

KONVOLIYUTSION NEYRON TARMOQLARI VA QO‘LLAB- QUVVATLASH VEKTOR MASHINASINI BIRLASHTIRGAN GIBRID YONDASHUV YORDAMIDA SAYTLARARO SKRIPTLASH (XSS) HUJUMLARINI ANIQLASHNING YAXSHILANGAN USULI

Choriyev Anvar Alisher o‘g‘li
Toshkent amaliy fanlar universiteti
assistent, choriyevanvar08@gmail.com
<https://orcid.org/0009-0007-0341-1568>

Annotatsiya. Saytlararo skript (XSS) hujumlari web-xavfsizlikka duch keladigan tahdidlar qatoriga kiradi, bu HTML formatlarining xilma-xilligi va murakkabligidan kelib chiqadi. Tadqiqotlar shuni ko‘rsatdiki, ba’zi matnni qayta ishlashga asoslangan usullar ushbu turdagi hujumni aniqlash qobiliyatida cheklangan. Ushbu maqolada ma’lum texnikalarning cheklovlarini hisobga olgan holda, ushbu turdagi hujumni aniqlashni yaxshilashga qaratilgan yondashuv taklif qilinadi. U konvolyutsion neyron tarmoqlari (CNN) bilan ifodalangan chuqur o‘rganish samaradorligini va qo‘llab-quvvatlash vektor mashinalari (SVM) bilan ifodalangan tasniflash usullarining aniqligini birlashtiradi. U CNNlarning in‘ektsiya o‘zgarishlari oldida murakkab vizual naqshlarni samarali aniqlash qobiliyatidan va SVMning kuchli tasniflash qobiliyatidan foydalanadi, chunki XSS hujumlari ko‘pincha faqat matn usullari bilan aniqlash qiyin bo‘lgan chalkashtirish yoki shifrlash texnikalaridan foydalanadi. Ushbu ish Kaggle-da mavjud bo‘lgan va ushbu hujumlar bilan bog‘liq zararli va zararli holatlarni o‘z ichiga olgan skript shaklida 13 686 ta jumlani o‘z ichiga olgan XSS hujumlariga qaratilgan ma’lumotlar to‘plamiga asoslangan. Xavfsiz ma’lumotlar 6313 ta holatni, zararli ma’lumotlar esa 7373 ta holatni ifodalaydi. Model ushbu ma’lumotlarning 80% bo‘yicha o‘qitildi, qolgan 20% esa sinov uchun ajratildi. Tasvirlardagi vizual naqshlarni tahlil qilish va o‘ziga xos xususiyatlarni ajratib olish uchun kompyuter ko‘rish texnikasidan foydalanildi, matnli tasvirdan vizual tasvirga o‘tdi, bu yerda har bir belgi ASCII kodlashiga, so‘ngra kulrang piksellarga aylantirildi. Oddiy va zararli kod satrlarining xususiyatlarini va ularning vizual tasviridagi farqlarni vizual ravishda ajratish uchun tahlilda CNN modeli ishlatilgan. Konvolyutsiya va subnamunalash (pul yig‘ish) qatlamlari turli darajadagi abstraktsiyalarda muhim naqshlarni ajratib oladi, yakuniy natija esa optimallashtirilgan SVM kabi tasniflash algoritmi tomonidan ishlatilishi mumkin bo‘lgan xususiyat vektoriga aylantiriladi. Eksperimental natijalar model uchun (99,7%) aniqlik bilan ajoyib ishlashni ko‘rsatdi va bu model haddan tashqari moslashish yoki ishlashni yo‘qotish xavfisiz samarali umumlashtirishga qodir. Bu murakkab XSS tahdidlaridan ishonchli himoyani ta’minlash orqali web-illovalar xavfsizligini sezilarli darajada oshiradi.

Kalit so‘zlar: Saytlararo skriptlash (XSS), web xavfsizlik, konvolyutsion neyron tarmoqlari (CNN), qo‘llab-quvvatlash vektor mashinasi (SVM).

