BACHELOR OF COMPUTER

SCHOOL OF COMPUTER SCIENCE

BINA NUSANTARA UNIVERSITY

JAKARTA

ASSESSMENT FORM

Course: COMP6549 – Software Security

Method of Assessment: Case Study

Semester/Academic Year : 1/2021 - 2022

Name of Lecturer : **NADIA, S.Kom., M.TI**

Date : **08 Mar 2022**

Class : **LC07**

Topic : **Tech Startup/Company Threat Modelling**

Group Members :	1. 2440008941 - Vincent 2. 2440040904 - Maximilianus Raymond 3. 2440053245 - Fathan Ashthofani Abdillah Zakaria 4. 2440046233 - Muhammad Raifani Ath-Thaariq Rahman Dilaga 5. 2440009244 - Hosea Glen Effendi

ASSESSMENT METHOD

Instructions

1. Student are divided into groups of 4-5 people

2. In this project, students are expected to

a. Pick one (or more) technology startup/companies in Indonesia and gather data (interview, etc.) regarding their business flow and the threats they might face as a company

Shopee merupakan sebuah platform belanja online ternama yang menyediakan pengalaman berbelanja online yang mudah, aman dan cepat bagi pelangannya.Shopee memiliki peran sebagai penengah antara pembeli dan penjual.

b. Study the gathered information and apply STRIDE modelling correctly

1. Spoofing

Spoofing adalah jenis penipuan di mana penjahat menyamarkan alamat email, nama tampilan, nomor telepon, pesan teks, atau URL situs web untuk meyakinkan target bahwa mereka berinteraksi dengan sumber yang dikenal dan terpercaya.

Contoh kemungkinan penerapan *spoofing* di aplikasi shopee:

1. Meminta kode OTP seolah-olah menjadi admin di shopee
2. Terkena *Phising* dan *scamming* di website shopee

2. Tampering

Tindakan menyentuh atau membuat perubahan pada sesuatu yang tidak seharusnya Anda lakukan, biasanya saat Anda mencoba merusaknya atau melakukan sesuatu yang ilegal

Contoh kemungkinan penerapan *Tampering* di aplikasi shopee:

1. Merubah harga asli dari harga penjual sehingga si penyerang mendapatkan harga murah
2. Memodifikasi isi pesan user dengan penjual.

3. **Repudiation**

Repudiation adalah tindakan seorang yang tidak dapat membuktikan bahwa transmisi data telah dilakukan antara dia dengan pengguna yang lainnya, sehingga pengguna lain dapat menyangkal bahwa dia telah mengirim atau menerima data.

Contoh kemungkinan penerapan Repudiation di aplikasi shopee :

1. Disaat pengguna memesan suatu barang tetapi ke alamat yang salah, atau kasus yang serupa yaitu pengguna hanya iseng memesan barang dengan transaksi COD (Cash On Delivery) dan tidak bayar atau menunjukan alamat palsu atau dengan kata lain ‘Paket tidak bertuan’ . Tetapi seharusnya hal ini sudah diantisipasi oleh pihak shopee dengan sistem keamaanan non-Repudiation dengan pengguna tidak dapat menghapus pesanan yang telah dilakukan dan juga memberi Syarat dan ketentuan dalam melakukan transaksi COD ini dan memberikan fasilitas Help Center yang dapat dihubungi jika hal tersebut terjadi.

4. **Information Disclosure**

Information Disclosure adalah tindakan seseorang yang dapat mengakses sebuah data atau informasi yang tidak seharusnya dapat ia akses dan tidak memiliki hak untuk dapat mengakses informasi tersebut dengan kata lain kebocoran data.

Contoh kemungkinan penerapan Information Disclosure di aplikasi shopee :

1. Disaat orang yang dapat meretas Shopee atau orang yang dapat mengakses data-data di Shopee tidak bertanggung jawab atas hak nya tersebut dan memperjual belikan data-data pribadi milik seorang pengguna didalam situs lain.

5. **Denial of Service**

Denial of Service adalah salah satu serangan pada sistem keamanan web yang dapat menghambat aktivitas kerja sebuah layanan sehingga user tidak bisa menggunakan layanan tersebut.

Contoh kemungkinan penerapan Denial of Service di aplikasi shopee :

1. Saat DoS telah menyerang sistem layanan service shoppe maka para user tidak akan bisa mengakses shoppe karena layanan shoppe telah dihambat

6. **Elevation of Privilege**

Elevation of Privilege adalah dimana pengguna dengan akses level yang rendah bisa mengakses akses level yang lebih tinggi.

