РЕЗЮМЕ

Истеъмолчиларга сувни дискрет етказиб бериш шароитида ирригация тизимларида оптимал сув тақсимлаш учун канал бўлинмаларида сув оқимининг конвектив-диффузион, тўғри ва кинематик ҳаракати тенгламаларидан иборат сув тақсимлашнинг математик моделлари ишлаб чиқилди. Шунингдек, канал бўлинмаларидаги барча гидравлик параметрларни ҳисобга олган ҳолда тўлиқ ностанцион ҳаракат тенгламасининг математик модели ишлаб чиқилди.

РЕЗЮМЕ

В работе разработаны математические модели оптимального распределения воды в магистральных каналах ирригационных систем, которыми является модели прямой волны, кинематической волны, конвекционно-диффузная модель, а также полная модель неустановившегося движения потока воды на участке магистрального канала, которая учитывает все основные гидравлические свойства участка магистрального канала.

SUMMARY

In the work mathematical models of optimum water distribution in channels of irrigation systems under the conditions of discrete water supply to consumers have been developed. These include the models of direct wave, kinematical wave, convectional and diffusive model, as well as complete model of unsteady water flow in channel sections, that takes into account all main hydraulic characteristics of the channel section.

WEB ИЛОВАЛАР МАЪЛУМОТЛАР БАЗАСИ ХАВФСИЗЛИГИНИ ТАЪМИНЛАШДА SQL СЎРОВЛАР ЗАИФЛИГИГА АСОСЛАНГАН ТАҲДИДЛАРНИ БАРТАРАФ КИЛИШ УСУЛЛАРИ

Б.С.Самандаров – *техника фанлари бўйича фалсафа доктори*
Ш.Х.Тажибаев – *ассистент ўқитувчи*
Бердақ номидаги Қорақалпоқ давлат университети

Таянч сўзлар: WEB илова, SQL сўров, SQL инъекция, ахборот хавфсизлиги.
Ключевые слова: WEB приложения, SQL запрос, SQL инъекция, информационная безопастность.
Key words: WEB applications, SQL query, SQL injection, information security.

Бугунги кунга келиб корхона ва ташкилотлар маълумотларига ҳужумлар энг хавфли таҳдидлардан бири бўлиб бормоқда. Биргина 2019 йил III кварталида хавфсизлик бўйича мутахассислар томонидан тармоқда ҳимояланмаган маълумотлар базаси мавжудлиги ва унда 419 миллион Facebook фойдаланувчилари маълумотлари бор эканлиги аниқланган. Ушбу маълумотлар базаси маълумотлар йиғиш ва тахлил қилиш билан шуғулланувчи компаниялардан бирига тегишли эканлиги аниқланган [1].

Статистик маълумотларга кўра 2018 йилда маълумотларга тизимда юқори имтиёзларга (privilege) эга бўлган ходимлар (рахбарлар, тизим администраторлари) нисбатан кўпроқ хавф туғдирган [2]. Бу ўз ўрнида кўплаган компаниялар мурожаат имтиёзларини назорат қилишга етарли даражада эътибор қаратмаётганлигини кўрсатади.

1-расм. Ахборот тизимларига хавф туғдирувчилар тоифаси

Бугунги кунда ихтиёрий ташкилот ўзининг серверида катта хажмдаги маълумотларни бошқариш учун маълумотлар базасини бошқариш тизимига эга. Маълумотлар базасини бошқариш тизимидаги маълумотлар етарли даражада химояланган ва махфий маълумот ғаразгўй шахс томонидан бошқарилишини олдини олиш учун унинг заиф томонларини аниқлаш ва камайтиришга эришиш зарур [3].

Одатда ғаразгўй шахслар ички оператив маълумотларга, ходимларнинг шахсий маълумотларига, молиявий маълумотларга, буюртмачи ёки клиент хақидаги маълумотларга, интелектуал мулкга, тўлов маълумотларига қизиқади [4]. Бу маълумотлар эса корпоратив омборларда ва маълумотлар базаларида сақланади.

Бундан кўринадики, нафақат коммуникация тармоқлари ва операцион тизимлар хавфсизлигини, балки, маълумотлар базалари ҳам ғаразгўй шахслар хужумидан химояни талаб қилади. Буларни амалга оширишда маълумотлар базасини бошқариш тизими администраторлари ва ушбу соҳа бўйича таълим берувчи мутахассисларнинг асосий вазифаларидан бири фойдаланувчи (ўқувчи)ларни ахборот хавфсизлиги талабларини таъминлашга ўргатишдан иборат ҳисобланади [5].