1. Kirish

So‘nggi paytlarda internet va murakkab qurilmalardan tobora ko‘proq foydalanish tufayli web ilovalarning xizmatlarni ko‘rsatishdagi foydasi sezilarli darajada oshdi. Ular ko‘plab biznes va tashkilotlar, ayniqsa moliya, ta’lim va tijorat sohalarida muhim vositalarga aylandi. Raqamli texnologiyalarning rivojlanishi bilan web-illovalar Internetda ma’lumotlarni taqdim etish va xizmatlarni yetkazib berishning afzal ko‘rilgan vositasiga aylanib bormoqda. Biroq, ularning murakkabligi va yuqori interaktivligi ortib borayotgani sababli, ushbu ilovalar zaifliklarga ayniqsa moyil bo‘lib, ularni kiberhujumlar uchun asosiy nishonga aylantiradi. Kiberjinoyatchilar

muntazam ravishda ushbu kamchiliklardan foydalanadilar va shu bilan onlayn xizmatlar xavfsizligiga doimiy tahdid soladilar. Web-ilovalardagi eng keng tarqalgan zaifliklar orasida saytlararo skriptlash (XSS) mavjud bo'lib, bu xavfsizlik kamchiligi bo'lib, u tajovuzkorga boshqa foydalanuvchilar tomonidan ko'rilgan web-sahifaga zararli kodni - ko'pincha JavaScript-ni - kiritish imkonini beradi. OWASP Foundation (2023) [1] ma'lumotlariga ko'ra, XSS hujumlari web-ilovalarga ta'sir qiluvchi eng yaxshi o'nta zaiflik qatorida qolmoqda. Bu hujumlar, xususan, jabrlanuvchining xabarisiz cookie-fayllarni o'g'irlash, sessiyalarni egallash, web-sayt tarkibini o'zgartirish yoki hatto zararli dasturlarni ishga tushirish imkonini beradi. Foydalanuvchilarning brauzerlarini shu tarzda buzish orqali XSS parollar, kredit karta raqamlari va shaxsiy ma'lumotlar kabi maxfiy ma'lumotlarning o'g'irlanishiga olib kelishi mumkin. Ularning chastotasi va potentsial ta'siri tufayli XSS hujumlari kiberxavfsizlik mutaxassislari tomonidan juda muhim deb hisoblanadi. Ushbu doimiy tahdid tadqiqotchilarni aniqlash, oldini olish va bartaraf etish mexanizmlarini ishlab chiqishga faol e'tibor qaratishga olib keldi, bu esa XSSni web-ilovalar xavfsizligi sohasida dinamik tadqiqot sohasiga aylantiradi. Saytlararo skriptlash (XSS) - bu dastur qatlamiga qaratilgan in'ektsiya tipidagi hujum bo'lib, u zaif web-ilovaga zararli kodni kiritishni o'z ichiga oladi. Ikkinchisi asosan kirishni tekshirishning yetarli emasligi tufayli yuzaga keladi, bu esa XSS hujumlarining asosiy sababidir [2]. Web-ilova foydalanuvchi ma'lumotlarini uning turini, formatini yoki tarkibini tekshirmasdan qabul qilganda va ko'rsatganda, u zararli skriptlarga eshik ochadi. Tegishli filtrlashning yo'qligi va samarali xavfsizlik mexanizmlarining yo'qligi hujumlar xavfini sezilarli darajada oshiradi, zararli kontentning e'tiborga olinmasligiga va brauzer tomonidan bajarilishiga imkon beradi va shu bilan foydalanuvchilarni tahdidlarga duchor qiladi. Natijada, bu zaiflik jabrlanuvchining brauzerini zararli skriptlarning majburiy bajarilishiga duchor qiladi, chunki u zararli kontentni qonuniy kontentdan ajrata olmaydi [3]. Saytlararo skriptlash (XSS) hujumlarini aniqlash usullari qo'lda bajariladigan texnikalardan sun'iy intellektga (AI) asoslangan ilg'or yondashuvlarga o'tib, tobora rivojlanib bordi. Dastlab, himoya manba kodini qo'lda tahlil qilish va foydalanuvchi kiritgan ma'lumotlarni tekshirishni o'z ichiga olgan. Keyinchalik, `<script>` teglari kabi shubhali elementlarni aniqlash uchun oldindan belgilangan naqshlarga tayanib, qoidaga asoslangan filtrlar joriy etildi [4]. Biroq, bu mexanizmlar murakkab hujumlarga yoki chalkashtirish texnikalari yordamida yashiringan hujumlarga qarshi yetarli emas. Ushbu rivojlanayotgan landshaftda tobora murakkablashib borayotgan hujumlarga javoban yangi vositalar ishlab chiqildi. Ushbu vositalar dasturni bajarish paytida uning xatti-harakatlarini tekshirish uchun manba kodining ham statik, ham dinamik tahliliga tayanadi [5]. Keyinchalik, koddan olingan xususiyatlarga, masalan, kirish uzunligi, maxsus belgilar soni va ma'lum JavaScript funktsiyalarining mavjudligiga asoslangan tasniflash modellaridan foydalangan holda mashina o'rganish (ML) texnikalari joriy etildi. XSSni aniqlash uchun eng ko'p ishlatiladigan mashina o'rganish algoritmlari Tasodifiy o'rmon (RF), Qo'llab-quvvatlash vektor mashinalari (SVM) va K-Yaqin qo'shnilar (KNN). Hujum texnikalarining tez rivojlanishi tufayli ularga qarshi turish uchun yanada ilg'or usullarni qo'llash zarurati paydo bo'ldi. An'anaviy usullar, ayniqsa, hujum naqshlarining rivojlanayotgan tabiati va murakkabligidan kelib chiqadigan yuqori soxta ijobiy va soxta salbiy ko'rsatkichlar tufayli jiddiy qiyinchiliklarga duch kelmoqda. Sun'iy intellekt (AI) sohasidagi yutuqlar tufayli XSS hujumlarini aniqlash uchun chuqur o'rganish (DL) texnikalari qo'llanildi. Takrorlanuvchi neyron tarmoqlari (RNN), uzoq muddatli qisqa muddatli xotira tarmoqlari (LSTM) va BERT modeli kabi ilg'or modellar qo'llanildi. Ushbu modellar murakkab yoki chalkashtirilgan ma'lumotlardan yashirin naqshlarni ajratib olish qobiliyatiga ega, bu esa aniqlash va tasniflashning aniqligini sezilarli darajada yaxshiladi. Barcha usullarda

