Web Application Penetration Testing Methodology

3 Hr 29 Min Remaining

Instructions Resources Help  100%

Exercise 2: Web Application Vulnerability Assessment Using Vega

Scenario

Vega is a free and open source scanner and testing platform to test the security of web applications. Vega can help to find and validate SQL Injection, Cross-Site Scripting (XSS), inadvertently disclosed sensitive information and other vulnerabilities. It is written in Java, GUI based and runs on Linux, OS X, and Windows. Vega includes an automated scanner for quick tests and an intercepting proxy for tactical inspection. The Vega scanner finds XSS, SQL injection, and other vulnerabilities. Vega can be extended using a powerful API in the language of the web: Javascript.

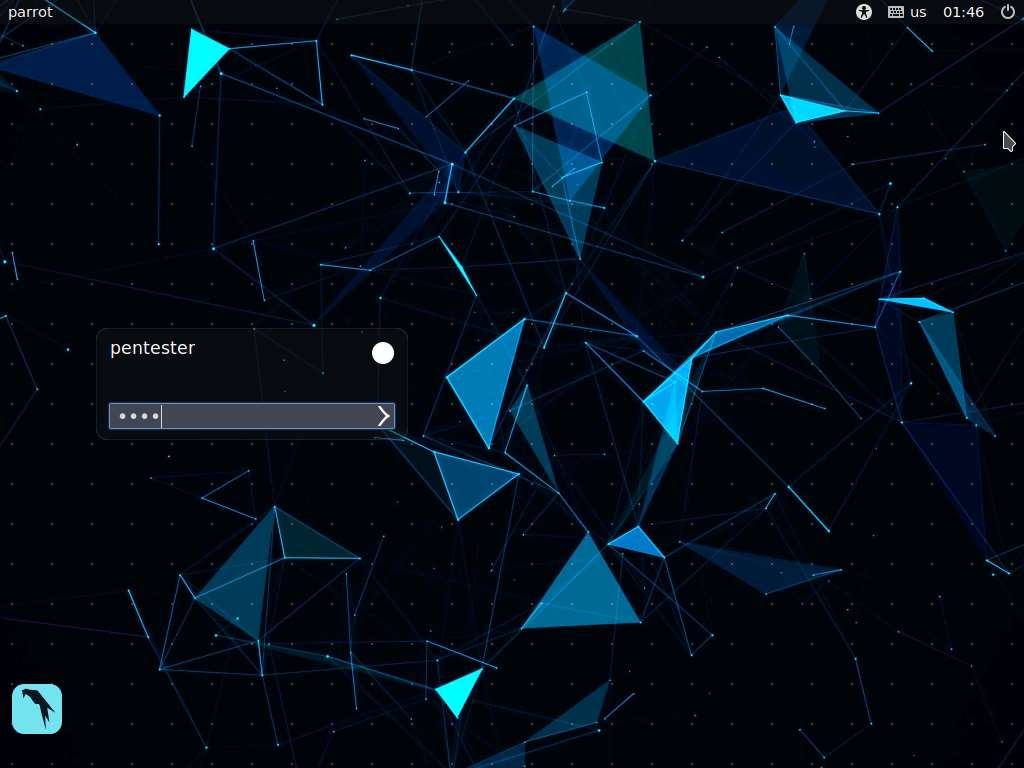
The objective of this lab is to help students to learn how to:

* Use Vega and perform Web Application Vulnerability Assessment
* Generate reports and examine them

