Универзитет у Крагујевцу
Факултет инжењерских наука

Назив студијског програма: Машинско инжењерство

Ниво студија: Основне академске студије

Модул: Информатка у инжењерству

Предмет: Базе података

Број индекса: 196/2016

Стефан С. Голубовић

Сигурност база података

Завршни рад

Комисија за преглед и одбрану:

1. **Проф. др Милан Ерић**
2. **_____**
3. **_____**

Датум одбране:_____

Оцена:_____

Универзитет у Крагујевцу
Факултет инжењерских наука

Основне студије: Машинско инжењерство – Информатика у инжењерству

Име и презиме: Стефан Голубовић

Број индекса: 196/2016

ПРИЈАВА ЗАВРШНОГ РАДА

Тема рада: **Сигурност база података**

Задатак: Циљ завршног рада је да кандидат проучи литературу и презентира основне концепте заштите база података. Завршни рад треба да обухвати уводна разматрања, основне концепте заштите података са становишта администратора база података и становишта приступа подацима из апликативног софтвера, конкретне студијске примере и закључна разматрања.

Ментор:

Крагујевац, 31.05.2019

Проф. др Милан Д. Ерић

Изјава о самосталној изради рада

Изјављујемдасамовајзавршнирадурадиосамостално, служећи се стеченим знањем и искуством као и наведеном литературом.

196/2016 Стефан Голубовић

_____

(потпис)

Садржај:

1. Увод

База података су намењене за прикупљање, организовање, чување и манипулацију подацима на основу којих се добијају информације које су потребне крајњим корисницима. Обавезан су део савремених дистрибуираних апликација и омогућавају несметано извршавање конкурентних апликација које раде у реалном времену имају потребу за истовременим приступом подацима (унос, брисање, мењање, читање). Служе као подршка пословању као неизоставни део информационих система различите намене. Имају развијене механизме за опоравак података у случајевима отказа система или нарушавања самих података у бази. Базама података се може управљати на начин да се различитим корисницима могу дефинисати специфичне привилегије за приступ и коришћење података.

У базама података чувају се милиони заштићених података који су свакодневно изложени претњама споља и изнутра без обзира што се база података налази иза ватреног зида. Како би се подаци заштитили потребно је користити лозинке, додељивати права корисницима од стране админа, стварати backup-ове (чување података у случају да један део система откаже), користити сигурносне програме. Злонамерни корисници траже „рупе“ помоћу којих приступају заштићеним подацима. Приступити базама података омогућени су пенетрацијским тестовима. Пенетрацијски тестови служе за тестирање сигурности података на интернету, али и за искоришћавање рањивости базе података.

Базама података приступају удаљени корисници применом различитих технологија као што су Web читач (browser-и), дигитални телефони, говорни аутомати и сл. Због велике конкуренције у свим областима пословања, може се очекивати да технологија база података добије још већи значај. Менаџери траже начин да из базе података брже дођу до нових сазнања како би били у предности у односу на своју конкуренцију. На пример, детаљна база података о продаји се може искористити како би се сазнало који купци купују које производе, што се користи као основа за рекламу и маркетингшку кампању. Организације могу да укључе у своје базе података процедуре које се зову окидачи – тригери (alerts) који упознавају о могућим ванредним догађајима (као што су предстојећи недостатак залиха неке робе или шанса за продају додатне количине робе) и на основу којих могу настати одговарајуће реакције. Многе организације данас праве посебне базе података које се зову „складишта података“ које служе за апликације за подршку у одлучивању.

2. О сигурности

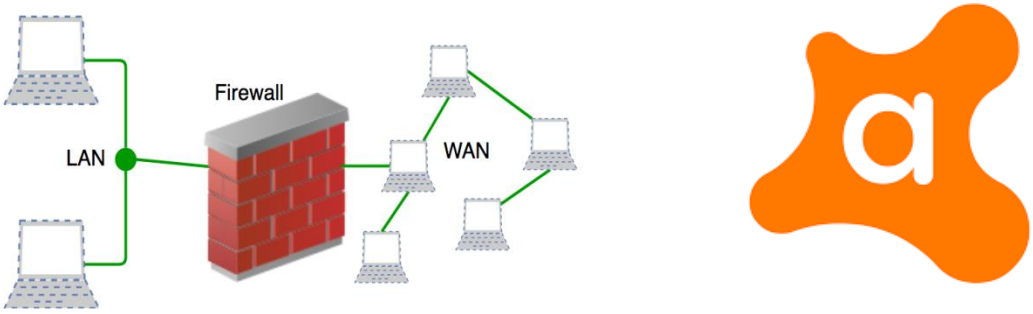
Сигурност на интернету означава тајност и целовитост, сигурност података, сигурност рачунара, тајност Web и mail промета и банкарских система.

