VEB INTERFEYSGA QARATILGAN TARMOQ HUJUMLARINI ANIQLASH USULI VA ALGORITMI

Botirov Fayzullajon Baxtiyorovich
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
Ta'lim sifatini nazorat qilish bo'limi
botirov_fz@mail.ru

Ibroximov Azizbek Ravshonbek o'g'li
"Kiberxavfsizlik markazi" DUK, Axborot tizimlari va resurslari bo'limi
info@csec.uz

ANNOTATSIYA

Bugungi kunda axborot texnologiyalar ko'lami kattalashib borishi natijasida nisbatan qisqa davr ichida Internet foydalanuvchilariga turli axborot yoki xizmatlarni taqdim qiluvchi veb-ilovalar soni ham kundan kunga ortib bormoqda. Birinchi ishlab chiqarilgan an'anaviy veb ilovalar mavjud texnologiyalar yordamida turli qurilmalardan foydalanib ular bilan aloqa o'rnatish imkonini bergan bo'lsa, veb-ilovalar foydalanuvchilarini sonini deyarli doimiy o'sishi natijasida bunday tizimlarni ishonchli ishlashini ta'minlash muammosini keltirib chiqardi. Chunki ishlab chiqilgan texnologiya foydalanuvchilarga qulaylik yaratish bilan bir qatorda, ushbu texnologiyani boshqa tizimlarga integratsiya qilish natijasida axborot xavfsizligini ta'minlash tizimini samaradorligini pasaytirishi va tizim xavfsizligini buzilish holatigacha olib kelish xavfi paydo bo'ldi.

Kalit so'zlar: veb-interfeys, neyron tarmoq, cross site scripting, CSS, DOS, DDoS.

METHOD AND ALGORITHM FOR DETECTING NETWORK ATTACKS AIMED AT THE WEB INTERFACE

ABSTRACT

Today, as the scale of information technology increases, the number of web applications that provide various information or services to Internet users in a relatively short period of time is also increasing day by day. While the first traditional web applications produced made it possible to communicate with them using different devices using existing technologies, the almost constant increase in the number of users of web applications caused the problem of ensuring the reliable operation of such systems. Because in addition to making the technology developed more user-friendly, the integration of this technology into other systems resulted in the risk of reducing the efficiency of the information security system and bringing the system security to a state of disruption.

Keywords: web interface, neural network, cross site scripting, CSS, DOS, DDoS.

KIRISH

Bugungi kunda yaratilgan veb ilovalarni testlamasdan tizimga joylash orqali ya'ni veb serverni ishchi holatiga integratsiya qilib, foydalanuvchilar foydalanishi uchun imkon yaratish natijasida veb ilovani ishlab chiqishdagi mavjud kamchiliklar aniqlamasdan veb serverga muvaffaqiyatli hujum amalga oshirish imkoniyati mavjud. Bunday turdagi hujumlar veb serverdagi veb ilovalarning veb interfeysiga qaratilgan tarmoq hujumlarni amalga oshirish natijasida erishish mumkin.

ADABIYOTLAR TAHLILI VA METODOLOGIYA

Zamonaviy veb-ilova – bu foydalanuvchilar so‘rovlariga javoblarni generatsiyalovchi va katta hajmli ma'lumotlarni qayta ishlay oladigan dasturiy ta'minotdir. Veb-ilovalarni ishlashini murakkabligi apparat resurslariga yuqori yuklamalarga olib keladi, foydalanuvchilarni katta moqdori esa kompyuter hujumi uchun yaxshi o‘ljaga aylantiradi. Veb-interfeysga hujumlar turli maqsadlarda amalga oshirilishi mumkin, masalan, shaxsiy ma'lumotlarni o‘g‘irlash yoki foydalanuvchi kredit kartalari to‘g‘risidagi axborotni o‘g‘irlash kabi bunga misol bo‘lishi mumkin. Veb interfeysga qaratilgan hujumlardan ko‘zgangan asosiy maqsad hizmat ko‘rsatishni rad etish holatiga DOS yoki DDOS hujumlarni amalga oshirmasdan erishishdir. “Xizmat ko‘rsatishni rad etish” veb interfeysni to‘liq yoki qisman o‘chirish va foydalanuvchilarni undan to‘liq miqyosda foydalanish imkoniyatidan mahrum qilish hisobalanadi. Veb-interfeys infratuzilmasiga yo‘naltirilgan hujumlardan himoyalanishni amalda foydalanib kelinayotgan quyidagi usullari mavjud [1]:

