ETHICAL HACKING TRAINING

PROBLEM STATEMENT

We are glad that you have completed the training and cleared the final test. Now, it's time to test your skills in a practical manner and for that, we have setup a real life-like web application in the form of an online e-commerce portal.

Your task is to test this e-commerce platform and find all possible vulnerabilities and loopholes in it, collect relevant PoCs and then prepare a Detailed Developer Level Report.

For reporting each vulnerability, you must make sure the following things are mentioned:

- Title of Vulnerability.
- A Short Description.
- Exact URL which has the vulnerability.
- The parameters which are vulnerable (with parameter type like GET, POST, Cookie, Header, etc.).
- Payload that you used to trigger the vulnerability.
- Observation slides containing step by step information to replicate the exploit with PoCs.
- Business Impact of the vulnerability, explaining in detail what can be done by a hacker.
- Recommendations on how to fix the vulnerability.
- Reputed References for the vulnerabilities.

Remember, each and every kind of vulnerability you learnt about, might be somewhere in this application. All you have to do is open the application and start exploring its features. Once you have understood each feature the website has, you can start playing around with it and fuzzing into various places.

A big part of the VA has been already done for you as you have the exact IP and the application which you have to test, but there could be hidden pages and components too, so keep that in mind.

Happy bug hunting!