За већу сигурност података потребно је на постојећи оперативни систем инсталирати одређене програме одбране од различитих врста злонамерних програма. Инсталацијом програма заштите подаци нису максимално сигурни па интернетска веза захтева одређени скуп одговорности одржања рачунара и коришћења.

Злонамерни програми нападају рачунаре без сазнања корисника тј. невидљиви су. Злонамерни корисници врше измене података, оштећење података, краду податке, нападају остале рачунаре, врше неовлашћени приступ на рачунар, приказе реклама, шаљу нежељене електронске поште (енгл. Spam) (Понављање истих лажних порука више од једног пута на сат или дан) и друго.

Минимална сигурност заштите података је:

- обавезно коришћење антивирусног софтвера (неки од бесплатних алата су Avast, Avira, AVG, PCTools, Comodoи сл.),
- чешће и редовно ажурирање антивирусног софтвера, скенирања рачунара једном недељно,
- Обавезно коришћење ватреног зида (енгл. Firewall).



Слика 1. *Ватрени зид (енгл. Firewall) и Avastантивирус.*

Интернет је највећи извор злонамерних програма. Злонамерни програми се налазе у крековима, генераторима кључева, серијским бројевима, торентима. Странице са торентима садрже ограничену регистрацију и мању могућност садржаја са злонамерним програмом. Корисник разне врсте злонамерних програма прима преко заражене датотеке скинуте са интернета, а понека и прегледом различитих страница.

Малициозни програми је појам који означује злоћудни софтвер тј. злонамерни код који врши категорију софтверских радњи усмерених на мрежне и различите податке. Такве радње обухватају црве, тројанце, бомбе итд.

Злонамерни програм израђен је да зарази оперативни систем, не извршава никакве акције, смештен је на нападнутом рачунару док други облици злоћудних програма, активирају и оштећују податке на тврдом диску (енгл. Hard Disk), уништавају оперативни систем или се смештају на остале рачунаре. Најчешће онемогућавају рад рачунара и шире се на остале рачунаре. Утврђивање зараженог рачунара има неке од ових „симптома“:

- учитавање програма траје дуже него обично,
- на тврдом диску појављују се стране датотеке или се постојеће бришу,
- величина програма је измењена,
- Web читач и програм за обраду текста се чудно понашају,
- рачунар се гаси,
- систем се не подиже.

Слика 2. *Хексадецимални запис вируса црва послата Бил Гејтсу од стране програмера вируса црв.*

Windows оперативни системи је најраспростанији на свету. Највише се користи и на мети су напада злонамерних корисника. Новим вестима прказани су откривени пропусти, нове могућности и искоришћавања таквих пропуста и нови напади.

Уз злонамерне програме на интернету, већи проценат пробоја сигурности узрок је проблема изнутра, у оперативном систему и опште заштити рачунара.

Многи ризици уклоњени су ажурирањем и надоградњом одређених програма и употребом одређених мера.

Слика 3. *Widows XP, Vista, 7, 8, 8.1, 10.*

3. Како се заштитити?

Лозинке користе сви корисници, без обзира на права и колико је информатички писмен. Коришћење лозинком започиње одабиром јаке лозинке која је дефинисана као лозинка коју није лако предвидети и задовољава критерије сигурности.

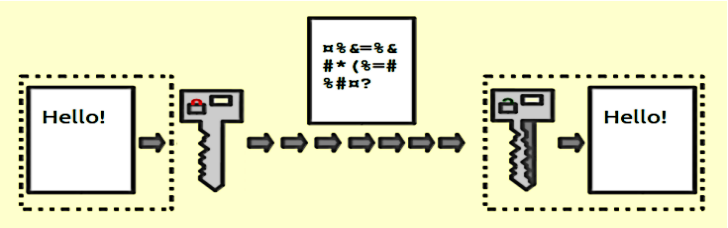
Смањење људске меморије узрок је појаве случајева у којима корисници записују лозинке на видљива места или покушавају сакрити спремајући је тада на мање видљива места.

Јака лозинка дефинисана је као лозинка која није лака за откривање било којем програмском алату у одређеном периоду, која је лако памтљива и тајна.

Карактеристике јаке лозинке, која није лака треба бити одабрана приказаним низом:

- минимална дужина 6 знакова,
- садржај комбинација малих и великих слова,
- садржај слова и бројева,
- садржај знакова интерпункције,
- садржај минимално једног специјалног знака,
- минимално четири различита знака која се не појављују,
- изглед као случајан низ одабраних знакова,
- мењање лозинке,
- различита од предходне и
- лака за памћење кориснику.