- ma'lumotlar parametrlarini chetlash usuli;
- ehtimoliy ma'lumotlarni parametrlarini o‘zgartirish usuli;
- ma'lumotlarni intellektual tahlilidan foydalanib aniqlash usuli;
- signaturalar bo‘yicha yo‘llarni qayta tiklash usuli;
- paketlarni markirovkalash usuli;
- xizmatlar paketlarini generatsiyalash usuli shular jumlasidandir.

Ushbu usullar ilova sathida amalga oshirilgan veb-interfeysga hujumlarni tahlil qilish uchun yaxshi qo‘llanilmaydi. Buning sababi, zamonaviy veb-ilovalarning turli tarkibiy qismlari apparat resurslaridan foydalanish va integratsiya qilishda juda katta farq qilishi, shuningdek, zamonaviy veb-ilovalar kurish uchun mavjud bo‘lgan sahifalar sonini doimiy ravishda ortib borishidir. Ilova sathida, Xizmat ko‘rsatishni rad etish kabi hujumlar veb-interfeysga turli xil zaifliklarni paydo bo‘lishiga va veb-ilovalar tomonidan doimiy ravishda qayta ishlanishi mumkin bo‘lgan ruxsat etilgan miqdordagi so‘rovlardan oshib ketilishiga olib kelishi mumkin. So‘rovlar oqimining intensivligini oshirish orqali veb-ilovada bir vaqtning o‘zida ko‘rib chiqilayotgan so‘rovlar sonining ko‘payishinini amalga oshirish mumkin [2].

NATIJALAR

Faoliyat avtomatik dasturlar (botlar) tomonidan foydalanuvchi harakatlarini simulyatsiya qilish natijasida kelib chiqadigan so‘rovlar oqimining ko‘payishi tufayli yuzaga keladigan xizmat ko‘rsatishni rad etish hujumlarini bilan bog‘liq. Hozirgi vaqtda ushbu turdagi hujumni aniqlashning umumiy qabul qilingan tasniflari va samarali usullari mavjud emas. Ilova sathida arizalarni yo‘qotish ehtimolini baholashga asoslangan xizmat ko‘rsatishni rad etish hujumini aniqlash usuli ma’lum, ammo u faqat past faolllikka ega hujumlar holatida qo‘llaniladi. Shu sababli ilova sathida ishlaydigan veb-ilovada xizmat ko‘rsatishni rad etish kabi veb interfeysga qaratilgan hujumlarni aniqlash uchun usul yaratish vazifasi muhimdir. Veb interfeysga qaratilgan xujumlardan himoyalanish uchun taklif etilayotgan usulning mohiyati quyidagicha [3]:

1. Foydalanuvchilar harakatlari to‘g‘risidagi statistik axborotni tayyorlash;
2. Xizmat ko‘rsatishni rad etishga olib keluvchi hujum ta’sirlarini turli toifalari to‘g‘risida statistik axborotni generatsiyalash;
3. Ko‘rsatkichlarni (va statistik tuzilmalarni muvofiq ko‘rsatkichlari) qiymatlarini ko‘rilayotgan vaqt davrida hisoblash;
4. Hujumlarni turli toifalarni aniqlash uchun eng muvofiq ko‘rsatkichlar to‘plamini shakllantirish va ko‘rsatkichlarni qo‘llanishini baholash;
5. Hujumlarni aniqlash sifati va hujumlarni turli toifalari uchun neyron tarmoqlar arxitekturasi eng yaxshi parametrlarini aniqlash;
6. Foydalaniladigan neyron tarmoqlar miqdorini kamaytirish uchun hujum qilinuvchi kuchlar sinflari bo‘yicha hujumni turli toifalarini guruhlash;
7. Neyron tarmoqlarni o‘qitish;
8. Xizmat ko‘rsatishni rad etish toifasidagi hujumlarni aniqlash uchun neyron tarmoqlardan foydalanish;
9. Zarur bo‘lganda yangi statistika asosida neyron tarmoqlarni qayta o‘qitish.

