МАСОФАВИЙ ЎҚИТИШ ТИЗИМЛАРИГА ҚАРАТИЛГАН ВЕБ ҲУЖУМЛАРНИ АНИҚЛАШ ВА БАРТАРАФ ЭТИШ АЛГОРИТМИ

Файзиева Дилсора Салимовна
Тошкент Ахборот Технологиялари Университети
E-mail: fayziyeva.dilsora@gmail.com

Ахмедова Наима Қодировна
Тошкент Ахборот Технологиялари Университети
E-mail: Naima212@mail.ru

АННОТАЦИЯ

ушбу мақолада, масофавий таълим тизимлари веб тизимлар шаклида амалга оширилгани боис, ундаги SQL инъекция хужум турлари тахлили ҳамда уларни аниқлаш ва бартараф этиш алгоритми таклиф этилади.

Калит сўзлар: SQL инъекция, тавтология, union сўровлари.

ABSTRACT

in this article, since distance learning systems are implemented in the form of web systems, SQL injection attack types are proposed in it, as well as an algorithm for their detection and elimination.

Key words: SQL injection, tautology, union requests.

Замонавий ахборот ва коммуникация технологиялари воситаларини таълим жараёнига кириб келиши анъанавий ўқитиш усулларига қўшимча равишда янги ўқитиш шакли - масофавий ўқитиш тизимидан фойдаланишга сабаб бўлди. Масофавий таълимда талаба ва ўқитувчи жойлашувидан бир-биридан ажралган ҳолда ўзаро махсус ишланган ўқув курслари, назорат шакллари, электрон алоқа ва Интернетнинг бошқа технологиялари ёрдамида доимий мулоқотда бўладилар. Интернет технологиясини қўллашга асосланган масофавий ўқитиш жаҳон ахборот таълим тармоғига кириш имконини беради, интеграция ва ўзаро алоқа тамойилига эга бўлган муҳим бир туркум янги функцияларни бажаради.

SQL инъекция заифлиги. Веб заифликлар орасида SQL инъекция энг катта улушга эга бўлиб, 2018 йилда энг машҳур 4 та иловада (масалан, Wordpress, Joomla, Drupal ва Magento) аниқланган SQL инъекция заифликлари сони ўтган йилларга қараганда 267%га ошган.

SQL инъекция ҳужумининг 8 та гуруҳи мавжуд [1, 2]:

Тавтология. Ушбу турда ҳужумчи SQL сўровнинг шарт қисмида (яъни, WHERE) зарарли код фрагментини киритади ва натижада сўров ҳар доим TRUE қийматни қайтаради. Ушбу ҳужумдан асосий мақсад аутентификация механизмини айланиб ўтиш ҳисобланади.

Ножоиз - мантиқий ножоиз сўровлар. Сўровни модификациялаш натижасида ҳужумчи синтактик, тип билан боғлиқ ёки мантиқий хатоликни юзага келтиради ва натижада маълумотлар базаси ҳақида қўшимча маълумотга эга бўлади. Ушбу маълумотлардан бошқа ҳужумларни амалга оширишда фойдаланилади.

Union сўровлари. Ҳужумнинг мазкур турида бузғунчи берилган сўровга UNION командаси билан бошқа сўровларни ҳам қўшади ва бир қанча натижаларни қўлга киритади. Ушбу ҳужум турини амалга оширишдан асосий мақсад маълумотлар базасидаги қўшимча жадваллардан маълумотларни олишдан иборат.

Эргаштирилувчи (Piggy-backed) сўровлар. Бу турдаги сўровлар ҳужумчига ҳақиқий сўровга камида битта қўшимча сўровни қўшиш имконини беради. Шу боис маълумотлар базаси бир вақтда кўплаб сўровларни қабул қилади.

Сақланган процедуралар. Сақланган сўровлар – бу такрорланувчи вазифани қамраб олувчи SQL сўровлари гуруҳи. Сақланган процедуралар, шунингдек, бошқа дастур, буйруқ қатори ёки бошқа сақланган процедура томонидан чақирилиши мумкин бўлган операцион тизим билан ўзаро мулоқот қилиш имконини беради.

Мулоҳаза. Ушбу турдаги ҳужумда дастур ва маълумотлар базаси фикр-мулоҳаза ёки хато хабарларни қайтаришдан ҳимоялангани боис, ҳужумчи инъекция натижасини билмайди. Мулоҳаза туридаги SQL инъекция ҳужумида ҳужумчи маълумотлар базасида сақланган ахборотни TRUE/FALSE шаклидаги жавобга эга саволлар бериш орқали олишга ҳаракат қилади.

