

Регистрација и автентикација на корисници

Берат Ахметај [216130]

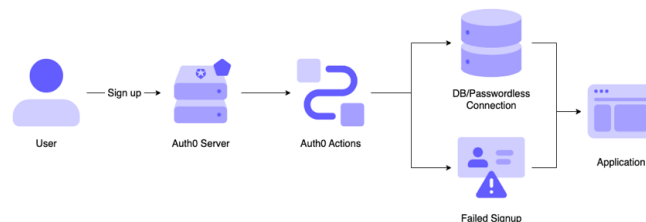
Факултет за информатички науки и компјутерско инженерство

Скопје

berat.ahmetaj@students.finki.ukim.mk

Апстракт: Во дигиталната ера, регистрацијата и автентикацијата на корисници стануваат неделиви делови од практично секоја онлајн платформа, обезбедувајќи безбеден пристап до услуги и заштита на податоците на корисниците. Оваа теза истражува предизвиците и можностите во регистрацијата и автентикацијата на корисници, со цел да се зголеми безбедноста и корисничкото искуство во дигиталните системи.

Клучни зборови – веб апликација, регистрација, автентикација, корисници, безбедност



слика 1 - Шема за регистрација и автентикација

II. Значењето на безбедноста во регистрацијата и автентикацијата на корисници:

I. ВОВЕД

Во дигиталната ера, корисничката регистрација и автентикација станаа неизоставни делови од практично секоја онлајн платформа. Овие процеси овозможуваат безбеден и приватен пристап до различни услуги и апликации, доколку се правилно изведени. Зголемувањето на бројот на корисници и онлајн податоци, како и појавата на нови технологии, предизвикуваат потреба за напредни и сигурни методи за регистрација и автентикација на корисниците. Стратегиите и механизмите за заштита на податоците и личната приватност постаа суштинска составница за успешната и безбедна дигитална комуникација.

Изјава за проблемот и истражувачките цели: Во овој контекст, проблемите поврзани со регистрацијата и автентикацијата на корисници се значајни и потребно е да се истражат и разрешат. Некои од најчести проблеми се слаба безбедност, недоволна заштита на личните податоци, компрометираност на корисничките сметки, недостаток на удобност и сложеност на постоечките методи. Ова истражување се насочува кон решавање на овие предизвици и претставува синтеза на најдобрите практики и техники за подобрување на безбедноста и корисничкото искуство при регистрацијата и автентикацијата на корисниците во дигиталните системи.

[1]

Безбедноста е од суштинско значење во контекстот на регистрацијата и автентикацијата на корисници во дигиталните системи. Оваа безбедност претставува важна составница за заштита на личните податоци и спречување на недозволен пристап и злоупотреба на корисничките сметки. Неколку аспекти искачуваат како повеќе значајни во ова поле:

Заштита на личните податоци: Корисниците при регистрацијата и автентикацијата ги даваат своите лични податоци, како што се името, адресата, лозинката и други. Безбедноста игра критична улога во заштитата на овие информации од погрешен пристап или неовластено откривање. Недоволно обезбедени системи можат да станат цел на хакерски напади и да доведат до компрометирање на податоците на корисниците.

Спречување на идентитетска кражба: Регистрацијата и автентикацијата служат како механизам за докажување на идентитетот на корисникот. Со недостатоци во безбедните методи, злонамерни личности можат да преземат или злоупотребуваат кориснички идентитети. Ова може да има сериозни последици, вклучувајќи финансиски загуби, оштетување на репутацијата и крајно нарушување на приватноста на корисниците. [2]

Зголемување на довербата и корисничкото искуство: Безбедноста на регистрацијата и автентикацијата ја зголемува довербата на корисниците во онлајн платформите и услугите. Кога корисниците ќе имаат повеќе доверба, тоа им помага да се чувствуваат безбедно и сигурно при користење на системот. Исто така, правилно имплемент

