THREAT MODELING LAB

1. PRIPREMA

TOOLS

1. Svaki tim bi trebao da preuzme i da se upozna sa jednim od sledećih alata (ili oba :D):
    a. Microsoft Threat Modeling tool (https://docs.microsoft.com/en-us/azure/security/azure-security-threat-modeling-tool)
    b. OWASP Threat Dragon (https://owasp.org/www-project-threat-dragon/)

i da kreira threat model nekog prethodnog projekta.

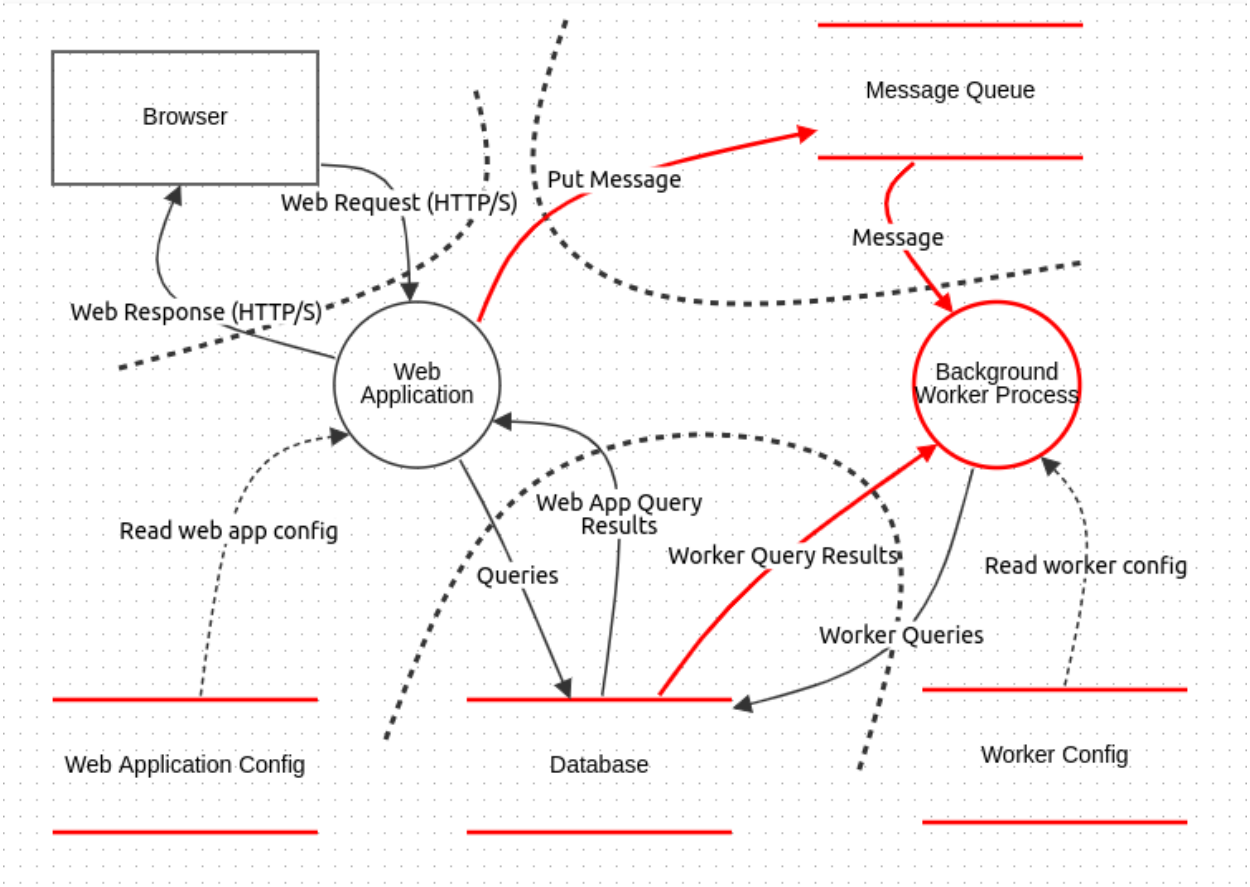
2. UVOD

Modelovanje pretnji (Threat Modeling) obuhvata i procenu rizika (risk assessment) (u tom slučaju govorimo o modelovanju pretnji na nivou zahteva (requirements-level TM)) i analizu dizajna bezbednosti (security design) (poznato i kao modelovanje pretnji na nivou dizajna). To podrazumeva primenu bezbednosnog načina razmišljanja na sistem, gde se identifikuju potencijalni napadači (threat actors) i njihovi ciljevi, a površina napada (attack surface) se mapira.

Primer

Razvijamo inovativnu platformu za e-trgovinu pod nazivom "ElectroShop". ElectroShop je online platforma koja omogućava korisnicima širom sveta brzu i sigurnu kupovinu elektronskih uređaja i dodatne opreme. Naš sistem se sastoji od web servera koji prima HTTPS zahteve od kupaca i PostgreSQL baze podataka za skladištenje proizvoda i informacija o korisnicima. ElectroShop se suočava sa velikim brojem narudžbina, te da bi se osigurala brza i efikasna obrada ovih zadatka, uvodi se background worker process nazvan "ElectroProcessor". ElectroProcessor je odvojeni radni proces koji efikasno procesira narudžbine i rukuje plaćanjem.

Kako bi se prilagodili dinamičkim potrebama sistema, i web server i background worker process imaju zaseban *config store*.