Foydalanuvchilarni veb-ilovalarga so‘rovini tavsiflash uchun quyidagi ma’lumotlarni vektor formati ishlab chiqilgan [4]:

$(Time_i;\ SessionID_i;\ IsSessionStart_i;\ URL_i;\ Parameters_i;\ IP_i;\ Referer_i;\ UserAgent_i;\ Latency_i;\ DocSize_i;\ Memory_i;\ CpuTime_i)$;

- $Time_i$– veb-ilovalardagi so‘rovni seriyali raqami;
- $SessionID_i$ – seans identifikatori;
- $IsSessionStart_i$ – sessiya boshlanish identifikatori;
- URL_i– so‘rovni URL manzili;
- $Parameters_i$- GET-so‘rovi parametrlari;
- IP_i– so‘rov amalga oshirilgan IP manzil;
- $Referer_i$ – oldingi kirilgan sahifa manzili;

- $UserAgent_i$–mijoz dastur identifikator qatori;
- $Latency_i$ –so‘rovi qayta ishlanishida serverni javob vaqti;
- $DocSize_i$ – foydalanuvchi tomonidan so‘rovga javobi yuklangan ma’lumot hajmi;
- $Memory_i$ - so‘rovni qayta ishlash uchun foydalanilayotgan serverni tezkor xotirasi hajmi;
- $CpuTime_i$– so‘rovga javob qaytarishni protsessor vaqti.

Taklif qilingan formatda statistik ma’lumotlar yig‘ilgandan so‘ng so‘rov parametrlari tartibini sozlash va o‘chirish, manzillarni o‘zgartirish qoidalaridan foydalanib, kanonik shakldagi URL-so‘rovlarni o‘zgartirish zarur. Bunda Quyidagi belgilanishlar kiritiladi:

- URL qatori;
- so‘rov qatorisiz URL skript URL qatori (“?” simvoligacha URL ni boshlang‘ich fragmenti);
- n – so‘rovda parametrlarni maksimal miqdori;
- s – veb-tizimda barcha parametrlarni miqdori;
- $\{parameter_i; parameter_s\}$ – veb-tizimda barcha bo‘lishi mumkin bo‘lgan parametrlari to‘plami;
- $parameter_i^j$ - $j \in \{1, \dots, n\}$, $i \in \{1, \dots . s\}$ so‘rovlarda birinchi j-parametrlarni ba’zilari;
- $parameter = parameter_{i_1}^j \& \dots \dots \& parameter_{i_k}^k$ - parametrlardan iborat parametrlar qatori;
- URLFilter (ScriptURL) – maxsus kontruksiyalarsiz serverga resurslarga yo‘llarni generatsiyalash algoritmini tavsiflovchi funksiya;
- ParametersSequence $(parameter_{i_1}, \dots . . parameter_{i_k})$ - $parameter_{i_1}, \dots . . parameter_{i_k}$, $i_j \in \{1, \dots . s\}$, $j \in \{1, \dots . k\}$ ketma-ketlik parametrlarini shakllantirish va ketma-ketligi parametri uchun qoidalarni qo‘llanilishini tavsiflovchi funksiya, natija argumentlar tartibiga bog‘liq emas;
- ParameterPresence. ($parameter_i$)- $parameter_i$, $i \in \{1, \dots . s\}$ sozlanma ba’zi parametrlarini o‘chirish uchun qoidalarni qo‘llashni tavsiflovchi funksiY.

Kiritilgan URL belgilanishlar quydagicha ifodalanishi mumkin.