tajovuzkorlar foydalanuvchi ma'lumotlarini buzish uchun foydalanishi mumkin bo'lgan ma'lum cheklovlar mavjud. Shu nuqtai nazardan, bizning hozirgi ishimiz XSS hujumlarini aniqlash uchun gibril usulni ishlab chiqishga qaratilgan. Ushbu usul chuqur o'rganish va mashina o'rganishining kombinatsiyasiga asoslangan, xususan, konvolyutsion neyron tarmoqlari (CNN) va SVM klassifikatoridan foydalangan holda. U CNNning ma'lumotlardan xususiyatlarni samarali ajratib olish qobiliyatidan foydalanadi, SVM esa tasniflashni amalga oshirish uchun ishlatiladi. CNNlar, ayniqsa, tajribasiz bilan birlashtirilganda samarali ekanligi isbotlangan.

2. Ma'lumot va tegishli ishlar

2.1. Saytlararo skriptlash (XSS)

Saytlararo skriptlash (XSS) - bu tajovuzkor boshqa foydalanuvchilar tomonidan ko'rib chiqilgan web-sahifaga zararli kodni, odatda JavaScript-da, kiritadigan xavfsizlik zaifligi. Ushbu kiritish tajovuzkorga maqsadli web-ilovaning yaxlitligi va xavfsizligini buzishga imkon beradi: undan cookie-fayllarni o'g'irlash, foydalanuvchi sessiyalarini egallash, sayt tarkibini o'zgartirish yoki hatto jabrlanuvchining xabarisiz zararli dasturlarni ishga tushirish uchun foydalanish mumkin [8,9]. Saytlararo skriptlash (XSS) hujumlari uchta asosiy toifaga bo'linadi: aks ettirilgan (doimiy bo'lmagan), doimiy (saqlanadigan) va DOM asosida. Har bir tur o'ziga xos xususiyatlarga ega.