Contoh kemungkinan penerapan Elevation of Privilege di aplikasi shopee :

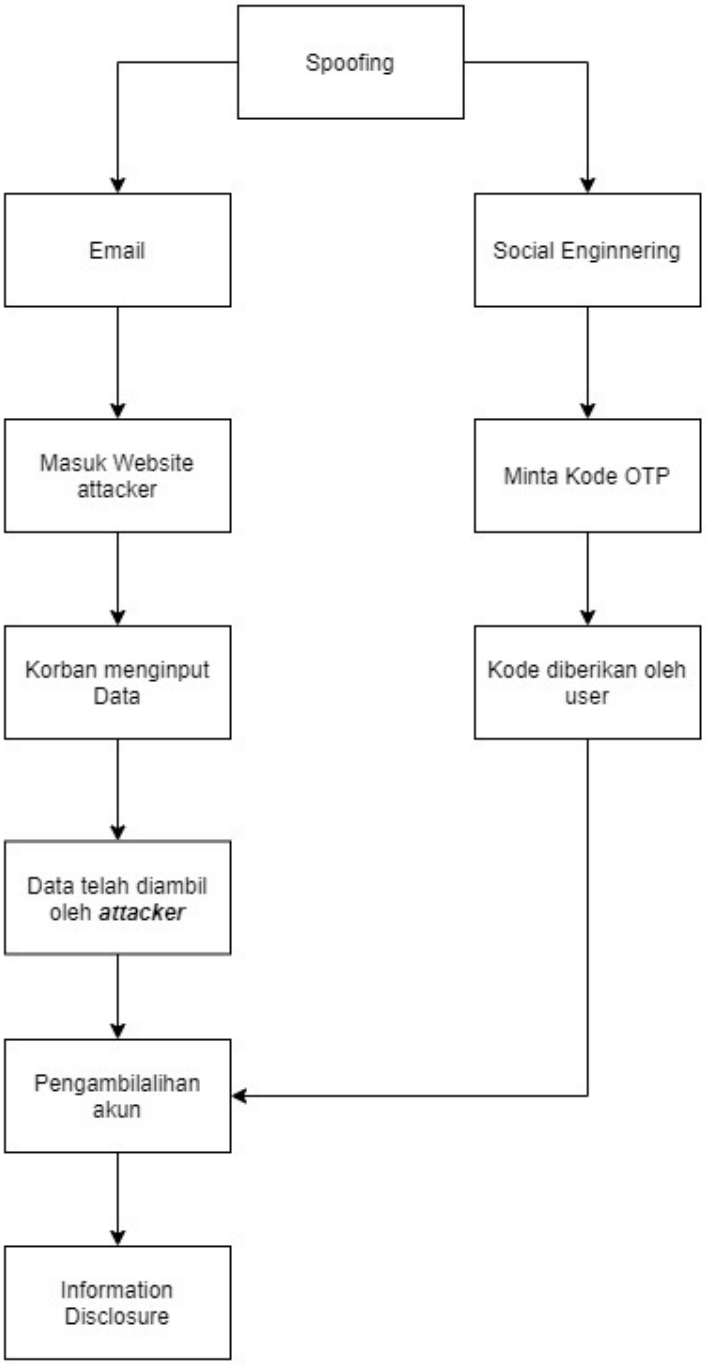
1. User bisa mengakses level yang lebih tinggi di aplikasi yang seharusnya dimana user tidak memiliki akses ke tempat tersebut karena yang bisa mengakses tempat tersebut hanyalah pekerja di aplikasi tersebut.

Scenario Analysis :
Ada telefon masuk dari seseorang yang mengatasnamakan pihak dari Shopee yang meminta code Otp. Pengguna mempercayai penelfon dan memberikan kode otpnya.

Pre-mortems
Karena sulit untuk membedakan penelfon yang benar dari pihak Shopee atau bukan dimana penipu sudah memiliki data-data si pengguna dan meyakinkan bahwa ia benar pihak dari Shopee, hal yang dapat terjadi adalah penipu dapat masuk kedalam akun pengguna.

Movie Plotting
https://www.youtube.com/watch?v=_G3NT91AWUE

Attack Tree


Spoofing
Email
Social Enginnering
Masuk Website attacker
Minta Kode OTP
Korban menginput Data
Kode diberikan oleh user
Data telah diambil oleh *attacker*
Pengambilalihan akun
Information Disclosure

Attack Library

CAPEC - Social Engineering

Tindakan memanipulasi tingkat emosi dan tingkah laku manusia untuk dapat berinteraksi dengan target. Contohnya penyerang menggunakan sebuah formulir kepada pegawai Shopee dengan alasan sangat memungkinkan dan membuat pegawai(korban) tersebut diharuskan untuk mengisi formulir tersebut lalu mendapatkan data dari pegawai tersebut.