EShop kontekstni threat model (OWASP TD Default Primer)

3. ZADACI

Cilj sledećih zadataka je izvođenje modeliranja pretnji na imaginarnom softverskom sistemu koji vodi međunarodna korporacija specijalizovana za pružanje turističkih usluga (slično Ekpedia: https://vvv.ekpedia.com). Ono što sledi je oglas koji ukratko opisuje imaginarnu korporaciju:

MegaTravel je multinacionalna kompanija za organizaciju putovanja. Naša misija je da vam pomognemo da isplanirate i doživite vrhunski odmor. Pokrivamo širok spektar usluga, uključujući:

• *Rezervacija smeštaja,* gde biramo najpogodniji smeštaj za vaše putovanje.

• *Prevoz,* gde nalazimo najbolje ponude da vas odvedemo do odredišta iz snova.

• *Planiranje odmora,* gde zakazujemo izlete, iznajmljujemo vozila, pripremamo zabave i obavljamo razne usluge kako bismo vam zaista pružili najbolje moguće iskustvo.

Naša korporacija se prostire širom sveta, sa tri glavna sedišta u Londonu, Bostonu i Hong Kongu, i desetinama filijala u većini metropola. Naših deset hiljada zaposlenih, podržani najnovijim i najvećim tehnološkim dostignućima, neumorno rade na istraživanju i planiranju vaših iskustava, tako da vi ne morate.

Sa preko sto miliona klijenata koji se vraćaju, imali smo priliku i vreme da usavršimo svoj zanat i da proizvedemo vodeću svetsku uslugu broj 1 za putovanja.

A. MOTIVACIJA NAPADAČA

Nisu svi informacioni sistemi mete sofisticiranih napadača organizovanih od strane država. Shodno tome, veb aplikacija za stomatološku ordinaciju ne zahteva istu količinu sigurnosti kao nuklearni reaktor.

ZADATAK 1

Ispitajte ko bi želeo da napadne *MegaTravel* i zašto. Odredite koje klase napadača bi oštetile sistem. Šta više, za svaku klasu napadača odredite njihov opšti nivo veštine, njihov inherentan pristup sistemu i njihove krajnje ciljeve.

B. IMOVINA (ASSETS)

Dok se o bezbednosti može razgovarati i planirati u vakuumu, često su potrebna finansijska ulaganja da bi se integrisala u sistem. Ovo zahteva određivanje prioriteta kroz procenu rizika (risk assessment), koja se postiže ispitivanjem ugroženih sredstava imovine (asset).

ZADATAK 2

Vođeni motivacijom napadača, poslovnim zahtevima MegaTravel-a i svim zakonima i propisima koji bi mogli da utiču na ovu korporaciju, odredite listu osetljive imovine. Za svako sredstvo ispitajte:

- Koja je njegova inherentna izloženost (exposure) – ko ima pristup imovini;
- Koji su bezbednosni ciljevi sredstva (tj. poverljivost, integritet, dostupnost (CIA));
- Kakav uticaj (impact) bi oštećenje tih bezbednosnih ciljeva (security goals) imala na korporaciju.

C. POVRŠINA NAPADA (ATTACK SURFACE)

Ispitujući koji korisnici imaju interakciju sa sistemom, moguće je identifikovati ulazne tačke u sistem i odatle površinu napada.

ZADATAK 3

Ispitajte koji korisnici (ljudski, eksterni sistemi) komuniciraju sa MegaTravel sistemom i odatle mapirajte površinu napada kao skup ulaznih tačaka sa kojih napadači mogu da sprovedu svoje napade.

D. DATA FLOW DIAGRAMS

Uz dobru ideju o površini napada i imovini, moguće je razviti dijagrame toka podataka koji ilustruju i površinu napada i različite slojeve poverenja (trust) koji postoje u sistemu. Iako sistem može biti izložen Internetu, to ne znači da je osnovna funkcionalnost direktno dostupna. Umesto toga, demilitarizovana zona (DMZ) deluje kao platforma za sletanje za sve zahteve, potvrđujući ih pre nego što ih pošalje u kritičniju zonu.

ZADATAK 4

Koristeći sve prikupljene informacije, nacrtajte dijagram toka podataka MegaTravel sistema, uključujući površinu napada, spoljne entitete i osetljivu imovinu. Obratite pažnju na granice poverenja (trust boundaries) koje postoje unutar sistema. Počnite sa kontekstnim dijagramom i odatle razložite sve složene procese dok ne prestanu značajne granice poverenja.

E. ANALIZA PRETNJI I MITIGACIJE (THREAT AND MITIGATION)

Dijagram toka podataka (data flow diagram) je zgodna apstrakcija za razmišljanje o pretnjama. Kroz identifikaciju pretnji mi ispitujemo koje događaje želimo da izbegnemo – najčešće nanošenje štete bezbednosnom cilju sredstva. Kada se pretnje identifikuju, mi ih razlažemo da bismo ispitali napade koji mogu da realizuju pretnje, ranjivosti (vulnerabilities) u sistemu koji omogućavaju ove napade, i bezbednosne kontrole (security controls) ili protivmere (countermeasures) koje rešavaju (resolve) ove ranjivosti.

ZADATAK 5

Koristeći nacrtane dijagrame toka podataka i STRIDE metodologiju identifikacije pretnji, identifikujte i dekomponujte pretnje. Za svaku pretnju definišite ublažavanja (mitigations) koja sprečavaju pojavu pretnje.

4. DODATNO ČITANJE – BIĆE VAM OKAČENO

1. Security Development Lifecycle (Michael Howard, Steve Lipner)
2. Online Banking Security Analysis based on STRIDE Threat Model (Tong Xin, Ban Xiaofang)