# UPB

## Zadanie 1 - Modelovanie hrozieb

Riešitelia: Emília Čurillová, Filip Harvančík, Lenka Puškášová

**Úloha1** (Všetci - 33%, 33%, 33%)

E-shop bude pozostávať z dvoch hlavných častí: **klientská časť** a **serverová časť**.

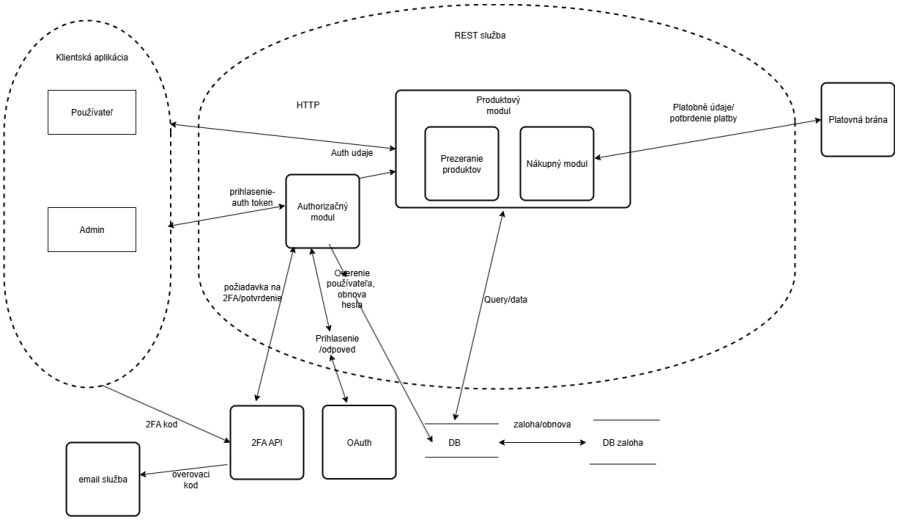
- **Klientská časť** zodpovedá za interakciu s používateľom – zobrazovanie produktov, prihlasovanie, zadávanie objednávok a platobný proces. Komunikuje so serverom prostredníctvom API rozhrania.
- **Serverová časť** spracováva požiadavky klienta, zabezpečuje prístup k dátam. Obsahuje API rozhranie, cez ktoré klientská časť získava a odosiela dáta.
- **Databázy:** Server sa pripája k hlavnej databáze, kde sú uložené všetky dáta o produktoch, objednávkach a používateľoch. Záložná databáza slúži na obnovu dát v prípade poruchy alebo straty.

Klientská časť využíva **OAuth 2.0 autentifikáciu** cez Google API poskytovateľa a je možné využiť aj 2FA autentifikáciu.
Serverová časť bude komunikovať s **externou platobnou bránou Paypal.**

Aplikácia má dve role užívateľov:
- používateľ: môže sa registrovať/prihlásiť, prezerať a vyhľadávať produkty, vytvárať objednávky, platiť cez integrovanú bránu.
- admin: môže spravovať produkty (pridať, upraviť, vymazať), spravovať používateľské účty, spravovať objednávky, pristupovať k reportom a štatistikám.

Zdroje:
OpenAI. (2023). ChatGPT (Mar 14 version) [Large language model].
https://chat.openai.com/chat - preformulovanie textu

**Úloha2** (Lenka)



**Úloha3** (Lenka)

SPOOFING

- Authorizačný modul
    - - brute force attack
        - Význam: hádanie hesiel
        - Mitigácia: zablokovanie prihlásenia po opätovnom neúspešnom pokuse o prihlásenie, 2FA authorizácia

TAMPERING

- Produktový modul
    - SQL injection
        - Význam: vloženie databázových SQL queries cez vložené dáta klienta
        - Mitigácia: povolenie len znakov zo zoznamu bežných hodnôt, zakázať potencionálne škodlivé znaky

REPUDIATION

- Autorizačný modul, produktový modul - chýbajú záznamy o prihlásení, objednávkach
        - Mitigácia: Logovanie prihlásení s ip adresou a timestampom, logovanie objednávok, Notifikovanie užívateľa o prihlásení z iného zariadenia

INFORMATION DISCLOSURE

- HTTP komunikácia
    - - Sniffing
        - Význam: čítanie nezašifrovanej komunikácie
        - Miitigácia - HTTPS protokol
    - IDOR = Insecure Direct Object Reference Prevention
        - Význam: Prístup k cudzím objednávkam zmenou ID v URL
        - Mitigácia: Prenášanie identifikátorov v session, overovanie prístupu používateľa pri každom pokuse o prístup

DENIAL OF SERVICE

- Produktový modul
    - Race Condition
        - Význam: Dvaja užívatelia dokončia objednávku pre tovar, ktorý je posledný na sklade
        - Mitigácia: využitie zámkov na obmedzenie prístupu k rovnakému zdroju

ELEVATION OF PRIVILEGE

- REST služba ↔ Databáza
    - Mass Assignment
        - Význam: nastavenie isAdmin=true cez API
        - Mitigácia: použitie Data Transfer Objektov, allow list - povolenie bezpečných polí, block list - zakázanie nebezpečných polí

Zdroje:

https://owasp.org/www-community/attacks/Brute_force_attack

https://owasp.org/www-community/attacks/SQL_Injection
https://www.comparitech.com/blog/information-security/sniffing-attack/
https://cheatsheetseries.owasp.org/cheatsheets/Insecure_Direct_Object_Reference_Prevention_Cheat_Sheet.html
https://medium.com/@vikaskumar01/race-condition-vulnerability-what-works-mitigation-techniques-detecting-89208f3263ff
https://cheatsheetseries.owasp.org/cheatsheets/Mass_Assignment_Cheat_Sheet.html

**Úloha4** (Filip, Emília)
Spoofing - útočník sa dokáže neoprávnene prihlásiť do konta iného používateľa
Bezp. opatrenia: heslová politika (povinné silné heslá, pravidelná povinnosť používateľov zmeniť si heslo) a viacfaktorová autentifikácia alebo prenesenie zodpovednosti na 3. stranu, t. j. používanie prihlasovania cez služby ako Google, Facebook.

