МАЪЛУМОТЛАР БАЗАЛАРИДАГИ ЗАИФЛИКЛАРНИ АНИҚЛАШ ВА ТАҲЛИЛ ҚИЛИШ

Абдуллаев Азизбек Дониёрбек ўғли
ИИВ Академияси курсанти

Аннотация: Маълумотлар базалари ҳар қандай ахборот тизимининг асосий қисмини ташкил этади ва уларнинг хавфсизлигини таъминлаш киберхавфсизлик соҳасидаги устувор йўналишлардан биридир. Ушбу тадқиқотда маълумотлар базаларидаги заифликларни аниқлаш ва таҳлил қилиш усуллари, шунингдек уларни бартараф этишда қўлланиладиган техник ва методологик ёндашувлар муҳокама қилинади. Заифликларни аниқлашда автоматлаштирилган сканерлар, қўлбола тестлаш усуллари, ҳамда сунъий интеллект воситаларининг аҳамияти очиб берилади. Шунингдек, маълумотлар базаларида аутентификация, рухсат даражалари ва шифрлаш каби механизмлар орқали хавфсизликни таъминлаш муҳим жиҳат сифатида кўриб чиқилади. Инновацион таҳлил платформалари, маълумотларнинг махфийлиги ва яхлитлигини таъминлашда янги ёндашувлар тақдим этилади. Тадқиқотда маълумотлар базаларидаги хавфсизликнинг фуқаролар ахборотлари, ташкилотларнинг ишончли фаолияти ва қонунийликни таъминлашдаги ўрнига алоҳида эътибор қаратилган.

Калит сўзлар: Маълумотлар базаси, заифлик, хавфсизлик таҳлили, ахборот хавфсизлиги, SQL инъекцияси, аутентификация, шифрлаш, автоматлаштирилган сканер, сунъий интеллект, инновацион таҳлил, қонунийлик, маълумотларни муҳофаза қилиш.

Аннотация: Базы данных являются неотъемлемой частью любой информационной системы, и обеспечение их безопасности представляет собой одно из приоритетных направлений в сфере кибербезопасности. В данном исследовании рассматриваются методы выявления и анализа уязвимостей в базах данных, а также технические и методологические подходы к их устранению. Особое внимание уделяется использованию автоматизированных сканеров, ручному тестированию и применению инструментов искусственного интеллекта для обнаружения уязвимостей. Также анализируются такие аспекты, как аутентификация, уровни доступа и шифрование как важные механизмы обеспечения безопасности. Приводятся современные аналитические платформы и инновационные подходы к защите конфиденциальности и целостности данных. В исследовании подчёркивается значимость безопасности баз данных для защиты персональной информации граждан, надёжной работы организаций и соблюдения законности.

Ключевые слова: База данных, уязвимость, анализ безопасности, информационная безопасность, SQL-инъекция, аутентификация, шифрование, автоматизированный сканер, искусственный интеллект, инновационный анализ, законность, защита данных.

Маълумотлар базалари (МБ) ҳар бир замонавий ахборот тизимининг асосий элементларидан ҳисобланади. Уларда фойдаланувчи маълумотлари, бизнес транзакциялари, шахсий маълумотлар ва турли хил техник ахборотлар сақланади. Шунингдек, уларнинг хавфсизлиги жуда муҳим бўлиб, хатоликлар ёки муаммолар ҳаккерлар томонидан фойдаланиладиган заифликларга айланиши мумкин. МБнинг заифликлари муайян таҳдидларга олиб келиши мумкин, шунинг учун уларни аниқлаш ва таҳлил қилиш доимий равишда эътиборга олиниши керак. Бу мақолада маълумотлар базасидаги заифликлар, уларни аниқлаш ва таҳлил қилиш усуллари, шунингдек заифликларга қарши курашиш чоралари муҳокама қилинади.