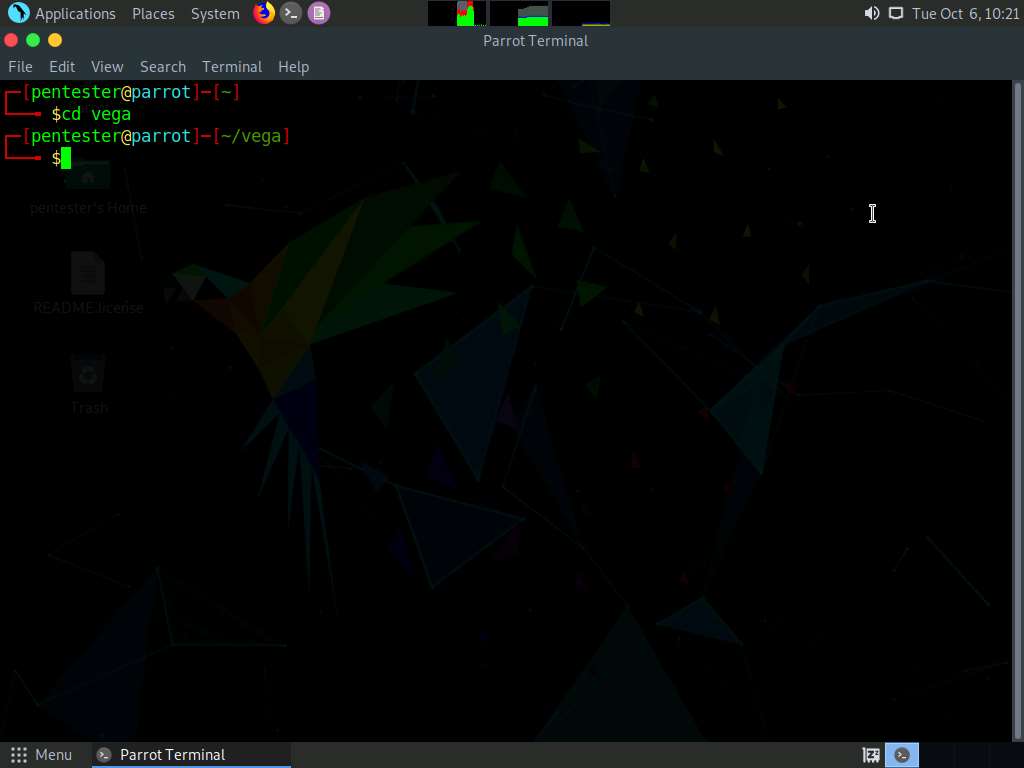
**Lab Duration**: **20** Minutes

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

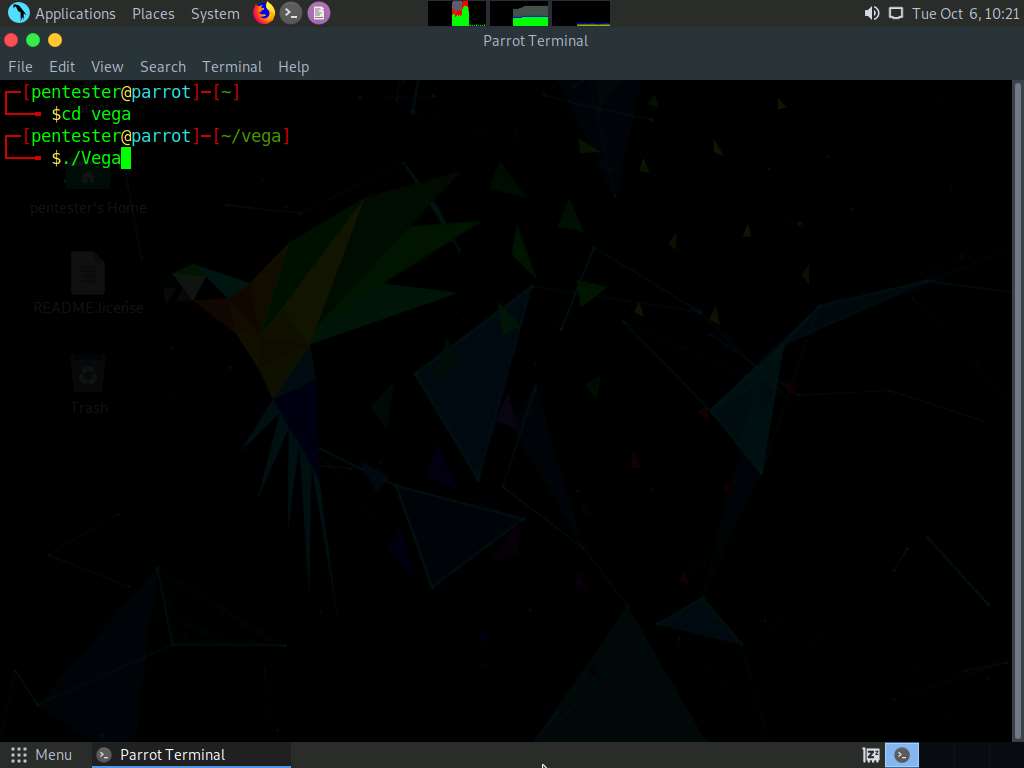
If you are already logged in skip to step **2**.