Маълумотлар базасини бошқариш тизимига хавф туғдирадиган асосий омиллар компьютер тизимлари, дастурлар, қурилмалар ва фойдаланувчиларнинг мухитга мурожаат имтиёзларини тўғри ташкиллаштирмаслик билан боғлиқ.

Кейинги йилларда дастурий воситаларни яратишда тасирчан ўзгаришларнинг бир кўриниши web браузер стилидаги фойдаланувчи интерфейсларини ишлаб чиқиш бўлмоқда. Ўз ўрнида бунинг самарали афзалликларига махсус мижоз дастурий қатламларига бўлган эхтиёж бартараф этилиши, платформа танлови муаммосининг ечилиши ва энг асосийси дастурий воситага ҳохлаган жойдан мурожаат қилиш имкониятининг пайдо бўлиши киради [6,7]. Шунингдек, web иловалардан фойдаланишда килент томонда қандай операцион тизим ўрнатилганлигининг аҳамияти йўқ [8].

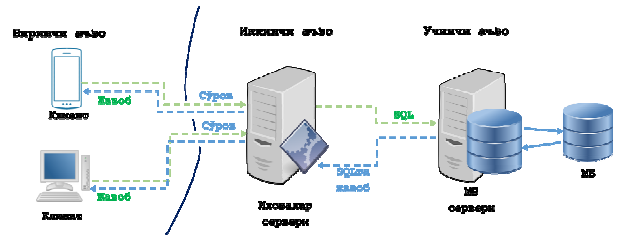
Веб технологиялари асосида фаолият кўрсатадиган дастурий воситаларнинг ташкил этувчиларини расмий равишда учта ўзаро мустақил турга ажратиш мумкин:

– мижоз томонда ўринланувчи модул – бундай дастурий воситалар браузерга мос хохлаган тилда ёзилиши мумкин;

– сервер томонда ўринланувчи модул – бундай дастурий воситалар танланган web сервер томонидан қўллаб-қувватланувчи тилларда ёзилиши мумкин. Кейинги вақтларда php тили кенг қўлланилмоқда;

– маълумотлар базаси – қаралаётган предмет соҳаси, дастурий воситаси ва бошқа параметрларга МБ кўра бажарилиши керак бўлган мақсад ва вазифалардан келиб чиқиб танланади.

WEBда ишлашга мўлжалланган дастурий воситалар архитектурасини яратишда иложи борича модуллар орасидаги боғлиқликлар камайтирилади. Бу маълумотларга таянган ҳолда модулларни браузер бошқарувида, web-сервер бошқарувида ишловчи ва маълумотлар базаси каби турларга ажратилади ҳамда умумлашган архитектура модели 2-расмдаги кўринишга эга бўлади.



2-расм. ДВ модул аъзолари боғлиқлик архитектураси

Юқоридаги боғлиқлик архитектурасига кўра икки хил алоқа модели келиб чиқади, яъни, браузер билан сервер орасида ва сервер билан МБ орасида алоқа. WEB технологиялари асосида ишлашга мўлжалланган дастурий восита модуллари фақатгина ўзига тегишли маълумотлар тўпламидан фойдаланади.

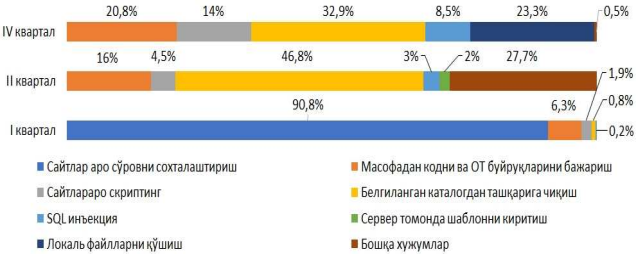
ДВ модул аъзолари боғлиқлик архитектурасига таянадиган бўлсак, клиент томондан юборилган сўровнинг таъсири иловалар серверидан ўтиб, то МБ сервери ва ундан жойлашган МБгача етиб келиши мумкин. Натижада ғаразгўй шахс томонидан серверга ўзгартирилган сўровлар жўнатишга имконият яратилиши мумкин. Одатда, web-иловалар орқали хужум қилишда SQL инъекциялар кенг қўлланилади.

