1.	A	Imagine you are working as a cybersecurity **nessus** **Nessus tool for vulnerability scanner** https://www.tenable.com/products/nessus/nessus-essentials 1. Download the Nessus package for Debian on the Nessus website and make sure you set the Platform to Linux-Debian-amd64. 3. Install Nessus using this command: sudo dpkg -i Nessus-10.4.1-debian9_amd64.deb 4. Start the Nessus service with this command: sudo systemctl start nessusd.service 5. On your browser, go to https://kali:8834/. 7. Choose the Nessus Product you prefer. If you want the free version of Nessus, click on Nessus Essentials. 8. Enter your name and email address to receive an activation code by email. Paste the activation code into the space provided and choose a username and password. 9. Allow Nessus to download the necessary plugins. 10. Once the plugin downloads have completed, you can start using the Nessus service. **Passwd Change** /opt/nessus/sbin/nessuscli chpasswd shubha After installing the required plugins, navigate to the 'newscan' module. Enter the IP address **Systemctl start nessusd.service** **https://kali:8834 in the browser.**
	B	Imagine you're a cybersecurity analyst tasked with assessing the security of a newly developed e-commerce website. You would utilize Burp suite and perform following activities to identify and mitigate security flaws in the web application. Start by describing the setup process for Burp Suite, including configuring proxy settings and initiating automated scans to detect common vulnerabilities like SQL. i. Manual Testing of SQL Injection Go to the target machine(Metaspoiltable 2)—in the terminal type below commands cd /var/www/mutillidae sudo nano config.inc Ensure dbname=owasp10 instead of metasploit Then save(ctrl+X, Y and enter) and exit. In the kali linux browser 192.168.62.129 Go to mutillidae and enter the username as ‘ and password field is empty , click on enter It displays errors, which indicates web application is vulnerable It displays the query in the Diagnotic information. • Now again click login/Register enter username as **admin** Password as **blahblah ‘ OR 6=6#** Then you can observe it is logged in as admin. • In mutillidae page, click on OwaspTOP10->A1 injection -> SQLi Extract Data -> User Info and Enter username=**admin** and password =**adminpass** , click on view account details Then Results for admin. 1 records found would be displayed **Username=admin** **Password=adminpass** **Signature= Monkey** **• Now for SQLi** Enter username=**admin** and password= ‘ **OR 1=’1—**

		ii. Proxy Attack with Burp Suite. ii) Proxy Attack with Burp suite. launch the Burp Suite application. • After Burp Suite has launched, set up the proxy configuration. • Open the Mutillidae application and log in using the credentials: username - "john" and password - "passwd." Before clicking on the login button, activate the intercept feature in Burp Suite. Proceed to click on the login button in Mutillidae. • Check the Burp Suite application to verify that it captured the login request, including the username and password information. • Modify the username and password to "admin" and "adminpass" respectively within Burp Suite. Then, click "Forward" to send the modified request. • Once the modified request is forwarded, observe in the Mutillidae application that the login is successful, indicating that the credentials have been changed to admin/adminpass. • Within the Burp Suite application, navigate to the "Target" tab to review the intercepted information from the target machine.