Assignment 3

For assignment 3 you will be exploiting DVWA in several ways. You are free to use existing code or create your own code where applicable. If you create your own code, please supply it in an appendix at the end of your report. If you use existing code, please tell me where you have found the code and include screenshots of any changes you make to the existing code.

For each part, include screenshots of your exploitation including any requests made to DVWA and the results of your exploitation, as if you were walking me through your exploitation of DVWA. For each part, also include one or two sentences explaining the vulnerability and what an attacker can do with it. For example, for the brute-force vulnerability, you can say something like:
“The web application is not configured with brute-force protection like a lockout policy. An attacker can continuously guess a user's credentials until they authenticate into the application”
You must also provide the applicable OWASP number using the 2021 OWASP Top 10 list. This must be done in the format like, for example if the vulnerability is applicable to OWASP Top 10 A01:
“OWASP A01:2021”

Each section will be scored out of 10 marks for completing the objective and providing all appropriate evidence (5 marks), describing the vulnerability (2 marks) , referencing the appropriate OWASP number (1 mark) and overall quality of writing (2 marks).

Part 1 - Command Injection
You will exploit the Command Injection part of the web application to run a netcat reverse shell or bash reverse shell to your Kali machine. Once you have the reverse shell, you will run the “whoami” and “ip a” commands.

You may need to install ncat on your Ubuntu machine first with “sudo apt install ncat”

Part 2 - File upload
You will upload a PHP **webshell** and use it to run the “whoami” and “ip a” commands. You will then upload a PHP **reverse shell** that connects to your Kali machine and run the same commands.

Part 3 - Reflected XSS
Use the <img onerror> method shown in class to craft a URL that will redirect the user to a web server running on your Kali machine. You can use the following command to set up a quick web server running on port 8080 of your Kali machine as a proof of concept for this part:
`python3 -m http.server 8080`

Part 4 - Stored XSS

Use the <script></script> method shown in class to create a message in the Stored XSS section of DVWA. This message should send the cookies of whoever visits the page to your Kali machine. You can use the same python command in Part 3 to accept cookies. You will need to show the contents of your comment, and you receiving the cookies on your Kali machine.

Part 5 - SQL injection

Use either the Burpsuite Repeater or DVWA's User ID field in the SQL Injection category to display all usernames and passwords in the users table.The passwords will be encrypted, so use hashcat and the password list provided to crack admin's password.