Week_3_wa
In **two to three** pages, describe the following:

- How would you ensure security for both the store and the customer's data?

According to the US National CyberSecurity Alliance nearly 62% of all cyber attacks are done against small to medium ecommerce businesses. In recent years this number has increased. In addition, hackers can steal the customer's identity, credit card or other sensitive data.

If we look at a high level, we have layers of data which passes from/to the web-site. One of the data passes via http protocol. If this data is not encrypted, then it can be seen and stolen very easily. The first step in our hardening would be the use of https. Next layer of data is this data that is stored in the family system, like the user's details, credit history, prices of the products and what not. If a hacker gains access to our server, it can see all files that are on the file system. Obvious step is to use permissions. However, a better choice is to use a cloud store system with replication, permissions and a lot of other features. AWS S3 is a good choice.

In addition, we need to log any transaction from the beginning to the end. Such a thing is called traceability. If something suspicious is going on we should send an alert/notification to the appropriate personnel.

Another important aspect of security is the ability to survive against DDoS attacks.

Let's say our customer should use long passwords that are not easy to guess. Site itself should use ssl certificates which are authorized by known organizations.

Every library that our site is using, should be recently upgraded. We remember the log4j accident which made it possible to run procedures remotely.

Next, any web application uses cookies which hold some private data related to the user's session, it can be a token or password of a credit card number. By doing simple tricks, hacks can steal a user's session.

It is also quite important to make backups of data. It can be a database, simple files of some sensitive data related to our customers. Also every single file like css also should be backed up. Our server can go down, hardware be blown or broken and it is our responsibility to manage the website up and running without compromises.

- How will the security features work with the rest of the website?
    - What components will be working to ensure security?

Cyber attacks can degrade performance of our web application, make our customers unhappy and destroy our reputation.

Our site should be monitored 27/7. We start with authentication and authorisation, one is telling if we know this user, and the second says what this user is allowed to do. Next, session fixation, XSS, sql injection protection should be taken into account.

If we use a well trusted hosting provider we can ask for on-demand IP blocking and Geo-Location blocking.

- Provide a rationale for your decisions based on sound research of website security practices.

As I mentioned earlier, use of HTTPS prevents hackers from changing the context of the website. If I remember correctly, nowadays even browsers add some kind of https support. Google has a program in which web-site owners can get some awards by using https. Next recommendation is changing passwords frequently. Others suggest crypto tokens. At my work we use a mechanism called passwordless. Our smart phone is recognized by our systems, and a program called PingID generates a password for each login.
Another practice is to give the user as few permissions as possible. For example, AWS Lambda has a read-only file system.
To prevent for example sql injection, any user's input should be validated.
In addition to cyber attacks, disasters can happen. A hard drive/ssd is broken, some files corrupted. In such cases the recommendation is to back up everything. Say, once a week full backup plus each hour delta backups.
Forthemore, if an accident happens or happens it is a good idea to monitor the system, trace a system and some suspicious behavior, send alerts to relevant people and limit the access to the site itself.
Adding third party security scanning as part of the CI/CD. Such scanning will scan libraries that web-site code uses, compares with known vulnerabilities databases and shows a report of scanning.

References:

1. https://www.hostinger.com/tutorials/ecommerce-security
2. https://www.siteground.com/blog/essential-website-security-features-you-need-are-they-on/
3. Lars Lofgren (June, 2021) Website Security Guide - https://www.quicksprout.com/website-security/
4. George Mutune. Top 12 website security practices. https://cyberexperts.com/website-security-practices/
5.