2.1.1. Saqlangan XSS (Doimiy)

Doimiy (saqlangan) XSS hujumlari asosan ijtimoiy tarmoqlar, forumlar yoki xabar almashish xizmatlari kabi interaktiv platformalarni nishonga oladi. Doimiy bo'lmagan XSS hujumlaridan farqli o'laroq, ular havola tuzog'ini talab qilmaydi: tajovuzkor zararli skriptni saytning boshqa foydalanuvchilar uchun ochiq bo'lgan qismiga, masalan, sharhlar, forumlar, sharhlar yoki HTML elektron pochta xabarlariga to'g'ridan-to'g'ri kiritadi va server ma'lumotlar bazasida saqlanib qoladi. Foydalanuvchi buzilgan sahifaga tashrif buyurganda, skript avtomatik ravishda ishga tushadi va barcha tashrif buyuruvchilarni ma'lumotlarni o'g'irlash yoki sessiyani egallab olish kabi xavflarga duchor qilishi mumkin. Bu jim, avtomatik xususiyat bu turdagi hujumni ayniqsa xavfli qiladi [10].

2.1.2. Aks ettirilgan (Doimiy bo'lmagan) XSS

Aks ettirilgan XSS ko'proq maqsadli hujumdur. Tajovuzkor jabrlanuvchini ko'pincha so'ralmagan elektron pochta xabarlar orqali zararli URL (Uniform Resource Locator) ga kirishga aldaydi. URL zararli kodni o'z ichiga oladi, keyin u jabrlanuvchining brauzerida bajariladi. XSSning bu turi vaqtinchalik va ma'lum bir foydalanuvchiga ta'sir qiladi [10].

2.1.3. DOM asosida XSS

An'anaviy XSS hujumlaridan (aks ettirilgan yoki saqlangan) farqli o'laroq, DOM (Document Object Model) asosidagi XSS zararli kodni serverdan o'tmasdan, dinamik DOM modifikatsiyalari orqali to'g'ridan-to'g'ri jabrlanuvchining brauzeriga kiritishga asoslangan [11]. Zararli skriptning bajarilishi odatda foydalanuvchining web-ilova bilan o'zaro ta'siri orqali ishga tushiriladi. Uning jiddiyligi uning yashirinligida, chunki serverdan hech qanday iz o'tmaydi, bu esa an'anaviy xavfsizlik vositalarining aniqlashini qiyinlashtiradi [12]. Ushbu turdagi doimiy bo'lmagan XSS filtrlanmagan foydalanuvchi kiritishi yordamida DOM manipulyatsiyasiga asoslangan. Bu o'lchov DOM asosidagi XSSni zamonaviy web-ilovalarda ayniqsa kuchli qiladi

2.2. Asosiy tushunchalar

Ushbu bo'limda ushbu XSS hujumini aniqlash yondashuvi asoslangan asosiy tushunchalar keltirilgan. U belgidan ASCII ga o'tkazish, ASCII dan tasvirga o'tkazish, konvolyutsion neyron tarmoqlari (CNN) va qo'llab-quvvatlash vektor mashinalarini (SVM) o'z ichiga oladi.

2.2.1. Gapning ASCII ifodasi

ASCII (Axborot almashinuvi uchun Amerika standart kodi) - bu har bir belgiga noyob raqamli kodni tayinlaydigan keng qo'llaniladigan belgi kodlash standarti. Versiyasiga qarab 7 yoki 8 bitdan iborat bo'lgan bu kod kompyuterlarga matnni standartlashtirilgan formatda ifodalash va almashish imkonini beradi [13].

2.2.2. ASCII asosidagi tasvirni qayta tiklash

Coumar va Kingston (2025) shuningdek, ASCII asosidagi tasvirni qayta tiklash ASCII belgilar va vizual ma'lumotlar o'rtasidagi moslikni anglatadi, deb ta'kidlashdi. Bu moslikni teskari yo'nalishda ham o'rganish mumkin, bu esa ASCII qiymatlariga asoslangan tasvirni qayta tiklash usullariga yo'l ochib beradi [14]. Ushbu usul ASCII belgining raqamli qiymatini berilgan o'lchamdagi tasvirdagi pikselga biriktirilgan vizual qiymat (masalan, kulrang rang) bilan to'g'ridan-to'g'ri bog'lashga asoslangan bo'lib, ko'pincha vizual tahlil uchun ishlatiladi.

