11.	A	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 Injection. i. Manual Testing of SQL Injection ii. Proxy Attack with Burp Suite. i) Manual testing for SQL injection: - Setting mutillidae app correctly for SQL injection Vulnerability Testing 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. • Now trying with username as admin ‘ # and password field must be empty, still you can observe it is logging 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—** Click on view account details. Then you would observe **Results for admin. 16 records found details…** ii) Proxy Attack with Burp suite. • Start both the Kali Linux virtual machine and the Metasploitable 2 virtual machine to ensure they are up and running. • Navigate to the "Applications" menu in Kali Linux and launch the Burp Suite application. • After Burp Suite has launched, set up the proxy configuration. • Download the Burp Suite certificate and import it into the relevant certificate store. • Access the proxy settings within Burp Suite and configure a manual proxy setup with the HTTP proxy set to 127.0.0.1 and port number 8080. Confirm the settings by clicking "OK." • 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.

	B	As part of a penetration testing engagement for a client, you're tasked with evaluating the security of their internal network. You suspect that sensitive data might be leaking from one of their development servers due to a potential misconfiguration or a compromised machine within their network. To investigate further, you plan to intercept network traffic using Wireshark to identify any unauthorized data transfers. Wireshark is a widely used, open source network analyzer that can capture and display real-time details of network traffic. It is particularly useful for troubleshooting network issues, analyzing network protocols and ensuring network security. Networks must be monitored to ensure smooth operations and security. Popular with academic institutions, government agencies, corporations and nonprofits, Wireshark is one such tool that can offer an in-depth view into network activities, diagnose network performance issues or identify potential security threats. Wireshark -Snipping Intercept target machine traffic(Metaspoiltable2 VM) with Wireshark • Ensure both the Kali Linux and Metasploitable2 virtual machines are up and running. • Open Kali Linux and navigate to Applications -> Snipping & Spoofing -> Wireshark. • Select the interface (eth0) to capture network traffic. • Access the browser on Kali Linux and enter the IP address of the Metasploitable2 VM (e.g., 192.168.62.129) to open the Mutillidae website. • Navigate to Mutillidae page and proceed to the login page. • Enter random credentials (e.g., username: admin, password: 12345) and attempt to log in, resulting in a login failure message. • Switch to Wireshark, where traffic interception has begun. • In the filter bar, type "http" and select the http with post stream contains login.php page. • Right-click on HTTP traffic, choose "Follow," then "HTTP stream" to open a new window. • The new window displays intercepted traffic containing the username and password entered on the DVWA login page, showcasing successful traffic interception using Wireshark.