1. Develop an E-Commerce web page that uses GET and POST methods. And identify and exploit vulnerabilities.
2. Implement a stack buffer overflow attack using a procedural language on the "Legacy Banking System". Explain the concept of stack buffer overflow and discuss techniques to prevent such attacks.
3. Create Social media Web Page and Perform a reflected cross-site scripting (XSS) attack on it .
4. Create Social media Web Page and Perform a Stored cross-site scripting (XSS) attack on it .
5. Create Net Banking Web Page and Perform a reflected cross-site scripting (XSS) attack on it .
6. Create Net Banking Web Page and Perform a Stored cross-site scripting (XSS) attack on it.
7. Use NMAP to perform port scanning on the network of Tech Startup Inc. to locate malware and vulnerabilities.
8. Implement a stack buffer overflow attack using a procedural language on the "Internal Inventory Management System".
9. Conduct a brute force password cracking attack on the login system of BWAPP. Username - User1234 and password will be a combination of letters a,b,c of length 5.
10. Perform penetration testing on the "HR Management Software" to identify and exploit application vulnerabilities.
11. Develop a "Blogging Platform" that uses GET and POST methods. And identify and exploit vulnerabilities.
12. Implement a stack buffer overflow attack on the "Food Delivery” application using a procedural language.
13. Implement a stack buffer overflow attack “Financial Analysis Software" in a simulated environment using a procedural language, documenting each step of the process.
14. Utilize NMAP to perform a port scan on the network of "Telecommunications Company".
15. Conduct a dictionary attack password cracking attack on the BWAPP. Username - vuStudent.
16. Perform penetration testing on the network infrastructure of "Healthcare Provider", identifying and exploiting vulnerabilities.
17. Investigate vulnerabilities in "Online Learning Management System", focusing on input validation and output encoding.
18. Implement a stack buffer overflow attack.
19. Utilize NMAP to perform a port scan on the network of "Retail Chain".
20. Perform penetration testing on "E-Commerce Platform" to identify vulnerabilities.
21. Utilize NMAP to perform an port scan on the network of Altoro Mutual - <http://altoro.testfire.net/> , identifying potential security risks.
22. Utilize NMAP to perform a detailed port scan on the network of testphp.vulnweb.com
23. Perform penetration testing on "Customer Support Ticketing System" to identify vulnerabilities, such as XSS and CSRF vulnerabilities.
24. Find a way to log in as an admin without using the correct password on the "User Login Page" of Altoro Mutual - <http://altoro.testfire.net/> . Explain how you did it and how this could be prevented.
25. Retrieve all user data from the "Customer Database" of Acuart website - <http://testphp.vulnweb.com/index.php> ; Explain how you accomplished this and suggest a method to stop this unauthorized access.