Енкрипција омогућава заштиту података мењањем самих информација, тако да је оригинални садржај видљив само особама које поседују кључ за декрипцију. На тај начин осигурана је и сигурна размена информација.



Слика 4. *Енкриптовање речи „Hello!“*

Сигурносне копије (енгл. backup) примењују се како би корисници осигурали немогућност губитка података, које касније не би могли вратити.

Брисање података је метода приликом које је извршено уништавање свих података на тврдом диску или неком дигиталном медију како не би дошло до откривања података након што уређај није употребљив.

Интегритет базе података значи чувати тачност и постојаност података. Тачност означава да сваки појединиподатак мора имати тачну вредност, док постојаност значи међусобну усклађеност између различитих података. Интегритет базе лако може угрозити погрешан рад апликација, погрешан рад оперативног система, погрешан упис непожељних корисника, погрешан рад базе података итд.

Интегритет података осигуравају тачност и постојаност података смештених у одређеној бази података. Постоје три врсте интегритета података: ентитетски интегритет, доменски интегритет и референцијални интегритет.

4. Сигурност база података

База података означава скуп међусобно организованих скупа података којима је потребан систем за управљање базама података (DBMS). Настанак базе података подразумева велику количину људског рада и труда. У базама података налазе се милиони информација из различитих подручја. Програми захтевају различите податке који се чувају, па подаци не смеју бити уништени или оштећени због техничких кварова, погрешних трансакција, непажње корисника или злонамерних радњи. Због тога се организације осигуравају са базама података јер такви системи прате, спремају и осигуравају приватне податке.

Због бољег разумевања дат је пример оштећене базе података. За рад са базом своди се покретање трансакција. Трансакција преводи базу из једног конзистентног стања у друго конзистентно стање. Пример таквих трансакција су банковне трансакције где се новац са једног рачуна пребацује на други рачун. Ако трансакција прекине са радом током пребацивања новца са једног рачунара на други, новац ће нестати или створити на неком другом рачунару. Зато база података мора осигурати опоравак података.

Осим података који се чувају, постоји неколико чињеница које доприносе рањивости базе података. Смештеност базе података је иза ватреног зида и изложен је различитим нападима. Осигурање базе података слично је осигурању рачунарских мрежа. У оба начина додељена су мања права кориснику, смањена је рањива површина, измене су стого пртаћене и систем је под надзором.

Рањивост база података могу произилазити из неисправних база података, програмиских пропуста или сигурносних недостатака унутар апликација повезаних са њима.

База података нема могућности заштите корисничког рачунара који је присутан код оперативног система. Првенствено се мисли на немогућност одређивања ваљаности корисничког рачунара. Рачунари и корисничке лозинке остају активне без икаквих промена.

У подручју управљања базама података није призната улога администратора за сигурност. Администратор базе података сам води рачуна о корисничким рачунарима и лозинкама и у исто време осигурава исправан рад и задовољавајуће перформансе.

База података има перформансе великих захтева и штедње диск простора. Због снижене ефикасности анализе одговорности је теже одредити. Метода надзора мора бити тачна, јер се бележи активност везана уз спремљене податке.

Одређеним апликацијама уграђен је сигурносни елемент, који занемарује базу података. Недостатак оваквог приступа је у томе што сигурности елементи делују само када корисник приступа бази података уз помоћ ODBC-а (енгл. Open Database Connectivity) или неког другог протокола који заобилази апликације са уграђеним елементима сигурности.

Програмским пропустима називају се грешке преписивања система које злонамерним корисницима омогућавају извођење напада базиране на ускраћивању ресурса или извршавању кода уз одређене последице.

База података је смештена иза ватреног зида, али га таква позиција не чини сигурним од напада. Постоји више врста напада који се изводе, а „убацивање“ SQL наредби је најчешћи.

„Убацивање“ SQL наредби није аутоматски напад на базу података, него представља покушаје мењања параметара који се шаљу апликацији са намером мењања SQL наредби која је послата бази података.

5. Елементи заштите база података

Исправан начин уклањања рањивости база података је уграђивање сигурносних елемената директно у бази података. Такви елементи садржавају коришћење методе надзора, пријављивања, надзор приступа над таблицама, примене лозинки и рачуна. Сигурност података извршена је на идентификацију власника објекта такође давању и узимању прави над објектима појединаца. Подаци се заштићују од приступа злонамерних корисника тако да само регистровани корисници могу имати приступ подацима.

