Informacije:

|  |  |
| --- | --- |
| Verzija aplikacije | 1.0 |
| Opis | Web aplikacija za gradsku skupštinu koja omogućava korisnicima obavljanje skupštinskih poslova i pregled do sada postignutog u skupštini preko interneta. Korisnici su:   * Web Admin * Predsednik skupštine * Odbornici u skupštini * Građani   Građani mogu pretraživati i pregledati akte. Odbornici mogu predlagati akte i amandmane na akte, uz mogućnosti koje imaju građani. Predsednici mogu updavljati sednicom, i uz to imaju mogućnosti odbornika. Web admin može dodavati nove korisnike, uz mogućnosti koje ima građanin. |
| Vlasnik dokumenta | Lazar Anđelić |
| Učesnici | Isidora Škulec |
| Recezenti | Nemanja Ilić, Prof. Goran Sladić, Nikola Luburić |

Permisije:

|  |  |  |
| --- | --- | --- |
| ID | Naziv | Opis |
| 0 | Anonymous | Korisnik koji nije ulogovan. Pretraga i pregled akata |
| 1 | Invalid login | Korisnik koji se pokušao ulogovati sa pogrešnim podacima. Pretraga i pregled akata |
| 2 | Odbornik | Anonymous + predlaže i povlači predloge na akte i amandmane akata, login |
| 3 | Predsednik | Odb + usvajanje akata |
| 4 | DB admin | Potpun pristup bazi koja je vezana za aplikaciju |
| 5 | Web admin | Konfiguracija web stranice, dodavanje korisnika |
| 6 | Web serv. user process | Proces koji komunicira sa bazom |
| 7 | DB read user | Korisnik baze sa mogućnošću čitanja |
| 8 | DB r-w user | Korisnik baze sa mogućnošću čitanja i pisanja |

Spoljne zavisnosti:

* Server je pokrenut na Windows Server 2012 R2
* Server je Play! Framework 1.4.2, koji je baziran na Akka toolkit-u
* Baza podataka je MS SQL 2012 Enterprise SP3.
* Komunikacija između baze i servera je na lokalnoj mreži, bazi nije moguće pristupiti van lokalne mreže
* Istorijski arhiv Novog Sada
* MarkLogic NoSQL baza podataka za XML
* CertGen aplikacija za izdavanje korisničkih sertifikata

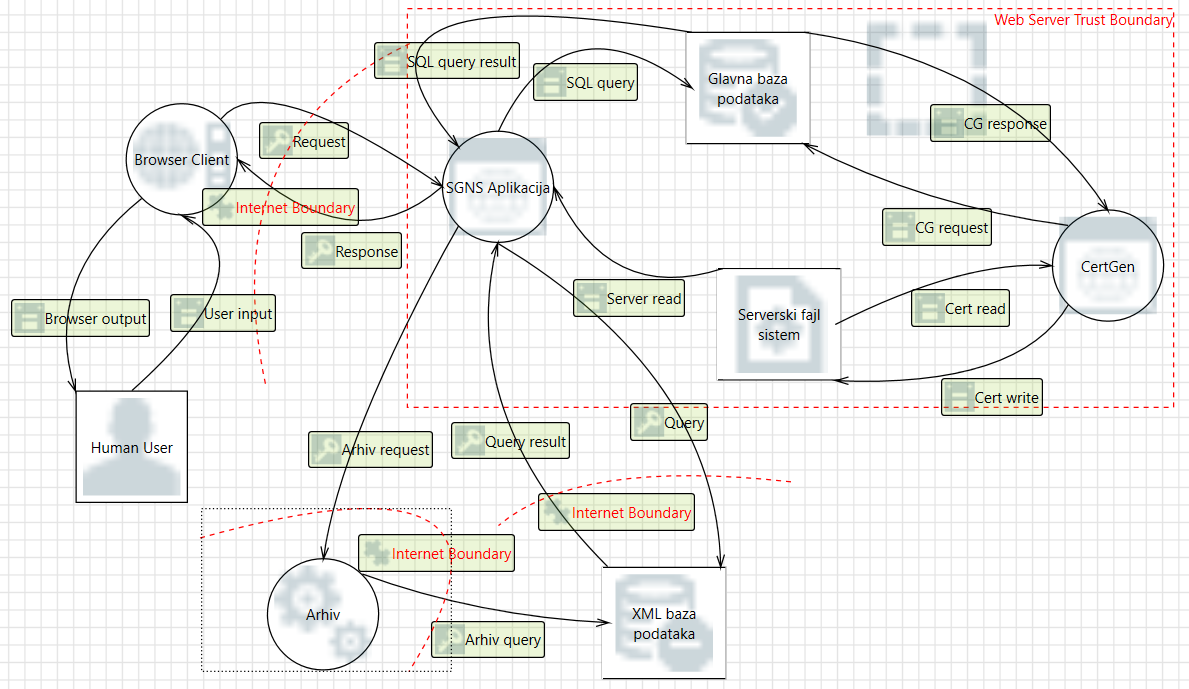
Ulazne i izlazne tačke:

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Naziv | Opis | Permisije |
| Ulazne tačke | | | |
| 1.1 | HTTPS port | Celoj aplikaciji se pristupa preko HTTPS | 0, 1, 2, 3, 5 |
| 1.2 | Login stranica | Korisnici se moraju ulogovati pre izvršavanja akcija | 0, 1, 2, 3, 5 |
| 1.3 | Login funkcija | Uzima prosleđene korisničke podatke i poredi ih sa onim u bazi | 1, 3, 5 |
| 1.4 | Glavna stranica | Stranica koja se prikazuje pri prvom pristupu aplikaciji | 0, 1, 2, 3, 5 |
| 1.5 | Pretraga | Stranica za pretragu i prikaz rezultata pretrage | 0, 1, 2, 3, 5 |
| 1.6 | Pregled akata | Stranica za pregled usvojenih i akata u proceduri | 0, 1, 2, 3, 5 |
| 1.7 | Predlog akta | Stranica za predlaganje/povlačenje predloga akta | 2, 3 |
| 1.8 | Predlog amandmana | Stranica za predlaganje/povlačenje predloga amandmana | 2, 3 |
| 1.9 | Rukovođenje sednicom | Stranica za rukovođenje sednicom (usvajanje akata) | 3 |

Resursi:

|  |  |  |  |
| --- | --- | --- | --- |
| Korisnički podaci | | | |
| 1.1 | Login podaci | Podaci koje korisnici koriste za logovanje | 4 – 8 |
| 1.2 | Login podaci odbornika | Podaci koje odbornik koristi da se uloguje | 2, 4 – 8 |
| 1.3 | Login podaci predsednika | Podaci koje predsednik koristi da se uloguje | 3 – 8 |
| 1.4 | Login podaci web admina | Web admin login | 4 – 8 |
| 1.5 | Lični podaci korisnika | Neka vrsta “lične karte” za aplikaciju | 2 – 9 |
| Sistem | | | |
| 2.1 | Dostupnost web aplikacije | Web aplikacija bi trebala biti dostupna 24/7 svim korisnicima | 4, 5 |
| 2.2 | Izvršavanje koda kao WSU | Mogućnost izvršavanja koda na web serveru kao WS User Proc. | 5, 6 |
| 2.3 | Izvršavanje upita kao DB R | Mogućnost izvršavanja SQL select upita – čitanje DB | 4, 7, 8 |
| 2.4 | Izvršavanje upita kao DB RW | Mogućnost izvršavanja SQL select, insert, update | 4, 8 |
| Web stranica | | | |
| 3.1 | Login sesija | Sesija ulogovanog korisnika | 2, 3, 4, 6 |
| 3.2 | Pristup DB serveru | Omogućava administraciju DB | 5 |
| 3.3 | Kreiranje novog korisnika | … | 5, 6 |
| 3.4 | Pregled audit logova | … | 6 |

Data flow:



STRIDE kategorizacija pretnji:

