

WEB security проект по предметот Информациска безбедност

Е - лекување

- Членови на тимот

- Борјан Костов- 181008
- Ана Богоевска- 181003
- Јана Велјаноска- 181108
- Зорица Карапанчева- 185003

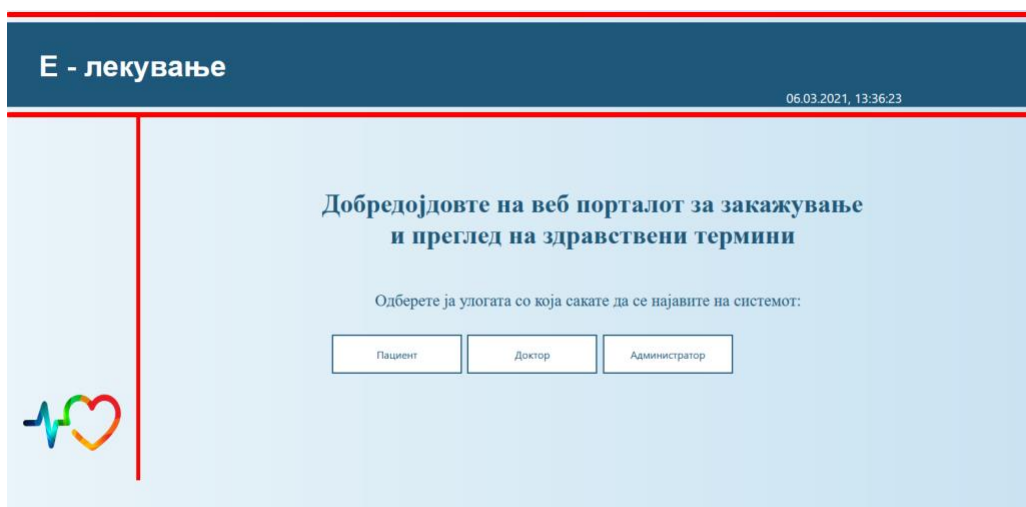
- Опис на проектот

Е-лекување е веб апликација за закажување на здравствени термини. Апликацијата подржува три типа на корисници: доктор, пациент и администратор.

Корисникот кој се најавува како пациент може да се најави користејќи го неговото корисничко име и лозинка. Откако ќе се најави успешно пациентот, му се прикажува табела со веќе постоечки термини. Откога ќе ја прегледа табелата може да се одјави и се враќа на почетната страница.

Корисникот кој се најавува како доктор може да креира термини кај одреден пациент и истите да ги избрише. Откако доктор ќе креира термин тој се сместува во соодветната табела кај пациентот за кој е наменет, а и во табела за термини кај соодветниот доктор. По завршувањето докторот се одјавува и се враќа на почетната страница.

Корисникот кој се најавува како администратор може да креира нови и брише постоечки термини кај било кој пациент или доктор.



Слика1: Почетна страница

Е - лекување

06.03.2021, 13:38:05


Најава на системот за пациенти

Најавете се на системот со внесување на вашите корисничко име и лозинка:

Корисничко име

Лозинка

Најави се



Слика2: Најава за пациенти

Е - лекување

06.03.2021, 13:39:57


Најава на системот за доктори

Најавете се на системот со внесување на вашите корисничко име и лозинка:

Корисничко име

Лозинка

Најави се



Слика3: Најава за доктор

Е - лекување

06.03.2021, 14:17:40


Најава на системот за администратори

Најавете се на системот со внесување на вашите корисничко име и лозинка:

Корисничко име

Лозинка

Најави се



Слика4: Најава за администратор

Е - лекување

06.03.2021, 14:05:39

Закажете термин

Изберете пациент

00000 Bojko Ban ▾

Изберете доктор

1 Bob Bob ▾

Внесете датум и време на преглед (пр. 2021/02/28 12:15)

Локација на прегледот

Закажи термин

Слика5:
Администратор
закажува термин

Е - лекување

06.03.2021, 13:43:09

Закажете термин

Изберете пациент

00000 Bojko Ban ▾

Внесете датум и време на преглед (пр. 2021/02/28 12:15)