URL = ScriptURL:?:parameters:

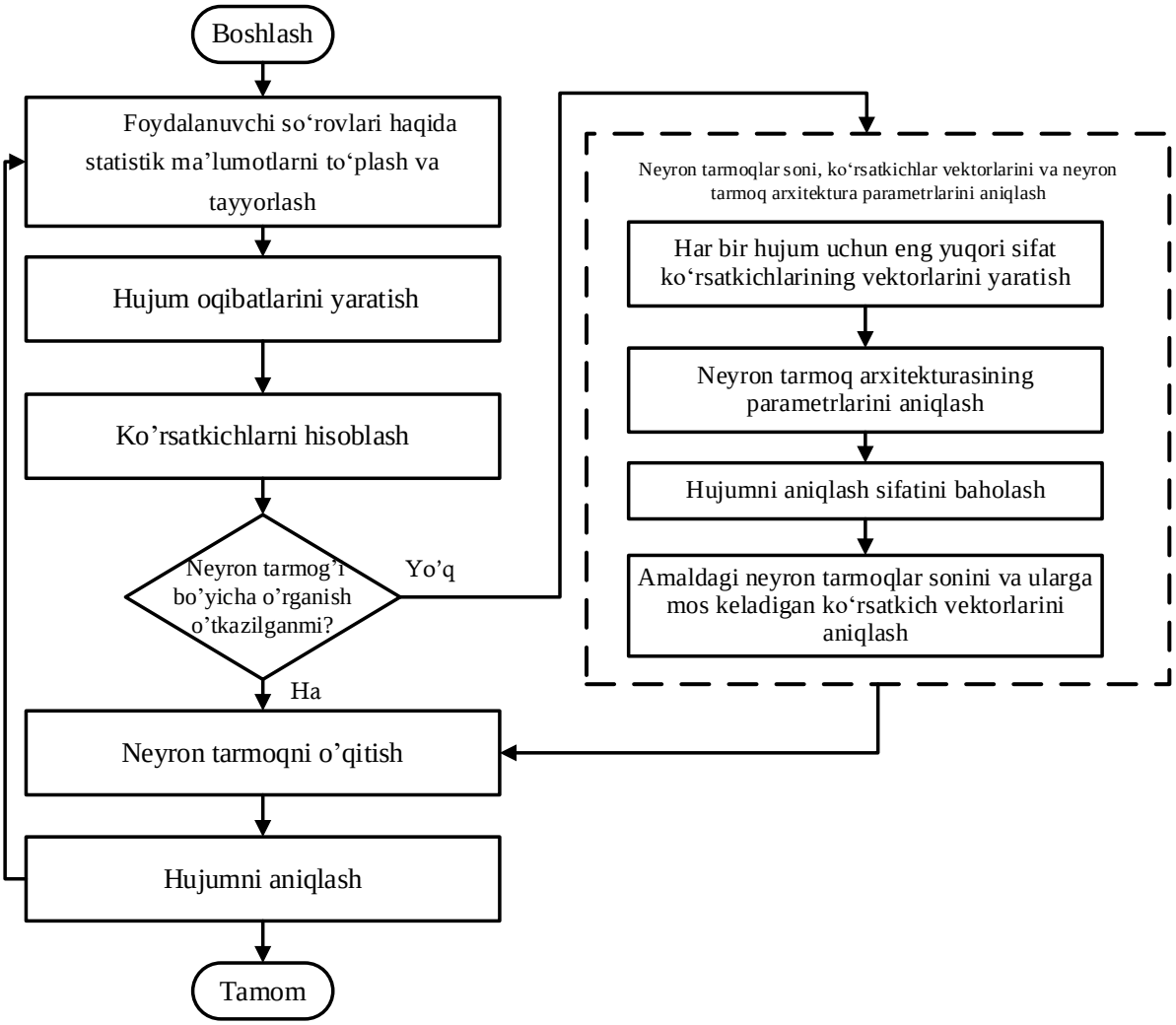
URL-manzil ba’zi so‘rovlari uchun so‘rovni kanonik shakli quyidagicha:

CanonicalURL(URL) = URLFilter(ScriptURL):?:

$$ParametersSequence\begin{pmatrix} ParameterPresence(parameter_{i_1}^{1}) \\ ParameterPresence(parameter_{i_k}^{k}) \end{pmatrix}.$$

$URLFilter\ (ScriptURL)\ path$ generatsiyalash algoritmini quyidagi tarzda ifodalash mumkin: domen nomi va portlari yaqinida *ScriptURL* qatorini bir qismidan o‘chirilishi quyidagicha bo‘ladi [5]:

1. konstruksiya ko‘rinishi “//”, ScriptURL qatoridan;
2. konstruksiya ko‘rinishi "/./ ", ScriptURL qatoridan;
3. konstruksiya ko‘rinishi “/text/ ../”, matn “/” simvolidan iborat bo‘lmagan, ixtiyoriy qator ko‘rinishida.