SQL инъекция (SQL кодини киритиш хужуми, SQL сўровлар заифлигига асосланган хужум) – бу маълумотлар базалари билан ишлайдиган сайтлар ва web-иловаларни бузишнинг кенг тарқалган усулларидан бири бўлиб, у ғаразгўй шахсга маълумотлар базасига ихтиёрий сўровни бажариш (жадвал мазмунини ўқиш, ахборотни ўзгартириш ёки қўшиш), локал файлларни ўқиш ёки ёзиш ва серверда ихтиёрий буйруқларни бажариш имкониятини бериши мумкин.

Ғаразгўй шахс сервер томоннинг тузилишидан етарли даражада хабардор бўлмасдан туриб, маълумотлар базасига ўзбошимчалик билан сўров юбориши (ихтиёрий жадвалнинг маълумотларини ўқиб олиши, мавжуд қийматларини ўзгартириши, хаттоки ўчириши) мумкин. Одатда, кўпчилик учун қизиқиш пайдо қиладиган жадвалларни (масалан, user ёки users) ўқиб олишга харакат қилинади, бу эса ўз ўрнида тизимнинг маъмурий қисми логин ва паролини аниқлашга имкон беради. SQL инъекция – бу кросплатформали заифлик бўлиб, барча маълумотлар базасини бошқариш тизимларига таъсир кўрсатади (масалан, MySQL, Oracle ва х.к.) [3].

2018 йилда SQL инъекция ёки сайтлараро сктиптинг каби хужумлар 38 фоизга ўсган [9]. Жумладан, таълим жараёнига АКТнинг жорий қилиниши натижасида айрим талабаларда электрон журналларни бузиш, имтихон материалларини ўғирлаш каби ғаразли мақсадларни амалга ошириш орқали ўз баҳоларини ўзгартиришга харакатлар кузатилмоқда [10].

2018 йилнинг иккинчи ярмидан таълим соҳасига тадбиқ қилинган дастурий махсулотларга web-илова ёки серверни бошқариш ва маълумотларга мурожаат хуқуқини қўлга киритиш учун «Масофадан кодни ва ОТ буйруқларини бажариш», «Белгиланган каталогдан ташқарига чиқиш» ва «SQL инъекция» каби хужумлар улуши ортганлигини кузатиш мумкин.



3-расм. Таълим соҳасига татбиқ қилинган дастурий махсулотларга хужумлар

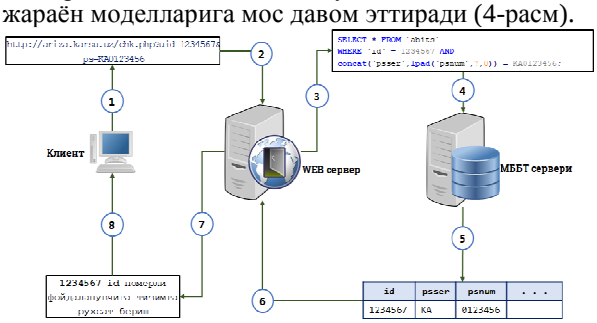
Юқоридаги маълумотларга таяниб, web-иловаларга нисбатан амалга оширилиши мумкин бўлган асосий SQL инъекцияларни ariza.karsu.uz тизими мисолида кўриб чиқамиз. Бунинг учун дастлаб, иловаларда SQL инъекцияларнинг пайдо бўлишининг асосий сабабларини аниқлаб оламиз.

SQL сўровларни динамик шакллантириш – усули дастурчилар томонидан иловаларни ишлаб чиқишда кенг қўлланилади. Қуйида ariza.karsu.uz тизимига кириш учун ишлаб чиқилган динамик сўров PHP тилида баён қилинган:

```
$query="SELECT * FROM `abits`
WHERE `id` = '".$uid."' AND
concat(`psser`,lpad(`psnum`,7,0))
= '".$ps."';";
```

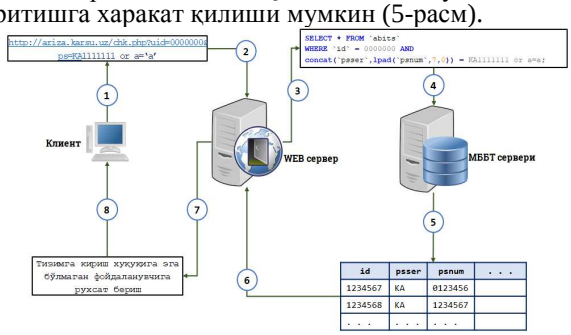
Дастурчилар орасида динамик сўровлардан фойдаланишнинг кенг оммалашишига асосий сабаб, уларнинг соддалиги ва фойдаланишга қулайлигида. Аммо, динамик сўровларнинг заиф шакллантирилиши SQL инъекцияларнинг келиб чиқишига имкон беради. Яъни, агар кирувчи маълумотлар етарли даражада текширилмаса ёки у маълумотлар базасини бошқариш тизимига қайта ишлашга жўнатилмасдан олдин кодланмаса, муайян шароитларда МББТ томонидан қўшимча буйруқлар сифатида қабул қилиниши мумкин.

