WAF SIYOSATLARINI ADAPTIV RISK BAHOLASH ASOSIDA SHAKLLANTIRISH VA WEB-TAHDIDLARNI KAMAYTIRISH MODELI

Ashurov Laziz Shoymardonovich
"IPS CLOUD" MChJ

Annotatsiya. *Mazkur tezisda web-ilovalar xavfsizligini ta'minlashda Web Application Firewall (WAF) siyosatlarini adaptiv risk baholash asosida shakllantirish va web-tahdidlarni kamaytirish masalalari tadqiq etiladi. An'anaviy WAF konfiguratsiyalarida statik qoidalardan foydalanish yangi va o'zgaruvchan kiberhujumlarga tezkor moslashish, noto'g'ri ijobiy holatlarni (false positive) kamaytirish hamda turli darajadagi tahdidlarni ustuvorlashtirish imkoniyatlarini cheklashi asoslanadi. Shu sababli web-so'rovlar, aniqlangan zaifliklar, hujum turi, tahdid darajasi va avvalgi xavfsizlik hodisalari haqidagi ma'lumotlarni kompleks tahlil qilishga asoslangan adaptiv yondashuv taklif etiladi. Modelda risk darajasini dinamik baholash natijalariga muvofiq WAF qoidalarini tanlash, ularning ustuvorligini belgilash va himoya siyosatini moslashtirish mexanizmi ko'zda tutiladi. Risk ko'rsatkichlarini shakllantirishda tahdid ehtimoli, zaiflikning kritikligi, himoyalanayotgan axborot resursining qiymati va hujumning potensial ta'siri kabi mezonlardan foydalanish nazarda tutiladi. Taklif etilayotgan yondashuv WAF siyosatlarini faqat oldindan belgilangan signaturalar asosida emas, balki joriy risk holatiga muvofiq boshqarish, yuqori xavfli web-tahdidlarga ustuvor javob berish va himoya mexanizmlarining samaradorligini oshirishga yo'naltirilgan. Natijada adaptiv risk baholashga asoslangan WAF modeli web-ilovalarga qaratilgan tahdidlarni aniqlash va kamaytirish jarayonini takomillashtirishning istiqbolli mexanizmi sifatida asoslanadi.*

Kalit so'zlar: *Web Application Firewall, WAF, web-ilova xavfsizligi, adaptiv risk baholash, WAF siyosati, kiberxavfsizlik, web-tahdid, zaiflik, risk darajasi, false positive, xavfsizlik siyosati.*

KIRISH

Raqamli xizmatlarning jadal rivojlanishi natijasida web-ilovalar tashkilotlarning axborot infratuzilmasidagi asosiy komponentlardan biriga aylandi. Web-ilovalar orqali

foydalanuvchilarni autentifikatsiya qilish, shaxsiy kabinetlardan foydalanish, elektron to‘lovlarni amalga oshirish, ma’lumotlarni qayta ishlash va turli axborot tizimlari bilan integratsiya qilish kabi muhim jarayonlar bajariladi. Shu bilan birga, web-ilovalarning ochiq tarmoq orqali foydalanilishi ularni kiberhujumlarning asosiy nishonlaridan biriga aylantiradi.

Web-ilovalarni himoyalashda Web Application Firewall (WAF) muhim xavfsizlik vositalaridan biri hisoblanadi. WAF web-server va foydalanuvchi o‘rtasidagi HTTP/HTTPS trafikni nazorat qilib, belgilangan xavfsizlik qoidalariga muvofiq zararli yoki shubhali so‘rovlarni aniqlash va bloklash imkonini beradi. Bunda SQL injection, Cross-Site Scripting (XSS), zararli so‘rovlar, protokol anomaliyalari va boshqa web-tahdidlarga qarshi himoya qoidalaridan foydalaniladi.

