Model pretnji

Dragan Grbić R2 8/2021 & Petar Nikolić R2 5/2021

# 1. Resursi od značaja

|  |  |  |
| --- | --- | --- |
| Oznaka | Naziv | Opis |
| A1 | Korisnički kredencijali | Kredencijali za prijavu na sistem. |
| A2 | Lični podaci korisnika | Ime, prezime, email adresa, podaci vezani za bankovni račun itd. |
| A3 | Baze podataka | Skladište podatke individualnih aplikacija u sistemu. |
| A4 | Biznis logika Payment Service Provider-a | Funkcionalnosti koje servis obezbeđuje. |
| A5 | Biznis logika Card servisa | Funkcionalnosti koje servis obezbeđuje. |
| A6 | Biznis logika QR kod servisa | Funkcionalnosti koje servis obezbeđuje. |
| A7 | Biznis logika Paypal servisa | Funkcionalnosti koje servis obezbeđuje. |
| A8 | Biznis logika Bitcoin servisa | Funkcionalnosti koje servis obezbeđuje. |
| A9 | Biznis logika Web shop-a | Funkcionalnosti koje servis obezbeđuje. |
| A10 | Biznis logika Bank servisa | Funkcionalnosti koje servis obezbeđuje. |
| A11 | Biznis logika PCC servisa | Funkcionalnosti koje servis obezbeđuje. |
| A12 | Zuul Gateway | Omogućava komunikaciju između dostupnih servisa plaćanja. |
| A13 | Eureka | Omogućava registrovanje servisa plaćanja kako bi bili dostupni Zuul Gateway aplikaciji. |
| A14 | Skladišta sertifikata (keystore i truststore) | Sadrže sertifikate pojedinačnih aplikacija u sistemu, kao i sertifikate servisa kojima verujemo (Coingate i Paypal sandbox API). |
| A15 | Konfiguracione datoteke | Sadrže podešavanja aplikacija u sistemu. |

