Web Application Penetration Testing Methodology

3 Hr 29 Min Remaining

Instructions Resources Help  100%

Exercise 1: Gathering Information About a Target Using WhatWeb

Scenario

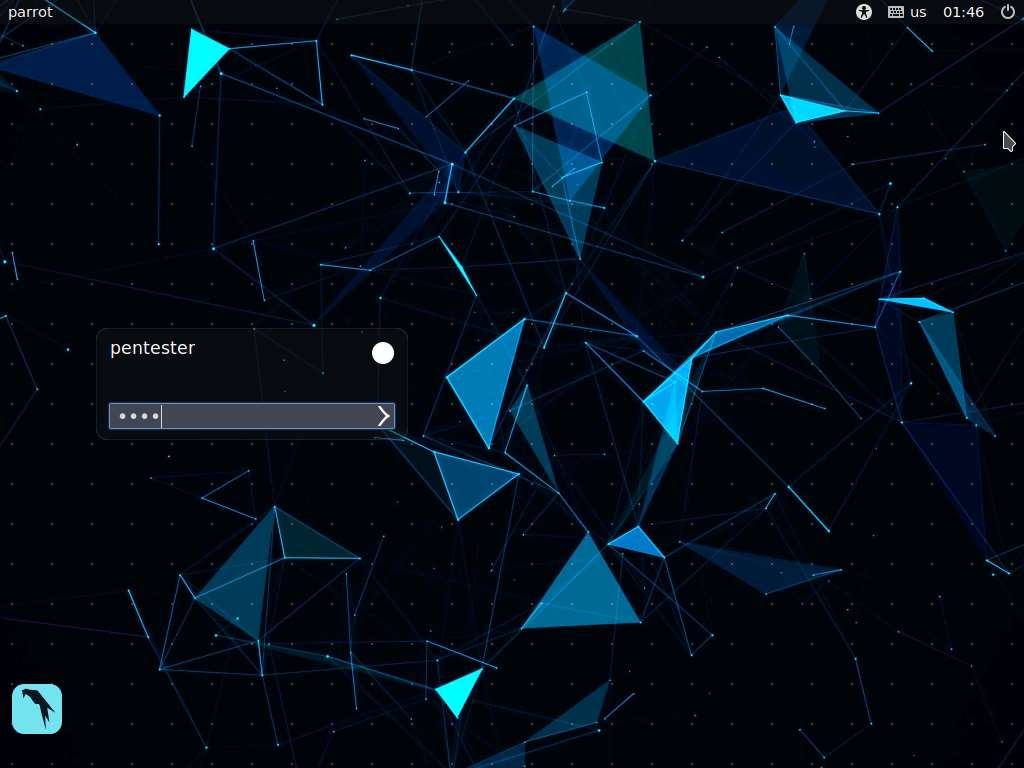
WhatWeb identifies websites. It recognises web technologies including content management systems (CMS), blogging platforms, statistic/analytics packages, JavaScript libraries, web servers, and embedded devices. WhatWeb identifies version numbers, email addresses, account IDs, web framework modules, SQL errors, and more.

The objective of this lab is to help students learn how to:

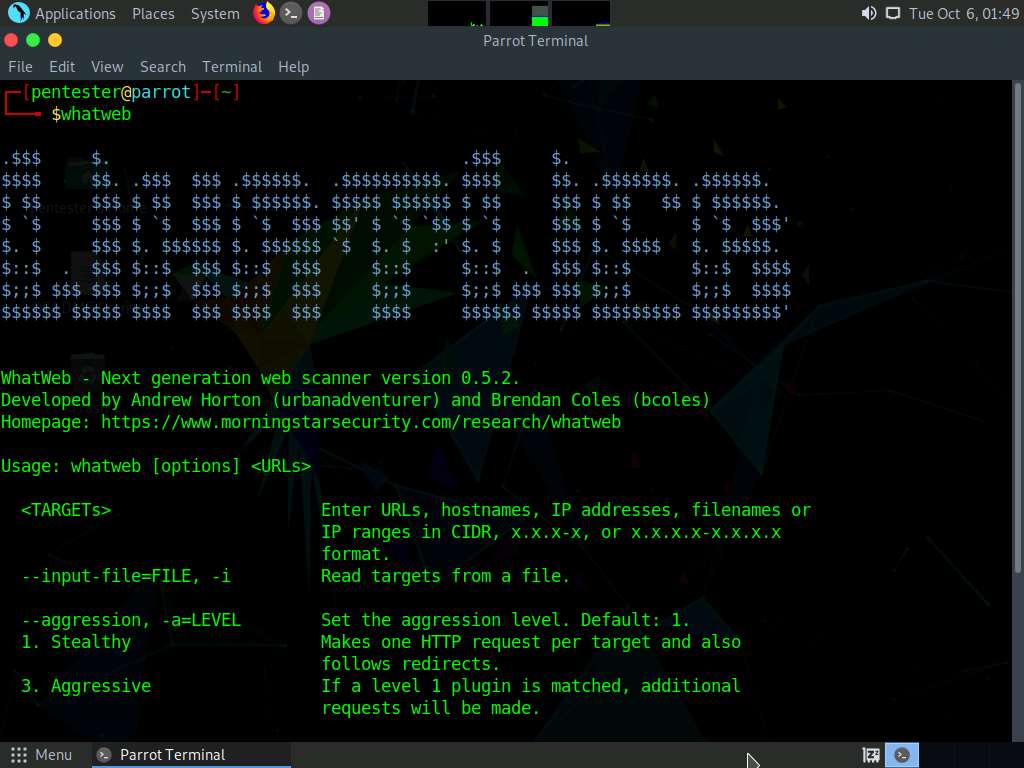
* Identify the target website technologies
* Perform aggressive scans
* Log output in an xml format

**Lab Duration**: **10** Minutes

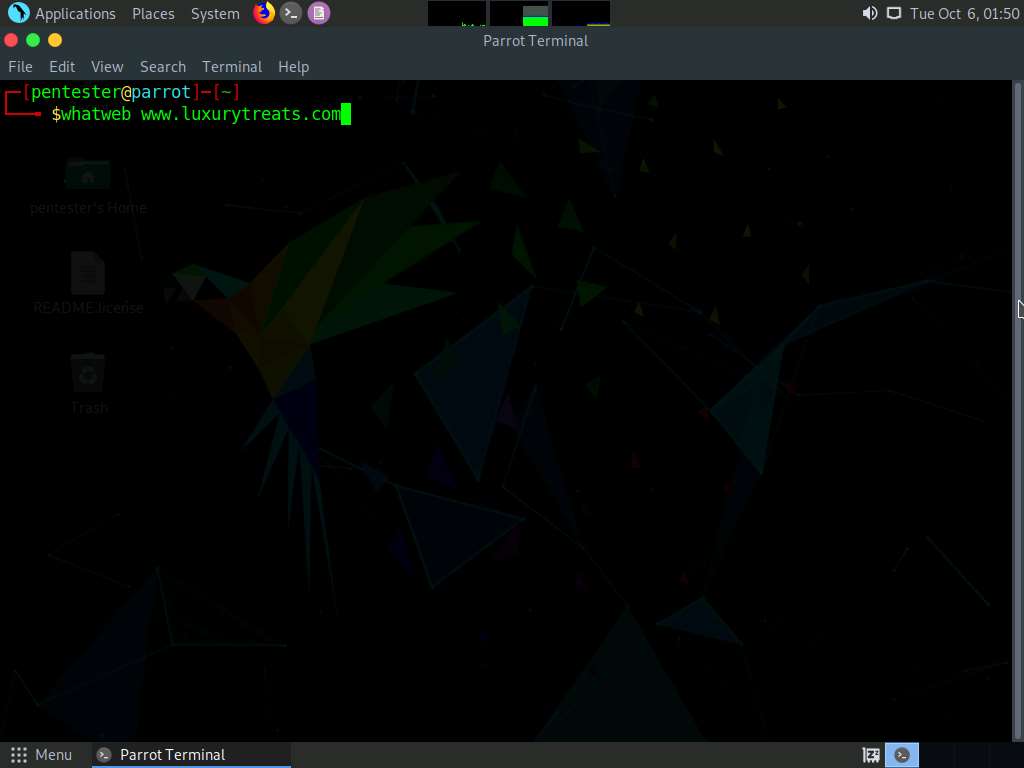
1. Click [Parrot](https://labclient.labondemand.com/Instructions/24205116-eb0d-48aa-9936-8931f0fd5efc?rc=10). Type **toor** in the **Password** field and press **Enter**.