Tampering - útočník neoprávnene zmení obsah databázy (napr. cez SQL injection)
Bezp. opatrenia: Používanie parameterizovaných SQL dotazov a ORM nástrojov namiesto dynamických dotazov, pravidelné penetračné testy a monitoring databázy. zavedenie ochrany voči SQL injection; transakčné logy;  Vytvorenie záložnej databázy, ktorá by sa aktualizovala bezpečnejším spôsobom ako primárna databáza.

Repudiation - útočník bez zanechania stopy zmení obsah databázy a popiera, že to urobil
Bezp. opatrenia: centralizované logovanie s ochranou integrity (napr. SIEM); bezpečné, nezmeniteľné záznamy auditu; záznamy s časovou pečiatkou; implementácia honeypotov.

Information disclosure - útočník je schopný čítať komunikáciu medzi klientom a serverom
Bezp. opatrenia: použitie bezpečného šifrovania (HTTPS, SSL/TLS certifikát); End-to-end šifrovanie

Denial of service - Útočník zahlcuje server veľkým počtom požiadaviek, čím zneprístupní službu pre legitímnych používateľov.
Bezp. opatrenia: Implementácia rate limiting (obmedzenie počtu požiadaviek na IP/časovú jednotku), použitie CDN a WAF (Web Application Firewall) na monitorovanie a filtrovanie prenosu požiadaviek, vykonávanie pravidelných kontrol siete
Zdroje:
Čo je obmedzenie rýchlosti? | Obmedzenie rýchlosti a roboty | Záblesk oblakov
Čo je sieť na doručovanie obsahu (CDN)? | Ako fungujú siete CDN? | Záblesk oblakov
Čo je to WAF? | Vysvetlenie Web Application Firewall | Záblesk oblakov

Elevation of privilege - Útočník získa vyššie oprávnenia než mu prináležia (napr. bežný používateľ sa stane adminom manipuláciou s rolami alebo tokenmi).

Bezp. opatrenia: zavedenie princípu minimálnych oprávnení (least privilege) – minimum oprávnení potrebných na vykonávanie ich funkcií. Zero Trust security model - žiadnemu používateľovi ani zariadeniu, či už v sieti alebo mimo nej, by sa predvolene nemalo dôverovať. Použitie RBAC (Role-Based Access Control) alebo ABAC (Attribute-Based Access Control) pre jasne definované role a prístupové politiky. Pravidelne vykonávať audit oprávnení a logov.
Zdroje:
Vysvetlenie eskalácie privilégií: Typy, príklady a prevencia

**Úloha5** (Emília)

ROOT: Získať neoprávnený prístup do používateľského konta

1. Využitie slabého overenia
    1.1. Brute-force attack
        1.1.1. Hádanie hesla
            1.1.1.1. Dictionary attack (útok cez slovník)
            1.1.1.2. Numeric/sequential guessing (číselné/sekvenčné hádanie)
        1.1.2. Credential stuffing (opakované použitie ukradnutých prihlasovacích údajov)
            1.1.2.1. Použitie uniknutých databáz hesiel
            1.1.2.2. Automatizované pokusy o prihlásenie (botnet)
    1.2. Sociálne inžinierstvo (Social engineering)
        1.2.1. Phishing
            1.2.1.1. Falošná stránka na prihlasovanie
            1.2.1.2. Podvodné emaily / linky
        1.2.2. Vishing / telefonický podvod
            1.2.2.1. Predstieranie podpory (support call)
            1.2.2.2. Podvodné SMS / OTP
    1.3. Zneužitie mechanizmov obnovy hesla
        1.3.1. Zneužitie resetovania cez email
            1.3.1.1. Zachytenie emailu s resetovaním hesla
            1.3.1.2. Kompromitácia emailového účtu
        1.3.2. Hádanie bezpečnostných otázok
            1.3.2.1. Vyhľadávanie verejných informácií
            1.3.2.2. Zber dát zo sociálnych sietí
2. Využitie zraniteľností správy relácií (Session management vulnerabilities)
    2.1. Session hijacking (únos relácie)
        2.1.1. XSS na ukradnutie session cookie
            2.1.1.1. Reflected XSS na prihlasovacej stránke
            2.1.1.2. Stored XSS cez komentáre / formuláre
        2.1.2. Man-in-the-Middle (MITM)
            2.1.2.1. Sniffing na verejnej Wi-Fi
            2.1.2.2. ARP spoofing
    2.2. Session fixation (fixácia relácie)
        2.2.1. Prednastavené session ID cez URL
            2.2.1.1. Vytvorenie odkazu s tokenom session

2.2.1.2. Phishing s pred-auth tokenom

2.2.2. Manipulácia cookies

2.2.2.1. Ukradnutie cookie cez XSS

2.2.2.2. Nastavenie cookie v prehliadači cez subdoménový útok