ЦЕНТЪР ПО ИНФОРМАТИКА И ТЕХНИЧЕСКИ НАУКИ

УЧЕБНА ПРОГРАМА

Утвърждавам:
Декан:

CS599

СИГУРНОСТ В БАЗИ ОТ ДАННИ

Приета: Протокол № 29 / 29.06.2023

Лектор: доц.д-р Веселина Жечева

АНОТАЦИЯ

Съвременните бази от данни съхраняват големи обеми от разнородни данни, често в разпределена, мрежова или Интернет среда, което води до повишени рискове, свързани с тяхната сигурност. Дисциплината има за цел да запознае студентите със заплахите и рисковете по отношение на информационната сигурност, свързани с базите от данни, както и с основните методи за защита. Дисциплината завършва със защита на курсова работа и изпит.

ОСНОВНИ ЦЕЛИ

Основна цел на дисциплината е да формира знания и умения у студентите за анализ и оценка на проблемите, свързани със сигурността на базите от данни.

След обучението си по сигурност в бази от данни, студентът ще:

- познава основните проблеми и дефинира концепцията за сигурност в бази от данни;
- анализира текущите заплахи и уязвимости в системите за управление на бази от данни;
- познава основни технически инструменти за криптография и сигурност на данните;
- познава процеса на изграждане на MySQL Security Lab;
- разбира концепциите за експлоатация на бази данни на Microsoft SQL Server и конфигурация за одит
- притежава умения за комбиниране на инструментите, за да поддържат различни изисквания за сигурност при обработка, съхранение на данни и комуникация

ПРЕДПОСТАВКИ

Дисциплината е заключителна в областта на информационните технологии и изисква предварителна подготовка на студентите по дисциплините Бази от данни, Анализ и проектиране на бази от данни Информационна сигурност, Програмиране, Компютърни мрежи и комуникации.

СТАТУТ И СТРУКТУРА

специалност	статут	Кредити	редовно обучение				задочно обучение			
			л	с	У	общ	Л	с	У	Общ
АД	задължителна	6	30	30		60	15	15		30

СЪДЪРЖАНИЕ НА КУРСА

Тема 1. Събиране и съхранение на данни. Сигурност на работното място. Поверителност и сигурност. Предизвикателства, свързани с анонимизирането на данни и компромиса между поверителността и полезността на данните.

Тема 2. Атаки срещу СУБД. Разпознаване и облекчаване на заплахи за бази данни. Видове атаки с изводи за бази данни. SQL/NoSQL инжекции.

Тема 3. Сигурност при съхранение на данни. Видове дисково съхранение. Процедури за управление на ключове за криптиране. Най-добри практики в управлението на ключове. Концепция за големи данни. Видове рамки за обработка на големи данни.

Тема 4. Технологии за сигурност в БД. Процес на изграждане на MySQL Security Lab. Анализ на архитектурата и експлойтите на MySQL

Тема 5. Криптография и защита на базите от данни. Сертификати и ключове. Цифрови подписи. Инфраструктура (Public Key Infrastructure). Сигурност на транзакциите. Протоколи.

СЕМИНАРНИ УПРАЖНЕНИЯ

Тема 1. СУБД и сигурност. Основни цели и практики.

Тема 2. Сигурност на MySQL. Основни положения. Сигурно съхранение на паролите. Защита на сървъра срещу атаки. Променливи на сървъра. Стартиране като администратор и обикновен потребител.

Тема 3. Сигурност на MySQL. Настройки и тестване след инсталацията. Контрол на достъпа и управление на акаунтите. Използване на криптирани връзки. Компоненти и плъгини за сигурност.

Тема 4. Сигурност на MS SQL. Сигурност на платформата и мрежата. Сигурност на обектите в базата. Сигурност на ниво ред и колона.

Тема 5. Сигурност на MS SQL. Сигурност на приложенията, използващи базата от данни. Криптиране на данните. Следене на процесите в сървъра.

КУРСОВА ЗАДАЧА

Курсовата задача се задава на всеки студент и съдържа задачи по анализ и оценка на текущите заплахи и защити за избрана от студента и консултирана от преподавателя тема. Всеки студент защитава курсовата си задача и получава оценка, характеризираща нивото на усвояване на учебния материал.

ПРЕПОРЪЧИТЕЛНА ЛИТЕРАТУРА

1. Christopher Diaz, Database Security: Problems and Solutions, Mercury Learning and Information, 2022.
2. Peter A. Carter, Securing SQL Server: DBAs Defending the Database, Apress, 2018.
3. Scott Gaetjen, David Knox, William Maroulis, Oracle Database 12c Security, McGraw Hill, 2015.
4. Gerardus Blokdyk, Database Security A Complete Guide, 5STARCooks, 2019.
5. Николай Манчев, Сигурност в Oracle Database/ Версия 10g и 11g, СофтПрес, 2009.
6. https://learn.microsoft.com/en-us/sql/relational-databases/security/
7. https://dev.mysql.com/doc/mysql-security-excerpt/8.0/en/security.html
8. https://www.tutorialspoint.com/database-management-systems-mysql/index.asp
9. https://www.ibm.com/topics/database-security

МЕТОДИ ЗА ОЦЕНЯВАНЕ

> Всеки студент разработва самостоятелна курсова задача, представляваща изследване на конкретен проблем в областта на защитата на корпоративните мрежи. Задачата включва самостоятелна разработка на определена тема от тематиката на дисциплината. Оценяват се реализацията и защитата на разработката - **до 30 т.** Критериите за оценяване на разработката са: оригиналност, задълбоченост на изследването, сложност на темата, представяне на разработката.

> За представяне на собствени идеи - **до 10 т.**

> За присъствия и участие в упражненията се получават **до 6 т.**

Изпитът е писмен и представлява тест с отворени въпроси, който се оценява с максимално **54 т.** Крайната оценка е комплексна и включва в себе текущ контрол на семинарните упражнения, оценка от курсовата работа и оценка от писмения изпит. За оформяне на оценката студентът набира точки, чиито максимална стойност е 100. Общата оценка се определя от сумата на точките през семестъра и от изпитната процедура:

36-50т. - Среден (3); 51-65 т. - Добър (4); 66-80 т.-Мн. Добър(5); 81-100 т.-Отличен (6).

Студентът трябва да има минимум 14 точки от контрола през семестъра и минимум 22 точки от изпитната процедура, за да му се формира положителна комплексна оценка.