Amaliyotda WAF samaradorligi ko‘p jihatdan unda shakllantirilgan xavfsizlik siyosatlarining sifatiga bog‘liq. Statik qoidalar to‘plamiga asoslangan yondashuvda barcha web-so‘rovlar oldindan belgilangan mezonlar asosida tekshiriladi. Biroq web-ilovaning funksional imkoniyatlari, zaifliklari va unga qaratilgan tahdidlar vaqt davomida o‘zgarib boradi. Natijada qat’iy konfiguratsiyalangan WAF siyosati ayrim yangi tahdidlarni yetarli darajada aniqlamasligi yoki aksincha, legitim so‘rovlarni zararli deb baholashi mumkin.

Mazkur holatda false positive — qonuniy trafikning xato ravishda tahdid sifatida aniqlanishi va false negative — zararli trafikning aniqlanmay qolishi WAF siyosatini optimallashtirishdagi muhim muammolar hisoblanadi. Himoya darajasini haddan tashqari oshirish legitim foydalanuvchilar faoliyatiga salbiy ta’sir ko‘rsatishi mumkin, qoidalarning yumshatilishi esa xavfsizlik darajasini pasaytiradi. Demak, WAF siyosatini shakllantirishda xavfsizlik va web-ilovaning normal ishlashi o‘rtasidagi muvozanatni ta’minlash talab etiladi.

Ushbu muammoni hal qilishning istiqbolli yo‘nalishlaridan biri WAF siyosatlarini adaptiv risk baholash asosida boshqarishdir. Bunda web-so‘rovga nisbatan xavfsizlik qarori faqat bitta signatura yoki qat’iy qoidaga emas, balki tahdid ehtimoli, aniqlangan zaiflikning kritikligi, himoyalanayotgan resursning qiymati, so‘rovning xususiyatlari va potensial zarar darajasi kabi bir nechta omillarning kombinatsiyasiga asoslanadi.

Riskga asoslangan yondashuvda barcha tahdidlarga bir xil himoya choralarini qo‘llash o‘rniga, ularning xavf darajasiga qarab differensial siyosat shakllantiriladi. Masalan, kritik axborot resursiga qaratilgan va yuqori risk ko‘rsatkichiga ega so‘rov avtomatik bloklanishi, o‘rta riskli so‘rov qo‘shimcha tekshiruvga yo‘naltirilishi, past riskli trafik esa monitoring ostida o‘tkazilishi mumkin. Shu tariqa riskni baholash →

qaror qabul qilish → WAF siyosatini moslashtirish → natijani monitoring qilish → riskni qayta baholash ko‘rinishidagi uzluksiz adaptiv sikl shakllanadi.

Taklif etilayotgan yondashuvning asosiy g‘oyasi WAFni faqat zararli trafikni filtrlovchi vosita sifatida emas, balki web-ilovaning joriy xavfsizlik holatiga moslasha oladigan riskga asoslangan himoya mexanizmi sifatida shakllantirishdan iborat.

Tadqiqotning maqsadi — web-ilovalarga qaratilgan tahdidlarning risk darajasini dinamik baholash asosida WAF xavfsizlik siyosatlarini adaptiv shakllantirish modelini ishlab chiqish hamda web-tahdidlarni aniqlash va kamaytirish samaradorligini oshirish yondashuvlarini asoslashdir.

TADQIQOT METODLARI

Mazkur tadqiqotda web-ilovalar xavfsizligini ta’minlashda WAF siyosatlarini adaptiv risk baholash asosida shakllantirishning nazariy va amaliy mexanizmlari o‘rganildi. Tadqiqotning metodologik asosini riskga asoslangan kiberxavfsizlik boshqaruvi, adaptiv himoya, web-trafikni tahlil qilish va xavfsizlik siyosatlarini dinamik boshqarish tamoyillari tashkil etdi.

Tadqiqot jarayonida tizimli tahlil, qiyosiy tahlil, xavf omillarini tasniflash, risk darajasini baholash, WAF qoidalarini ustuvorlashtirish hamda adaptiv qaror qabul qilish usullaridan foydalanildi. Web-ilovaga qaratilgan tahdidlarning xavf darajasini aniqlashda bir nechta mezonlarning o‘zaro bog‘liqligi hisobga olinadi.