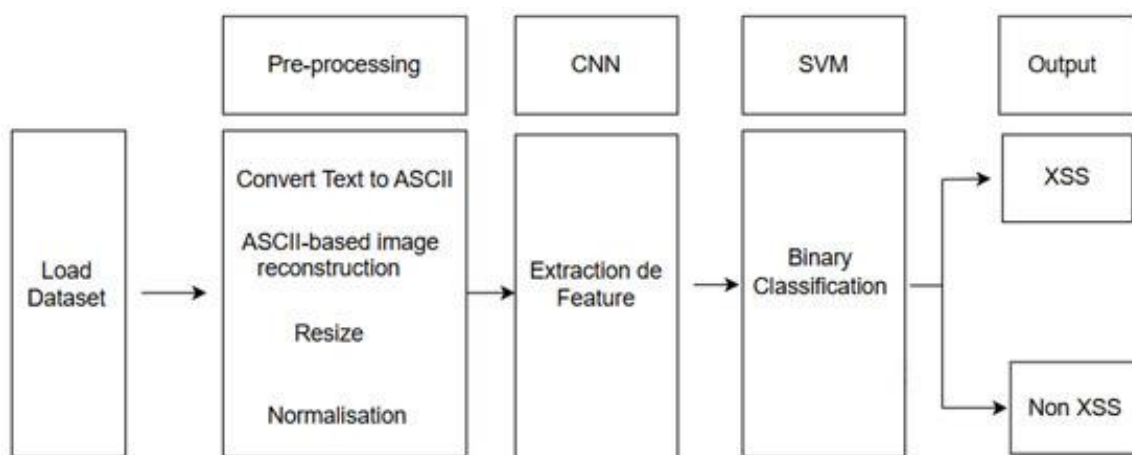
2.2.3. Konvolyutsion neyron tarmoqlari (CNN)

Konvolyutsion neyron tarmoq (CNN) - bu fazoviy ma'lumotlarni, xususan, tasvirlarni samarali qayta ishlash uchun maxsus ishlab chiqilgan chuqur o'rganish modelidir. Qatlamli arxitekturasi tufayli u vizual ma'lumotlarning ko'p qismini saqlab qolgan holda piksel matritsalarining hajmini kamaytiradi. Dastlab tasvirlardan xususiyatlarni avtomatik ravishda ajratib olish, xususan, tasniflash yoki segmentatsiya kabi vazifalar uchun ishlab chiqilgan CNN ko'plab kompyuter ko'rish ilovalarida muhim ma'lumotnoma sifatida o'zini namoyon qildi [15].

3. Taklif qilingan yondashuv

3.1. Yondashuv diagrammasi

1-rasmدا ushbu ishda qo'llanilgan yondashuvni yaxshiroq ko'rsatish va aniqlashtirish uchun biz quyida taklif qilingan XSS hujumlarini aniqlash bosqichlarining batafsil va keng qamrovli diagrammasini taqdim etamiz. Ushbu diagramma oldindan ishlov berish bosqichidan boshlanadi va yakuniy tasniflash bilan tugaydi. Butun jarayon bitta texnika atrofida aylanadi. Ushbu texnika belgining ASCII qiymati va uning vizual tasviri o'rtasidagi to'g'ridan-to'g'ri korrelyatsiyaga asoslangan. Keyin bu vizual qiymat ma'lum bir aniqlikdagi tasvirdagi pikselga beriladi. Ushbu texnika odatda vizual tahlilda qo'llaniladi. Ushbu tasvirlar xususiyatlarni ajratib olish uchun konvolyutsion neyron tarmoqlari yordamida tahlil qilinadi, keyin ular SVM tomonidan nazorat ostida tasniflanadi.