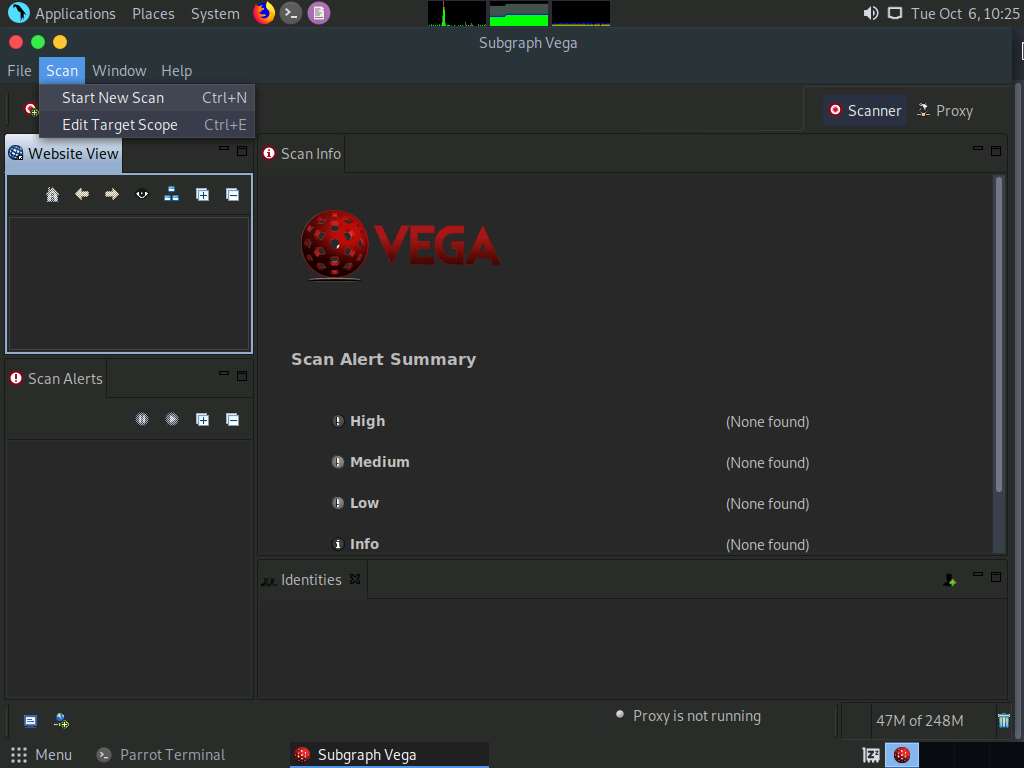
1. Launch a **Terminal** window from a menu bar. Type **cd vega** and press **Enter**.



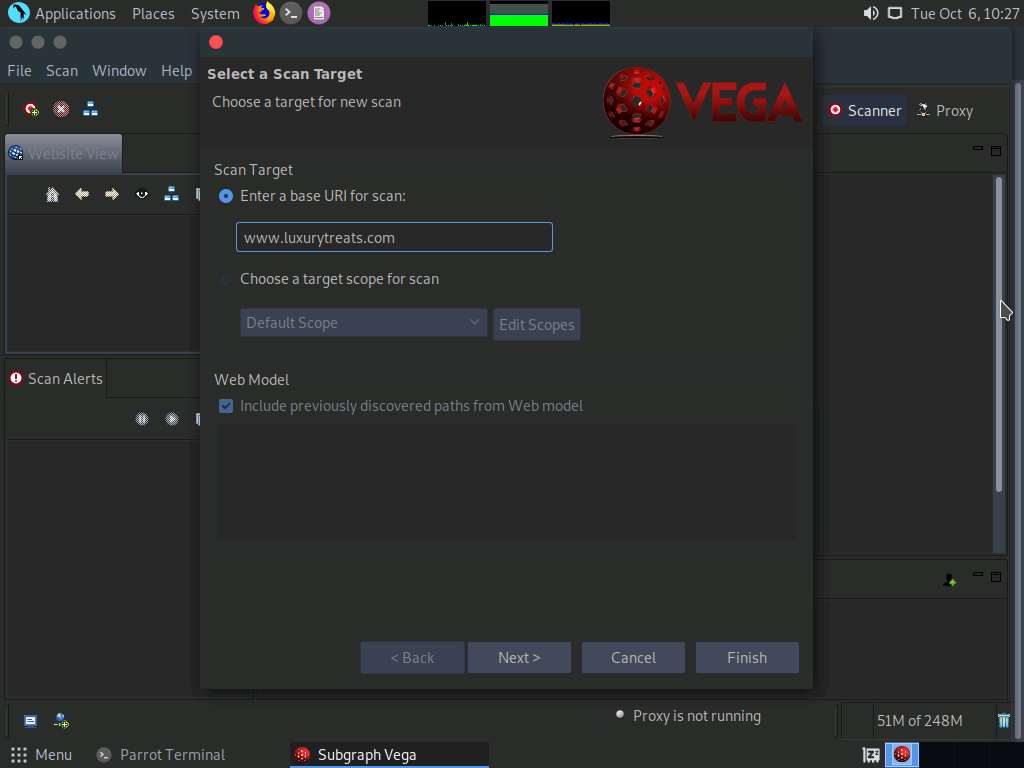
1. Type **./Vega** and press **Enter** to launch application.