Маълумотлар базасида учрайдиган асосий заифликлар. SQL инъекция (SQL Injection) инъекциялари маълумотлар базасини заифлаштиришнинг энг оммабоп усулларидан биридир. Бу ҳаккерлар томонидан фойдаланиладиган йўл, улар зарарли SQL сўровларини юбориш орқали базага кириш имконини топишади. Шу тарзда улар база маълумотларини ўғирлаш, ўзгартириш ёки олиб ташлашга муваффақ бўлишлари мумкин. SQL инъекцияларининг аниқланиши ва тўғри профилактик чораларни кўриш зарур.

Аутентификациянинг етишмаслиги Маълумотлар базасидаги аутентификация механизмларининг нотўғри ишлатилиши ҳам муҳим заифликни ташкил этади. Агар пароллар етарлича мустаҳкам бўлмаса ёки шифрлаш усуллари сўнгги хавфсизлик стандартларига мувофиқ келмаса, хакерлар тизимга киришлари мумкин. Шунингдек, аутентификация жараёнидаги хатоликлар ҳам ушбу заифликни оширади.

Ортиқча ҳуқуқлар ва ролларнинг нотўғри бошқарилиши. Маълумотлар базасига кириш ҳуқуқлари ортиқча ёки нотўғри таърифланган бўлса, фойдаланувчиларга маълумотларни сақлаш ёки ўзгартириш ҳуқуқлари бериш хавф туғдиради. Роллар ва ҳуқуқлар тўғри тартибга солинмаган бўлса, у ҳолда бу заифлик ҳам хавф остига олиб келиши мумкин.

Маълумотлар базасини ўрнатишдаги хатоликлар, автоконфигурацияларнинг сустлиги ёки хавфсизлик патчларининг ўрнатилмаганлиги маълумотлар базасининг хавфсизлигини заифлаштиради. Бундай хатоликлар МБга киришни осонлаштиради ва хакерлар учун йўл очади.

Маълумотлар базасидаги заифликларни аниқлаш учун бир нечта автоматлаштирилган воситалар мавжуд. Улар орқали МБни тезкор текшириш ва муаммоларни аниқлаш мумкин:

- **SQLMap** — SQL инъекцияларини аниқлаш ва эксплуатация қилишда самарали восита.
- **Nmap** — портларни, фойдаланилаётган хизматларни ва протоколларни аниқлаш.
- **Nessus/OpenVAS** — маълумотлар базаси ва серверларининг умумий хавфсизлик таҳлили.
- **Burp Suite** — веб-сайтлар орқали киришиш ва МБга йўналтирилган сўровларни таҳлил қилиш.

Қўлбола (manual) таҳлил автоматлаштирилган воситалардан ташқари, пентестерлар ёки хавфсизлик мутахассислари қўлбола усуллар орқали маълумотлар базасини текширади. Бу усулнинг афзаллиги шундаки, у муайян ҳолатларда аниқроқ ва мураккаб таҳлилни амалга оширади. Ҳакерлар фойдаланиши мумкин бўлган ноанъанавий усуллар қўлланилиши мумкин.

OSINT усуллари билан ёрдамчи маълумот йиғиш:

- **WHOIS, IP, DNS таҳлили** — сервернинг қандай ишлаши, қайси провайдерга мансуб эканлиги, ва бошқа техник маълумотлар.
- **Ижтимоий тармоқлар** — Фойдаланувчиларга оид маълумотлар топиш учун ижтимоий тармоқлардаги манбалардан фойдаланиш.

Заифлик аниқлангандан кейин, унинг хавф даражасини баҳолаш керак. CVSS (Common Vulnerability Scoring System) – бу заифликларни баҳолашнинг стандартлаштирилган тарзи бўлиб, у заифликнинг хавфини баҳолаш учун қўлланилади. Бу система заифликни аниқлаш ва хавфни камайтириш стратегияларини белгилашда ёрдам беради.

Маълумотлар базасидаги заифликларни аниқлаш ва бартараф этиш учун турли чоралар кўрилади:

- **Шифрлаш** — маълумотларни AES ёки RSA шифрлаш алгоритмлари билан шифрлаш орқали уларнинг хавфсизлигини таъминлаш.
- **Икки босқичли аутентификация (2FA)** — паролдан ташқари, фойдаланувчини тасдиқлаш учун қўшимча босқичлардан фойдаланиш.
- **Фойдаланувчи ҳуқуқларини чеклаш** — фойдаланувчиларга фақат керакли ҳуқуқларни бериш.
- **Патчларни мунтазам янгилаш** — маълумотлар базаси ва серверларини мунтазам янгилаш ва хавфсизлик патчларини ўрнатиш.