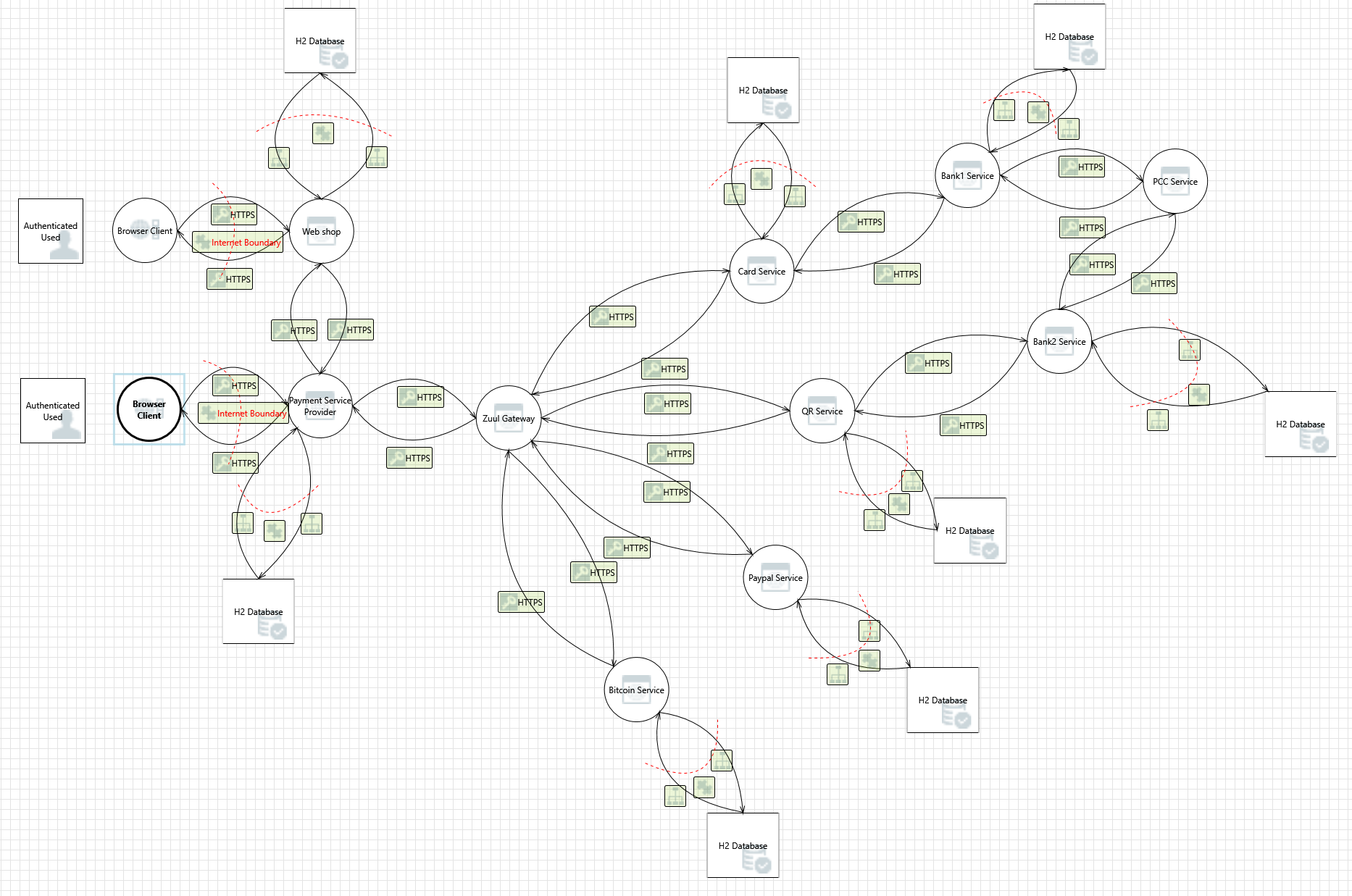
# 2. Nivoi poverenja korisnika sistema

|  |  |  |
| --- | --- | --- |
| Oznaka | Naziv | Opis |
| TA1 | Prodavac Webshop-a | Dodaje i briše proizvode koje želi da prodaje. |
| TA2 | Kupac Webshop-a | Pregleda i kupuje proizvode. |
| TA3 | Administrator Payment Service Provider-a | Registruje nove i briše postojeće Webshop-ove, načine plaćanja i prodavce. |