* Arhiv query(Arhiv->XML baza):
  1. Spoofing – Napadač može impersonirati XML bazu i tako preuzeti podatke koji su trebali da se sačuvaju u njoj – ne znamo da li je rešena jer to ne zavisi od nas
  2. DoS – Napadi koji zauzimaju veliku količinu resursa sistema XML baze podataka – ne znamo da li je rešena jer to ne zavisi od nas
  3. Repudiation – Poricanje da je nešto izvršeno na bazi – ne znamo da li je rešena jer to ne zavisi od nas
  4. Tampering – Ako napadač uspe presresti komunikaciju, može izmeniti podatke koji se šalju, što rezultuje korupcijom/invalidnim podacima – delimično rešeno sa korišćenjem HTTPS
* Arhiv request (SGNS->Arhiv) – za rešenja problema pretpostavljamo da je arhiv grada to implementirao:
  1. Tampering – Komunikacija prenosi XML. Postoji mogućnost XML(DTD/XSLT) napada – rešeno eskejpovanjem(enkodiranjem) podataka u zahtevima
  2. Elevation of priviledge – Arhiv bi mogao impersonirati SGNS Aplikaciju da dobije više privilegije – rešeno sertifikatima
  3. Tampering – Napadač može presresti komunikaciju i izvršiti kolizioni napad – pošto su u pitanju dve različite vrednosti sa istim hash-em, problem nam deluje nerešivo
  4. Tampering – Replay napadi – zahtevi bez timestamp-a i rednog broja se mogu ponoviti – rešeno slanjem zahteva sa timestamp-om i rednim brojem, što se proverava na serveru
  5. Elevation of priviledge – Napadač može u Arhiv poslati podatke koji bi skrenuli tok izvršavanja programa tako da njemu odgovara – rešeno enkodiranjem podataka koji se primaju
  6. DoS – Napadač može izvršiti neki od DoS napada nad Arhivom, ili Arhiv ne funkcioniše kako treba i tako sam sebe DoS-uje – delimično rešeno error handlingom u Arhivu
  7. Repudiation – Poricanje da je Arhiv primio podatke koje nije slala SGNS – rešeno logovanjem
* Query (SGNS->XML baza):
  1. DoS – Napadač može izvršiti neki od DoS napada nad XML bazom – ne znamo da li je rešeno jer ne zavisi od nas
  2. DoS – Napadač može izvršiti neki od DoS napada nad SGNS, ili SGNS ne funkcioniše kako treba i sam sebe DoS-uje – delimično rešeno error handlingom u SGNS
  3. Information Disclosure – Mogućnost pristupa XML bazi i zaobići permisije za njene podatke (zatim ih izmeniti na neki način) – ne znamo da li je rešeno jer ne zavisi od nas
  4. Repudiation – Poricanje da je nešto izvršeno nad bazom (npr neki upit) – ne znamo da li je rešeno jer ne zavisi od nas
  5. Tampering – Napadač može presresti komunikaciju sa bazom i menjati podatke, što dovodi do toga da baza sadrži korumpirane/invalidne podatke – delimično rešeno pomoću HTTPS
  6. Spoofing – Napadač može impersonirati XML bazu, što dovodi do toga da se podaci upisuju kod njega, a ne u bazu – ne znamo da li je rešeno jer ne zavisi od nas
* Query result (XML baza->SGNS):
  1. Repudiation – Poricanje da je SGNS primio podatke koji nisu poslati od XML baze – rešeno logovanjem
  2. Spoofing – Napadač može impersonirati XML bazu što dovodi do toga da SGNS dobija pogrešne podatke – ne znamo da li je rešeno jer ne zavisi od nas
  3. Tampering – Pošto se prenose XML podaci, moguće je izvršiti XML(DTD/XSLT) napad – rešeno enkodiranjem dobijenih podataka
  4. Elevation of priviledge – Napadač može u SGNS proslediti podatke koji bi promenili tok izvršavanja programa tako da to njemu odgovara – rešeno enkodiranjem dobijenih podataka
  5. DoS – Moguće izvršiti neki od DoS napada nad SGNS – možda delimično rešeno proverom origin i referer headera
* Request(Browser->SGNS):
  1. Tampering – U slučaju slanja XML-a u SGNS, mogući su XML(DTD/XSLT) napadi – rešeno enkodiranjem dobijenih podataka
  2. Repudiation – Poricanje da je SGNS dobila podatke koji nisu od Browsera – rešeno logovanjem
  3. DoS – SGNS ne funkcioniše pravilno, izazivajući DoS sama sebi – rešeno error handlingom
  4. Elevation of priviledge – Napadač može u SGNS proslediti podatke koji bi promenili tok izvršavanja programa tako da to njemu odgovara – rešeno enkodiranjem dobijenih podataka
  5. Tampering – Replay napad – rešeno upotrebom timestamp-ova i rednog broja zahteva
  6. Tampering – Kolizioni napad – prouzrokovan postojanjem dve vrednosti sa istim hash-em – nije rešeno
* Response(SGNS->Browser):
  1. Tampering – krađa JSON podataka – nije rešeno, ali JSON-om se ne prenose kritični podaci
* SQL query(SGNS->Baza):
  1. DoS – Mogućnost DoS napada, ili sa strane SGNS, da ona sama ne funkcioniše kako treba i time sebe DoS-uje – delimično rešeno error handlingom u SGNS
  2. Information Disclosure – Baza sadrži kredencijale korisnika SGNS, što omogućuje napadaču sa lokalne mreže da dobije kritične podatke o korisnicima – delimično rešeno salt+hash lozinkama, ali ne možemo garantovati da korisnik nije koristio isti email i lozinku na drugom mestu
  3. Tampering – SQL injection – rešeno enkodiranjem svih query-ja poslatih bazi
* CG request(CertGen->Baza):
  1. DoS – neki od DoS napada, sa lokalne mreže, ili da CertGen ne funkcioniše kako treba, pa sam sebe DoS-uje – delimično rešeno error handlingom
  2. Information disclosure – Korisnički kredencijali se čuvaju u bazi, pa ih je moguće ukrasti ako neko ima neovlašćen pristup bazi – rešeno salt+hash kredencijalima
* CG response(Baza->CertGen):
  1. Spoofing – Impersonacija baze podataka od strane napadača na lokalnoj mreži što može uzrokuje da CertGen dobije pogrešne podatke – rešeno autentikacijom