1-rasm. XSS hujumini aniqlash uchun taklif qilingan yondashuvning asosiy bosqichlari.

4. Munozara

Web-ilovalarning xavfsizligi, xususan, XSS (Saytlararo skriptlash) hujumlari kabi zararli kod in'ektsiyalarini aniqlash qobiliyatiga bog'liq. Ushbu tadqiqotda ikkilik tasniflash modeli qonuniy HTML kod parchalarini potentsial zararli skriptlarni o'z ichiga olganlardan farqlash

uchun o'rgatilgan. Modelning ishlashini baholash chalkashlik matritsasini tahlil qilishga, shuningdek, aniqlik, eslab qolish va F1 balli kabi standart ko'rsatkichlarga asoslangan. Olingan chalkashlik matritsasi modelning HTML ma'lumotlarini ikki toifaga ajratishdagi ajoyib ishlashini ta'kidlaydi: zararsiz kirishlar va zararli XSS skriptlarini o'z ichiga olganlar. Jami 2736 ta misoldan faqat 9 tasi noto'g'ri tasniflangan, bu umumiy aniqlik 99,65% ni tashkil qiladi. XSS klassi uchun aniqlik darajasi 99,66% ni tashkil qiladi, eslab qolish esa 99,73% ga etadi, bu esa noto'g'ri ijobiy va noto'g'ri salbiy natijalarning juda past ulushini ko'rsatadi, F1 balli 99,69% ni tashkil qiladi. XSS hujumlarini tasniflash uchun bir xil ma'lumotlar to'plami va qo'llaniladigan mashina o'rganish modellaridan (shu jumladan SVM, Naive Bayes, Decision Tree va Random Forest) foydalangan tadqiqot bilan taqqoslaganda, bizning gibrid yondashuvimiz barcha baholash ko'rsatkichlari bo'yicha ishlashda sezilarli yaxshilanishni ko'rsatadi. Olingan aniqlik, eslab qolish va F1 ball qiymatlari yuqorida aytib o'tilgan maqolada keltirilgan qiymatlardan sezilarli darajada yuqori bo'lib, taklif qilingan modelning tasniflash qobiliyati va mustahkamligining yaxshilanganligini aks ettiradi. Ushbu natijalar shuni ko'rsatadiki, model zararli ma'lumotlar va yaxshi ma'lumotlar o'rtasidagi farqni to'g'ri ajrata oladi.

5. Xulosa

Ushbu tadqiqotda XSS hujumlarini aniqlash uchun gibrid CNN-SVM yondashuvi joriy etilgan bo'lib, u HTML manba kodini ASCII kodlash orqali vizual tasvirga aylantirishga asoslangan. Eksperimental natijalar boshqa yondashuvlarga nisbatan model ishlashida sezilarli yaxshilanishni, shuningdek, chuqur neyron tarmoqlarining kuchli xususiyatlarni ajratib olish imkoniyatlari va yaxshi tuzilgan vektor tasvirlarida SVM samaradorligi tufayli hatto chalkash holatlarda ham zaif manba kodini samarali aniqlashni ko'rsatadi. Chalkashlik matritsasini tahlil qilish shuni ko'rsatadiki, taklif qilingan tasniflash modeli zararli HTML skriptlarini, xususan, XSS hujumlari bilan bog'liq skriptlarni aniqlashda ayniqsa samarali. Model juda past xato darajasi va kuchli umumlashtirish qobiliyatini namoyish etadi, shu bilan birga noto'g'ri ijobiy natijalarni samarali ravishda kamaytiradi. Ushbu istiqbolli natijalar, o'quv ma'lumotlar to'plamini yanada murakkab va xilma-xil hujum naqshlarini qamrab olish uchun kengaytirish sharti bilan, uni avtomatlashtirilgan zaifliklarni aniqlash tizimiga integratsiya qilish imkoniyatini ko'rsatadi.