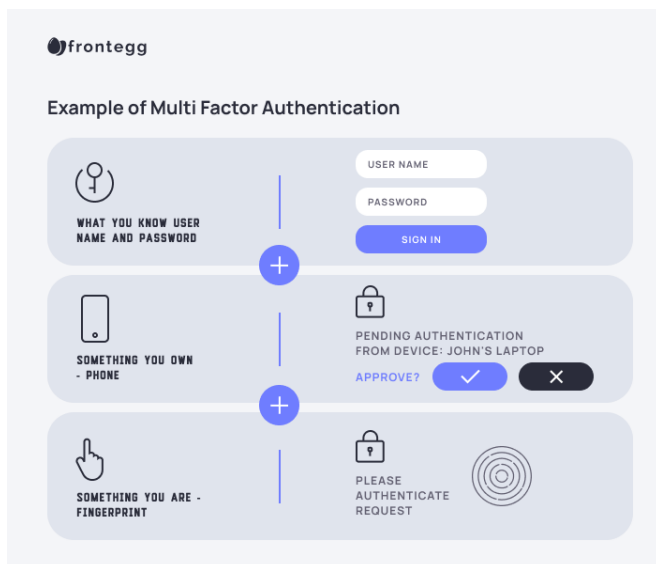
III. Типови на автентикација кои се користат во индустријата:

Лозинка-базирана автентикација: Оваа најраспространета форма на автентикација вклучува корисници да внесуваат лозинка за да потврдат својот идентитет. Лозинките треба да бидат комплексни, уникатни и безбедни за да се спречи неовластен пристап. Иако е широко користена, оваа метода може да биде подложна на ризици како лесно паметење на лозинките, лоши навики при изборот на лозинки или фишинг напади.

Двофакторска автентикација (2FA): Овој метод ги вклучува две независни форми на автентикација за да се потврди идентитетот на корисникот. Обично се комбинира нешто што корисникот знае (лозинка) со нешто што корисникот поседува (токен, SMS порака, мобилен апликација) или нешто што корисникот е (биометрија). Оваа форма на автентикација зголемува безбедноста бидејќи истовремено се бара нешто што знаете и нешто што имате. [3]

Биометричка автентикација: Оваа форма на автентикација користи физички карактеристики на корисникот за да го потврди неговиот идентитет. Примери на биометрички карактеристики вклучуваат препознавање на лице, скенирање на прстенот или ирис, гласовна идентификација итн. Биометријата овозможува посилна и безбедна автентикација бидејќи физичките карактеристики на корисникот се уникатни и тешко за подминување.

Картички за пристап (Access cards): Оваа форма на автентикација се користи во физички пристапни системи каде корисниците ги користат картичките за да се автентичираат и добиј



слика 2 - Мулти Автентикација

IV. Хеширање во системите за автентикација на корисници:

Хеширањето е важен технички процес што се користи во системите за заштита на лозинките и автентикација на корисниците. Во следниот текст ќе објасниме значењето и постапката на хеширањето на македонски јазик.

Хеширањето е процес на конвертирање на лозинката или било кој друг податок во кратен и непрепознатлив низ на знаци, познат како хеш. Оваа хеш вредност се чува во системот како дигест на претходно внесената лозинка и не може да се обратно претвори во почетната лозинка. Ова го чини безбедноста на лозинката, бидејќи хешот нема да раскрие оригиналната лозинка.

Кога корисникот се обидува да се автентичира, системот го зема внесениот хеш од базата на податоци и го споредува со хешот на внесената лозинка. Ако двата хешот се совпаѓаат, тоа значи дека внесената лозинка е точна и корисникот се автентичира успешно.

Хеширањето има неколку предности за безбедноста на системите:

- Омогукува непрепознатливо чување на лозинките во базата на податоци.
- Ја намалува веројатноста за компрометирање на лозинките поради неовластен пристап или хакерски напади.
- Осигурува безбедност при случај на пребарување на базата на податоци, бидејќи хешот не може да биде вратен во почетната лозинка.

How Hashing Works



слика 3 - Хеширање

Важно е да се истакне дека хеширањето не е безгрешно и дека одредени методи на хеширање можат да бидат подложни на одредени напади. Затоа е препорачливо користење на сигурни алгоритми за хеширање, како што се SHA-2 или bcrypt, за да се осигура максимална безбедност на автентикација

V. Развој и програмирање на систем за автентикација на корисници:

Дизајн и планирање

Идентификувајте потребите и барањата за автентикацијата на корисниците.

Дизајнирајте системска архитектура и база на податоци.