1. Launch a command line terminal from the taskbar, type **whatweb** and press **Enter**. It displays the list of commands used by whatweb.

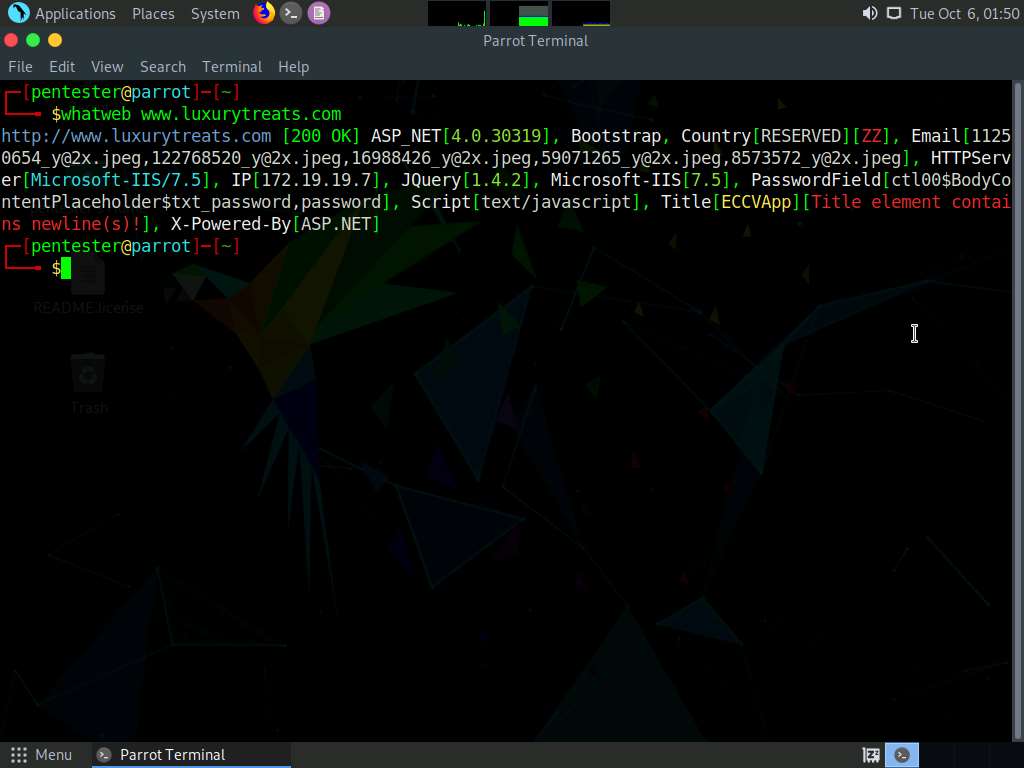


1. Assume **www.luxurytreats.com** is the target website. In this lab, you will be performing website fingerprinting on this website. Type the command **whatweb www.luxurytreats.com** and press **Enter**.