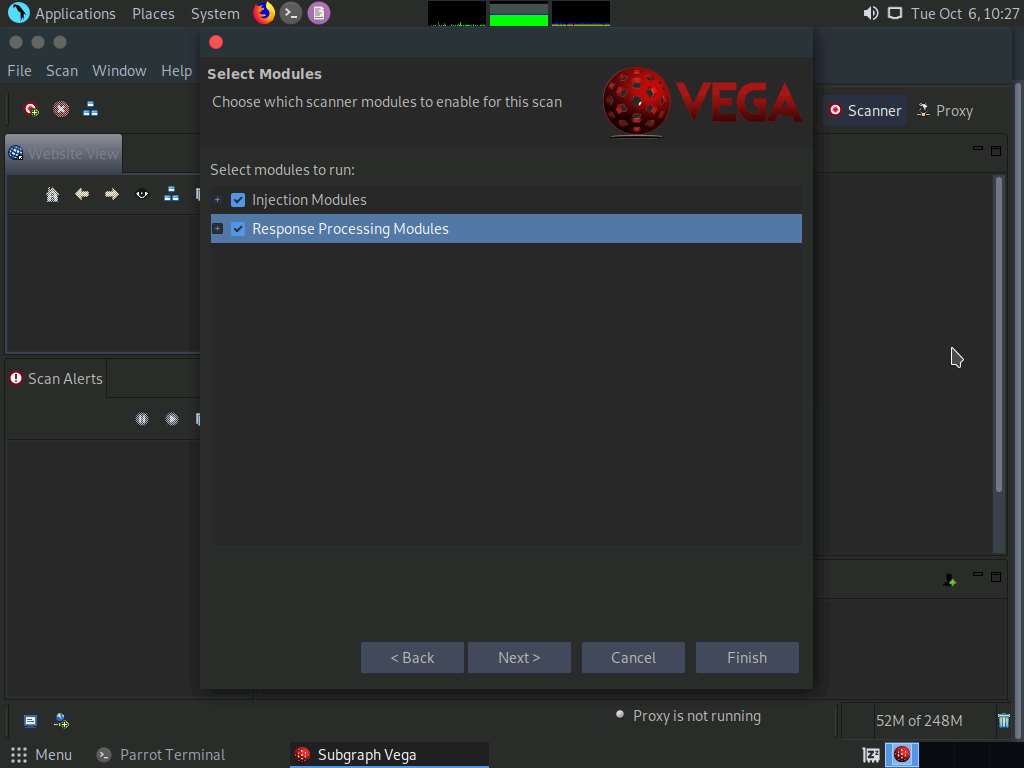
1. Vega vulnerability scanner main window appears as shown in the below screenshot. Click **Scan** from the menu bar and select **Start New Scan**.



1. Select a Scan Target Wizard appears on the screen. Select **Enter a base URI for scan** radio button under **Scan Target** section, enter the target URL in the text field and click **Next**. The target in this lab is **luxurytreats**, so the URL we enter is **www.luxurytreats.com**.

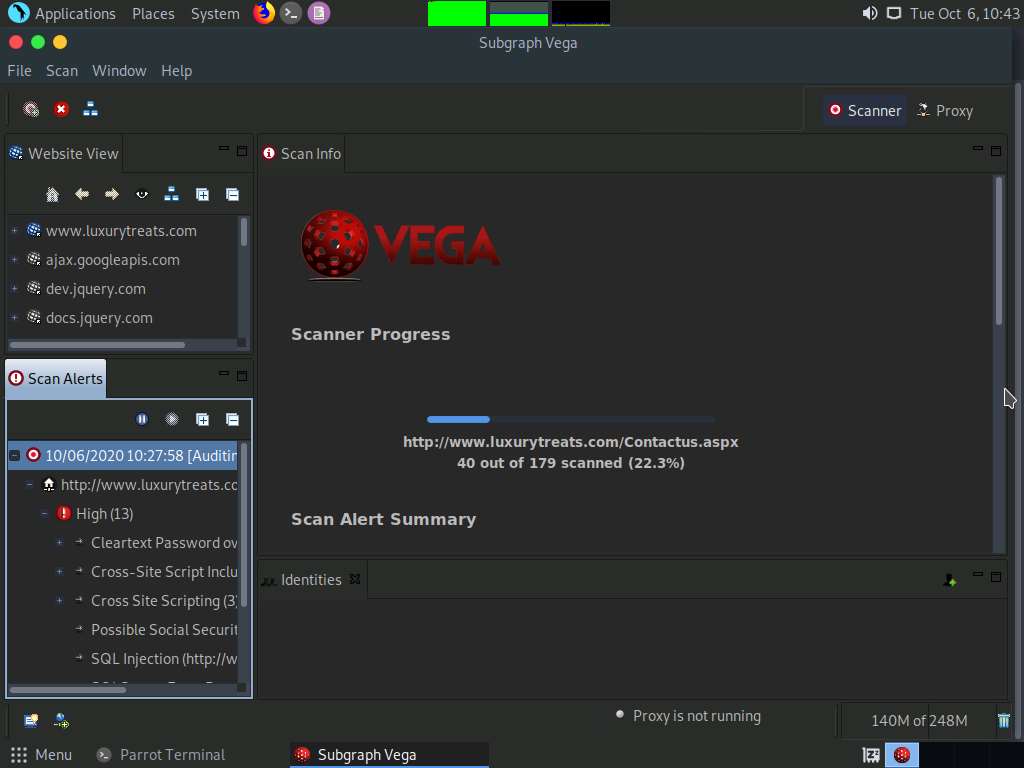


1. **Select Modules** section appears, check both **Injection Modules** and **Response Processing Modules** options. By checking these options, all the modules under these options will be selected. Click **Finish**.