Главна фаза заштите података је аутентификација тј. идентификација корисника. Корисничко име и лозинка потребна је за приступ бази података у процесу идентификације. Представљање корисника важно је да би започео рад са системом. Сви системи траже корисничко име и лозинку. Лозинке требају бити јаке и требају се редовно мењати како би се омогућила већа заштита од неовлашћеног корисника и провала у базу података. Израду таквих података извршава администратор и користи наредбу CREATE USER или CREATE ROLE, док наредба DROPUSER брише корисника. Системи имају више корисника на систему који раде са базом података, па није добро примењивати корисничка имена и лозинке на више корисника, нити да имају исте дозволе.

Неке базе података могу формирати задатог (енгл. default) корисника којег формира сам систем и такав корисник има све могућности на систему, задати корисник је претња јер свако може приступити систему преко задатог корисника који нема лозинку ни име.

Ако администратор направи корисника са корисничким именом и лозинком, како би радио унутар система, уноси податке (корисничко име и лозинку). Формирањем корисника потребно је дефинисати његове могућности, да ли постоји могућност израде таблице, новог корисника, додавања права. Након коришћеног имена израђује се лозинка.

Наредба CREATE USER је само друго име за CREATE ROLE која је наредба за формирање самог корисника. Разлика између наредби је да наредба CREATE USER подразумева да корисник може приступити бази података, док наредба CREATE ROLE омогућава кориснику да добије своја права, али не омогућава спајање на базу.

```
CREATE USER 'marko'@'192.168.1.6' IDENTIFIED BY '1234';

DROP USER 'marko'@'192.168.1.6';
```

„Last privilege“начело одређено је минималним правим корисника. Дефинисано је приступом само одређеним подацима базе који је потребан кориснику са обзиром на његов статус и улогу рада са базама података. Корисничким рачунима је додељена улога која представља поједина права за сваког корисника па је лакше додељивање и одузимање права корисницима који су везани уз радне задатке.

У права корисника спадају читање, брисање, ажурирање, уметање података итд. Појам овлашћења (права корисника) је способност извршавања наредби над објектима у бази података. SELECT права означавају да корисник користи таблицу само за читање. INSERT права омогућавају кориснику унос података у таблицу, а DELETE права омогућавају брисање одређених података. Права корисника додељена су наредбама GRANT и REVOKE.

Наредба GRANT омогућава додељивање различитих права кориснику или већем броју корисника. Таквом наредбом, одређују се права корисника (INSERT, DELETE, SELECT…) којом је дато право над базом, таблицом, функцијом итд.

```
GRANT SELECT,DELETE,INSERT,UPDATE ON tablica TO 'marko'@'192.168.1.6' WITH GRANT OPTION;
```

Наредба REVOKE узима овлашћења кориснику над таблицом, базом података, функцијом.

```
REVOKE SELECT,DELETE,INSERT,UPDATE ON tablica FROM 'marko'@'192.168.1.6';
```

Криптовање података је појам претварања података у облик којем нису погодни за читање и коришћење ако се пре тога не декриптују. Најчешћи разлог криптовања у базама података је шифровање података.

Шифровање података је један од сигурнијих облика за несигуран интернет. Корисник није увек у могућности прегледа података, зато се поидаци дефинишу за кориснике који имају приступ таквим подацима. Овлашћени корисник не може добити приступ подацима ни у читљивом ни у кодираном облику.

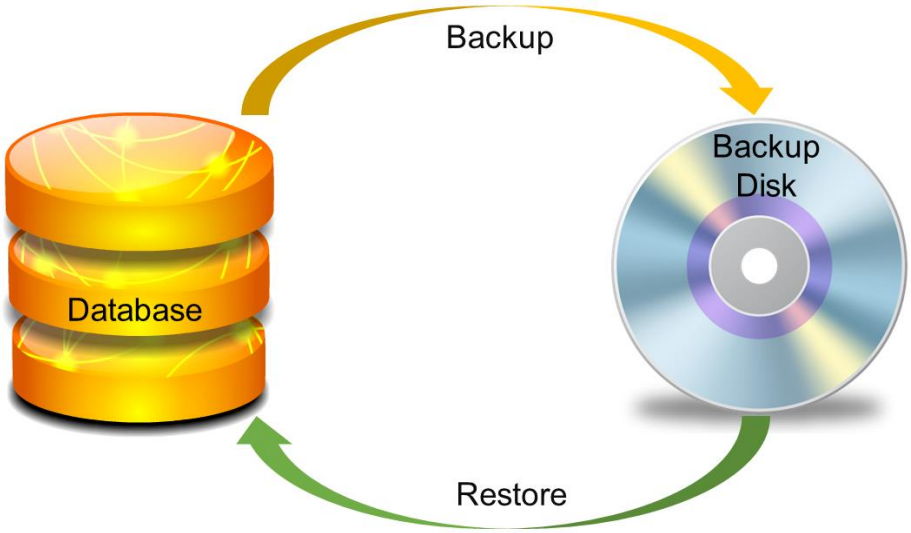
За време рада база података долази до недоступности базе или читање података. Недоступност базе података узрокује корисник уносом погрешних података и случајним брисањем података. Осим корисника друге проблеме са подацима могу изазвати грешке хардвера, администратора, проблеми са базом података, проблеми са оперативним системом. Спречавање оштећења података, ако дође до грешака, врши се копија базе података (енгл. backup).