1- rasm Veb-interfeysga qaratilgan xizmat ko‘rsatishni rad etish toifasidagi hujumlarni aniqlash usulining umumiy sxemasi

Foydalanuvchi agenti qatorini sintaktik tahlillash uchun identifikatir qatorini kanonik ko‘rinishi kerak. Foydalanuvchi agent joriy ma’lumotlarni tahlil qilishi murakkablashgan, chunki katta miqdordagi ma’lumotlar brauzerlar orqali real vaqi rejimida yetib keladi. Bunda qatorlar bir xil baruzerlarni turli versiyalarida ham sezilarli darajada farqlanadi. Shu sababli foydalanuvchi agent qatoridan mavjud

parametrlarni tanlash kerak va ularni qatorli yozuvini yagona shaklga keltirish zarur. Bu jarayon URL so‘rovlar qatorining kanonik shaklini olishga analogdir. Foydalanuvchi-agent qatorlar paremtrlarini tartiblash va o‘chirish qoidalarini yaratishi lozim. Keyin barcha so‘rovlarni mantiqiy va sahifa yuklanishi bo‘yicha so‘rovlarga ajratish mumkin bo‘ladi. Bunda mantiqiy chegaralar quyidagilarga asoslanadi [6]:

- foydalanuvchilar ma’nan o‘xshash yuklamalarga ega harakatlarni ma’lum ketma-ketligi bajarishga moyil: masalan, yangiliklarni ko‘rish odatda aniq yangiliklar sahifalari bilan navbatlanuvchi yangiliklar lentasini ko‘rishni nazarda tutadi;
- foydalanuvchini o‘xshash harakatlari (masalan, yangiliklar yoki profilni ko‘rish) serverda o‘xshash yuklamalarni paydo bo‘lishiga olib keladi.

Sahifalarni mantiqiy toifalar bo‘yicha ajratish ikki bosqichda amalga oshiriladi:

- veb-ilovalardagi ko‘plab sahifalarini katta mantiqiy harakatlarga ajratish (masalan, forum, chat, yangiliklar lentasi va shu kabilar);
- foydalanuvchi uchun har doimgi turli harakatlarini mantiqiy bo‘limlar bo‘yicha taqsimlash (masalan, forum uchun forumlar ro‘yhatini o‘qish, mavzular ro‘yhatini o‘qish, mavzularni o‘qish va shu kabilar).

Shu sababli so‘rovlar avval mantiqiy toifa bo‘yicha ajratiladigan, keyin esa so‘rovlar bitta mantiqiy sinfdan yana bir bor yuklama ko‘rsatkichlari bo‘yicha sinflarga ajratiladigan kombinatsion yondashuvdan foydalanish maqsadga muvofiq bo‘ladi. Foydalanuvchilar so‘rovlari orasida bog‘liqliklarni hisobga olgan holda ko‘rsatkichlarni shakllantirish uchun foydalanuvchilarni harakatlarini turli xususiyatlarini tavsiflaydigan qo‘shimcha statistik tuzilmalarni shakllantirish kerak. Taklif etilgan usul doirasida quyidagi bog‘liqliklarni tahlillash mumkin:

- so‘rovni oldingi so‘rovdan paydo bo‘lish bog‘likligi;
- foydalanuvchi seanslarida joylashuviga bog‘liq so‘rovni tashqi ko‘rinishlariga bog‘liqligi;
- oldingi so‘rovlar ketma-ketligidan so‘rovni paydo bo‘lish bog‘liqligi.

