**Question 1:**

a) **The environment setting:**

DVWA (Damn Vulnerable Web App), which is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications.

b) **Tools were used:** Weevely and Burp Suite

c) **Vulnerabilities of the file upload process:**

The attacker can use tool to upload a file with malicious code (eg: PHP file) that can be executed on the web server.

d) **How to find out webserver has file upload vulnerabilities:**

We can try to upload a file with malicious code and check the webserver accept it or not.

**Question 2:**

GET method is used to request data from a specified resource. With GET request, we can see the value of page in the URL, a page will request another page to include another page.

POST method is used to send data to a server to create/update a resource. With POST request, we cannot see anything change in the URL.

**Question 3:**

We first need to create a file with malicious code (eg: PHP file) then upload it to webserver. In some case, depend on the level of security of the webserver, we may need to rename the extension of malicious file. After upload it successfully, use Weevely to exploit.

**Question 4:**

* Check the file type and the file extension.
* Analyse the upload file itself, recreate it and rename it.
* Never allow users to upload executables (eg: php,exe….)