Riskni baholash uchun quyidagi asosiy parametrlar ajratildi: tahdidning yuzaga kelish ehtimoli, aniqlangan zaiflikning kritikligi, himoyalanayotgan resursning qiymati, hujumning potensial ta’siri, so‘rovning xatti-harakat xususiyatlari va avvalgi xavfsizlik hodisalari bilan bog‘liqligi. Ushbu omillar asosida har bir web-so‘rov yoki aniqlangan tahdid uchun integral risk ko‘rsatkichi shakllantiriladi.

Risk darajasini umumlashtirilgan ko‘rinishda quyidagi formula orqali ifodalash mumkin:

$$R = w_1P + w_2V + w_3A + w_4I + w_5B$$

bunda:

1-jadval. Adaptiv risk baholash modelining asosiy ko‘rsatkichlari

Belgi	Ko‘rsatkich	Mazmuni
R	Umumiy risk darajasi	Baholash natijasida shakllanadigan integral risk ko‘rsatkichi
P	Tahdid ehtimoli	Tahdidning amalga oshish ehtimolini ifodalaydi

V	Zaiflik kritikligi	Aniqlangan zaiflikning xavflilik darajasini hisobga oladi
A	Axborot aktivi qiymati	Himoyalanayotgan resursning kritikligi va qiymatini aks ettiradi
I	Potensial ta’sir	Hujum amalga oshganda yuzaga kelishi mumkin bo‘lgan zararni baholaydi
B	Xulq-atvor/anomaliya	So‘rovning shubhali yoki anomal xususiyatlarini hisobga oladi
w_1–w_5	Vazn koeffitsiyentlari	Mezonlarning modeldagi nisbiy ahamiyatini belgilaydi

Vazn koeffitsiyentlari himoyalanayotgan web-ilovaning arxitekturasi, biznes jarayonlarining kritikligi va tashkilotning xavfsizlik siyosatiga qarab belgilanadi. Natijada risk ko‘rsatkichi faqat hujum signaturasini emas, balki hujumning real xavflilik darajasini ham hisobga olish imkonini beradi.

Taklif etilayotgan modelda risk darajasi shartli ravishda uchta toifaga ajratiladi: **past, o‘rta va yuqori risk**. Past riskli trafik monitoring ostida o‘tkaziladi, o‘rta riskli so‘rovlar qo‘shimcha tekshiruv yoki cheklash mexanizmlariga yo‘naltiriladi, yuqori riskli so‘rovlar esa bloklanadi yoki xavfsizlik hodisasi sifatida ro‘yxatga olinadi. Shu asosda WAF siyosatlarining qattiqlik darajasi joriy risk holatiga mos ravishda dinamik o‘zgaradi.

Adaptiv boshqaruv jarayoni quyidagi ketma-ketlik asosida tashkil etiladi:

web-trafikni qabul qilish → so‘rovni tahlil qilish → tahdid va zaifliklarni aniqlash → riskni hisoblash → risk darajasini klassifikatsiya qilish → WAF siyosatini tanlash → javob chorasi → natijani monitoring qilish → riskni qayta baholash.

Model samaradorligini baholashda bir nechta ko‘rsatkichlardan foydalanish maqsadga muvofiq: zararli so‘rovlarni aniqlash darajasi, noto‘g‘ri ijobiy holatlar soni, aniqlanmay qolgan hujumlar ulushi, xavfsizlik hodisasiga javob berish vaqti va WAF qoidalarining umumiy samaradorligi.

Bunda quyidagi ko‘rsatkichlar alohida ahamiyatga ega:

Detection Rate = TP / (TP + FN)

False Positive Rate = FP / (FP + TN)

bu yerda **TP** — to‘g‘ri aniqlangan zararli so‘rovlar, **FN** — aniqlanmay qolgan zararli so‘rovlar, **FP** — xato ravishda zararli deb baholangan legitim so‘rovlar, **TN** — to‘g‘ri aniqlangan legitim so‘rovlardir.