Bu bog‘liqliklarni har birini hisobi uchun quyidagi statistik tuzilmalarni foydalanishni nazarda tutadi:

- oldingi so‘rovlardan bog‘liqlar matritsasi;
- seansda so‘rovlar raqamidan bog‘liqlar matritsasi;

Usulni amalga oshirish jarayonida veb-ilovalari foydalanuvchilari harakatlari modeli va harakatlari “xizmat ko‘rsatishdan rad etish”ga olib kelishi mumkin bo‘lgan avtomatik dasrturlarni asosiy toifalarini sinflashtirish ko‘rib chiqish mumkin. Taklif etilgan usulni mazmun mohiyatini to‘liq tushunish uchun biror bir veb serverga qaratilgan hujumlardan himoyalanish jarayonida amalga oshirish uchun uning algoritmi ishlab chiqib va ushbu algotirm asosida ishlaydigan dasturiy vositasini testlash orqali kerakli ma’lumotlarni olish mumkin. Veb-ilovalar odatda ikki turga bo‘linadi; ular statik veb-ilovalar va dinamik veb ilovalar.

Saytlar o‘rtasidagi skript (Cross site scripting) tarmoq hujumlarining turlaridan biridir. Taklif etilgan usul asosida ushbu hujumni aniqlash uchun quyidagi 4 ta ketma ketlikdan iborat alogoritm amalga oshiriladi [7].

1-qadam: foydalanuvchi kiritishini hisobga olish

2-qadam: **while**(foydalanuvchi kiritishi berilgan)

If(foydalanuvchi kiritgan matnda har qanday HTML teglari mavjud bo‘lsa (№1))

Kirishni ma’lumotlar bazasida saqlash.

If(foydalanuvchi kiritgan matnda har qanday maxsus belgilar, script teglar mavjud bo‘lsa(№2))