Сигурност копије извршавају се када су корисници спојени на базу и изводе различите операције. Код копирања потребно је имати спремљене промене које су изведене док је копирање било у извршавању.

Сигурносна копија може се извршавати када је база постојећа. Када је база у постојећем стању копирање је брже и копирају се само подаци датотеке јер нема никаквих промена базе података. Такве копије називају се „cold backups“.

Приликом копирања базе података, потребно је одредити место смештања података. Копирани подаци се смештају на физичким уређајима за копирање. Уређаји за копирање могу бити USB, преносни диск, CD итд. За податке користе се дискови јер је брзина већа од брзине уређаја који користе магнетне траке.

Копирање се може обављати на више физичких уређаја, али под условом да се ради о уређају истог типа. Коришћење више уређаја може убрзати процес копирања података. Исти резултат копирања може се пребацити на више уређаја истовремено. На тај начин се креира копија и постиже се редоданца.



Слика 5. *„Backup“*

6. Напади и пропусти

Злонамерним коришћењем привилегија сматра се корисник који добије веће функције него што је потребно. Такав пропуст је одређен администратовим недостатком времена како би одредио које улоге корисник мора и може обавити.

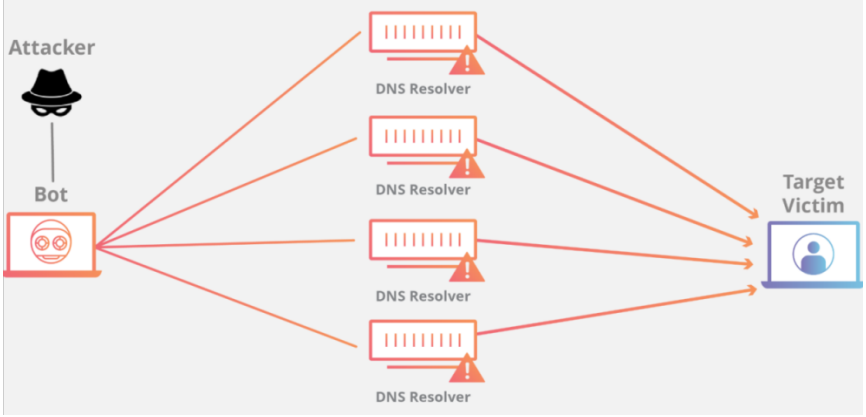
Решење таквог прпуста је аутоматско дефинисање улога код ограничавања приступа да би се радње онемогућиле и дојављивале администраторима.

Изменом права приступа базама података злонамерни корисници искоришћавају рањивост платформе. Такве рањивости налазе се у ускладиштеним процедурама, уграђеним функцијама, имплементацијама протокола и у SQL синтаксама.

Решење оваквог пропуста могуће је одређивањем права приступа и помоћу IPS-а.

Приликом напада SQL уметања злонамерни корисник убацује синтаксе базе података у рањиви SQL. Искоришћује се административно повезивање SQL синтаксе са корисничким подацима и умећу се SQL синтаксе. Уметнуте синтаксе се шаљу и обрађују у бази података.

„DOS“је напад који узрокује немогућност приступа ресурсима. „DOS“стање може се извршити преко техника као што су корупција података, мрежно преоптерећење, преоптерећење рачунарских ресурса и искоришћавање рањивости платформе на којој се база налази. Одбрана од „DOS“ напада извршена је коришћењем динамичког сервера који поставља различита руковања и ограничење извођења наредби. IPS и валидација протокола спречава злонамерне кориснике у искоришћавању програмских рањивости како би се изазвао „DOS“ напад.



Слика 7. *„DOS“ напад*

Неким базама података приступају се споља, што значи да база података нема механизме сигурности који управљају таквим приступима. Датотеке које се користе изложене су приступима споља. Ако датотеке нису заштићене, злонамерни корисници налазе начин да се подаци прочитају и неовлашћено приступају.

Приликом заштите датотека користе се сигурносни механизми за приступ датотекама, који су уграђени у оперативни систем.