Taklif etilgan metodika WAF siyosatlarini statik qoidalar to‘plamidan riskga moslasha oladigan dinamik xavfsizlik mexanizmiga aylantirishga qaratilgan. Bu esa web-tahdidlarni ustuvorlik asosida qayta ishlash, false positive holatlarini kamaytirish va kritik tahdidlarga tezkor javob berish imkonini beradi.

NATIJALAR VA MUHOKAMA

Tadqiqot doirasida ishlab chiqilgan adaptiv risk baholash modeli WAF siyosatlarini shakllantirishda web-so‘rovlarni faqat oldindan belgilangan signaturalar bo‘yicha tekshirishdan ko‘ra, ularning joriy xavf darajasini kompleks baholashga asoslanadi. Modelning asosiy xususiyati tahdid, zaiflik, himoyalanayotgan axborot aktivining kritikligi va so‘rovning anomal xususiyatlarini yagona risk ko‘rsatkichida birlashtirishdan iborat.

An’anaviy WAF siyosatlarida bir xil turdagi so‘rovlar, odatda, oldindan belgilangan qoidalar asosida bloklanadi yoki o‘tkaziladi. Adaptiv modelda esa xavfsizlik qarori risk darajasiga bog‘liq ravishda shakllantiriladi. Natijada bir xil turdagi anomal faollik turli axborot resurslariga nisbatan turlicha xavfsizlik choralarini talab qilishi mumkin. Masalan, ochiq axborot sahifasiga yuborilgan shubhali so‘rov bilan autentifikatsiya yoki ma’lumotlar bazasiga murojaat qiluvchi kritik komponentga yo‘naltirilgan so‘rovning xavf darajasi bir xil baholanmaydi.

Taklif etilgan modelda risk darajasiga mos ravishda WAFning javob siyosati quyidagicha shakllantirilishi mumkin:

2-jadval. Risk darajasiga mos adaptiv WAF javob siyosati

Risk darajasi	Holat tavsifi	WAF siyosati	Javob chorasi
Past	Anomaliya mavjud, lekin tahdid ehtimoli past	Monitoring	So‘rovni o‘tkazish va loglash
O‘rta	Shubhali xatti-harakat yoki zaiflik bilan bog‘liq belgi mavjud	Kuchaytirilgan nazorat	Qo‘shimcha tekshiruv, rate limiting yoki challenge
Yuqori	Hujum belgilari va yuqori potensial zarar mavjud	Qat’iy himoya	So‘rovni bloklash va hodisani qayd etish

Kritik	Kritik resursga yuqori ishonchlilikdagi hujum aniqlangan	Maksimal himoya	Darhol bloklash, ogohlantirish va hodisani eskalatsiya qilish

Mazkur mexanizm WAF siyosatining qattiqlik darajasini barcha trafik uchun bir xil oshirish zaruratini kamaytiradi. Bu ayniqsa false positive holatlarini boshqarishda muhimdir. Haddan tashqari qat'iy qoidalar legitim foydalanuvchi so‘rovlarini ham bloklashi mumkin. Riskga asoslangan yondashuvda esa so‘rovning konteksti va potensial xavfi hisobga olinishi sababli himoya choralarini differensial qo‘llash imkoniyati yuzaga keladi.

Modelning yana bir muhim elementi — qayta aloqa mexanizmidir. WAF tomonidan qabul qilingan qarorlarning natijalari loglarda qayd etilib, keyingi risk baholash jarayonida foydalaniladi. Agar muayyan qoida muntazam ravishda legitim so‘rovlarni bloklayotgan bo‘lsa, uning risk chegarasi yoki vazn koeffitsiyentlarini qayta ko‘rib chiqish mumkin. Aksincha, ma'lum turdagi zararli trafik mavjud qoidalardan muntazam o‘tib ketayotgan bo‘lsa, tegishli siyosat kuchaytirilishi talab etiladi.