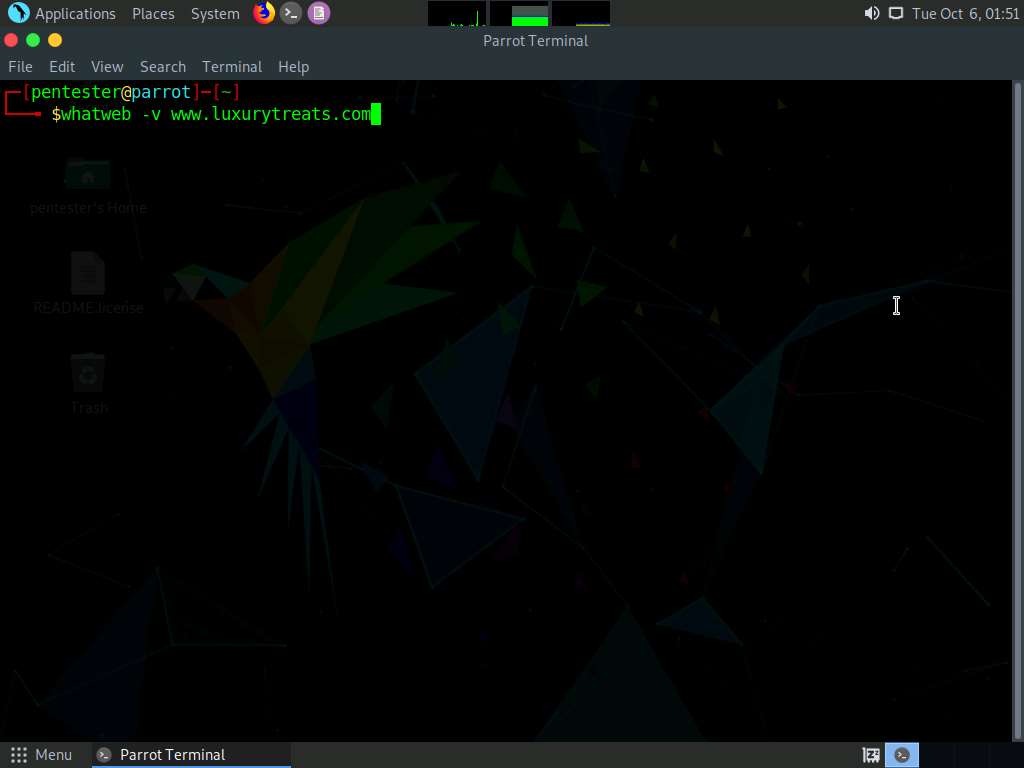


1. **whatweb** returns the luxurytreats website infrastructure as shown in the screenshot.

Ignore the warning messages.