7. Сигурности система за управљање база података

На тему сигурности система за управљање базом података описани су неки од најпознатијих система са нагласком на рањивости и заштиту самих система.

SQL сервер је систем за управљање базом података, развијен је од стране Microsoft-a. Као сервер базе података софтвер је са основном функцијом додавања и дохватања података према захтевима других апликација које се изводе на истом рачунару или на осталим рачунарима преко мреже.

SQL сервер имплементиран је као клијент сервер система или као самостални систем радне површине.

Клијент/сервер систем има двосложну или тросложну имплементацију. Са обзиром на имлементацију сервера и базе података, налази се на главном рачунару. Корисници користе удаљене рачунаре који се називају клијенти, а приступ базама података је помоћу апликација на клијент рачунарима (двосложна имплементација) или преко апликација које се покрећу на одвојеним рачунарима (тросложна имплементација).

У двосложним имплементацијама клијент покреће апликацију која приступа базама података директно преко мреже. Овакав систем је користан код малог броја корисника јер свака веза захтева мрежне ресурсе. Када долази до већег броја корисника двосложна имплементација постаје лоша, па је у таквим случајевима боље користити тросложну имплементацију.

Тросложна имплементација укључује апликацијски сервер, крлијент рачунара има задатак покренути захтеве на апликацијском серверу и приказати резултате. Предности тросложне имплементације јесте што може допустити апликацијском серверу организацију везе клијената и сервера база података, а не клијент сам одради свој део успостављања везе јер се троши ресурс сервера базе података.

SQL сервер може бити самостала сервер који се налази на радном или преносном рачунару. Клијент апликације се покреће на истом рачунару где је додат SQL сервер механизма или база података. У таквом систему постоји само један рачунар и нема веза клијент/сервер. Састав радне површине користан је где један корисник приступа бази података или више корисника, али не истовремено.

Провера идентитета сервера је обрада корисничких имена и лозинка.

Начини провере идентитета су:

- Windows 10 идентификација,
- Mixed.

Предности првог начина је што корисници не памте своја корисничка имена и лозинке, али је могзћност веће контроле сигурности података.

Идентификација се врши корисничким спајањем преко Windows корисничког рачунара, SQL сервер проверава кориснички рачун и лозинку користећи главну ознаку у оперативном систему. То значи да кориснички рачун потврђује Windows оперативни систем. SQL сервер не пита за лозинку и не обавља проверу ваљаности идентитета. Оваква

провера названа је поуздана веза јер SQL сервер верује подацима које нуди Windows оперативни систем.

Предности другог начина је што сваки корисник може приступити SQL серверу без обзира на мрежну библиотеку. Недостатак је имати више лозинки које стварају проблеме јер корисници са више лозинка записују податке, па је тиме систем мање сигуран.

За проверу идентитета корисник приликом Mixed начина отвара се Enterprise Manager и одабере картицу Security, а након тога одабран је SQL сервер и Windows 10.

Пријава омогућује кориснику приступ серверу, али не и ресурсима које он садржава.

Два типа пријавних налога:

- Windows 10,
- стандардни.

Пријава Windows 10 слична је стандардној пријави која је придружена појединцу, Windows 10 групи коју је израдио администратор и стандардна група.

Стандардна пријава извршена је када корисник нема могућност приступа поузданој вези са сервером. Израда такве пријаве врши се тако да отварањем Enterprise Manager-a, отвара се картица Security и Login. Након тога је одабрана картица Action и New login. У поље Name уписује се име, а у поље Password жељена лозинка. За поље Database одабирају се Pubs и на крају у поље Confirm new password уноси се лозинка.

Приликом извођења мешовите идентификације лозинке се сачувавају на различи локацијама. Лозинке се штите јаком енкрипцијом и имају високи ниво ограничења. Остале лозинке се штите ниским нивоом енкрипције и граничења. Прегледом системских таблица и процедура злонамерни корисници откривају где и како се лозинке сачувавају. Злонамерни корисник кроз неовлашћену улогу добија корисничка права убацивањем „тројанца“ у систем. Када би то учинио мора имати „db_ddladmin“улогу и променити већ додељене процедуре. Када корисник са вишим правима покрене промењену процедуру, злонамерни корисник добија улогу „db_owner“. Корисник тада нема могућност приступа помоћу процедура које је створио администратор базе података.

Најпознатије рањивости SQL сервера омогућене су приликом ускраћивања ресурса (DOS). Ствара се привремена таблица која покреће петљу која је пуни. Привремене таблице се спремају у „tempdb“која се приликом пуњења таблице повећава и долази до престанка рада послужитеља.