Mitigasi :

a. Meningkatkan kewaspadaan saat melakukan interaksi dengan orang baik didunia nyata maupun didunia maya
b. Mengadakan pelatihan atau sosialisasi terkait pentingnya pengelolaan sistem keamanan informasi
c. Bekerja dengan pihak ketiga yang dapat membantu memperkuat sistem keamanan

OWASP - Denial of Service

Tindakan yang dapat menggangu sumber jaringan agar sebuah layanan host tidak dapat lagi terhubung dengan internet untuk sementara maupun tanpa batas. Tindakan ini dilakukan dengan cara membanjiri lalu lintas jaringan server dengan data agar pengguna tidak dapat mengakses sistem jaringan karena penuh.

Mitigasi :

a. Dengan mengidentifikasikan tipe serangan
b. Menerapkan Best Current Practices (BCP) standar industri
c. Menggunakan infrastruktur jaringan seperti flowspec
d. Mmeperbesar bandwith yang dapat memberikan waktu agar sistem tidak down

CAPEC - Bypassing Physical Security

Tindakan yang dapat menembus atau membobol suatu keamanan yang berbentuk secara fisik. Hal ini dapat diibaratkan jika seorang penyerang berhasil memanipulasi sebuah kamera keamanan atau berhasil meretas sebuah cctv pada sebuah gedung Shopee lalu masuk kedalam gedung tersebut tanpa sepengetahuan pihak berwenang.

Mitigasi :

a. Menggunakan firewall untuk mengatur dan mengontrol lalu lintas
b. Melakukan autentikasi terhadap akses
c. Mencatat kejadian dan memberikannya kepada administrator

CAPEC - Identity Spoofing

Tindakan yang dapat menembus suatu jaringan keamanan dengan menggunakan identitas resmi perusahaan dengan cara yang ilegal. Sebagai contoh penyerang melakukan *social engineering* kepada pegawai Shopee lalu berpura-pura menjadi pegawai tersebut dan memasuki sistem jaringan dari perusaahan yang dapat diakses oleh pegawai tersebut.

Mitigasi :

a. Menggunakan SSL
b. Menghindari menekan tautan yang tidak jelas
c. Meningkatkan kewaspadaan dalam menerima email

Hasil dan Pembahasan

Shopee merupakan aplikasi belanja online di Asia Tenggara dan Taiwan. Melalui proses diatas kami dapat membuat analisa mengenai sistem keamanan perusahaan Shopee dengan model STRIDE dan juga threat modelling. Dengan melalui STRIDE kami dapat mengenal jenis-jenis celah keamanan yang terdapat didalam sistem keamanan Shopee dan melalui thret modeling kami dapat mengenal jenis-jenis ancaman kemanan yang mungkin akan terjadi didalam aplikasi Shopee yang dilengkapi dengan Attack Tree.

Penutup

Tingkat kemanan suatu perusahaan sangat penting untuk diperhatikan agar dapat melindungi setiap data yang bersangkutan baik data perusahaan maupun data konsumen. Adapun tingkat kemamanan yang sudah dimiliki, setiap perusahaan pasti memiliki berbagai celah yang terletak didalam sistem keamanannya yang memungkinkan dimanfaatkan oleh orang yang tidak bertanggung jawab mencari keuntungan dibalik itu. Dengan melakukan beberapa analisa seperti diatas, kami dapat mencegah hal tersebut untuk terjadi. Lalu kami juga memberikan solusi disetiap kemungkinan jika suatu saat terjadi hal yang tidak diinginkan. Maka dari itu laporan analisa seperti ini dapat meminimalisir terjadinya ancaman pada suatu perusahaan.

Daftar Pustaka

"*CAPEC-Social Engineering*". https://capec.mitre.org/data/definitions/403.html . Accessed 14 Juni 2022.

"*OWASP - Denial of Service*". https://owasp.org/www-community/attacks/Denial_of_Service . Accessed 10 Juni 2022.

"*CAPEC - Bypassing Physical Security*". https://capec.mitre.org/data/definitions/391.html#:~:text=An%20attacker%20uses%20techniques%20and,cases%2C%20or%20other%20such%20devices. Accessed 15 Juni 2022.

"*CAPEC - Identity Spoofing*". https://capec.mitre.org/data/definitions/151.html#:~:text=Identity%20Spoofing%20refers%20to%20the,identity%20to%20accomplish%20a%20goal. Accessed 14 Juni 2022.