Bundan tashqari, chalkashlik matritsasining tahlili shuni ko'rsatadiki, model nafaqat umumiy aniqlik nuqtai nazaridan, balki xavfsizlikka oid amaliy vazifalarda ham yuqori samaradorlikka ega. Xususan, noto'g'ri salbiy (False Negative) natijalarning juda kamligi alohida ahamiyat kasb etadi, chunki aynan shu turdagi xatolar xavfli XSS skriptlarining aniqlanmasdan tizimga kirib kelishiga sabab bo'lishi mumkin. Tadqiqot natijalariga ko'ra, model zararli skriptlarning deyarli barchasini muvaffaqiyatli aniqlagan bo'lib, bu uni real vaqt rejimida ishlovchi veb-ilovalar xavfsizlik tizimlariga integratsiya qilish imkoniyatini yaratadi.

Modelning yuqori samaradorligi gibrid yondashuvdan foydalanilganligi bilan izohlanadi. Ushbu yondashuv HTML kodlarining sintaktik va semantik xususiyatlarini birgalikda hisobga olib, zararli skriptlarga xos bo'lgan murakkab naqshlarni aniqlash imkonini beradi. An'anaviy mashina o'rganish algoritmlari ko'pincha qo'lda tanlangan xususiyatlarga tayanadi, bu esa yangi yoki o'zgartirilgan hujum vektorlarini aniqlashda cheklovlariga olib kelishi mumkin. Taklif etilgan model esa ma'lumotlarning ichki tuzilmasini chuqurroq o'rganib, turli ko'rinishdagi XSS hujumlarini aniqlashda yuqori moslashuvchanlikni namoyish etdi.

Natijalar shuningdek modelning muvozanatlashgan ishlashini ham ko'rsatadi. Ko'plab xavfsizlik tizimlarida aniqlik ko'rsatkichining yuqori bo'lishi evaziga eslab qolish darajasi pasayishi yoki aksincha holat kuzatiladi. Biroq mazkur modelda aniqlik va eslab qolish

ko'rsatkichlarining deyarli bir xil darajada yuqori bo'lishi F1 ballining ham maksimal qiymatlarga yaqinlashishiga olib kelgan. Bu esa modelning nafaqat zararli skriptlarni aniqlashda, balki qonuniy HTML kodlarini noto'g'ri ravishda xavfli deb belgilash ehtimolini ham sezilarli darajada kamaytirishini anglatadi.

Tadqiqot davomida olingan natijalar modelning umumlashtirish qobiliyati yuqori ekanligini ham tasdiqlaydi. Sinov ma'lumotlari ustida erishilgan yuqori natijalar modelning faqat o'quv to'plamidagi namunalarni yodlab olmaganligini, balki yangi va ilgari uchramagan HTML fragmentlarini ham to'g'ri tasniflay olishini ko'rsatadi. Bu xususiyat kiberxavfsizlik sohasida ayniqsa muhim hisoblanadi, chunki hujumchilar doimiy ravishda yangi usullar va obfuskatsiya texnikalaridan foydalanib keladilar.

Amaliy nuqtai nazardan qaralganda, ishlab chiqilgan model veb-ilovalar xavfsizligini ta'minlashda qo'shimcha himoya qatlami sifatida qo'llanilishi mumkin. U foydalanuvchilar tomonidan yuboriladigan ma'lumotlarni avtomatik tahlil qilish, xavfli skriptlarni filtrlash hamda xavfsizlik devorlari (Web Application Firewall) va kirishni nazorat qilish tizimlari bilan integratsiyalash imkoniyatiga ega. Bunday yechimlar XSS hujumlarining oldini olish, foydalanuvchi ma'lumotlarini himoya qilish va veb-resurslarning ishonchliligini oshirishga xizmat qiladi.

Umuman olganda, tadqiqot natijalari taklif etilgan gibrid model XSS hujumlarini aniqlash vazifasida yuqori aniqlik, barqarorlik va ishonchlilikni namoyish etishini ko'rsatdi. Olingan ko'rsatkichlar modelning mavjud klassik mashina o'rganish algoritmlariga nisbatan ustunligini tasdiqlaydi hamda uni zamonaviy veb-ilovalar xavfsizligini ta'minlash uchun istiqbolli yechim sifatida tavsiya etish imkonini beradi. Kelgusidagi tadqiqotlarda modelni boshqa turdagi veb-hujumlar, jumladan SQL Injection, Command Injection va Cross-Site Request Forgery (CSRF) hujumlarini aniqlash vazifalariga moslashtirish.

