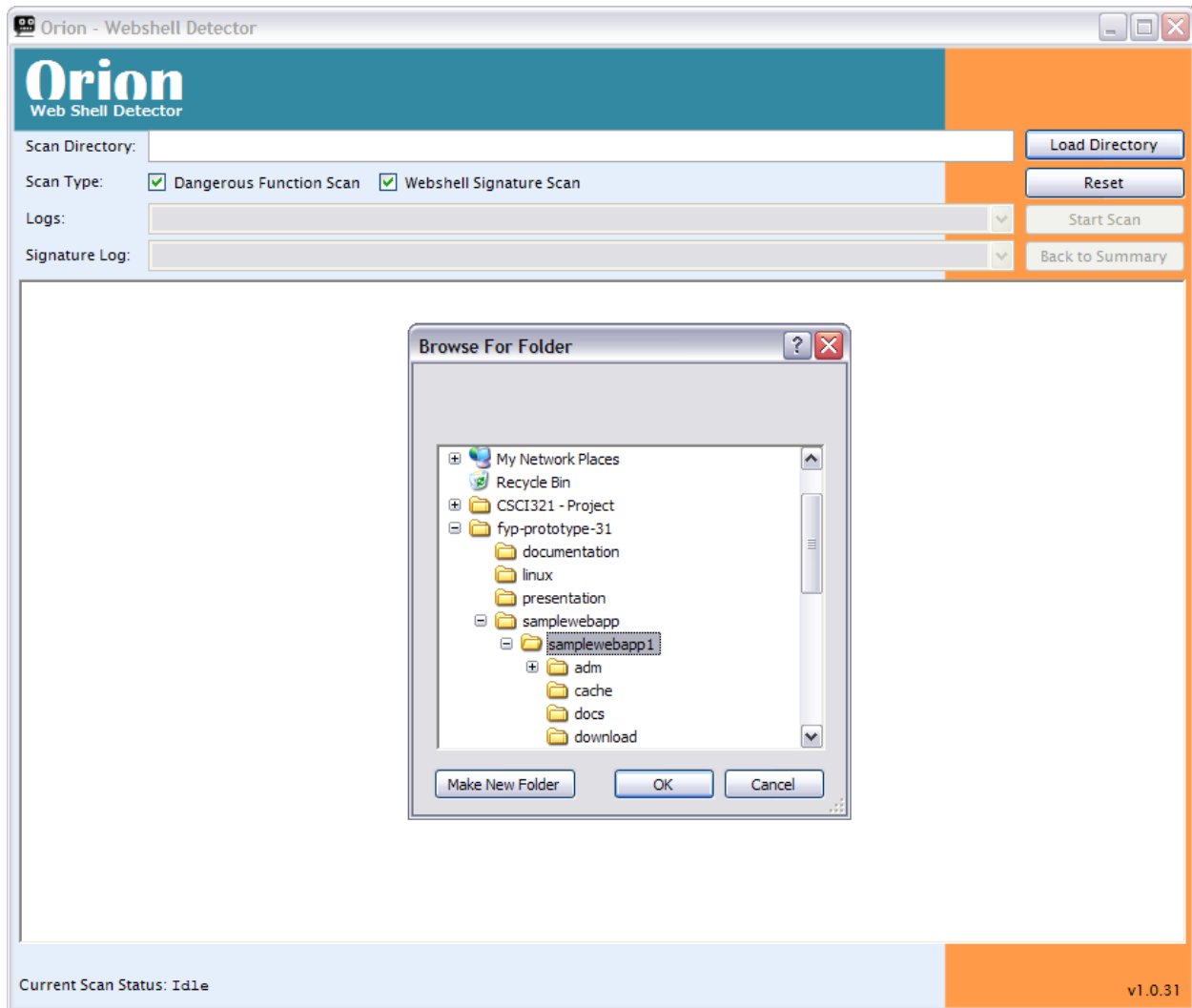
- This is the overall GUI of the web shell detector.