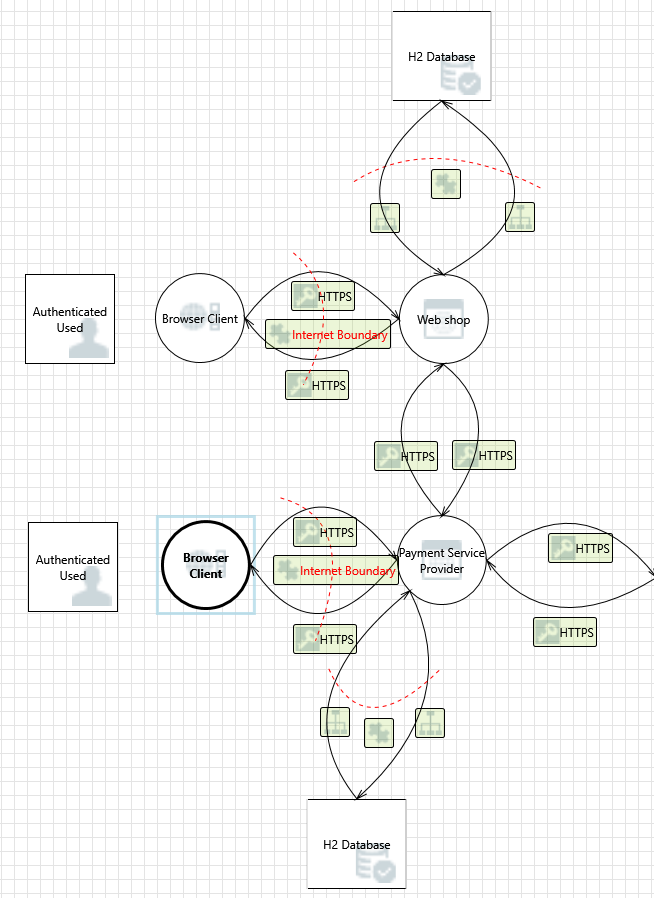
# 3. Ulazne tačke sistema

|  |  |  |
| --- | --- | --- |
| Oznaka | Naziv | Nivoi poverenja |
| EP1 | Stranica za prijavu na Webshop | TA1, TA2 |
| EP2 | Stranica za pregled proizvoda | TA1, TA2 |
| EP3 | Stranica za pregled porudžbina | TA1, TA2 |
| EP4 | Stranica za prijavu na Payment service provider | TA3 |
| EP5 | Stranica za pregled servisa plaćanja | TA3 |
| EP6 | Stranica za dodavanje servisa plaćanja | TA3 |
| EP7 | Stranica za pregled Webshop-ova | TA3 |
| EP8 | Stranica za pregled korisnika (administratora i prodavaca) | TA3 |
| EP9 | Stranica za dodavanje prodavca | TA3 |
| EP10 | Stranica za odabir načina plaćanja | TA2 |
| EP11 | Stranica za potvrdu Paypal plaćanja | TA2 |
| EP12 | Stranica za kreiranje Paypal pretplate | TA2 |
| EP13 | Stranica za potvrdu Paypal pretplate | TA2 |
| EP14 | Stranica za potvrdu plaćanja putem Coingate-a | TA2 |
| EP15 | Stranica za potvrdu plaćanja putem kartice | TA2 |
| EP16 | Stranica za potvrdu plaćanja putem QR koda | TA2 |