Планирајте функционалности и основни потреби на системот.

Креирање на кориснички интерфејс:

Дизајнирајте и развијте кориснички интерфејс што овозможува внес на податоци, како лозинка и корисничко име.

Обезбедете кориснички валидација и пораки за грешки при невалидни податоци.

Регистрација на корисници:

Креирајте формулар за регистрација со потребните полиња, како име, презиме, е-пошта и лозинка.

Извршете валидација на внесените податоци, вклучувајќи го хеширањето на лозинката пред зачувување.

Систем за складирање на податоци:

Користете безбедна база на податоци за чување на регистрираните корисници.

Заштитете базата на податоци од неовластен пристап, како што е користење на криптирање и контрола на пристапот.

VI. Имплементација на систем за автентикација на корисници во мобилни апликации за регистрација на студенти

Во денешно време, кога користењето на мобилни апликации стана неизбежна реалност, имплементацијата на систем за автентикација на корисници станува критична задача за апликации за регистрација на студенти. Овој систем ги обезбедува безбедноста и приватноста на корисниците, го ограничува неовластен пристап до приватните информации и ги дава на студентите контролата врз нивните лични податоци. Во оваа есеј, ќе се разгледа имплементацијата на систем за автентикација на корисници во мобилни апликации за регистрација на студенти.

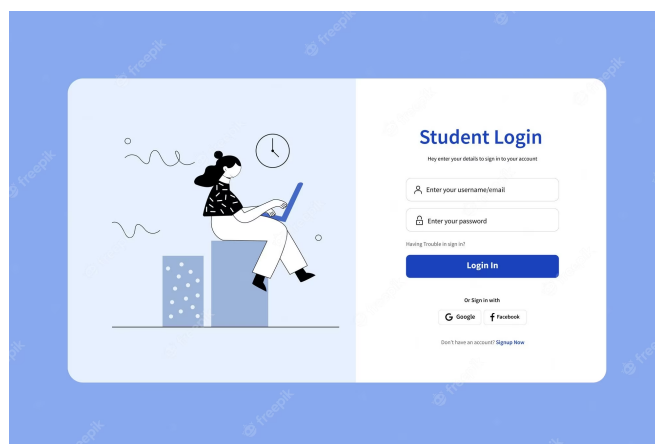
Првично, дизајнот на корисничкиот интерфејс игра значајна улога во имплементацијата на системот за автентикација. Дизајнот треба да биде прилагоден за мобилните уреди, со лесно снемвање и внес на податоци. Осигурете интуитивно корисничко искуство со употреба на елементи како формулари за внес на информации и копчиња за потврда.

Второ, имплементацијата на функционалноста за регистрација на студентите бара создавање на формулар со соодветни полиња за внес на информации како име, презиме, корисничко име и лозинка. За да се обезбеди безбедност на податоците, потребно е да се изврши валидација на внесените податоци и да се обезбедат пораки за грешки во случај на невалидни податоци. Потоа, регистрираните кориснички податоци треба да се зачуваат во безбедна база на податоци, која ја ограничува пристапот до нив само на овластени корисници.

Трето, имплементацијата на системот за автентикација ги обезбедува студентите со механизам за најавување во апликацијата преку корисничкото име и лозинка кои беа регистрирани. При најавувањето, е потребно да се изврши проверка на внесените податоци со зачуваните податоци во базата на податоци. За да се осигура дополнителна безбедност, може да се имплементираат и дополнителни методи за автентикација, како двофакторска автентикација или биометрички методи.

Имплементацијата на системот за автентикација мора да вклучува и мерки за безбедност и заштита од различни напади. Некои од примерите на мерки за безбедност вклучуваат заштита против SQL инјекции, XSS напади и brute force напади. Ова се постигнува со примена на безбедносни стандарди и алгоритми за хеширање и криптирање на податоците.

Важно е да се имплементираат и мерки за приватност на корисниците, како што е обезбедување на контрола врз нивните лични податоци и спроведување на соодветни политики за приватност. Корисниците треба да имаат можност да ги контролираат своите податоци и да имаат пристап до информации за начинот на користење и заштитата на нивните лични податоци.



