VEB-ILOVALARGA TAHDIDLAR VA HIMOYA QILISHNING MAVJUD USULLARI TAHLILI

Raxmatov Furqat Abdirazzoqovich
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
Hududiy o‘quv muassasalari boshqarmasi boshlig‘i, texnika fanlari nomzodi.
https://doi.org/10.5281/zenodo.11380401

Annotatsiya. *Ushbu maqolada SQL in’eksiyasi, saytlararo skript va boshqalar kabi veb-ilovalarga turli xil hujumlar, veb-ilovalar xavfsizligini ta’minlash uchun qo‘llanilishi mumkin bo‘lgan mavjud usullar tahlil qilinadi. YAkunida veb-ilovalarga tahdid va hujumlardan samarali himoya qilish uchun mashinani o‘qitish va sun’iy intellekt usullaridan foydalanish afzalliklari ko‘rsatilgan.*

Bugungi kunda veb-ilovalar foydalanuvchilarning shaxsiy ma’lumotlari, moliyaviy ma’lumotlari va korporativ ma’lumotlar kabi nozik ma’lumotlarni qayta ishlash va saqlash uchun keng qo‘llaniladi. Biroq, veb-ilovalarning tobora ommalashib borayotgani, shuningdek, veb-ilovalarning zaifliklarini topishga va ulardan foydalanishga intilayotgan tajovuzkorlarning e’tiborini tortmoqda. Ular ma’lumotlarni buzish, ilovalarning funksionalligini buzish yoki hatto veb-serverlarni butunlay buzishga qaratilgan turli hujumlarni amalga oshirishi mumkin.

Veb-ilovalar tajovuzkorlarning turli tahdidlari va hujumlariga duchor bo‘ladi. Quyidagilar veb-ilovalarga tahdid va hujumlarning eng keng tarqalgan turlariga quyidagilar keltirish mumkin [3, 4]:

1. SQL in’eksiya.
2. Saytlararo skript.
3. O‘g‘irlangan sessiyalar.
4. Fishing.
5. Xizmatni rad etish hujumlari.

SQL in’eksiya veb-ilovalar uchun eng keng tarqalgan tahdidlardan biridir. Ma’lumotlar bazasi bilan ruxsatsiz amallarni bajarish uchun tajovuzkorlar zararli SQL-kodini foydalanuvchi kirish oynalari orqali kiritadilar. Ko‘pgina hollarda, tajovuzkor ushbu ma’lumotlarni o‘zgartirishi yoki o‘chirishi mumkin. Muvaffaqiyatli SQL in’eksiya hujumi parollar, kredit karta ma’lumotlari yoki foydalanuvchilarning shaxsiy ma’lumotlari kabi maxfiy ma’lumotlarga ruxsatsiz kirishga olib kelishi mumkin.

Saytlararo skript zararli kod yoki skriptlar bo‘lib, hujumchilar veb-sahifalarga ularni kiritadilar. Keyinchalik bu kod yoki skriptlar mijoz tomonida bajariladi. Bu ularga seanslarni o‘g‘irlash yoki foydalanuvchini zararli saytlarga yo‘naltirish kabi turli xil operatsiyalarni bajarishga imkon beradi. Uning asosiy xavfi shundaki, tajovuzkor ulardan to‘lov kartalari, foydalanuvchilarning kompyuterlari va boshqalarga kirish uchun foydalanishi mumkin.

O‘g‘irlangan sessiyalar faol foydalanuvchi sessiyalarining noqonuniy egallanishi bo‘lib, hujumchilar ruxsatsiz kirish yoki haqiqiy foydalanuvchilar nomidan turli harakatlarni amalga oshirishi mumkin. Hujumchilar foydalanuvchi sessiyasiga kirish uchun foydalanishi mumkin bo‘lgan bir nechta usullar mavjud, jumladan paketlarni ushlash, saytlararo skript va “o‘rtada odam”

hujumlari. Quyida turli dasturlash tillarida sessiyalarni o‘g‘irlanishiga sababchi bo‘ladigan zaif kod namunasi keltirilgan:

PHP:

```
session_start();
$session_id = session_id();
echo "Your session ID is: ".$session_id;
```

Ushbu kod sessiyani o‘g‘irlash hujumlariga qarshi himoyasiz, chunki u shunchaki joriy sessiya identifikatorini takrorlaydi, agar u foydalanuvchi brauzeriga yoki tarmoq trafigiga kirish imkoniga ega bo‘lsa, tajovuzkor tomonidan osongina o‘g‘irlanishi mumkin.

Python:

```
import requests
session = requests.Session()
response = session.get("https://example.com")
print("Your session ID is: "+session.cookies.get_dict()["session_id"])
```

Ushbu kod sessiyani o‘g‘irlash hujumlariga ham zaifdir, chunki u javobda oddiy matnda sessiya identifikatorini taqdim etadi.

JavaScript:

```
var session_id = localStorage.getItem("session_id");
console.log("Your session ID is: "+session_id);
```

Ushbu kod sessiyani o‘g‘irlash hujumlariga qarshi himoyasiz, chunki u foydalanuvchi brauzeriga kirish huquqiga ega bo‘lgan tajovuzkor osongina kira oladigan mahalliy xotiradan sessiya identifikatorini oladi.

