Part 1: describing BattleOff

This study describes the imaginary company BattleOff, which is loosely based on the real world company Artix Entertainment, which hosts the website Battleon and features multiple (mmo)rpg flash games. A couple of years ago, the company would actually mail your exact password when you chose to do password recovery, from which we can conclude that the passwords were not stored as hashes in their database. This interesting security flaw inspired us to choose this company.

BattleOff is a relatively successful game studio that has published a handful of popular flash games targeted at a young audience. The studio employs around 30 people to maintain and develop their games, provide customer service and occasionally release merchandise based on the games. After being founded in 2002 by CEO John Smith the company produced its first successful title, a flash game called Adventure RPG. In the years that followed five more games were released, with the last and most popular game being Adventure RPG Online. This mmorpg made for Adobe flash player is still running to this day, with regular updates keeping the community interested.

Over the years, BattleOff hired more employees to help with maintaining the software. At the top of the company is John Smith, who used to help out with the programming but has shifted more to managing the development of his games. About 10 out of the 30 employees work as artists, performing various tasks such as creating art or making animations. Every game has a handful of developers/programmers assigned to it, to fix bugs or work on developing the game. BattleOff employs 16 developers total. They are divided in two DevOps teams. Both are responsible for new features and for providing technical support when needed. Because BattleOff is a relatively small company, most employees perform multiple roles. The DevOps teams are also in charge of managing the website and managing the database. The last few employees perform miscellaneous roles across the company.

BattleOff has multiple games, each with its own user base. A user can create an account on BattleOff's website which allows access to all of their games. In each game, the user will have a different character to play with each time, nothing is connected. In practice, a user will login on the BattleOff website with their chosen username and password. After that, they can navigate to the game they want to play. If the game is not down for maintenance or because of technical issues, the system will automatically login in the specific game. What actually happens is that each game maintains its own database of characters, linked to an account by the users BattleOff username, and data is retrieved whenever the player launches the game in their browser.

One of the key focus points of BattleOff is to ensure that all their users are able to register and maintain their account on the BattleOff website as described above. BattleOff has to make sure that an user can trust them to keep their account information private as well as their payment

information when the user pays for extras or for a premium account.. Another issue of great importance is to make sure that all the in-game items get to the right account and that nobody else can access them. BattleOff does not want to lose players because of people losing their items.

To ensure that users can register their account safely BattleOff provided their website with a secure socket layer (SSL). This way they provide a safe channel to send a player his account information. BattleOff their games are protected against brute force attacks by the google reCaptcha. The database is stored at the Microsoft Azure platform. They provide the database with a firewall and other protection measures.

The games themselves feature some level of protection against players that attempt to hack or bot their way to higher power levels. This is mostly custom made by BattleOff's developers. As the game has only a small amount of people that succeed in performing illegal services so it can be considered to be quite successful.

Part 2: security analysis

A. Summarize the organizational context

This analysis will focus on BattleOff's handling of user data, as this is where the most obvious security issues are. More specifically, proper handling of both user credentials and in-game purchases are vital to the success of the company.

Improper handling of user credentials can cause users to lose access to their accounts, which would likely discourage them from purchasing in-game items in the future.

We won't look at fake merchandise because it is not as related to software as other security issues.

B. Study the assets

The most significant assets of the company are the appealing games. It is the main and only way BattleOff attracts an audience. Secondary, users are important. Especially a massive multiplayer online game is very reliant on a large active player base to stay alive. Having a healthy player base and community makes the game more interesting and fun for players, as they have fellow users to interact and discuss the game with.

An important part of the games and user accounts are the premium account service and the cash shop in each game. Money comes from people paying for the premium accounts and the cash shop items and services. The assets of the cash shop are account services like name and gender change for characters and cosmetic items. The cosmetic items vary from weapons to

armor to pets that follow the player around. The income comes mainly from the cosmetic items, by a large margin.

Lastly, some revenue comes from the vendoring of merchandise related to the BattleOff games. This is not of interest to us and only mentioned here for completeness. What can be observed, is that the games' worlds and atmosphere are assets in a way. Players are reminded of their good times in the game and their involvement with the story when seeing popular characters from the game.

C. Identify security issues:

As described in the first paragraph of this document BattleOff did not hash the passwords in their database. This provides a huge security leak for their users. If someone has access to a player's email that person can retrieve their password by clicking on the password forgotten link. Every user of every website/platform on the world should be able to trust them to store their password hashed or encrypted in some form.

A huge problem would be if player A pays for an item and player B receives the item. Especially if the item wasn't bought with in-game currency, but with real life money. If this happens and support would not be able to restore the bought items to the legitimate owner. This player would be likely to turn his back to the game and BattleOff will lose a paying player. This could have been caused due to a bug, but it could also have been caused by someone with malicious intent.

Lastly, malignant players always try to find ways to get an advantage over other players in unintended or illegal ways. This can include writing scripts that play the game for them, or carefully searching for vulnerabilities that give advantages when exploited.

D. Prevention and mitigation of security issues

A solution to the password not being encrypted is to simply encrypt it. If an user does want to reset his password BattleOff can send a link to the website where they can change the password. Another solution is to send a randomly generated password to the user and to let them change the password after they logged on the site.

Mistakes are bound to happen when a player base grows, but the way BattleOff handles them is important . A great tool to track which player bought something and which did receive them is by logging every business process and their steps. By correlating the steps of logging the developers in the DevOps teams can see where the fault was and correct it for the particular users affected as well as find a solution that it will not happen again.
Define possible treatments for the security issues identified in the previous paragraphs. Explain how they prevent or mitigate security risks described above.

Every Time a malicious player is reported BattleOff will inspect the case and look into ways to prevent this from happening again by installing or developing anti-cheating scripts. If it is not possible to do this they will actively monitor the game if it happens more often. They will manually ban all players that use this cheat or hack. If a lot of players use this cheat or hack they will hire an external party to help them with the issues.