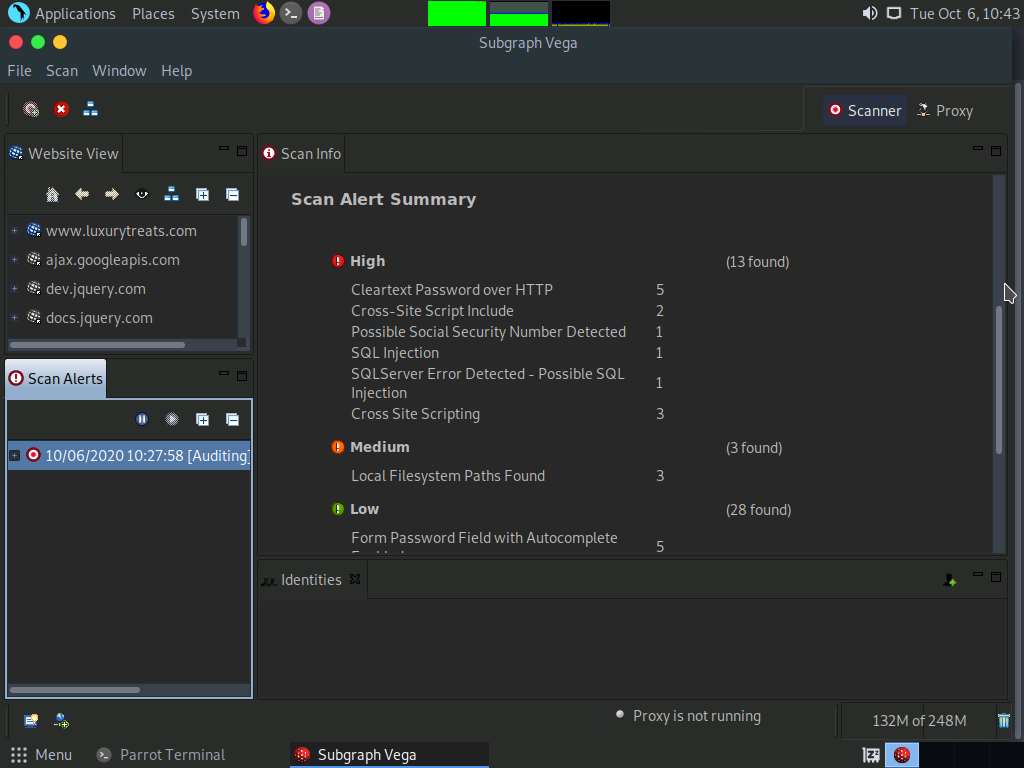


1. It will start scanning **www.luxurytreats.com**.

It will take approximately of 40 minutes to complete the scan. If you got the scan results of our target website you can continue with the next process.