Альтернатив кодлаш. Инъекциянинг аниқланишидан қочиш учун ҳужумчилар уни маълумотлар базасига юборишда турли кодлаш усулларидан фойдаланадилар. Илованинг ҳар бир қатламида кодлашни амалга оширишда турли ёндашувлар талаб этилади. Кодлаш ёрдамида илова сатҳида тақиқланган белгиларни маълумотлар базаси сатҳида ишга туширилувчи белгиларга алмаштириш амалга оширилади.

Иккинчи тартибли инъекциялар. Иккинчи тартибли инъекция ҳужумида ўзининг инъекция кодини маълумотлар базасида сақлаш учун ўзининг тайёрланган SQL сўровини маълумотлар базасига юборади. Ушбу инъекция коди маълумотлар базасида бошқа сўров натижасида қайтарилмагунча

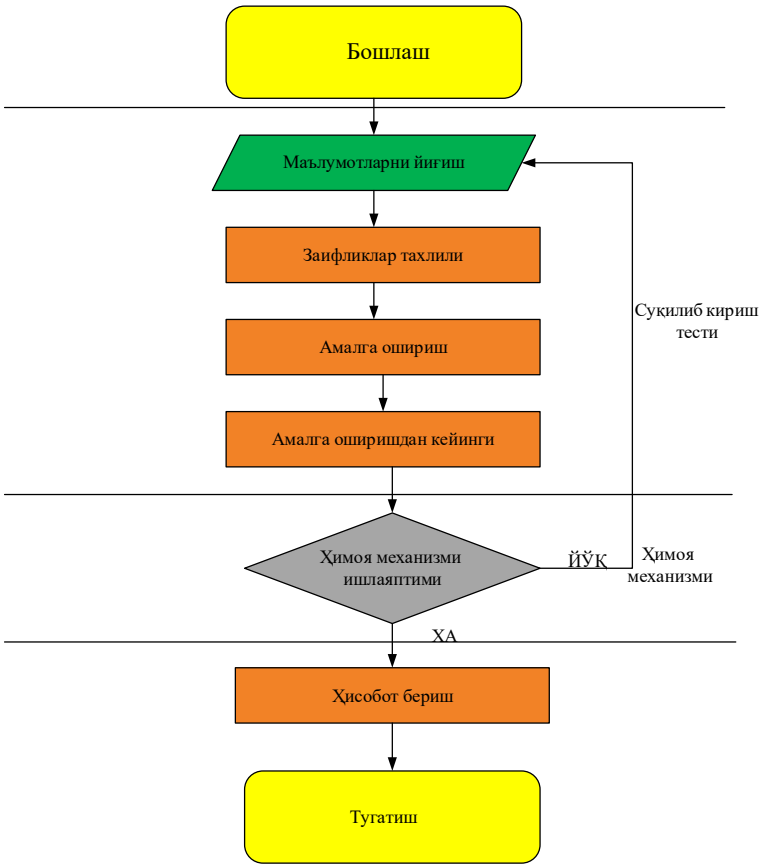
ҳаракатсиз қолади. Зарарли инъекция кодидан бошқа SQL сўровини яратиш учун хавфсиз фойдаланилади.

SQL инъекцияни олдини олишга қаратилган усуллар ва алгоритмлар статик ва динамик таҳлиллашга асосланган [3]. Биринчи ёндашувга кўра веб илованинг манба кодидан статик тарзда инъекция аниқланса, иккинчи ёндашувга кўра фойдаланувчи томонидан киритилган маълумотлар кузатилиб борилади ёки жоиз SQL сўровларининг профили яратилади.

Таклиф этилаётган алгоритм. Юқорида келтирилган заифликларни эрта аниқлаш учун қонуний фойдаланувчи томонидан суқилиб киришга асосланган тестлашлар амалга оширилади. Тестлаш натижаларидан олинган хулосалар асосида аниқланган заифликлар бартараф этилади.

Умумий ҳолда таклиф этилаётган веб заифликларни аниқлаш алгоритми учта босқичдан иборат:

1. Веб сервер ҳақида, хусусан, заифликларни қидириш, ҳужум турини аниқлаш ва ҳужум жараёнини ўз ичига олган, маълумотларни тўплаш.
2. Ушбу босқич веб тизимдаги заифликларни унга қаратилган ҳимоя тизимлари асосида бартараф этиш тартибидан иборат.
3. Сўнги босқич эса ҳимоя механизми ўрнатилган тизимда заифликни бартараф этилганлигини, ҳужум дарасини пасайганлигини текшириш амалга оширилади.