Юқорида берилган кодга кўра, клиент томондан WEB серверга нормал сўров жўнатилса, ўз ўрнида PHP интерпретатор томонидан МББТ серверига жўнатилган SQL сўров тегишли тартиб қайта ишланиб, зарур жавоб қайтарилади ва WEB илова ўз ишини ишлаб чиқилган жараён моделларига мос давом эттиради (4-расм).



4-расм. WEBиловaнинг таҳдид кузатилмаган нормал иш жараёни модели

Ғаразгўй шахс хавфсизлиги таъминланмаган ахборот тизими устидан белгиланган хуқуққа эга бўлмасдан назорат ўрнатиш харакат қилиб, динамик шакллантириладиган SQL кодга қўшимча код киритишга харакат қилиши мумкин (5-расм).



5-расм. WEB иловaнинг SQL инъекция кузатилган ҳолатдаги иш жараёни модели

Юқоридаги ҳолат келиб чиқмаслиги учун клиент томонидан киритилган ҳар бир маълумот хавфсизликка текширилиши лозим. Бунда фойдаланувчи томонидан киритиладиган (юбориладиган) маълумотларни фильтрлаш талаб қилинади, яъни, махсус белгилардан қочиш, киритиш майдонларидаги маълумотларни аниқ турга конвертация қилиш каби усулларсамарали саналади.

Жумладан, ariza.karsu.uz ахборот тизимини SQL инъекциялардан фойдаланиб бузиб киришни олдини

олиш мақсадида, тизимга киришга имкон берувчи параметрларни МББТ серверига узатмасдан олдин ортиқча белги ва буйруқлардан тозалаш амалга оширилади:

```
function Fix($str) { //майдонларни тозалаймиз
    $str = trim($str);
    if(get_magic_quotes_gpc()) {
        $str = stripslashes($str);
        }
    return $str;
}

...
 $uid = Fix($_POST['uid']);
$uid = $mysqli->real_escape_string($uid);
$ps  = Fix($_POST['ps']);
$ps  = $mysqli->real_escape_string($ps);
...
```

6-расм. Фойдаланувчи киритган маълумотларни тозалаш

Ушбу тозалаш амалга оширилиши натижасида, ғаразгўй шахс томонидан ахборот тизими устидан назорат ўрнатишга қаратилган хужумни бартараф қилишга эришамиз.

SQL сўровлар заифлигига асосланган тахдидлар асосан WEB-иловалар орқали амалга оширилади. Шунга қарамасдан SQL сўровлар заифлигига асосланган тахдидлардан ҳимояланишнинг бир қанча усуллари мавжуд. Одатда тахдидларни бартараф қилиш қуйидаги иккита босқичда амалга оширилади:

1. WEB - илова кодини ўзгартиришга асосланган химоя босқичи;

2. WEB - илова кодини ўзгартирмасдан химояланиш босқичи;

Мақолада SQL инъекциялардан химояланишнинг фойдаланувчи киритган маълумотларни тозалаш орқали химояланиш усули баён қилинди. Албатта SQL инъекциялардан химояланишда хавфсизликни таъминлашга қаратилган бир қанча усулларидан [11,12] фойдаланиш мумкин. Бизнинг холат учун аутентификация ойнаси орқали киритилган маълумотлардан тозалаш етарли саналади.

Юқоридагиларга асосланиб қуйидаги хулосаларни қилиш мумкин. Қараб ўтилган усуллар орқали нафақат маълумотлар базаси хавфсизлигини, балки ташкилот ходимлари шахсий маълумотлари хавфсизлиги ва конфиденциал маълумотларни рухсатсиз тарқалиб кетишининг олди олинади. Маълумотлар базаси ахборот хавфсизлигини таъминлаш нуқтаи назаридан олиб қарайдиган бўлсак, маълумотлар базасига мурожаат имтиёзларини бошқариш дискрет назоратдан яхши ва самарали хисобланади.