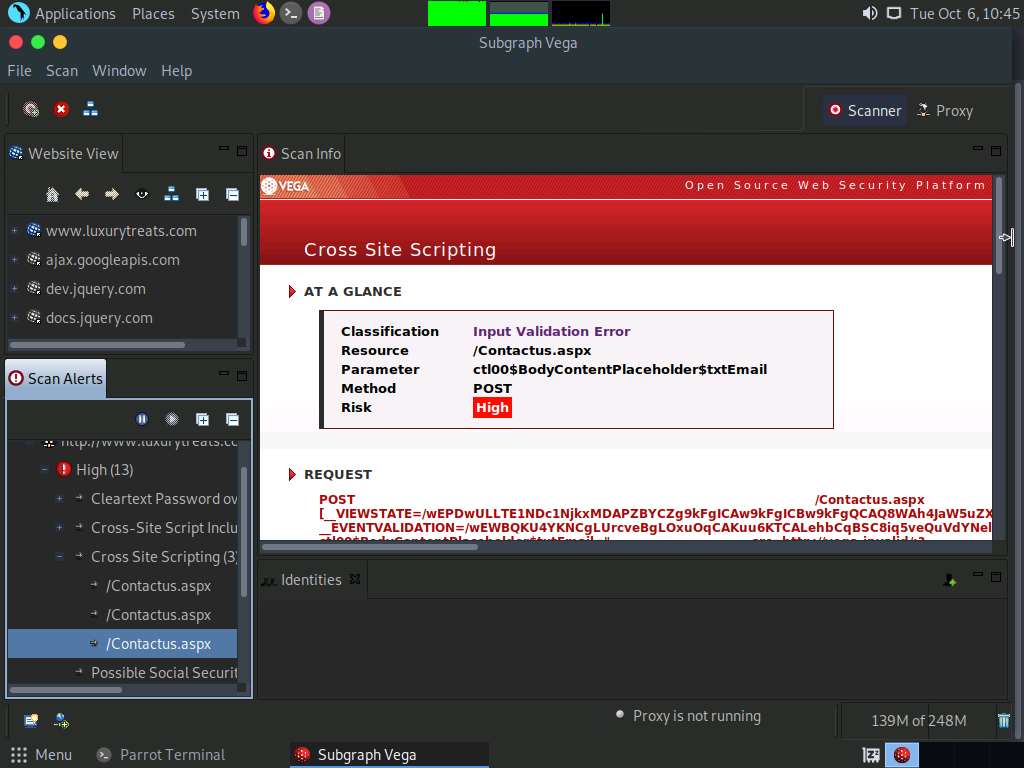


1. On completion of the scan, vega displays the scan alert summary, as shown in the screenshot.



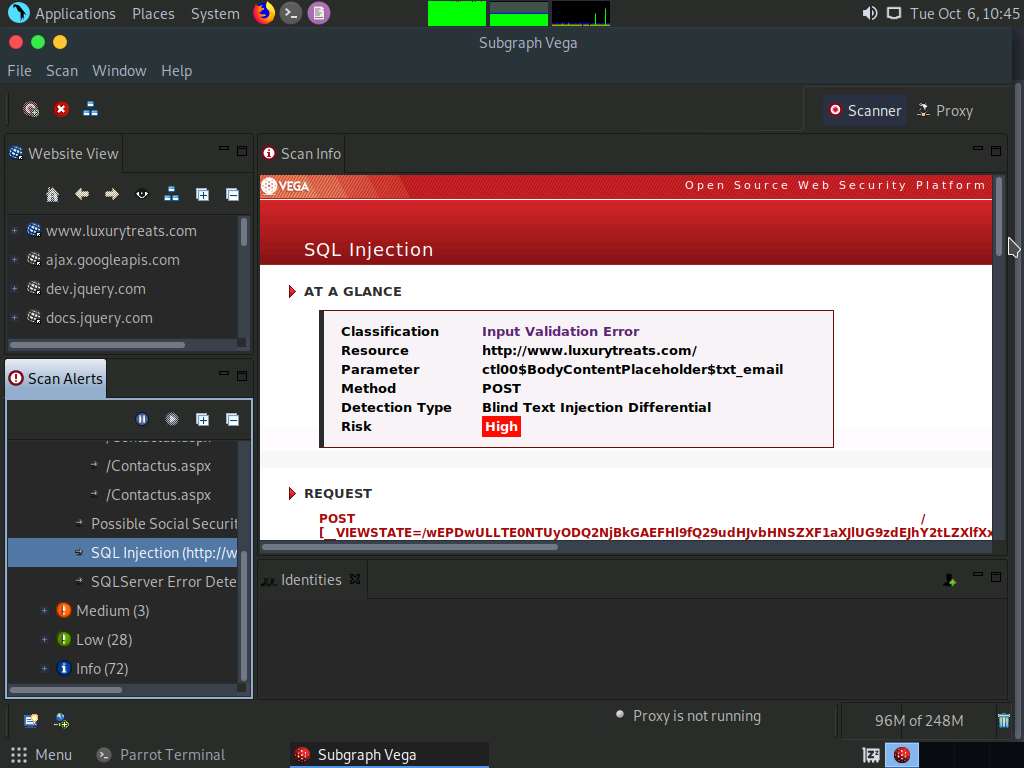
1. To view the scan alerts, expand the following nodes under **Scan Alerts** section. Node containing the data and time --> **http://www.luxurytreats.com** --> **High** --> **Cross Site Scripting (3)** and click **Contactus.aspx**. This displays the vulnerabilities associated with the selected node under the Scan Info section in the right pane as shown in the screenshot.

This is a screenshot for XSS Vulnerability present in the scanned website. We will be demonstrating how to exploit this vulnerability in the next exercise.