Маълумотлар базаларидаги заифликларнинг келажакдаги таҳдидлари ва уларга қарши курашиш. Маълумотлар базасидаги заифликлар доимий равишда ўзгариб боради, чунки хавфсизлик технологиялари ҳам

ривожланиб, янги таҳдидларга жавоб беришга мўлжалланмоқда. Қўшимча равишда, замонавий хавфсизлик таҳдидлари ва уларга қарши курашиш стратегияларини тўғри ишлаб чиқиш зарур.

Искусственный интеллект ва машинани ўрганиш (ML) технологиялари хавфсизлик таҳдидларини аниқлаш ва уларга жавоб беришда муҳим роль ўйнайди. МБдаги заифликларни аниқлашда машинанинг ўрганиш алгоритмларидан фойдаланиш имконияти кўпаймоқда. Масалан, бу тизимлар маълумотлар билан ишлашда нотўғри фойдаланиш усулларини аниқлаш ва ёлғон сўровларни тез орада бошқаришга ёрдам беради. Машина ўрганиш усуллари маълумотлар базасининг фаолиятини таҳлил қилишда хавфсизликка бўлган янгиликларни тўғри башорат қилиш учун самарали восита бўлиши мумкин.

Блокчейн технологиялари ҳам маълумотлар базаси хавфсизлигини таъминлашда муҳим рол ўйнашга бошлади. Маълумотларни блокчейнга интеграция қилиш орқали уларнинг хатарларга қарши қўриқланиши мумкин. Блокчейннинг ўзга ҳакерлар томонидан ўзгартириш ёки тўхтатишнинг имкониятини йўқ қилиши билан маълумотларни сақлаш ва етказиш жараёни янада хавфсизроқ бўлади. Бу технология, айниқса, муҳим маълумотларнинг хавфсизлигини таъминлаш учун самарали ва ишончли восита ҳисобланади.

Мақсадли фирмалар ва ташкилотлар учун маълумотлар базасининг хавфсизлиги нафақат ўзаро алоқаларда, балки интернет ва клауд хизматларида ҳам муҳим аҳамият касб этмоқда. Клауд хизматлари орқали маълумотларни сақлаш кўплаб компаниялар учун аёнли ҳамда самарали ечим бўлса-да, уларнинг хавфсизлигини таъминлаш ҳар доим ташвиш уйғотади. Шунинг учун, клауд сақлашда маълумотларни шифрлаш, аутентификация ва ҳуқуқларни текшириш механизмларини ишлатиш талаб этилади.

Zero Trust архитектураси орқали ҳар бир трафик ва фойдаланувчи текширилади ва хулоса чиқарилади. Маълумотлар базасини ушбу турдаги архитектурада ишлатиш, ҳар қандай таҳдидни ранжировкалаган ҳолда аниқлашга имкон беради. Ушбу ёндошув хавфсизликка янги қадам бўлиб, маълумотларга киришда ишончсизлик асосида бирлашган турли хил хатоликлар ва заифликлардан ҳимоя қилишда самарали.

Технологиялар ривожланган сари, маълумотлар базасидаги заифликларни аниқлаш жараёни ҳам автоматлаштирилади. Бунинг натижасида хавфсизлик мутахассислари маълумотлар базасини тезроқ ва самарали текшириш имконига эга бўладилар. Келажакда, машғулотлар ва тестлашлар кўпинча чегараларсиз автоматлаштирилган технологиялар орқали амалга оширилади.

Келажакда, роботлар ва дронлар ҳам маълумотлар базаси хавфсизлигини текширишда иштирок этиши мумкин. Ушбу қурилмалар ёрдамида физик

хавфсизликни сақлашга қаратилган тизимлар мавжуд. Масалан, ушбу роботлар бино ва сервер хоналарини кузатиш, шунингдек маълумотлар базаларига киришни баҳолаш учун фойдаланишлари мумкин.