Адабиётлар

1. III квартал: число утечек сократилось, но они стали опаснее. URL:https://www.infowatch.ru /resources/analytics/digest/16916 (мурожаат қилинган сана: 20.10.2019).
2. Исследование инцидентов информационной безопасности, связанных с действиями увольняющихся сотрудников, 2018. URL: https://www.infowatch.ru/resources/analytics/reports/17083 (мурожаат қилинган сана: 20.10.2019).
3. Клепцов М.Я., Любимова Л.В., Миронов М.М. Анализ угроз и уязвимостей СУБД Oracle // Вопросы кибербезопасности №2(26). –Москва: 2018,-С. 16-23.
4. Информационная безопасность бизнеса. Исследование текущих тенденций в области информационной безопасности бизнеса. 2014. URL: http://media.kaspersky.com/pdf/IT_risk_report_Russia_2014.pdf (мурожаат қилинган сана: 20.10.2019).
5. Самандаров Б.С., Бекназарова Г.Ж. MySQL маълумотлар базасини бошқариш тизимига мурожаатларни бошқариш // «Ҳозирги замон аниқ ва техник фанлар муаммолари ва уларнинг ечимлари» Республика илмий-назарий анжумани материаллари. –Нукус: 2017, 139-141-б.
6. Самандаров Б.С. Электрон ахборот ресурслар ҳолатини баҳолашнинг адаптив модели. //Узб.журнал «Проблемы информатики и энергетики». –Ташкент: 2016, №1. -С. 39-45.
7. Самандаров Б.С. Жумақулов А.Ж. Синдаров А.Э. MOODLE виртуал таълим тизими учун мониторинг юритиш тизимини яратиш. // Республика илмий-техник конференцияси – Ахборот технологиялари ва телекоммуникация муаммолари. –Тошкент: 2013, 85-87-б.
8. Астапенко Н.В., Носов А.А. Разработка web-приложения «мероприятия» для сайта кафедры ИС // Математические структуры и моделирование. 2014, № 4(32). -С. 152–156.
9. Akamai State Of The Internet / Security Summer 2018: Web Attack Report Shows Hospitality Industry Under Siege From Botnets. URL: https://www.akamai.com/us/en/about/news/press/2018-press/akamai-releases-summer-2018-state-of-the-internet-security-report.jsp(мурожаат қилинган сана: 05.11.2019).
10. Новосибирский школьник попался на взломе «электронного дневника». URL:https://www.securitylab.ru /news/489466.php(мурожаат қилинган сана: 06.11.2019).
11. Adam Shostack. Threat Modeling: designing for security. Wileypublication,2014.
12. Satapathy Soumya Ranjan. Threat Modeling in Web Applications. Thesis-NIT, Rourkela, 2014.

РЕЗЮМЕ

Мақолада динамик сўровлар заифлигига асосланган тахдидларни бартараф қилиш ҳамда улардан қандай химояланиш ariza.karsu.uz тизими мисолида қараб ўтилган.

РЕЗЮМЕ

В статье рассматривается как бороться с угрозами основанными на уязвимости динамических запросов и защита на примере системы ariza.karsu.uz.

SUMMARY

The article discusses how to deal with threats based on vulnerabilities of dynamic queries and protection on the example of using the ariza.karsu.uz system.

НОВЫЕ ДЕФОЛИАНТЫ НА ОСНОВЕ ХЛОРАТА НАТРИЯ, СОДЕРЖАЩЕГО ПОВЕРХНОСТНО-АКТИВНЫЕ ВЕЩЕСТВА

Ф.Э.Умиров – *доктор технических наук*
Г.Р.Номозова – *докторант*
Н.Ф.Сайфуллаева – *магистрант*
Навоийский государственный горный институт
Ф.И.Худойбердиев – *доктор PhD*
Нукусский филиал Навоийского государственного горного института

Таянч сўзлар: ишлабчиқиш, технология, кимёвий, дефолиант, хомашё, пахта, дефолиация, экология, иқтисод.
Ключевые слова: разработка, технология, химический, дефолиант, сырьё, хлопок, дефолиация, экология, экономика.
Key words: development, technology, chemical, defoliant, raw materials, cotton, defoliation, ecology, economics.

В мире при выращивании сельскохозяйственных культур отдельное внимание уделяется разработке технологии получения и использованию высокоэффективных, токсичных и безвредных химических средств на основе местного сырья или же отходов производства химической промышленности. Синтетическое удаление листов хлопчатника с использованием дефолиантов имеет важное значение при получении высокого, качественного урожая и уборки хлопка-сырца в короткие сроки. Успешное проведение дефолиации с обеспече-