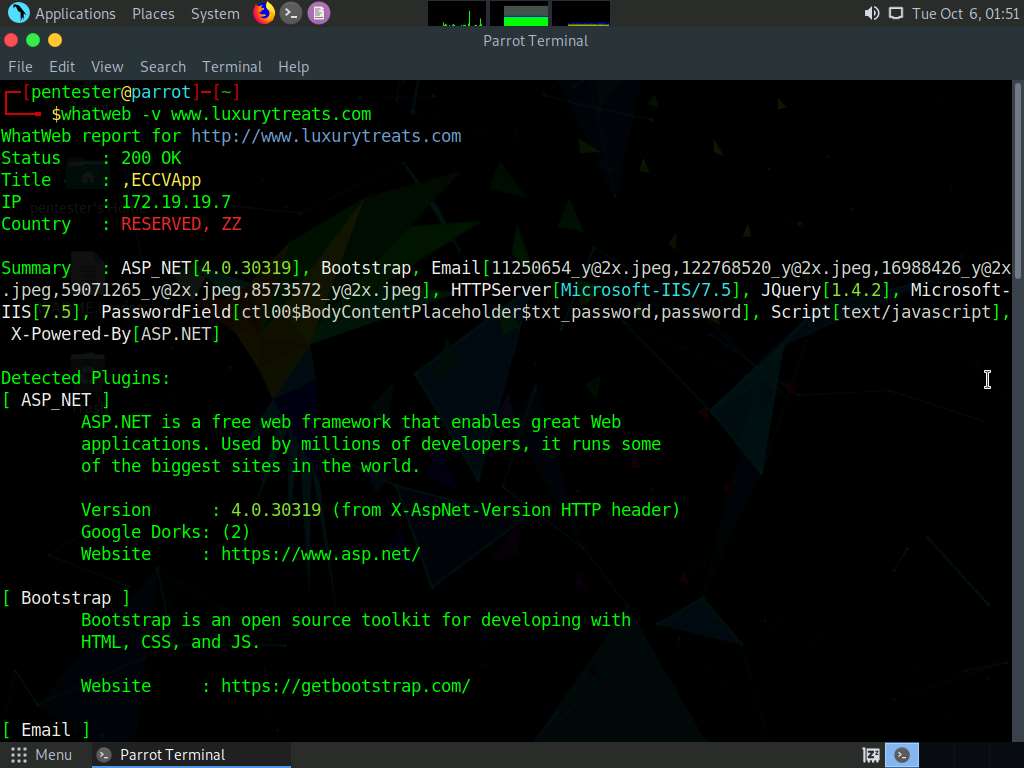


1. Since the result returned by whatweb is difficult to analyze, you can apply verbosity so that whatweb arranges the result in a clear way. Type the command **whatweb -v www.luxurytreats.com** and press **Enter**.