SQL сервер може бити инсталиран на више Windows система датотека. Приликом инсталације препоручљиво је коришћење NTFS (система датотека) за SQL сервер и за датотеке са подацима јер се ограничава приступ одређеним датотекама. Приликом инсталације одабира се кориснички рачун који је додељен SQL серверу са тиме да се додавањем права ограничи могућност напада злонамерних корисника на SQL сервер.

8. Заштита базе података на Web-у

Web странице угрожене су сво време. Корисници тврде да њихова Web страница нема нешто вредно што је занимљиво злонамерним корисницима, али већина Web страница нису угрожене само како би се украли подаци, него да би се и слали spam-ови.

Дати су примери како заштитити податке на Web страницама:

- одржавање софтвера ажурираним – дат пример можда је очигледан, али омогућава софтверу покретање са Web страницом као што је CMS (систем који омогућава управљање садржајем)или форму. Када је сигурносна рупа у софтверу отворена подаци су на дохват руке злонамерним корисницима.
- SQL инекција – злонамерни корисник користи „терен“ Webобрасца или URL-а како би добио приступ или би извршавао манипулацију над базама података. Када се користи стандардни SQL упит, несвесно уметање лажног кода може користити за промену таблица, добитак информације или брисање података. Овакав начин заштите могуће је провести користећи параметре упита, а већина језика има већ овакву функцију.
- XSS – (енгл. Cross Site Scripting) када злонамерни корисник покуша заобићи JavaScript или друго скриптовање кода у Web образац, приликом израде најбоље је да се провере подаци који се доносе и кодирају или скидају из било којег HTML-а.
- Error поруке – Пажљиво руковање са информацијама које су приказане на порукама грешака.

Нпр. треба размишљати о језику који ће бити приказан приликом неуспеха у покушају пријаве. Најлакше је користити генеричке поруке попут нетачно корисничко име или лозинка како се не би навело када је корисник успео погодити пола упита. Ако злонамерни корисник покуша груби напад како би добио корисничко име или лозинку, не би било пожељно да када погоди један упит па да се може концентрисати на други.

- Провера тачности – провера се извршава на страни претраживача и на страни сервера. Претраживач разуме једноставне кварове попут поља која су празна и када се унесу бројке у поље за текст. Препоручљива је провера исправности свих података и на страни сервера, а као недостатак провере долази до уметања злонамерног кода који је уметљив у базу података или може изазвати нежељене резултате.
- Лозинке – корисници користе сложене лозинке, али се не придржавају правила. Неопходно је коришћење јаких лозинка на серверу и Web страницама админа, али је једнако важно инсистирати на јаким лозинкама осталих корисника због заштите корисничких рачуна. Лозинке се чувају као шифроване вредности, коришћењем барем једног алгоритма као што је SHA.
- Постављање датотека – могућност дељења датотека може бити велики ризик. Ризик је било која дељена датотека која у потпуности отвара Web страницу. Решење сигурне методе дељења датотека је коришћење преноса на серверу са SFTP или SSH.
- SSL протокол – протокол за коришћење сигурности на интернету. Препоручује се користити сигурносни сертификат када се прилази подацима између Web страница и сервера или базе података. Злонамерни корисник прегледа информације комуникацијског медија који није сигуран па користи информације како би омогућио приступ корисничким рачунарима и личним подацима.
- Сигурносни алат – тестирање. Најефикаснији начин је путем коришћења сигурносних алата који се често називају пенетрацијски алати или оловке за тестирање на кратко

Приликом извршавања администрације постоје задаци који се понављају, као што је израда сигурносних копија, трансфери података, почетна организација, покретање скрипти. Такви задаци изводе се према редоследу. Аутоматизације података је корисно јер се смањује количина посла администраторима, мање су могућности грешака, ако се догоди грешка административни подаци се заустављају.

Аутиматизациони задаци садрже акције у којима је потребна већа привилегија унутар база података и оперативног система. Такве скрипте мењају податке на бази или спољним програмима који бришу датотеке са диска па је осигуравање података неопходно како злонамерни корисници не добијају право извођења акција на које заправо немају дозволу.

Спречавање извођења неовлашћених задатака препоручљиво је направити следеће:

- постављање корисника у одговарајуће уграђене сигурносне групе,
- онемогућити право покретања туђих задатака ако није потребно,

- поставити сервис за аутоматизационе податке да се извршавају под неким корисничким рачуном са ниским привилегијама.