слика 4 - Апликацијата за автентикација на студенти

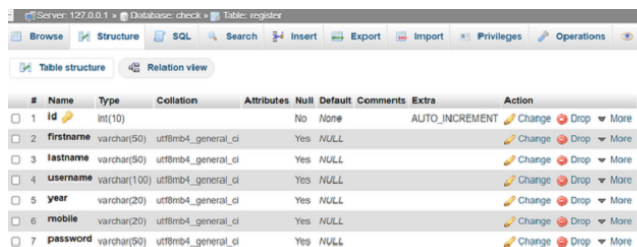
VII. Имплементацијата на системот за автентикација во апликацијата за студенти беше изведена со користење на SQL и PHP.

Првично, користејќи SQL, креиравме соодветна табела во базата на податоци за чување на информациите за корисниците. Табелата содржи полиња за корисничко име, хеш на лозинката и други потребни информации. Ова ни овозможува да зачуваме и пребаруваме информации за корисниците во базата на податоци.

Со помош на PHP, креиравме скрипти кои се поврзани со базата на податоци. Имплементиравме функции за регистрација и автентикација на студентите. При регистрацијата, внесените податоци од корисникот се процедираат, лозинката се хешира и се зачувува во базата на податоци за безбедно чување. При автентикацијата, корисникот внесува своето корисничко име и лозинка. Скриптата ги проверува внесените податоци со информациите во базата на податоци и дава пристап на студентот доколку се успешно автентичирани.

Овој систем со SQL и PHP ни овозможува да ги манипулираме и обработиме податоците на корисниците, како и да ги провериме нивните автентикациони информации. SQL ни овозможува да работиме со базата на податоци, додека PHP ни овозможува да го извршиме серверскиот код и да го врземе со корисничкиот интерфејс.

Имплементацијата на системот за автентикација со користење на SQL и PHP во апликацијата за студенти ни обезбедува безбедност и приватност на корисниците, со задоволување на нивните потреби и барања. [4]



#	Name	Type	Collation	Attributes	Null	Default	Comments	Extra	Action
1	id	int(10)			No	None		AUTO_INCREMENT	Change Drop More
2	firstname	varchar(50)	utf8mb4_general_ci		Yes	NULL			Change Drop More
3	lastname	varchar(50)	utf8mb4_general_ci		Yes	NULL			Change Drop More
4	username	varchar(100)	utf8mb4_general_ci		Yes	NULL			Change Drop More
5	year	varchar(20)	utf8mb4_general_ci		Yes	NULL			Change Drop More
6	mobile	varchar(20)	utf8mb4_general_ci		Yes	NULL			Change Drop More
7	password	varchar(50)	utf8mb4_general_ci		Yes	NULL			Change Drop More

слика 5 -Изгледот на табелата во SQL за информации за автентикација

VIII.. Клучевите во SQL и нивната важност во автентикацијата на корисниците во апликацијата за студенти

Во контекстот на автентикацијата на корисници во апликацијата за студенти, клучевите во SQL играат важна улога. Клучевите се користат за идентификација и побрза пребарување на податоци во базата на податоци. Тие ни овозможуваат да ги врземе податоците на корисниците и да ги провериме нивните автентикациски информации.

Еден од најчесто користените клучеви е примарниот клуч (Primary Key). Примарниот клуч е уникатен идентификатор за секој запис во табелата. Во контекстот на автентикацијата на корисници, примарниот клуч може да биде корисничкото име или некој друг уникатен идентификатор. Користењето на примарен клуч ни овозможува брза и ефикасна пребарување на податоците за конкретен корисник.

Дополнително, можеме да користиме и страни клучеви (Foreign Keys) за да ги поврземе податоците помеѓу различни табели. На пример, можеме да имаме табела за корисници и табела за роли. Со помош на страните клучеви, можеме да ги поврземе записите од двете табели, што ни овозможува да доделуваме одредени роли на корисниците.

Клучевите имаат голема важност во автентикацијата на корисниците во апликацијата за студенти поради нивните следни карактеристики:

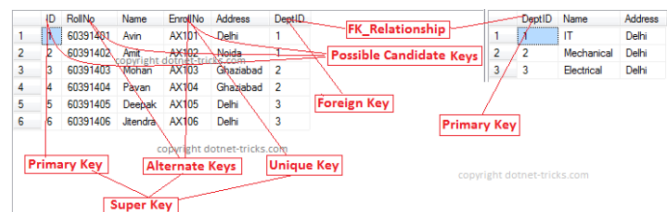
Уникатност: Клучевите мора да бидат уникатни за секој запис во табелата, што ни овозможува точна идентификација на корисниците.