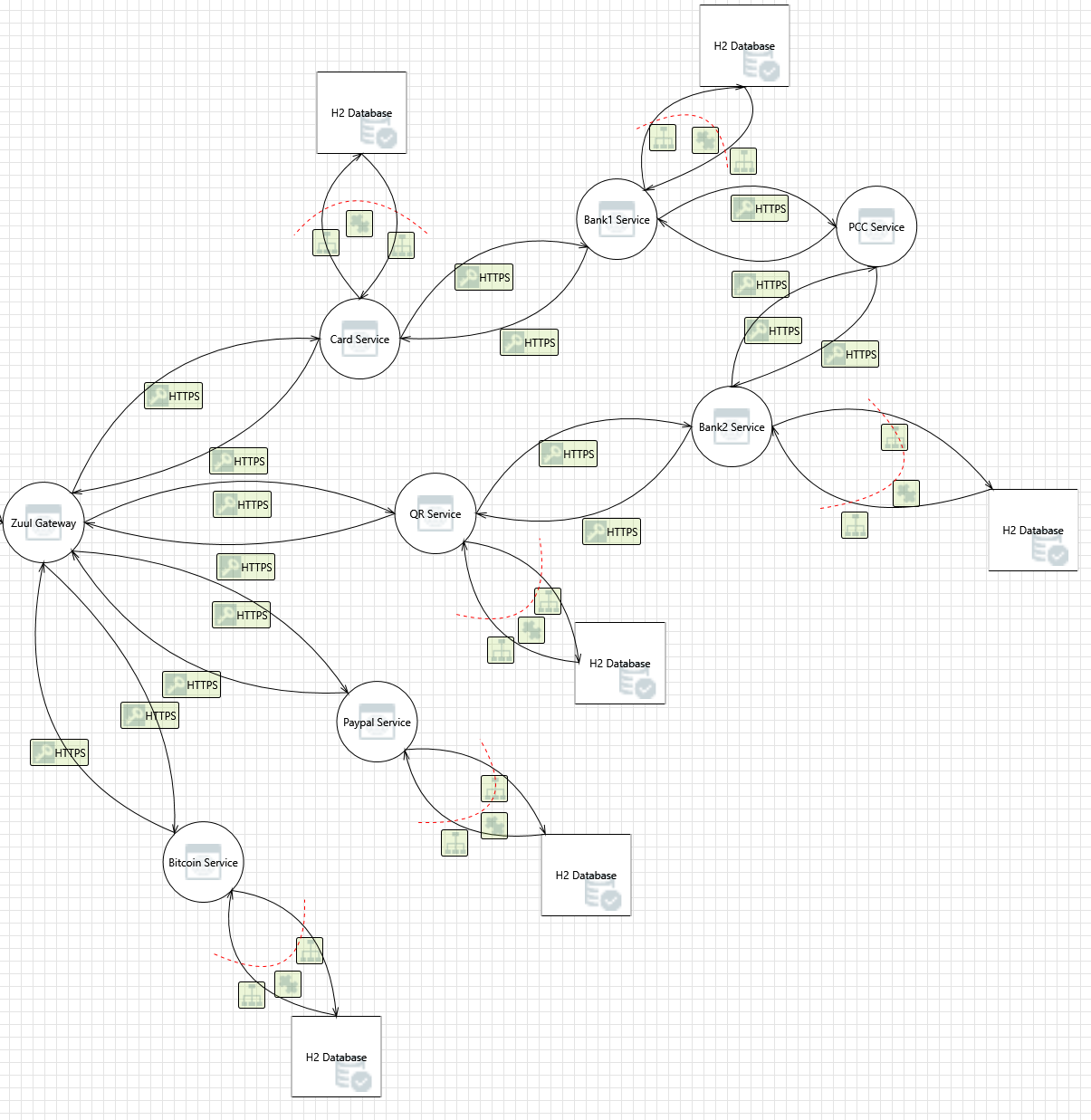
# 4. Dijagram toka podataka



Slika 1 - Dijagram toka podataka



Slika 2 - Dijagram toka podataka



Slika 3 - Dijagram toka podataka

# 5. Identifikacija rizika

|  |  |  |  |
| --- | --- | --- | --- |
| Oznaka | Opis | Uticaj na sistem | Verovatnoća  pojavljanja |
| Spoofing | | | |
| T1 | Spoofing of Source Data Store | Medium | Low |
| T2 | Spoofing of Destination Data Store | Medium | Low |
| T3 | Spoofing the Web Service Process | High | High |
| Tampering | | | |
| T4 | Cross Site Scripting | Low | Low |
| T5 | Data Store Could Be Corrupted | High | Medium |
| T6 | Web Service Memory Tampered | Low | Low |
| T7 | Replay Attacks | High | Medium |
| T8 | Potential SQL Injection Vulnerability for SQL Database | High | Medium |
| Repudation | | | |
| T9 | Potential Data Repudiation by Web Service | High | Low |
| T10 | Data Store denies File System/SQL Database Potentially Writting Data | High | Low |
| Information disclosure | | | |
| T11 | Weak Credential Storage | High | High |
| T12 | Weak Access Control for a Resource | Low | Medium |
| T13 | Authorization Bypass | Medium | Medium |
| T14 | Data Flow Sniffing | High | High |
| T15 | Weak Authentication Scheme | High | High |
| Denial of service | | | |
| T16 | Potential Process Crash or Stop for Web Service | High | High |
| T17 | Data flow is potentially interrupted | High | High |
| T18 | Data Store Inaccessible | High | Low |
| T19 | Potential Excessive Resource Consumption | High | Medium |
| Elevation of privilege | | | |
| T20 | Web service may be subject to Elevation of Privilege Using Remote Code Execution | High | High |
| T21 | Elevation by Changing the Execution Flow in Web service | Medium | High |
| T22 | Elevation Using Impersonation | Medium | Medium |
| T23 | Cross Site Request Forgery | Medium | Low |

# 6. Analiza rizika

Rizik = Uticaj na sistem \* Verovatnoća pojavljivanja

|  |  |  |  |
| --- | --- | --- | --- |
| žerovatnoća pojavljivanja/Uticaj na sistem | Low | Medium | High |
| Low | Low | Low | Medium |
| Medium | Low | Medium | High |
| High | Medium | High | High |