Пенетрацијско тестирање је метода анализе сигурности рачунарских система која симулира напад злонамерних корисника. Таква анализа укључује активну и детаљнију анализу рачунарских система и потрази за пропустима у дизајну, имплементацији и одржавању. Пенетрацијско тестирање омогућава осигурати следеће пропусте:

- финансијске губитке,
- рачунарске сигурности компаније (нпр. престанак сарадње)
- заштита личног интереса

„**Rapid7 Nexpose**“је скенер рањивости чији је циљ подупрети трајање циклуса управљања рањивости, укључујући и откриће рањивости као што је провера, класификација ризика, анализа утицаја, извештаји. „Nexpose“ је интегрисан са „Metasploit“ скенером који искоришћава рањивост.

Продаје се као самосталан софтвер или виртуална машина. Корисник интеракцију извршава преко Web претраживача.

„**Metasploid**“ је „open source“пенетрацијски алат за коришћење развоја и извршавања рањивости. Користи се за тестирање рањивости система како би се исти заштитили, а са друге стране се користи као „провалник“ за удаљене системе.

„Metasploid“ се користи на Unix и Windows оперативним системима.

„**SQLmap**“ је процес аутоматизације детекције и експлоатације пропуста SQL инекције и преузима сервер база података. „SQLmap“ долази са могућношћу детекције, као и низом својства пенетрацијског тестирања који имају распон приступа системом датотека до извршавања наредби на оперативном систему кроз „out-of band“ конекције. „SQLmap“ такође подржава процес повећања привилегија користећи Metasploit-ов„getsystem“ наредбу.

„SQLmap“ је један од најпопуларнијих и могућних алата за убризгавање SQL инекције. Када се SQLmap-у додаје рањиви URL он тада искоришћава удаљену базу података и узима податке као што су имена, таблице, колоне тј. све податке о таблицама.

„SQLmap“ писан је з Python-уи један је од најмоћнијих алата SQL инекције.

9. Закључак

Сигурност база података је опсежна тема која је важна данас јер је свет повезан са интернетом који преноси разнолике опасности. Избор правих технологија је битно за рад. Сваки систем за управљање базе података има рањивост и није могуће одредити који је најсигурнији или најрањивији међу њима. За сигурност система за базу података потребно је моного више информација, исправка и тестирања.

Што се тиче будућег развоја пенетрацијског тестирања, предподставља се да ће развој сигурносних рачунарских система остати нерешена. Пенетрацијско тестирање представља неколико техника које се у овом тренутку могу супротставити сигурносним претњама. Тестирање је започело као ручно, а данас је све више аутоматизовано.

Такви алати и методе данас се примењују у сврхе тестирања као и илегалне радње. Сврха рада била је показати основне начине напада како би се разумели сигурносни проблеми и на тај начин лакше заштитили подаци. SQL инекција је метода помоћу које се извршава напад на SQL упите. Таква метода је корисна јер се може предвидети и тестирати база података на Web-у и уочити њене грешке које се касније исправљају. Други алати као што је SQLmaркоји преузима сервере базе података и ради са SQL инекцијом је јачи и бржи. Помоћу њега аутоматски се може сазнати параметар који се убацује у базу података. SQLmaрдаје тачне резултате обраде и тестирања помоћу којих се касније долази до већих сазнања. Алати корисни и снажни као Nexposeпомажу да се открију слабије тачке мреже како би се заштитило од откривене рањивости. Врло је важно одржавати сигурност на вишем нивоу. Методологија пенетрацијског тестирања бави се решењем оваквог проблема сигурности и у овом тренутку представља најслабију тачку целог процеса. Пенетрацијско тестирање се јако брзо развија што пружа оптимистична очекивања за технике одбране рачунарског система и могућностима њихове злоупотребе.

10. Литература

[1] Предавања професора Др. Милана Ерића

[2] Бранислав Лазаревић, Зоран Марјановић, Ненад Аничић, Слађан Бабарогић, Базе података (2003.), Београд

[3] Семинарски рад „Сигурност базе података“, Марина Грубеша

[4] Семинарски рад „Базе података“, Драган Максимовић

[5] https://makseniteja.files.wordpress.com/2012/03/access-danijela.pdf, Октобар 2019.

[6] https://bib.irb.hr/datoteka/648415.1-DIPLOMSKI-Matija_Paravac.pdf, Октобар 2019.

[7] https://singipedia.singidunum.ac.rs › preuzmi › 41813-zastita-podataka-u-bazi, Октобар 2019.

[8] https://studenti.rs/tag/baze-podataka/, Октобар 2019.

[9] https://www.carnet.hr/usluga/abuse-sluzba/, Октобар 2019.

[10] https://sites.google.com/site/sigurnostinterneta/, Октобар 2019.

[11] https://www.f-secure.com/v-descs/vb_bi.shtml, Октобар 2019.