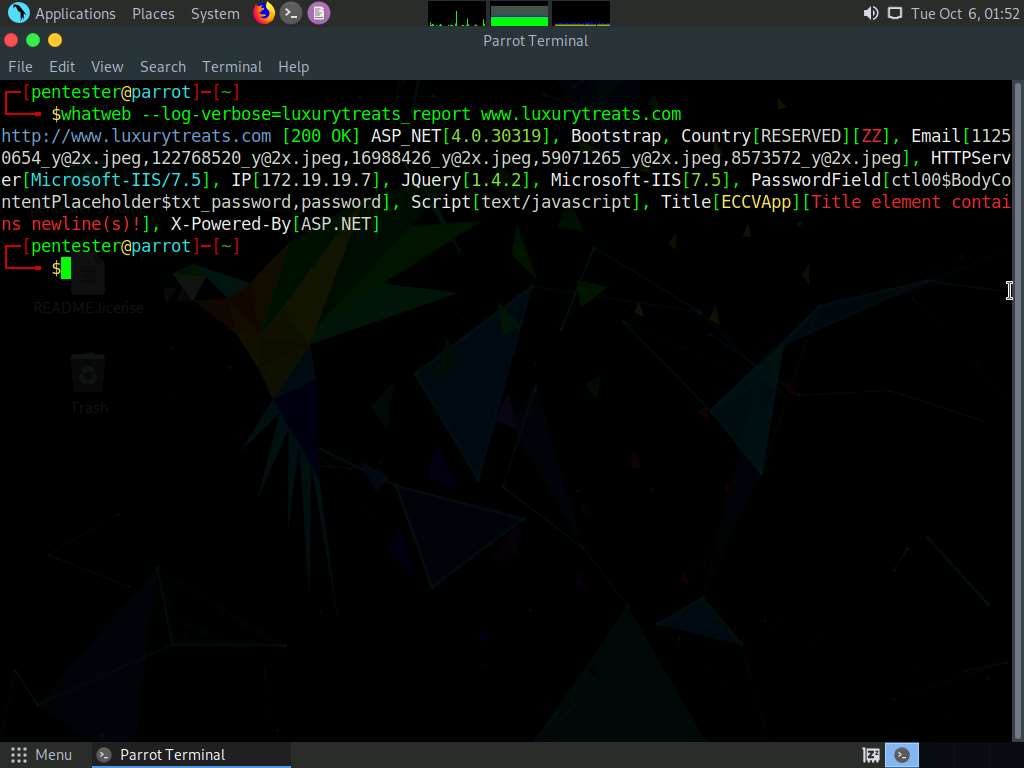


1. WhatWeb re-arranges the result in a better understandable manner as shown in the screenshot.

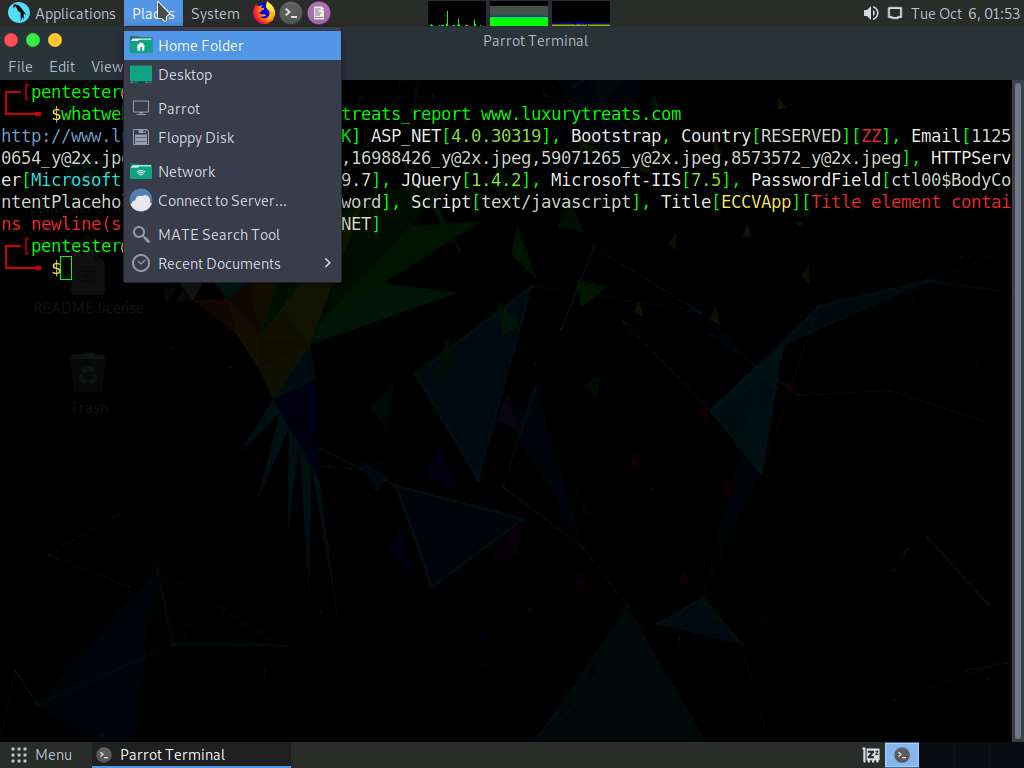
You may set WhatWeb in **aggressive** mode to obtain the version numbers of plugins used in the website.



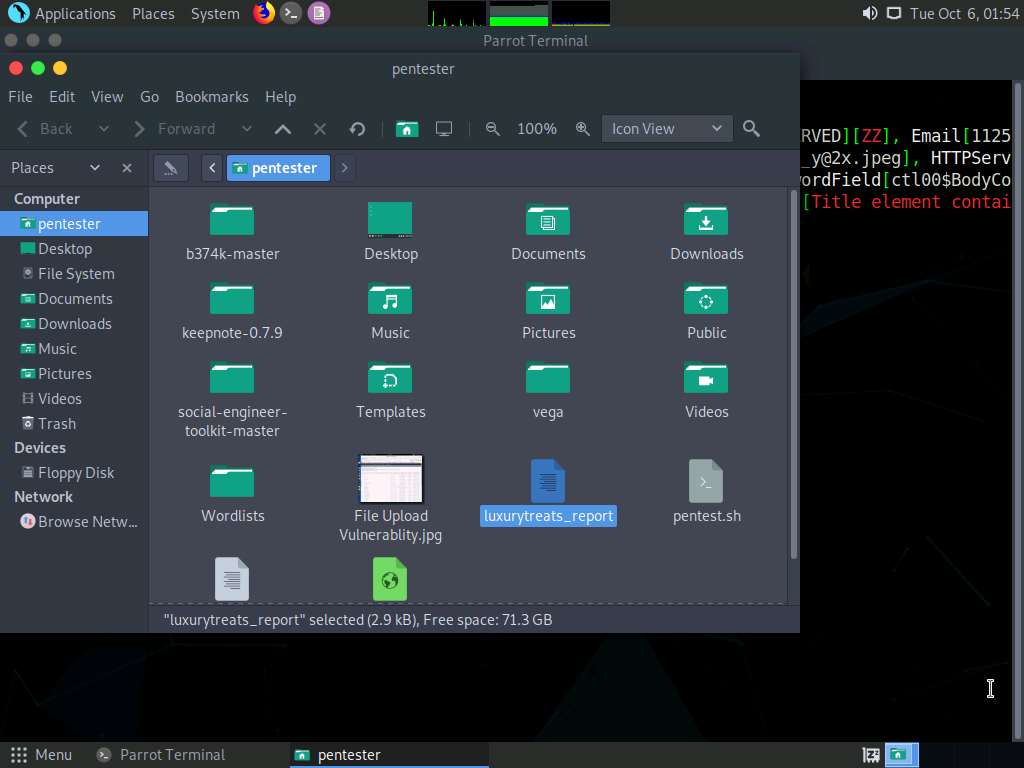
1. You can export the result returned by WhatWeb. To export the result to a text file, type the command **whatweb --log-verbose=luxurytreats\_report www.luxurytreats.com** and press **Enter**. This will generate a report with the name **luxurytreats\_report** and saves this file in **root** folder.