Running and Using Web Shell Detector

Entering Required Information

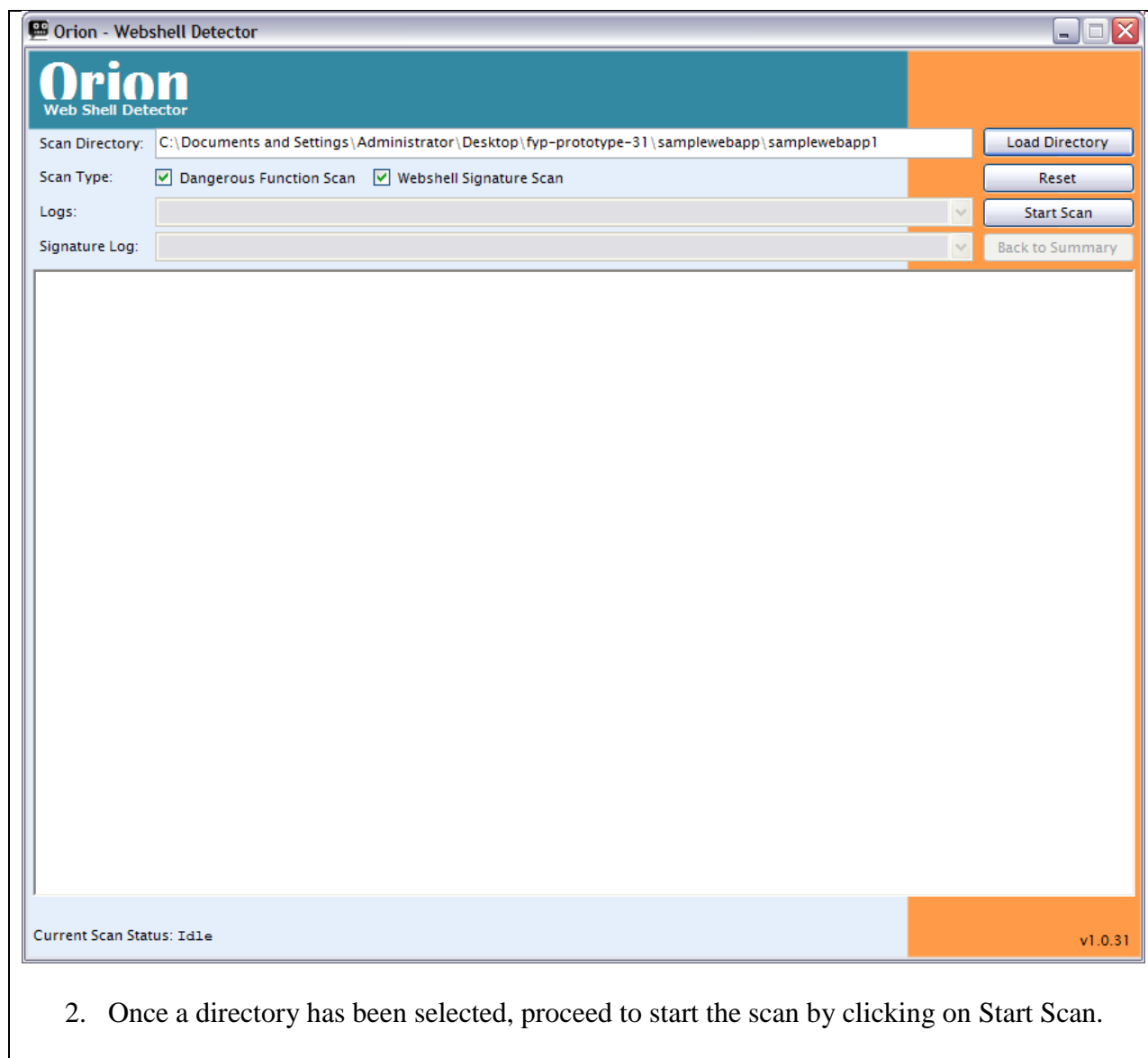
The user will first select the directory where the scan is to be conducted. It is usually the root path of the web server application in question.