1-расм. Веб заифликларни аниқлаш ва бартараф этиш алгоритми

Ушбу босчиқларни ўз ичига олган алгоритм блок-схемаси 1-расмда келтирилган бўлиб, у бешта қадамдан иборат:

1. Веб сервер ҳақида маълумот йиғиш.
2. Заифликлар таҳлили - заифликларни сканерлаш, бўлиши мумкин бўлган ҳужум турини аниқлаш.
3. Амалга ошириш қадамида аниқланган заифлик асосида ҳужум бўлиши мумкинлиги ёки мумкин эмаслиги аниқланади.
4. Амалга оширишдан кейинги қадамда заифликларни бартараф этиш, ҳимоя механизмларини қўллаш ва қайта тестлаш амалга оширилади.
5. Ҳисобот бериш қадамида дастлабки ҳолат ва ҳимоя механизми амалга оширилганидан кейинги ҳолатлар бўйича таҳлил натижалари генерация қилинади.

Таклиф этилаётган алгоритмни амалга оширишда қатор воситалар талаб этилгани боис, уларнинг айримлар ҳақида қуйида айтиб ўтилади.

Маълумот йиғиш. Ушбу босқич мақсади муаммони аниқлаш ва кейинги қадам учун мос бўлган воситани тўғри танлаш. Ушбу босқичда мос ҳолда қуйидаги воситалардан фойдаланиш мумкин:

- NMAP (Network Exploration or Security Auditing) – пассив ахборот тўплаш воситаси;
- Whois (Who is lookup) – домен ҳақида пассив ахборот тақдим қилувчи восита;

Заифликлар таҳлили. Ушбу босқичда тизимли ва актив ёндашувлар танланиб, улар асосида заифликларни аниқлаш, таснифлаш ва тизим ичида даражаларга ажратиш амалга оширилади. Ушбу босқичда қуйидаги воситалардан кенг фойдаланиш мумкин:

- Nikto – веб иловалардаги хавфсизлик бўшлиқларини аниқлаш, заифликларни баҳолаш воситаси;
- Acunetix – турли платформаларда қурилган иловалардаги ҳар хил заифликларни аниқловчи, хавфлилик даражаси бўйича даражаларга ажратувчи восита.

Амалга ошириш. Ушбу босқичда турли воситалар асосида заифлик орқали ҳужум амалга оширилади. Масалан, XSS ёки SQL инъекция сўровлари веб илова ичига киритилади. Ушбу босқичда қуйидаги воситалардан фойдаланиш мумкин:

- Wireshark – трафик қайдловчиси;
- SQL инъекция сўровлари ёки XSS скриптлари.

Амалга оширишдан кейилги бочқич. Ушбу босқичда ҳужум амалга оширилган заифликни бартараф этиш учун ҳимоя механизмлари қўлланилади. Мазкур босқичда муаммони ечишнинг энг яхши усули заифликларга қарши

манба кодини тузатиш, махсус белгиларга нисбатан текширишларни амалга ошириш ҳисобланади. Ушбу босқич икки қисмбосқичда амалга оширилади. Дастлаб веб серверга хавфсиз кодни (тузатиш учун) қўшиш амалга оширилса, сўнгра амалга оширилган ҳимоя механизмининг муаммони бартараф этгани текширилади.

ФОЙДАЛАНИЛ АДАБИЁТЛАР РЎЙХАТИ: (REFERENCES)

1. Johannes Dahse and Thorsten Holz. 2014. Static Detection of Second-order Vulnerabilities in Web Applications. In Proceedings of the 23rd USENIX Conference on Security Symposium. 989–1003.
2. William G Halfond, Jeremy Viegas, Alessandro Orso, et al. 2006. A classification of SQL-injection attacks and countermeasures. In Proceedings of the IEEE International Symposium on Secure Software Engineering. 13–15
3. Rasoul Jahanshahi, Adam Doupé, and Manuel Egele. 2020. You shall not pass: Mitigating SQL Injection Attacks on Legacy Web Applications. In Proceedings of the 15th ACM Asia Conference on Computer and Communications Security (ASIA CCS '20). Association for Computing Machinery, New York, NY, USA, 445–457. https://doi.org/10.1145/3320269.3384760