University of Oslo
IN2120 Information Security
Autumn 2018
Workshop Questions

Lecture 12: Application Security and GDPR

Question 1: Cyber Kill Chain

a. What is the Cyber Kill Chain?
b. What are the steps of the Cyber Kill Chain?

Question 2: Worm Propagation

In general terms, how does a computer worm propagate?

Question 3: Botnet Attacks

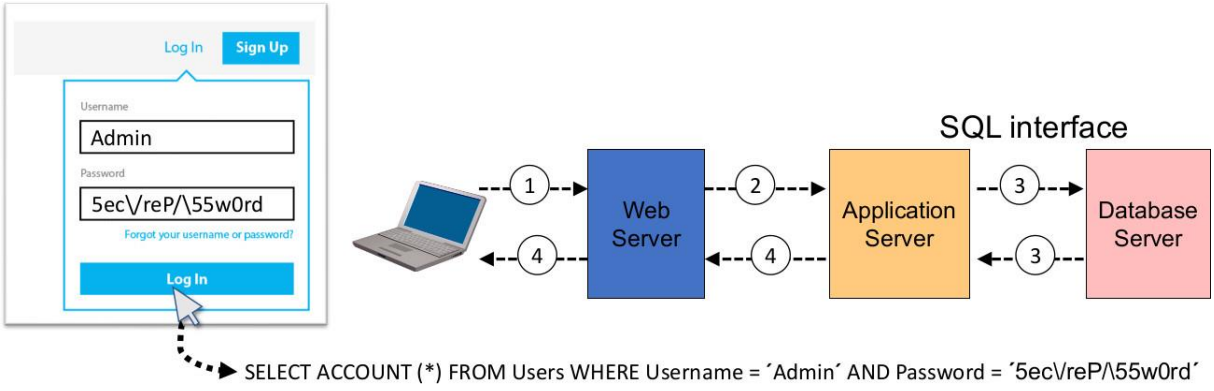
a. What is a botnet?
b. What is a DDoS, and how can a botnet be used to mount a DDoS attack?
c. Describer two other attacks that can be executed with botnet.

Question 4: SQL Injection

a. What is an SQL injection attack and how can it be prevented?
b. What is a Cross-Site Scripting attack, and how can it be prevented?

Question 5: SQL Injection Example

A Web application has a system for user authentication where the input from the login screen is used directly without filtering to form SQL commands sent to the back-end SQL database as illustrated in the diagram below. The logic is that the user authentication is successful if the typed password matches the stored password for the selected user.



An attacker wants to log in as Admin and types the password: A´ OR ´X´ = ´X
a. What is the resulting SQL command sent to the SQL Database Server?
b. What is the effect of doing this?

Question 6: OWASP

a. What is the meaning of the abbreviation OWASP ?
b. What is the main goal of OWASP ?
c. What is the OWASP Top 10 ?
d. What is nr.1 in the OWASP Top 10 ?
e. What is the reason why nr.1 has been at the top for many years ?
f. What is the meaning and purpose of OWASP ASVS ?

Question 7: Secure Agile

a. In which way is agile different from waterfall in system development?
b. How can security be integrated in agile system development?

Question 8: Privacy and Security by Design

GDPR (General Data Protection Regulation) became EU law on 25 May 2018. GDPR translated into Norwegian is called PVF (Personvernforodningen). The text from GDPR translated into Norwegian became the new Personopplysningsloven on 20 July 2018.

a. Which are the core elements of privacy by design according to GDPR Article 5?
b. Which are the core elements of privacy and security by design in system development and operation according to Datatilsynet?

https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/programvareutvikling-med-innebygd-personvern/

Question 9: Data Protection in the Cloud

An IT company which processes personal information decides to transfer storage and processing of personal data to a cloud service located abroad.

a. Is this allowed according to GDPR (Personopplysningsloven in Norway)?
b. What must the company do in order to make the outsourcing lawful according to GDPR?

Question 10: Sanctions for violations of GDPR

Two IT companies, let's call them Alpha and Omega, develop two separate systems that will process personal data. They both follow principles (a)-(e) of Article 5 in GDPR. Alpha does not carry out any threat and risk assessment for security during system development, but the system is tested for known security vulnerabilities during operations. Omega, on the other hand, performs threat and risk assessment for security, and eliminates vulnerabilities found during development. Assume that both the systems of Alpha and Omega get hacked, resulting in security incidents with severe privacy impact and leakage of sensitive personal information.

a. According to GDPR, were Alpha and/or Omega allowed to put their systems in operation?
b. Could Alpha and/or Omega be fined according to GDPR as a result of the security incidents, and/or as a result of the way in which the systems were developed/operated?
c. What is the maximum fine for violating GDPR (Personopplysningsloven in Norway)?