Shu asosda adaptiv modelning ishlash sikli quyidagicha ifodalanadi:

TAHDIDNI ANIQLASH → RISKNI BAHOLASH → WAF QARORINI SHAKLLANTIRISH → JAVOB CHORASINI QO‘LLASH → NATIJANI LOGLASH → SAMARADORLIKNI BAHOLASH → SIYOSATNI KORREKSIYA QILISH → QAYTA BAHOLASH.

Bunday siklik mexanizm WAF siyosatini bir marta sozlanadigan statik konfiguratsiyadan muntazam ravishda takomillashtiriladigan himoya tizimiga aylantirish imkonini beradi.

Model samaradorligini baholashda faqat bloklangan hujumlar soniga tayanish yetarli emas. Detection Rate, False Positive Rate, False Negative Rate, aniqlash va javob berish vaqti hamda legitim trafikning uzluksizligi birgalikda tahlil qilinishi lozim. Chunki yuqori aniqlash ko‘rsatkichi false positive darajasining keskin oshishi hisobiga erishilgan bo‘lsa, bunday konfiguratsiyani optimal deb baholash metodologik jihatdan to‘g‘ri bo‘lmaydi.

Shuningdek, adaptiv risk modeli SQL injection, Cross-Site Scripting (XSS), path traversal va boshqa web-tahdidlarni aniqlashda mavjud WAF mexanizmlarini bekor qilmaydi. Aksincha, signatura va qoidalar asosida olingan natijalarni risk konteksti bilan boyitadi. Demak, taklif qilinayotgan yondashuv mavjud himoya mexanizmlariga

qo‘shimcha riskga asoslangan qaror qabul qilish qatlami sifatida qaralishi maqsadga muvofiq.

Nazariy tahlil asosida modelning asosiy afzalligi uchta jihatda namoyon bo‘ladi: tahdidlarni kritikligi bo‘yicha ustuvorlashtirish, WAF siyosatlarini joriy xavfsizlik holatiga moslashtirish va noto‘g‘ri xavfsizlik qarorlarini qayta aloqa asosida korreksiya qilish. Biroq ushbu afzalliklarning miqdoriy samaradorligini tasdiqlash uchun modelni real yoki nazorat qilinadigan test muhitida sinovdan o‘tkazish hamda an’anaviy WAF konfiguratsiyasi bilan qiyosiy eksperiment o‘tkazish talab etiladi.

XULOSA

Web-ilovalar xavfsizligini ta’minlashda WAF siyosatlarini samarali shakllantirish zamonaviy kiberxavfsizlik tizimining muhim vazifalaridan biri hisoblanadi. Web-tahdidlarning dinamik o‘zgarishi, yangi hujum usullarining paydo bo‘lishi hamda himoyalanayotgan axborot resurslarining turli darajadagi kritikligi statik WAF qoidalaridan riskga asoslangan adaptiv boshqaruv mexanizmlariga o‘tish zaruratini yuzaga keltiradi.

Tadqiqot doirasida taklif etilgan model web-so‘rovlarni baholashda tahdid ehtimoli, zaiflikning kritikligi, axborot aktivining qiymati, hujumning potensial ta’siri va so‘rovning anomal xususiyatlarini kompleks hisobga olishga asoslanadi. Ushbu ko‘rsatkichlarning integratsiyalashuvi har bir aniqlangan holat uchun risk darajasini shakllantirish hamda WAFning tegishli himoya siyosatini tanlash imkonini beradi.

Taklif etilgan modelning muhim jihati risk darajasiga qarab differensial javob choralarini qo‘llashdir. Past riskli trafikni monitoring qilish, o‘rta riskli so‘rovlarga qo‘shimcha nazorat mexanizmlarini qo‘llash, yuqori va kritik riskli so‘rovlarni esa bloklash hamda xavfsizlik hodisasi sifatida qayd etish WAF resurslaridan maqsadli foydalanish imkonini beradi. Bunda himoya darajasini oshirish bilan bir qatorda legitim trafikning asossiz bloklanishini kamaytirish ham muhim mezon sifatida qaraladi.