Foydalanilgan adabiyotlar

1. OWASP. OWASP Top Ten. 2025. Available online: <https://owasp.org/www-project-top-ten/> (accessed on 1 November 2025).
2. Ayeni, B.K.; Sahalu, J.B.; Adeyanju, K.R. Detecting Cross-Site Scripting in Web Applications Using Fuzzy Inference System. *J. Comput. Netw. Commun.* 2018, 2018, 8159548.
3. Sarmah, U.; Bhattacharyya, D.K.; Kalita, J.K. A Survey of Detection Methods for XSS Attacks. *J. Netw. Comput. Appl.* 2018, 118, 113–143.
4. Minamide, Y. Static Approximation of Dynamically Generated Web Pages. In Proceedings of the 14th International Conference on World Wide Web (WWW'05), Chiba, Japan, 10–14 May 2005; ACM Press: Chiba, Japan, 2005; p. 432.
5. Doupé, A.; Cui, W.; Jakubowski, M.H.; Peinado, M.; Kruegel, C.; Vigna, G. deDacota: Toward Preventing Server-Side XSS via Automatic Code and Data Separation. In Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security (CCS'13), Berlin, Germany, 4–8 November 2013; ACM Press: Berlin, Germany, 2013; pp. 1205–1216.
6. Shen, J.; Cheng, X.; Yang, X.; Zhang, L.; Cheng, W.; Lin, Y. Efficient CNN Accelerator Based on Low-End FPGA with Optimized Depthwise Separable Convolutions and Squeeze-and-Excite Modules. *AI* 2025, 6, 244.
7. Zhang, L.; Yang, X.; Cheng, X.; Cheng, W.; Lin, Y. Few-Shot Image Classification Algorithm Based on Global–Local Feature Fusion. *AI* 2025, 6, 265.

8. Disawal, S.; Suman, U.; Rathore, M. Investigation of Detection and Mitigation of Web Application Vulnerabilities. *Int. J. Comput. Appl. IJCA* 2022, *184*, 30–36.
 9. Pasini, S.; Maragliano, G.; Kim, J.; Tonella, P. XSS Adversarial Attacks Based on Deep Reinforcement Learning: A Replication and Extension Study. *arXiv* 2025, arXiv:2502.19095.
 10. Rodríguez, G.E.; Torres, J.G.; Flores, P.; Benavides, D.E. Cross-Site Scripting (XSS) Attacks and Mitigation: A Survey. *Comput. Netw.* 2020, *166*, 106960.
 11. Hartono, H.; Triloka, J. Method for Detection and Mitigation of Cross-Site Scripting Attack on Multi-Websites. In Proceedings of the International Conference on Information Technology and Business (ICITB 2021), Bandar Lampung, Indonesia, 17 November 2021; pp. 26–32. Available online: <https://jurnal.darmajaya.ac.id/index.php/icitb/article/view/3037/> (accessed on 1 November 2025).
 12. Falana, O.J.; Ebo, I.O.; Tinubu, C.O.; Adejimi, O.A.; Ntuk, A. Detection of Cross-Site Scripting Attacks Using Dynamic Analysis and Fuzzy Inference System. In Proceedings of the 2020 International Conference in Mathematics, Computer Engineering and Computer Science (ICMCECS), Ayobo, Nigeria, 18–21 March 2020.
 13. Salama, A.; Tarek, Z.; Darwish, Y.; Elseuofi, S.; Darwish, E.; Shams, M. *Neutrosophic Encoding and Decoding Algorithm for ASCII Code System*; Zenodo: Geneva, Switzerland, 2024.
 14. Coumar, S.; Kingston, Z. Evaluating Machine Learning Approaches for ASCII Art Generation. *arXiv* 2025, arXiv:2503.14375.
- El Sakka, M.; Ivanovici, M.; Chaari, L.; Mothe, J. A Review of CNN Applications in Smart Agriculture Using Multimodal Data. *Sensors* 2025, *25*, 472.