Брзина: Клучевите ни овозможуваат брзо пребарување на податоците во базата на податоци. Со користење на индекси и правилно дизајнирани клучеви, можеме да оствариме ефикасно пребарување и автентикација на корисниците.

Заштита: Клучевите ни овозможуваат заштита на податоците и контрола врз пристапот до нив. Соодветно дизајнирани клучеви и правилна конфигурација на базата на податоци ни помагаат да ги заштитиме информациите на корисниците и да спречиме неовластен пристап.

Поврзаност: Преку страните клучеви, можеме да поврземе информациите од различни табели и да ги обезбедиме потребните поврзаности помеѓу нив. Ова ни овозможува да имаме комплетна слика за корисниците, нивните роли и дополнителни информации потребни за автентикацијата.

Во заклучок, клучевите во SQL играат критична улога во автентикацијата на корисниците во апликацијата за студенти. [4]



слика 6 -SQL Keys

IX. Заклучок:

Во оваа теза, ние истражувавме и разбравме значењето и техничките аспекти на регистрацијата и автентикацијата на корисници во дигиталната ера. Проучувајќи ги различните типови на аутентикација, техничките аспекти на системите за регистрација и автентикација, и важноста на безбедноста, ние го откриеме значењето на овие аспекти во развојот на безбедни и функционални системи.

Преку изучување на хеширањето, клучевите во SQL и важноста на безбедноста, ние го разбравме техничкото развој на системите за автентикација. Исто така, ги разгледавме методите за програмирање на системите за регистрација и автентикација со користење на SQL и PHP, што ни овозможува да го развиваме безбедни системи со приватност и контрола на пристапот.

Имплементацијата на системот за автентикација во апликацијата за студенти ни покажа конкретен пример на примена на концептите и техниките што ги изучувавме. Овој систем не само што ги задоволува потребите на корисниците, туку и им обезбедува безбедност и приватност при регистрацијата и пристапот до апликацијата.

Според заклучоците од истражувањето и имплементацијата, можеме да заклучиме дека регистрацијата и автентикацијата на корисници се критични аспекти во развојот на безбедни и функционални системи. Одбирањето на соодветни методи и техники, како и имплементацијата на безбедни системи, ни овозможува да ги заштитиме податоците и приватноста на корисниците, и да им обезбедиме сигурен и контролиран пристап до системите.

Во иднина, континуираното истражување и развој на технологиите и стандардите за регистрација и автентикација на корисници треба да биде во фокус на организациите и развивачите на апликации. Се очекува дека со текот на времето ќе се појават нови предизвици и напредни техники за автентикација, како што се двофакторската аутентикација, биометријата, и анализата на однесувањето на корисниците.

Овој истражувачки труд и имплементацијата на системот за автентикација во апликацијата за студенти имаат своја значајна вредност и примена. Се надеваме дека овој труд ќе биде исходна точка и водич за развивачите и организациите кои се заинтересирани за сигурноста и приватноста на своите корисници. Исто така, се надеваме дека ќе биде инспирација за идни истражувања и развој на нови и посовремени методи за регистрација и автентикација на корисници во мобилните апликации.

На крај, ова истражување потврди дека регистрацијата и автентикацијата на корисници се неопходни компоненти во развојот на сигурни и успешни апликации. Примената на правилни техники и методи за заштита на информациите на корисниците не само што го подобрува корисничкото искуство, туку и го гарантира поверението и лојалноста на корисниците кон апликацијата.

X. Референци

[1] *"Web Application Security: A Beginner's Guide" by Bryan Sullivan and Vincent Liu.*

[2] *"Authentication in the Digital Age: A Practical Guide" by Kelvin Coleman and Marko Komar.*

[3] *"OAuth 2.0 Cookbook: Protect your web applications using OAuth 2.0" by Adolfo Eloy Nascimento.*

[4] *"Secure PHP Development: Building 50 Practical Applications" by Tim Specht.*