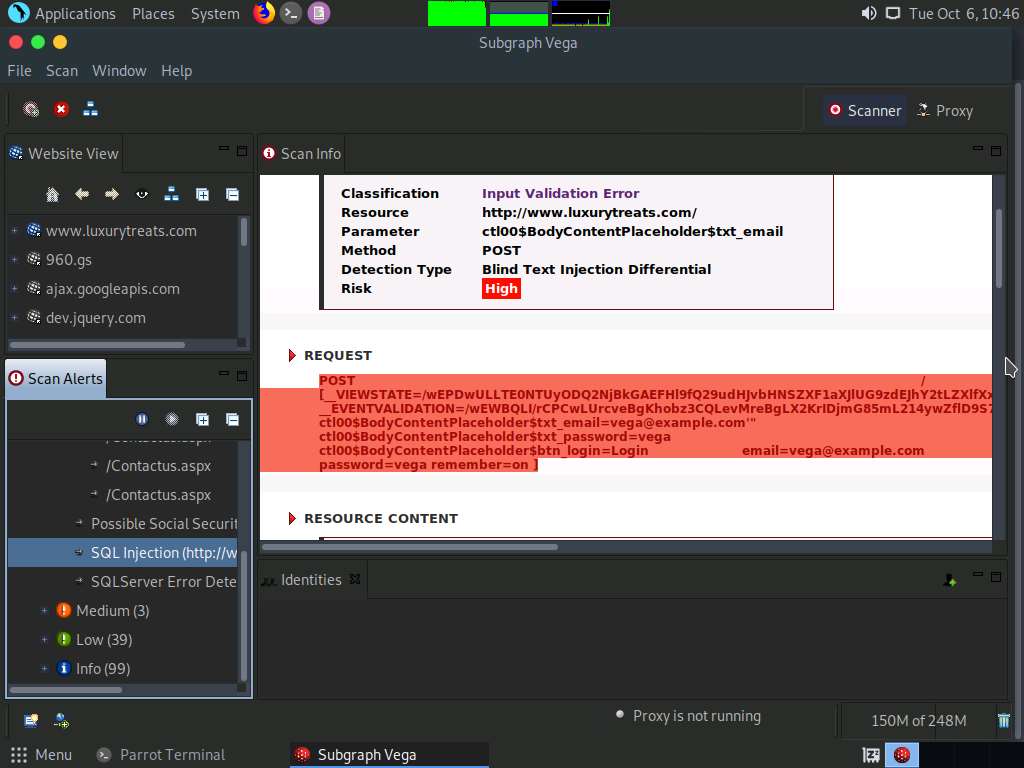


1. In the same way, you can expand **SQL Injection (http://www.luxurytreats.com/)** node to view information regarding the selected SQL Injection vulnerability.

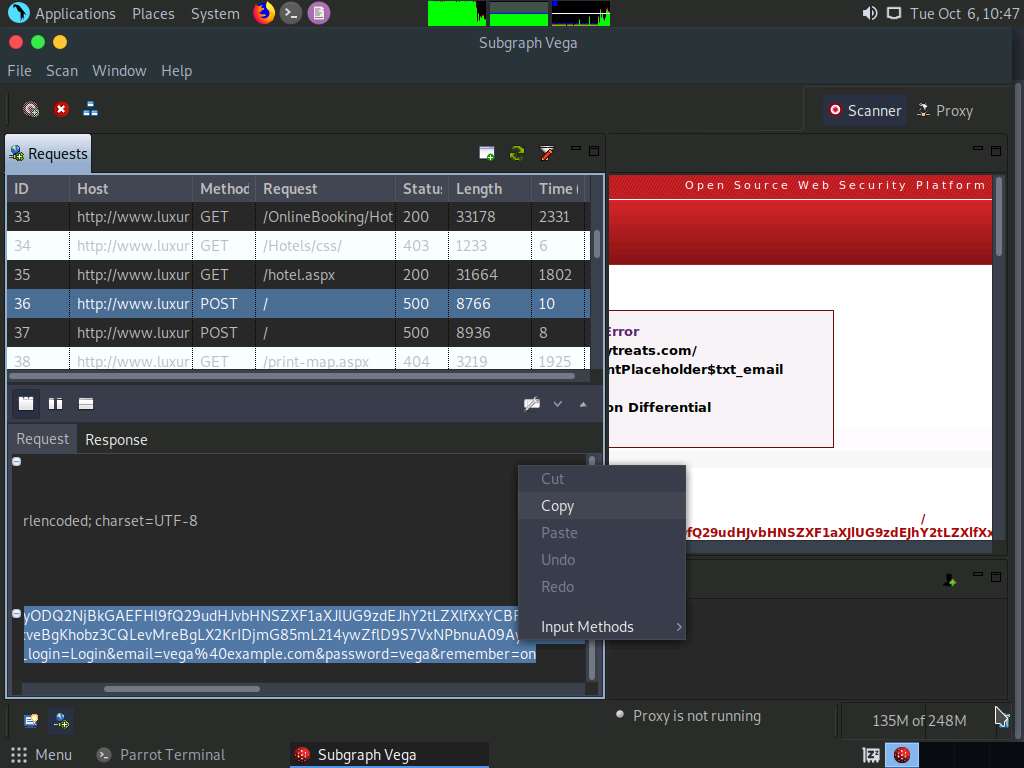
This is a screenshot for SQL Injection Vulnerability present in the scanned website. We will be demonstrating how to exploit this vulnerability in the next exercise.