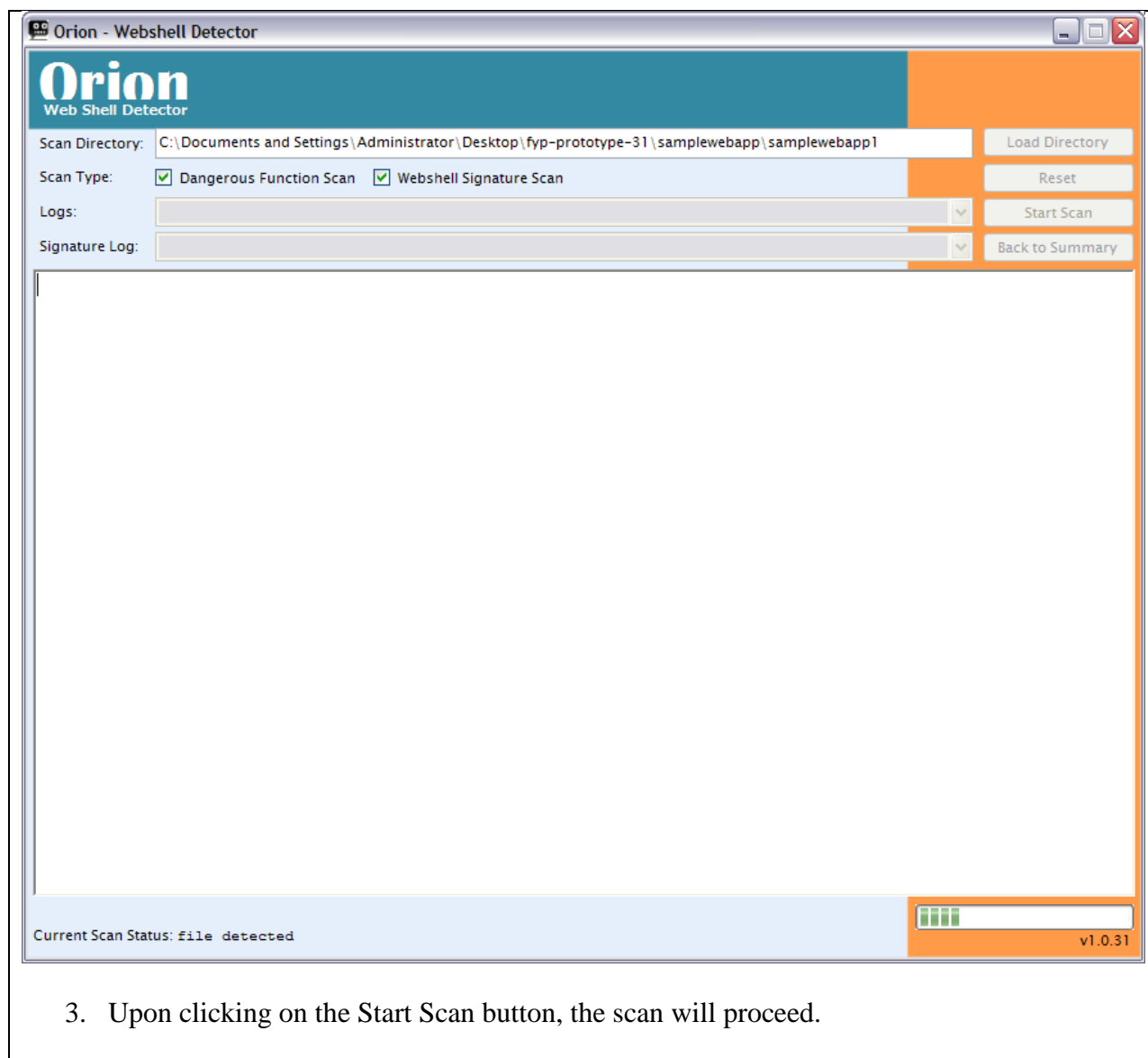
The user will be allowed to select the type of scan to be carried out, either a Web Shell Scan, Dangerous Function Scan, or both, using the checkboxes.