2021/02/28 12:15

Локација на прегледот

Soba 23

Закажи термин

Слика6: Доктор
закажува термин

Е - лекување

06.03.2021, 13:42:08

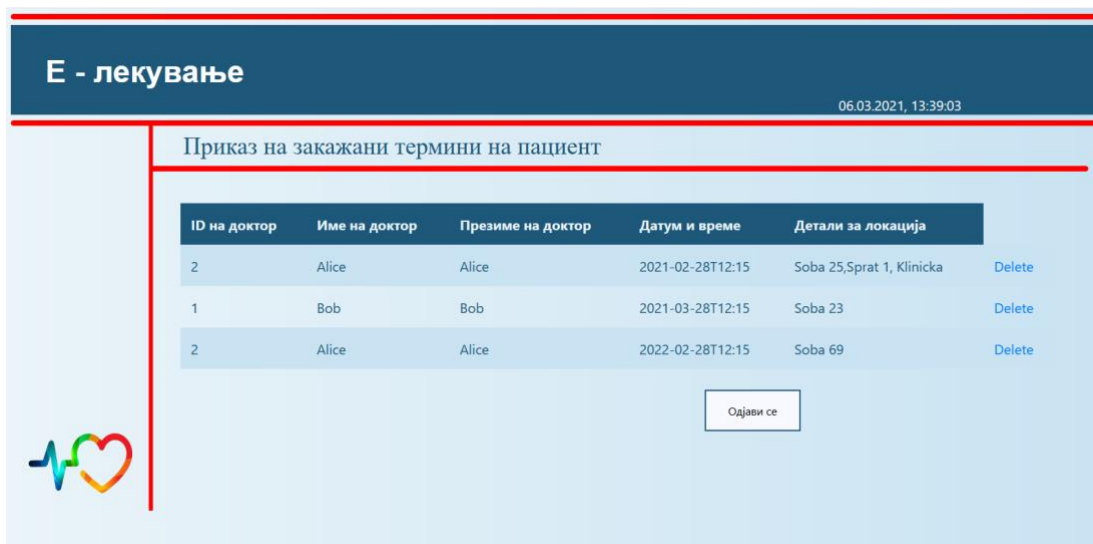
Приказ на закажани термини на доктор

ID на пациент	Име на пациент	Презиме на пациент	Датум и време	Детали за локација	
0	Bojko	Banana	2021-03-28T12:15	Soba 23	Delete

Закажи термин

Одјави се

Слика7: Приказ на
термини кај доктор



Слика8: Приказ на термини кај пациент

- Безбедност

Нашиот систем поддржува 3 типа на корисници: администратор, пациент и доктор. Различните улоги имат различни пермисии.

Пациентот може само да гледа веќе закажани термини кои се однесуваат за него.

Докторот може да ги разгледува сите термини за неговите пациенти. Додатно може да креира нови термини и да брише термини, но само неговите. Ако се обиде да избрише нешто во термин што не е негов ќе му биде вратена грешка.

Администраторот може да ги разгледува сите термини, кај било кој доктор или пациент. Истите може да ги избрише или пак може да создаде нов термин.

Кај сите 3 типа корисници имаме основна (basic) автентикација која се состои од корисничко име (username) и лозинка (password). Освен основната автентикација, докторот и администраторот дополнително користат и mutual authentication со цел пристап на страните кои се наменети за нив. Mutual authentication е автентикација каде даден корисник се автентифицира со сертификат, односно корисникот му се претставува на серверот, но и серверот му се претставува на корисникот, т.е. има автентикација од двете страни.

Секој доктор и секој администратор имаат свој уникатен сертификат кои се сврзани со база, односно нивните соодветни кориснички имиња се сврзани. Поради ова не може да се случи администраторот со својот сертификат да се логира како доктор, односно да се логира во негово име.

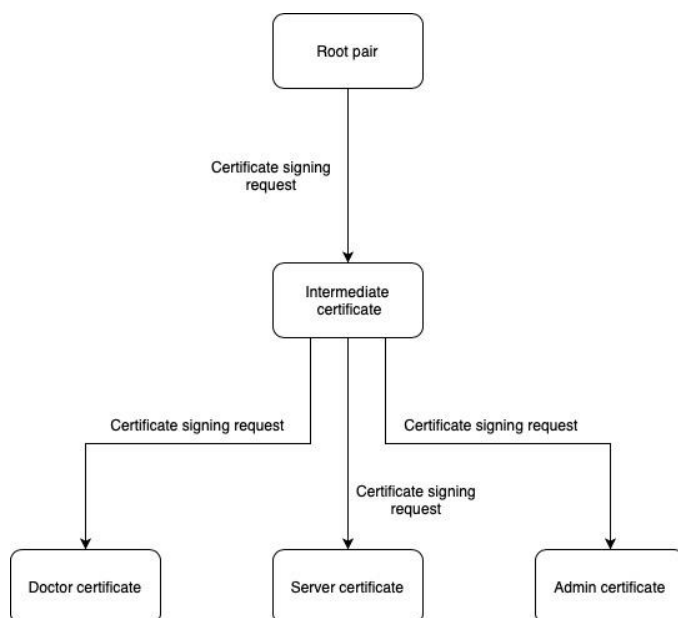
Сертификатите служат како прва линија на автентикација за докторот и за администраторот. Откако тие ќе го прикажат соодветниот сертификат, доколку е

прифатен, ќе треба потоа да се автентифицираат со внесување на нивното корисничко име и лозинка, соодветно.

Доколку има обиди за логирање со туѓо корисничко име и лозинка, освен тие што се назначени во одредениот сертификат, ќе се исфрли грешка и нема да се даде пристап на корисникот кој се обидува да се логира.

Архитектурата на нашиот систем, всушност е составена од два микросервиса:

- 1) првиот има https и ги поддржува операциите на докторот и на администраторот.
- 2) вториот има http, односно има еднослојна, основна, автентификација и е задолжен за пациентите.



Во нашиот систем генерирањето на сертификати се одвива така што првично се генерира root pair, односно генерираме основен пар приватни клучеви и сертификати. Root pair е главен, т.е. е корен од кој понатаму се генерира нов пар, intermediate pair. Тука исто се генерира приватен клуч со сертификат, но овој сертификат е потпишан од root pair. Ова го правиме за root pair да не биде директно изложен.

Intermediate pair понатаму се користи за да се генерираат и потпишат клиентски сертификати, а исто така и серверски сертификати (https).

- Напади

Нашата апликација е ригорозно отпорна на десетте најчести напади класифицирани од OWASP фондацијата

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE) – во ниту еден дел од нашата апликација не се процесира кориснички зададен XML
- Broken Access Control
- Security Misconfiguration.
- Cross-Site Scripting (XSS)
- Broken Access Control – во ниту еден дел од нашата апликација не користиме десеријализација
- Insecure Deserialization
- Using Components with Known Vulnerabilities – има основно логирање на пристап и queries на базата на податоци