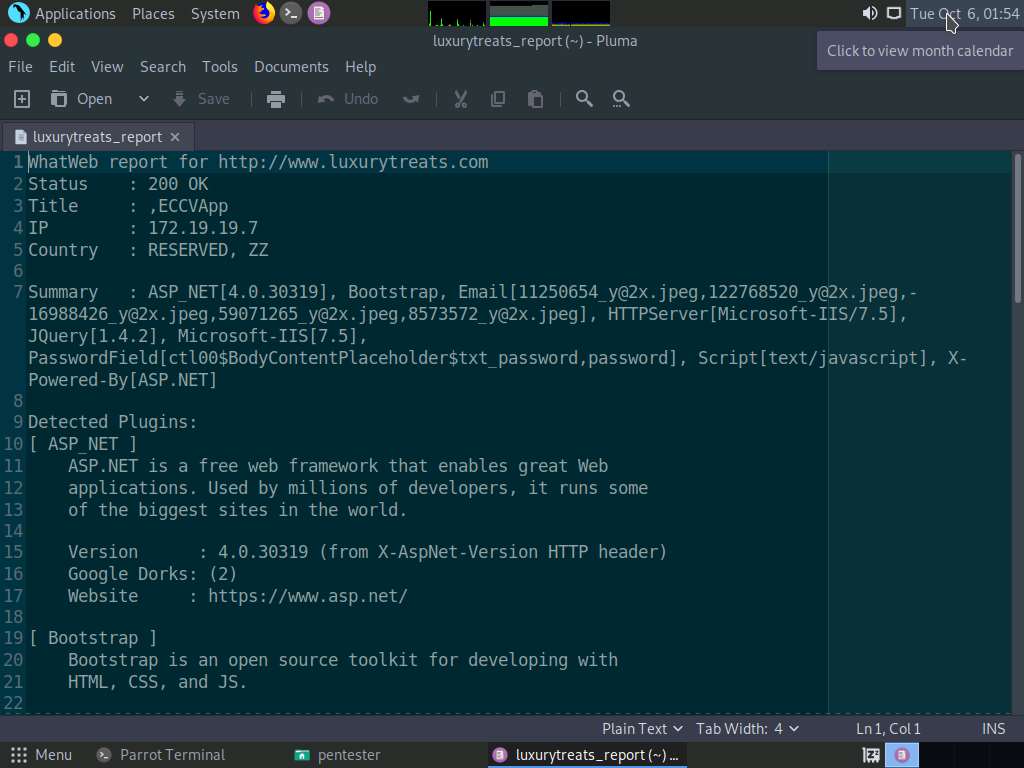
1. Navigate to **Places** folder to find the report containing the result. To open root folder, go to **Places** --> **Home Folder** .



1. **pentester** folder appears, double-click **luxurytreats\_report**.



1. The report appears in the text file as shown in the screenshot. Analyze the result to get an idea about the website infrastructure.



1. Close all the opened windows.

In this lab, you have learned how to:

* Identify the target website technologies
* Perform aggressive scans
* Log output in an xml format