Adaptiv modelning yana bir ustunligi qayta aloqa mexanizmining mavjudligidir. WAF tomonidan qabul qilingan qarorlar va ularning natijalarini loglash, tahlil qilish hamda risk chegaralari va qoidalarni qayta sozlash orqali xavfsizlik siyosati muntazam ravishda takomillashtirib boriladi. Natijada riskni baholash → qaror qabul qilish → himoya choralarini qo‘llash → monitoring → korreksiya → qayta baholash sikli shakllanadi.

Shunday qilib, WAF siyosatlarini adaptiv risk baholash asosida shakllantirish web-ilovalar xavfsizligini boshqarishda istiqbolli yondashuv hisoblanadi. Taklif etilgan model mavjud signatura va qoidalarga asoslangan himoya mexanizmlarini almashtirmaydi, balki ularni riskga asoslangan qaror qabul qilish mexanizmi bilan

to‘ldiradi. Modelni amaliy test muhitida sinovdan o‘tkazish, Detection Rate, False Positive Rate, False Negative Rate va javob berish vaqti kabi ko‘rsatkichlar asosida an’anaviy WAF konfiguratsiyasi bilan qiyoslash keyingi tadqiqotlarning muhim yo‘nalishi hisoblanadi.

FOYDALANILGAN ADABIYOTLAR

1. Ross R. Guide for Conducting Risk Assessments. NIST Special Publication 800-30 Revision 1. — Gaithersburg: National Institute of Standards and Technology, 2012. DOI: 10.6028/NIST.SP.800-30r1. Mazkur standart riskni tahdid, zaiflik, yuzaga kelish ehtimoli va potensial ta’sir kabi omillar asosida baholash uchun metodologik asos beradi. (NIST)

2. OWASP Foundation. OWASP Top 10:2021 — The Ten Most Critical Web Application Security Risks. — 2021. Ushbu manbada web-ilovalar uchun Broken Access Control, Injection, Security Misconfiguration, Identification and Authentication Failures, SSRF va boshqa asosiy xavf kategoriyalari tizimlashtirilgan. (OWASP Foundation)
OWASP Top 10:2021

3. OWASP Foundation. OWASP Core Rule Set (CRS). OWASP CRS ModSecurity va boshqa mos WAF tizimlari uchun umumiy hujumlarni aniqlash qoidalari majmuasi bo‘lib, keng turdagi web-hujumlardan himoyalanish va false alert holatlarini minimallashtirishga yo‘naltirilgan. (devguide.owasp.org)
OWASP Core Rule Set

4. Ristić I. ModSecurity Handbook: Getting Started. — Feisty Duck. Ushbu manbada ModSecurity asosidagi web-ilovalar xavfsizligi, trafikni tekshirish va himoya qoidalarini shakllantirishning amaliy jihatlari yoritilgan. (feistyduck.com)

5. National Institute of Standards and Technology. Managing Information Security Risk: Organization, Mission, and Information System View. NIST SP 800-39. — Gaithersburg: NIST. Axborot xavfsizligi risklarini tashkilot, biznes vazifalari va axborot tizimlari darajasida integratsiyalashgan holda boshqarishga metodologik asos beradi. (NIST Computer Security Resource Center)

6. National Institute of Standards and Technology. Security and Privacy Controls for Information Systems and Organizations. NIST SP 800-53 Rev. 5. — Gaithersburg: NIST. Axborot tizimlarida xavfsizlik nazorati choralarini shakllantirish va risklarni kamaytirish uchun kompleks nazorat mexanizmlarini belgilaydi. (NIST Computer Security Resource Center)

7. OWASP Foundation. OWASP Top 10 Project — Official Document Repository. OWASP Top 10 metodologiyasi va web-ilovalar xavfsizligi risklarining yangilanib boruvchi tasnifini o‘z ichiga oladi. Rasmiy repozitoriyda 2025-yilgi yakuniy versiya ham e’lon qilingan. (GitHub)