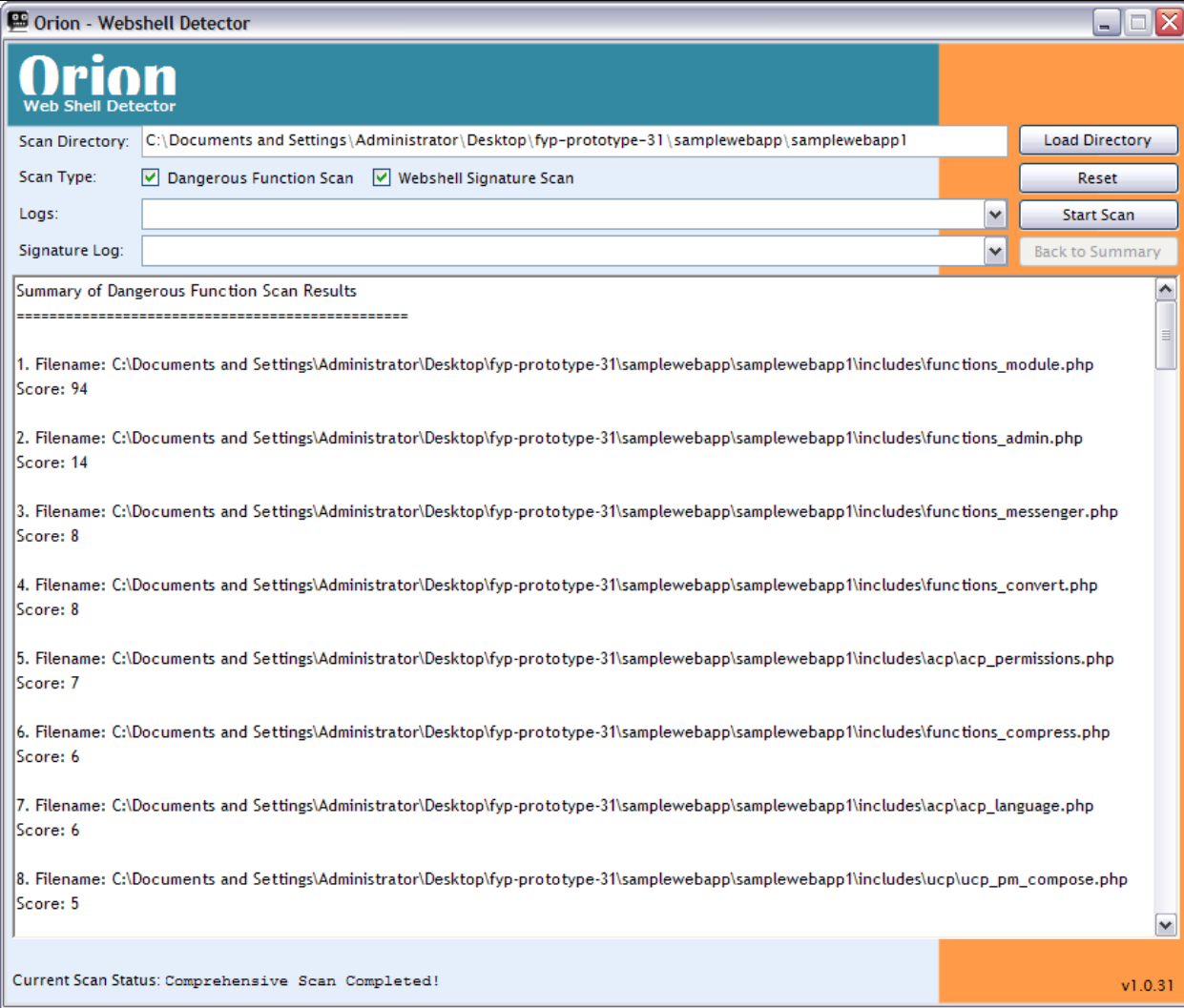


Steps:

1. Load a web application directory to scan by clicking the load directory button and subsequently click on OK.







The screenshot displays the Orion Web Shell Detector application window. The title bar reads "Orion - Webshell Detector". The interface has a blue header with the "Orion Web Shell Detector" logo. Below the header, there are input fields for "Scan Directory" (set to "C:\Documents and Settings\Administrator\Desktop\fypp-prototype-31\samplewebapp\samplewebapp1"), "Scan Type" (with checkboxes for "Dangerous Function Scan" and "Webshell Signature Scan"), "Logs", and "Signature Log". Action buttons include "Load Directory", "Reset", "Start Scan", and "Back to Summary".

The main content area shows a "Summary of Dangerous Function Scan Results" with a list of 8 files and their scores, ranked in descending order:

1. Filename: C:\Documents and Settings\Administrator\Desktop\fypp-prototype-31\samplewebapp\samplewebapp1\includes\functions_module.php
Score: 94
2. Filename: C:\Documents and Settings\Administrator\Desktop\fypp-prototype-31\samplewebapp\samplewebapp1\includes\functions_admin.php
Score: 14
3. Filename: C:\Documents and Settings\Administrator\Desktop\fypp-prototype-31\samplewebapp\samplewebapp1\includes\functions_messenger.php
Score: 8
4. Filename: C:\Documents and Settings\Administrator\Desktop\fypp-prototype-31\samplewebapp\samplewebapp1\includes\functions_convert.php
Score: 8
5. Filename: C:\Documents and Settings\Administrator\Desktop\fypp-prototype-31\samplewebapp\samplewebapp1\includes\acp\acp_permissions.php
Score: 7
6. Filename: C:\Documents and Settings\Administrator\Desktop\fypp-prototype-31\samplewebapp\samplewebapp1\includes\functions_compress.php
Score: 6
7. Filename: C:\Documents and Settings\Administrator\Desktop\fypp-prototype-31\samplewebapp\samplewebapp1\includes\acp\acp_language.php
Score: 6
8. Filename: C:\Documents and Settings\Administrator\Desktop\fypp-prototype-31\samplewebapp\samplewebapp1\includes\ucp\ucp_pm_compose.php
Score: 5

The status bar at the bottom indicates "Current Scan Status: Comprehensive Scan Completed!" and the version "v1.0.31".

4. When the scan is completed, a summary of the scan results will be displayed. The files are ranked accordingly to their scores in descending order.

The screenshot displays the Orion Web Shell Detector application window. The interface includes a header with the Orion logo and title. Below the header, there are input fields for 'Scan Directory' and 'Scan Type' (with checkboxes for 'Dangerous Function Scan' and 'Webshell Signature Scan'). A 'Logs' dropdown menu is open, showing a list of log files. The 'Summary of Dangerous Files' section lists eight files with their scores. The status bar at the bottom indicates 'Current Scan Status: Comprehensive Scan Completed!' and the version 'v1.0.31'.

Orion - Webshell Detector

Orion
Web Shell Detector

Scan Directory: C:\Documents and Settings\Administrator\Desktop\fypprototype-31\samplewebapp\samplewebapp1

Scan Type: ☒ Dangerous Function Scan ☒ Webshell Signature Scan

Logs: [Dropdown Menu]

Signature Log: [Dropdown Menu]

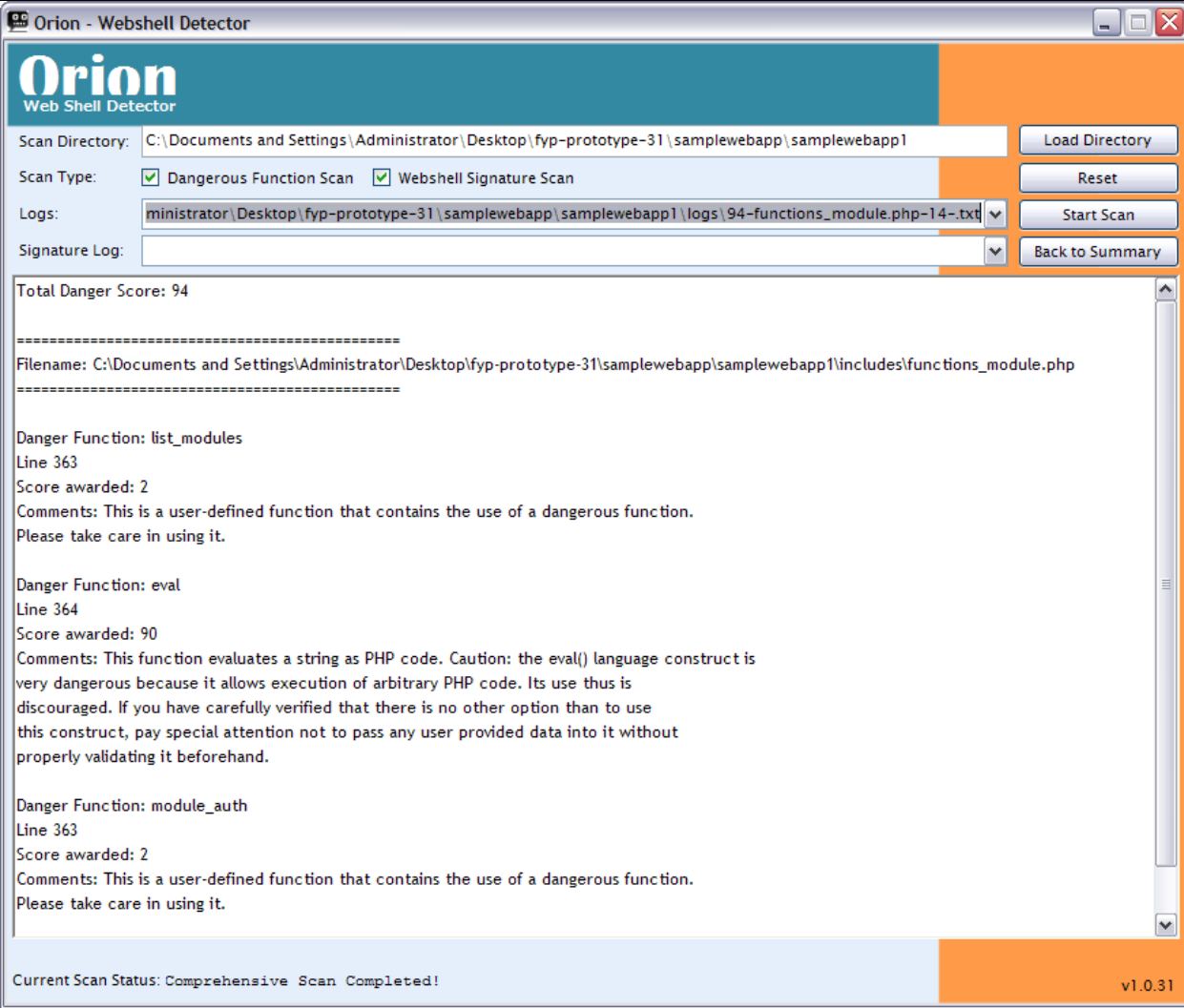
Buttons: Load Directory, Reset, Start Scan, Back to Summary