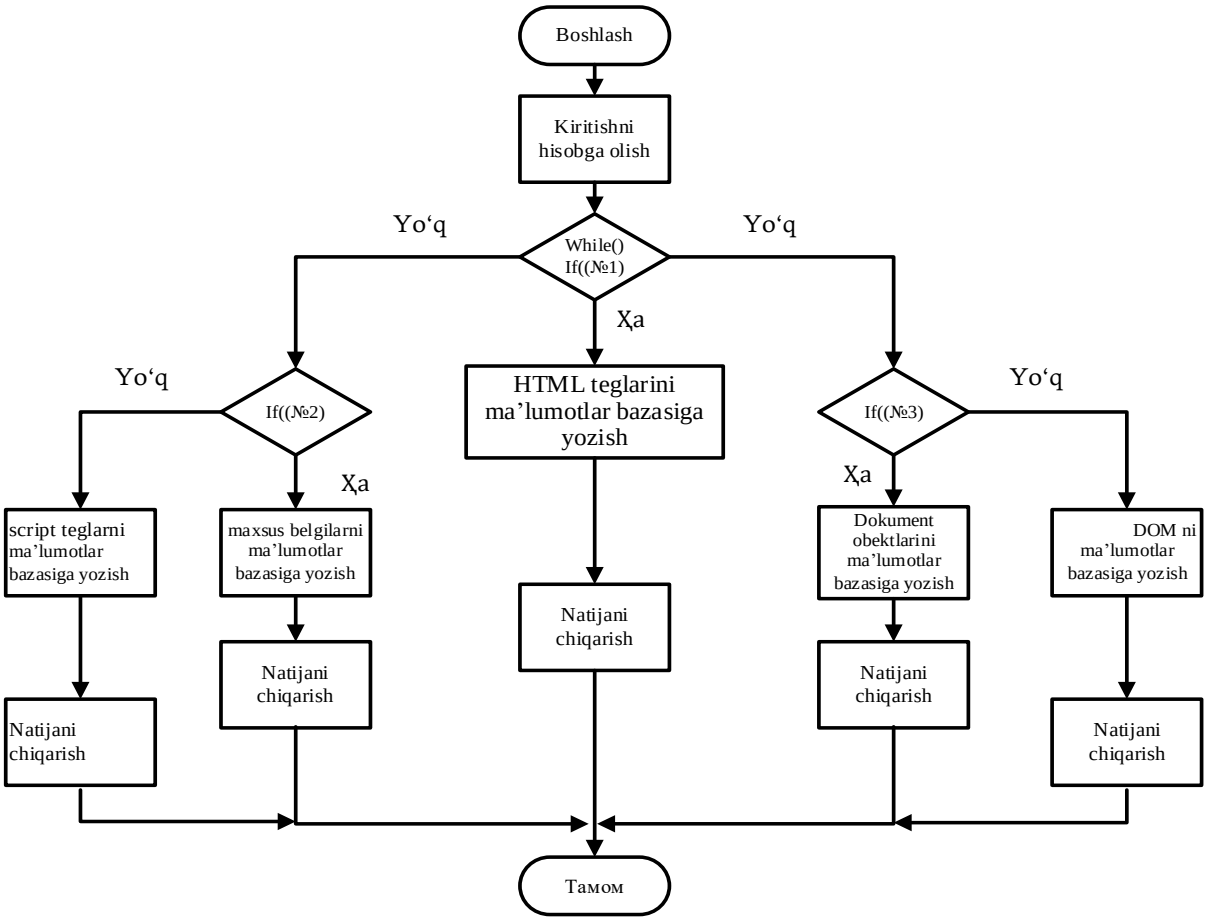
Kirishni ma’lumotlar bazasida saqlash

If(foydalanuvchi kiritgan matnda har qanday maxsus dokument obyektlari yoki Document Object Model (DOM) mavjud bo‘lsa(№3))

Kirishni ma’lumotlar bazasida saqlash

3-qadam: Foydalanuvchi ma’lumotlarini kiritish va 2-bosqichga o‘tish

4-qadam: Natijalarni ko‘rsatish



2- rasm Saytlar o‘rtasidagi skript (Cross site scripting) tarmoq hujumlarini aniqlash algortimning blok sxemasi.

XULOSA

Ilova sathida veb-iterfeysga qaratilgan tarmoq hujumlarini aniqlash iumkonini beruvchi ushbu usul, hujumlarni aniqlash tizimini qurish va joriy qilishda foydalanish, ko‘rsatkichlar to‘plamini qurish bo‘yicha ta’riflangan yondashuv asosida veb-ilovalarning vaqt o‘tishi bilan, haftaning turli kunlarida yoki veb-ilovalarning keng tarqalganligi yoki tabiiy ravishda o‘zgartirganligi sababli ulardagi ko‘rsatkichlarni baholash va hujum vektorlarini shakllantirish usullarida ishlatiladigan neyron tarmoqlar indikatorlarning vektorlarini kamaytirish orqali usulning samaradorligini oshirishi mumkin.

FOYDALANILGAN ADABIYOTLAR

1. S. Aftergood, “Cybersecurity: the cold war online,” *Nature*, vol. 547, no. 7661, pp. 30-31, 2017.
2. M. A. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, and M. Guizani, “A survey of machine and deep learning methods for internet of things (iot) security,” 2018, http://arxiv.org/abs/ 11023.
3. A. Aleesa, B. Zaidan, A. Zaidan, and N. M. Sahar, *Review of Intrusion Detection Systems Based on Deep Learning Techniques: Coherent Taxonomy, Challenges, Motivations, Recommendations, Substantial Analysis and Future Directions. Neural Computing and Applications*, Springer, Berlin, Germany, 2019.
4. G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido, and M. Marchetti, “On the effectiveness of machine and deep learning for cyber security,” in *Proceedings of 2018 10th International Conference on Cyber Conflict (CyCon)*, pp. 371–390, IEEE, Tallinn, Estonia, June 2018.
5. D. Berman, A. Buczak, J. Chavis, and C. Corbett, “A survey of deep learning methods for cyber security,” *Information*, vol. 10, no. 4, p. 122, 2019.
6. M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, “Deep learning for cyber security intrusion detection: approaches, datasets, and comparative study,” *Journal of Information Security and Applications*, vol. 50, p. 102419, 2020.
7. C. S. Wickramasinghe, D. L. Marino, K. Amarasinghe, and M. Manic, “Generalization of deep learning for cyber-physical system security: a survey,” in *Proceedings of IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society*, pp. 745–751, IEEE, Washington, DC, USA, October 2018.