|  |  |  |
| --- | --- | --- |
| Oznaka | Opis | Rizik |
| Spoofing | | |
| T1 | Spoofing of Source Data Store | Low |
| T2 | Spoofing of Destination Data Store | Low |
| T3 | Spoofing the Web Service Process | High |
| Tampering | | |
| T4 | Cross Site Scripting | Low |
| T5 | Data Store Could Be Corrupted | High |
| T6 | Web Service Memory Tampered | Low |
| T7 | Replay Attacks | High |
| T8 | Potential SQL Injection Vulnerability for SQL Database | High |
| Repudation | | |
| T9 | Potential Data Repudiation by Web Service | Medium |
| T10 | Data Store denies File System/SQL Database Potentially Writting Data | Medium |
| Information disclosure | | |
| T11 | Weak Credential Storage | High |
| T12 | Weak Access Control for a Resource | Low |
| T13 | Authorization Bypass | Medium |
| T14 | Data Flow Sniffing | High |
| T15 | Weak Authentication Scheme | High |
| Denial of service | | |
| T16 | Potential Process Crash or Stop for Web Service | High |
| T17 | Data flow is potentially interrupted | High |
| T18 | Data Store Inaccessible | Medium |
| T19 | Potential Excessive Resource Consumption | High |
| Elevation of privilege | | |
| T20 | Web service may be subject to Elevation of Privilege Using Remote Code Execution | High |
| T21 | Elevation by Changing the Execution Flow in Web service | High |
| T22 | Elevation Using Impersonation | Medium |
| T23 | Cross Site Request Forgery | Low |

# 7. Protivmere

|  |  |  |
| --- | --- | --- |
| Oznaka | Opis | Protivmere |
| Spoofing | | |
| T1 | Spoofing of Source Data Store | Da, putem konfiguracije u application.properties. |
| T2 | Spoofing of Destination Data Store | Da, putem konfiguracije u application.properties. |
| T3 | Spoofing the Web Service Process | Da, autentifikacijom upotrebom Spring Security. |
| Tampering | | |
| T4 | Cross Site Scripting | Da, Angular ima ugrađenu zaštitu. |
| T5 | Data Store Could Be Corrupted | Ne |
| T6 | Web Service Memory Tampered | Memory tampering interakcije su veoma malo verovatne u REST web service komunikaciji. |
| T7 | Replay Attacks | Da, upotrebom HTTPS-a, koji štiti od ovakvih napada na mrežnom nivou. |
| T8 | Potential SQL Injection Vulnerability for SQL Database | Da, Spring pruža zaštitu prilikom korišćenja @Query anotacije. |
| Repudiation | | |
| T9 | Potential Data Repudiation by Web Service | Da, logovanjem. |
| T10 | Data Store denies File System/SQL Database Potentially Writting Data | Da, logovanjem. |
| Information disclosure | | |
| T11 |  |  |
| T12 | Weak Access Control for a Resource | Da, definisanjem prava pristupa. |
| T13 | Authorization Bypass | Ne |
| T14 | Data Flow Sniffing | Da, korišćenjem TLS konekcije sa bazama podataka, korišćenjem HTTPS-a i šifrovanjem osetljivih podataka. |
| T15 | Weak Authentication Scheme | Ne |
| Denial of service | | |
| T16 | Potential Process Crash or Stop for Web Service | Da, pokretanjem više instanci. |
| T17 | Data flow is potentially interrupted | Da, upotrebom HTTPS-a i šifrovanjem osetljivih podataka. |
| T18 | Data Store Inaccessible | Ne |
| T19 | Potential Excessive Resource Consumption | Da, kod listanja zarad prikaza na frontendu se koristi paginacija. Takođe, query-iji u sistemu su jednostavni, te nema dugog vremena izvršavanja uzrokovanog njihovom kompleksnošću. |
| Elevation of privilege | | |
| T20 | Web service may be subject to Elevation of Privilege Using Remote Code Execution | Da, Angular pruža automatsku sanitizaciju i escape-ovanje. |
| T21 | Elevation by Changing the Execution Flow in Web service | Da, Angular pruža automatsku sanitizaciju i escape-ovanje. |
| T22 | Elevation Using Impersonation | Da, definisanjem i proverom korisničkih privilegija. |
| T23 | Cross Site Request Forgery | Da, podešavanjem Spring security-a da onemogućava CSFR. |