# Assignment 1

## Question 1

DoorDash Hack: A hack on food-delivery service DoorDash leaked the personal data of 4.9 million customers, delivery workers, and merchants. The breach took place on May 4, 2019, but DoorDash officials didn’t learn of it until earlier September when they noticed unusual activity involving an unnamed third-party service provider.

Data obtained by the attacker could include names, email addresses, delivery addresses, order histories, phone numbers, and cryptographically hashed and salted passwords.

Also exposed were the last four digits of customers' payment cards and the last four digits of delivery workers' and merchants' bank accounts. Driver license numbers for about 100,000 delivery workers were also accessed.

DoorDash has no evidence to indicate people who joined the service after April 5, 2018, had their data taken. The 4.9 million figure includes only a portion of users who joined on or before that date. The company said it's in the process of directly notifying those affected (Dan Goodin).

**Attacker**: unnamed third-party service provider

**Target**: DoorDash customers, delivery workers and merchants

**When**: start from May 4, 2019 found by Sep 2019

**How and underlying vulnerabilities**: somebody guess may cause by the type of hashing DoorDash used. Hashes are one-way, meaning there's no mathematical way to convert hashes into the plaintext they were derived from. Hackers can sometimes work around this protection by running large lists of password guesses through hash generators and looking for results that match the hashes found in a breach. Many services in the past have used weak algorithms such as MD5 and SHA1, which were never intended to be used to protect stored passwords. The result: it's trivial for the intruders to crack the hashes generated with these algorithms (Dan Goodin).

**Damage**: 4.9 million consumers, Dashers and merchants who joined DoorDash on or before April 5, 2018 are affected. The type of user data accessed could include (DoorDash):

* Profile information including names, email addresses, delivery addresses, order history, phone numbers, as well as hashed, salted passwords — a form of rendering the actual password indecipherable to third parties.
* For some consumers, the last four digits of consumer payment cards. However, full credit card information such as full payment card numbers or a CVV was not accessed. The information accessed is not sufficient to make fraudulent charges on your payment card.
* For some Dashers and merchants, the last four digits of their bank account number. However, full bank account information was not accessed. The information accessed is not sufficient to make fraudulent withdrawals from your bank account.
* For approximately 100,000 Dashers, their driver’s license numbers were also accessed.

**Mitigation**:

1. DoorDash:

DoorDash have taken a number of additional steps to further secure user’s data, which include adding additional protective security layers around the data, improving security protocols that govern access to our system, and bringing in outside expertise to increase our ability to identify and repel threats.

1. Consumers: change DoorDash password, check whether their credit card has some unknown billings
2. Dasher and merchant: also need to check their bank account for safty.

## Question 2

Seven Touchpoints used as a software development artifacts, while SDL and OWASP works on software life cycle phases. All three can be used standalone.

Training: at the beginning of software development, SDL and OWASP provide an education part. In Microsoft SDL it calls Provide Training (ensure everyone understand security best), in OWASP it calls Education & Guidance (focus on increasing the knowledge in the organization regarding secure software). But the 7 Touchpoints doesn’t have this part.

Project Inception: 7 Touchpoints collect and evaluate metrics, SDL define metrics and compliance reporting, OWASP strategy & metrics/policy & compliance. In this part 3 secure model doesn’t have big difference. All will set some metrics and define some basic points. One difference is touchpoint may not have compliance management.

Analysis and Requirement: Touchpoint abuse cases/security requirements/ risk analysis, SDL establish security requirements/create quality gate/bug bars/security & privacy risk assessment, in OWASP it moves analysis and requirement part to design part. So, it will not only set the basic security requirements as other two, but also design a secure architecture to make the software safer.

Design: Touchpoint risk analysis, SDL establish design requirement/analyze attack surface/perform threat modeling, OWASP threat assessment/security requirement/secure architecture. In this part 7 Touchpoint looks very weak which didn’t have any practice related to design.

Implement: Touchpoint code review, SDL use approved tools/deprecate unsafe functions/static analysis, OWASP secure build/secure deployment/defect management. Also, in this part 7 Touchpoint rely more on programmers to write safe code without any tools as SDL or any management as OWASP. Only code review to make safe is not enough. But the OWASP is the best one from the build to deployment then manage the defect. This process will help the team make a secure software from the beginning part.

Testing: Touchpoint risk-based security test/risk analysis/penetration testing, SDL dynamic analysis/fuzz testing/attack surface review, OWASP architecture analysis/requirements-driven testing/security testing. In this part, all three model use their own way to test the software. 7 Touch and SDL do the testing more based on risk, OWASP test more on architecture and system requirement.

Release and Other: Touchpoint security operations, SDL incident response plan/final security/release archive, OWASP incident management/environment management/operational management. 7 touch didn’t make a practice as release part, only some feedback. SDL and OWASP both care about the incident, but OWASP also focus on the data protect software environment and some other part like legacy management.

I’d like to use the OWASP SAMM model for my own software. Just use my project of CS673 for example. It’s a plan management software with some simple functions. We have three people in our develop team. One focus on the architecture design, one focus on the front-end design and implement and last one focus on the server-side implement.

The reason I choose the OWASP is because if we want to make the software safer. We need to know more about the secure software more, so we need to learn which part should be focus on. Also, OWASP more care about the software architecture, it’s the beginning of a software. As the testing part OWASP test the software use the requirement-driven test case also more fit our project. Can better test according to customer needs, easier to reach customers' goals

## References

Dan Goodin. (2019) DoorDash hack spills loads of data for 4.9 million people. Retrieved from: https://arstechnica.com/information-technology/2019/09/doordash-hack-spills-loads-of-data-for-4-9-million-people/

DoorDash (2019) Important security notice about your DoorDash account. Retrieved from: <https://blog.doordash.com/important-security-notice-about-your-doordash-account-ddd90ddf5996>

SAMM model overview Retrieved from: <https://owaspsamm.org/model/>

What are the Microsoft SDL practices? Retrieved from: https://www.microsoft.com/en-us/securityengineering/sdl/practices#practice1