Summary of Dangerous Files

1. Filename: C:\Documents and Settings\Administrator\Desktop\fypprototype-31\samplewebapp\samplewebapp1\logs\94- module.php
Score: 94
2. Filename: C:\Documents and Settings\Administrator\Desktop\fypprototype-31\samplewebapp\samplewebapp1\includes\functions_admin.php
Score: 14
3. Filename: C:\Documents and Settings\Administrator\Desktop\fypprototype-31\samplewebapp\samplewebapp1\includes\functions_messenger.php
Score: 8
4. Filename: C:\Documents and Settings\Administrator\Desktop\fypprototype-31\samplewebapp\samplewebapp1\includes\functions_convert.php
Score: 8
5. Filename: C:\Documents and Settings\Administrator\Desktop\fypprototype-31\samplewebapp\samplewebapp1\includes\acp\acp_permissions.php
Score: 7
6. Filename: C:\Documents and Settings\Administrator\Desktop\fypprototype-31\samplewebapp\samplewebapp1\includes\functions_compress.php
Score: 6
7. Filename: C:\Documents and Settings\Administrator\Desktop\fypprototype-31\samplewebapp\samplewebapp1\includes\acp\acp_language.php
Score: 6
8. Filename: C:\Documents and Settings\Administrator\Desktop\fypprototype-31\samplewebapp\samplewebapp1\includes\ucp\ucp_pm_compose.php
Score: 5

Current Scan Status: Comprehensive Scan Completed! v1.0.31

5. Individual file logs can be loaded to and viewed by using the Logs drop down list.



The screenshot displays the Orion Web Shell Detector application window. The title bar reads "Orion - Webshell Detector". The interface has a blue header with the "Orion Web Shell Detector" logo. Below the header, there are input fields for "Scan Directory" (C:\Documents and Settings\Administrator\Desktop\myp-prototype-31\samplewebapp\samplewebapp1), "Scan Type" (checked for "Dangerous Function Scan" and "Webshell Signature Scan"), "Logs" (a dropdown menu showing "ministrator\Desktop\myp-prototype-31\samplewebapp\samplewebapp1\logs\94-functions_module.php-14-.txt"), and "Signature Log". Buttons for "Load Directory", "Reset", "Start Scan", and "Back to Summary" are on the right. The main area shows the "Total Danger Score: 94" and a list of detected dangerous functions: `list_modules` (Line 363, Score 2), `eval` (Line 364, Score 90), and `module_auth` (Line 363, Score 2). Each function entry includes a comment explaining its danger. The status bar at the bottom indicates "Current Scan Status: Comprehensive Scan Completed!" and the version "v1.0.31".

6. Upon clicking on a selected log, it will be loaded and displayed as shown above.