* **PROBLEM STATEMENT:**

Web vulnerability assessment is an important aspect in cyber security. You will be getting a vulnerable web server (DVWA). Perform a complete vulnerability assessment on this site and categorize the vulnerabilities found. Manually perform the penetration testing on the vulnerabilities found and create a report on how you performed it. Finally provide a solution to close the vulnerability. Prepare a detailed report including all the steps starting from vulnerability assessment to solutions provided.

* **TITLE OF PROJECT:**

VAPT ON DVWA

* **OBJECTIVE AND KEY LEARNING:**

The aim of DVWA is to practice some of the most common web vulnerability, with various difficulties levels.

The primary objective behind a Web Application Penetration Testing (WAPT) is to identify exploitable web application vulnerabilities, weaknesses, and technical flaws in applications before attackers can discover and exploit them.

* **INTRODUCTION:**

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn defenceless. Its primary objective is to be a guide for Web Security experts to test their abilities and instruments in a lawful domain, help web designers better comprehend the procedures of securing web applications and help instructors/understudies to educate/learn web application security in a classroom situation. Seriously it is too vulnerable. In this app security professional, ethical hackers test their skills and run this tool in a legal environment. It also helps web developer better understand the processes of securing web applications and teacher/students to teach/learn web application security in a safe environment.  
The aims of DVWA are to practice some of the most common web vulnerability, with various difficulties levels.

* **Vulnerability**

1. Brute force
2. Command Injection
3. CSRF
4. File Inclusion
5. File Upload
6. SQL Injection
7. SQL Injection (Blind)
8. Weak Session Ids
9. XSS (DOM)
10. XSS (Reflected)
11. XSS (Stored)
12. CSP Bypass
13. JavaScript

* **What are the Benefits of DVWA?**

1. In DVWA we do not have to take permission from other. We can simply install this in a virtual environment and start using it.
2. It is very simple to install.
3. This is the best place to do **hacking**.
4. In fact, this is running in our local environment and it is **totally legal**

* **There are four levels in each vulnerability:**

1. Low
2. Medium
3. High
4. Impossible

* **Tools used in the project:**

1. KALI LINUX
2. DVWA
3. BURPSUITE
4. VIRTUAL BOX/VMWARE
5. APACHE2
6. MYSQL
7. NESSUS
8. NIKTO
9. NMAP