Маълумотлар базасининг хавфсизлиги бўйича янги тенденциялар ишлаб чиқилади ва бўлиб ўтган шахсий ёки жамоавий таҳлиловий тажрибалардан олинган ўрганишлар ҳақида илмий тадқиқотлар тарқатилади. Ҳозирги кунда ҳамкорлик муҳити, хавфсизликни таъминлашда муҳим рол ўйнамоқда. Ҳар бир технологик жиҳатда янгиликлар ва ижобий тажрибаларни биргаликда жамлаш хавфсизликни катта даражада мустаҳкамлайди.

Маълумотлар базалари ахборот тизимларининг ажралмас қисмидир ва уларнинг хавфсизлиги жуда муҳим. Заифликларни аниқлаш ва бартараф этиш учун замонавий технологиялар, автоматлаштирилган воситалар ва қўлбола текширишлар самарали ёндошув бўлиши мумкин. Маълумотлар базасининг хавфсизлиги ташкилотнинг умумий хавфсизлиги билан боғлиқдир, шунинг учун унинг хавфсизлигини таъминлаш учун комплекс чоралар ва замонавий технологиялардан фойдаланиш керак.

Фойдаланилган адабиётлар:

1. *Рубинштейн Д.* ***"Безопасность баз данных: принципы и практика".*** *– Москва: ДМК Пресс, 2020.*
2. *Хаффман Б., Сталлинс М.* ***"SQL Injection Attacks and Defense".*** *– Syngress Publishing, 2016.*
3. *Павлов Д.* ***"Информационная безопасность: учебник для вузов".*** *– Москва: Академия, 2021.*
4. *Джонсон К.* ***"Database Security: What Students Need to Know".*** *– CreateSpace Independent Publishing, 2019.*
5. *Чесвик Б., Белловин С.* ***"Firewalls and Internet Security: Repelling the Wily Hacker".*** *– Addison-Wesley, 2003.*
6. *OWASP Foundation.* ***“OWASP Top 10: The Ten Most Critical Web Application Security Risks”*** *– https://owasp.org, 2023.*
7. *MITRE Corporation.* ***“Common Vulnerabilities and Exposures (CVE)”*** *– https://cve.mitre.org, 2024.*
8. *NIST.* ***“Database Security Guidelines”*** *– National Institute of Standards and Technology, https://www.nist.gov, 2023.*
9. *Offensive Security.* ***“SQLMap Official Documentation”*** *– https://sqlmap.org, 2024.*
10. *IBM Security.* ***“Modern Approaches to Database Security”*** *– IBM White Paper, 2022.*
11. *Коновалов А.А. Информационная безопасность баз данных: угрозы, уязвимости и методы защиты. – Санкт-Петербург: Питер, 2019.*

12. *Чирков С.Ю. Методы анализа уязвимостей в информационных системах. – Москва: Радио и связь, 2020.*
13. *Гришин А.В. Практическая кибербезопасность: от уязвимости до защиты. – Москва: БХВ-Петербург, 2021.*
14. *Cert.ru. Рекомендации по обеспечению безопасности баз данных. – ФГБУ НИИ **“Восход”**, https://www.cert.ru, 2023.*
15. *Cisco Systems. Database Security Best Practices. – Cisco White Paper, https://www.cisco.com, 2022.*
16. *Баранов П.А. SQL-инъекции: методы обнаружения и предотвращения. – // Журнал **“Информационные технологии”**, №4, 2021.*
17. *Google Cloud Security. Securing Cloud SQL databases. – Google Documentation, https://cloud.google.com/sql/docs/security, 2024.*
18. *Microsoft Docs. Best practices for SQL Server security. – https://learn.microsoft.com, 2024.*
19. *Oracle Corporation. Database Security Guide (Oracle 21c). – Oracle Documentation, https://docs.oracle.com, 2023.*
20. *Kali Linux Tools Documentation. SQLMap, Nmap, Metasploit usage for database security auditing. – https://tools.kali.org, 2024.*