1. Click on **REQUEST** content in the right-pane.

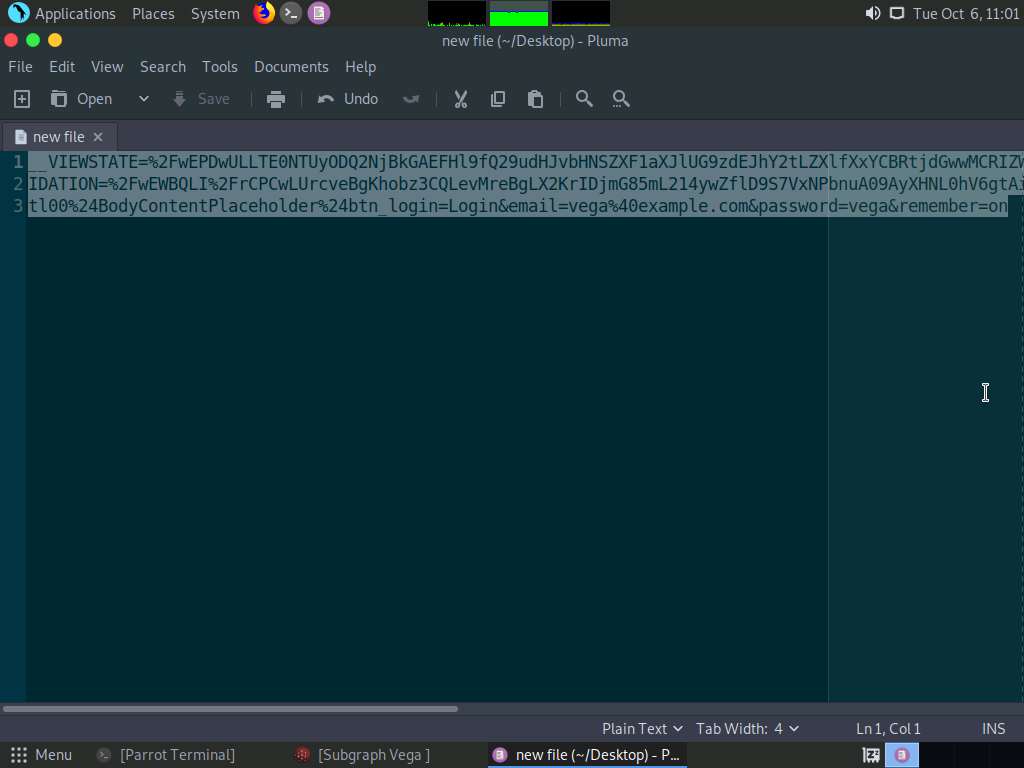


1. You will be redirected to **Requests** tab. In the bottom of the right-pane, click on **Request** tab to view the request content as shown in the screenshot. Select and **copy** the complete content.

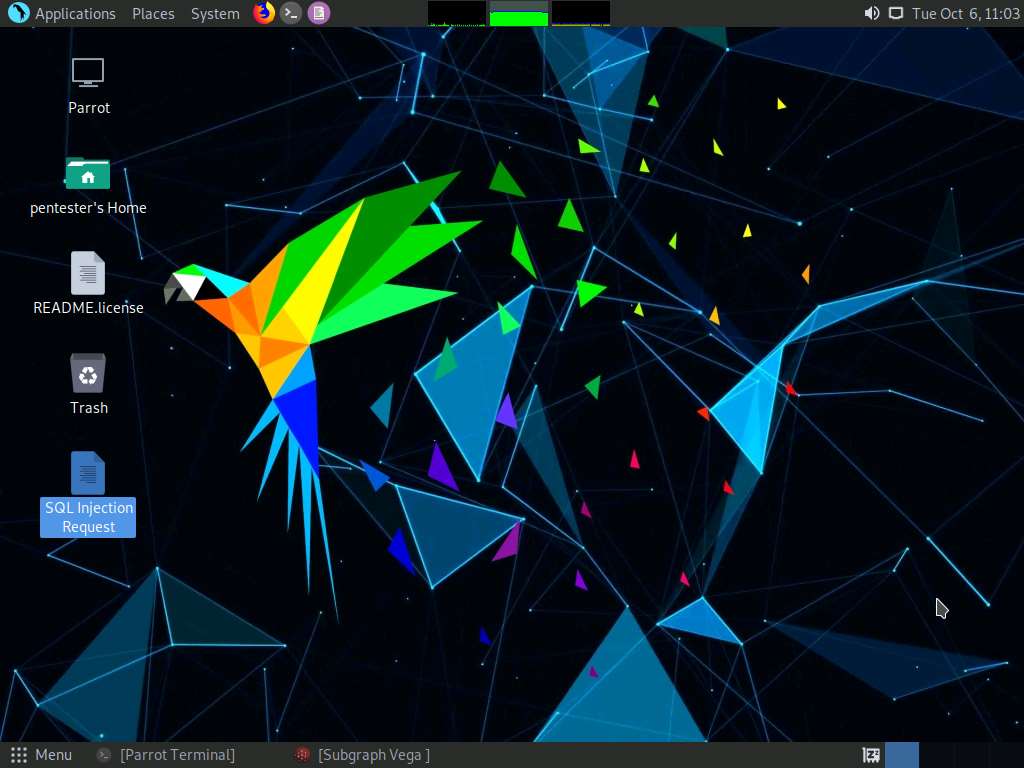


1. Minimize the **Vega** application. Open a new text file and paste the copied **POST request** on **Desktop**.
2. Ensure that all the unwanted spaces and new line entries are removed i.e., the complete request content should be continuous. Close the Text document.

You can maximize Vega application and compare the content with the vega request and remove the new line entries from the request content.



1. Now, rename the file as **SQL Injection Request**.



In this lab, you have learned how to:

* Use and perform Web Application Vulnerability Assessment through Vega
* Generate reports and examine them