Fishingda soxta veb-sahifalar yoki elektron pochta xabarlaridan foydalaniladi. Ushbu hujumda tajovuzkorlar foydalanuvchilarni osongina aldash va ularning maxfiy ma’lumotlarini olish uchun qonuniy platformalar yoki tashkilotlarni taqlid qiladigan soxta veb-sahifalar yoki elektron pochta xabarlarini yaratadilar. Kirish uchun foydalanuvchi o‘zining shaxsiy ma’lumotlaridan foydalanadi va natijada tajovuzkor bu ma’luotlarga ega bo‘ladi.

Xizmatni rad etish hujumlari DoS (Denial-Of-Service) va taqsimlangan xizmatni rad etish Distributed Denial Of Service (DDoS) nomlari bilan mashxur. Bular veb-serverni yoki boshqa hisoblash tizimini ishdan chiqaradi. Tajovuzkorlar veb-dastur resurslarini bitta manbadan (DoS) yoki bir nechta manbalardan (DDoS) ortiqcha yuklaydi. Bu qonuniy foydalanuvchilar uchun veb-ilovadan foydalanish imkoniyatini kamaytiradi. Hukumat veb-saytlari, yirik portallar, onlayn ommaviy axborot vositalari, onlayn o‘yin serverlari, onlayn-do‘konlar va moliya sektorining korporativ veb-saytlari bunday hujumlarning qurboni bo‘ladi [1].

Mavjud himoya usullarini

Veb-ilovalarga tahdid va hujumlardan himoya qilishning ko‘plab usullari mavjud. Bu ular veb-ilovalarni samarali himoya qilish bilan birga qator kamchiliklarga ham ega. Quyida ular qaida batafsil ma’lumot keltirilgan [4, 6, 7]:

1. *Kirishni filtrlash va tasdiqlash usullari* foydalanuvchi tomonidan zararli kod kiritilishini yoki yaroqsiz belgilar uchun tekshirish imkonini beradi. Ammo bu usullar filtrlar va tekshirish qoidalarini diqqat bilan aniqlash va sozlashni talab etadi, shuningek noto‘g‘ri sozlash qaysidir ilova funsiyalariga va foydalanish qulayligiga ta’sir qilishi mumkin.

2. *Ma’lumotlarni shifrlash usullari* mijoz va server o‘rtasida uzatiladigan ma’lumotlarni himoya qilish uchun, shuningdek uni saqlashda ishlatiladi. SHifrlash ma’lumotlarning maxfiyligini

ta’minlaydi. Ammo shifrlash serverlariga qo‘shimcha yuk qo‘shishi va javob vaqtini oshiradi hamda xavfsiz shifrlashni ta’minlash uchun yaxshi kalit va sertifikatlarni boshqarish talab qilinadi.

3. *Sessiyani boshqarish usuli* foydalanuvchi seanslarini boshqarish va tekshirish uchun xavfsiz mexanizmlardan foydalanish belgilaydi. Kuchli sessiya identifikatorlarini yaratish, sessiya ma’lumotlarini to‘g‘ri saqlash va o‘chirish kabi choralar sessiya o‘g‘irlanishini oldini olishga yordam beradi. Ushbu usulning kamchiligi sessiya ma’lumotlarini saqlash va qayta ishlash uchun qo‘shimcha resurslarni talab qiladi, sessiyani noto‘g‘ri boshqarish faol sessiyalarni ushlab qolish yoki autentifikatsiyaning etarli emasligi kabi zaifliklarga olib kelishi mumkin.

4. *Ko‘p faktorli autentifikatsiya usuli* parol, biometrik ma’lumotlar, bir martalik kod kabi ikki yoki undan ortiq autentifikatsiya omillarini talab qiladi. Ko‘p faktorli autentifikatsiya foydalanuvchiga kirish xavfsizligini oshiradi, chunki muvaffaqiyatli kirish nafaqat parolni bilishni, balki boshqa omilning mavjudligini ham talab qiladi. Ushbu usuldan foydalanish bir nechta omillarni taqdim etish zarurati tufayli foydalanuvchilar uchun noqulaylik tug‘diradi, bunday tizimni amalga oshirish uchun qo‘shimcha integratsiya va sozlamalarni talab qiladi.

Tahlilllar shuni ko‘rsatadiki mavjud himoya usullari o‘zining afzalliklari bilan birgalikda kamchiliklariga ham ega. SHuning uchun veb-ilovalarni samarali himoya qilish ko‘pincha yangi usullarni talab qiladi.

Sun’iy intellekt usullaridan foydalanish

An’anaviy xavfsizlik usullari statik bo‘lishi mumkin va hujumlarning yangi turlariga yoki tajovuzkorlarning xatti-harakatlaridagi o‘zgarishlarga moslasha olmaydi. Signaturali aniqlash kabi ushbu himoya usullari oldindan ma’lum bo‘lgan hujumlariga asoslangan. Biroq, hujumlarning yangi turlari signatura ma’lumotlar bazasida tavsiflanmagan noma’lum bo‘lishi mumkin. Mashinani o‘qitish va sun’iy intellekt (SI) usullaridan foydalanish tizimga katta hajmdagi ma’lumotlarni tahlil qilish va nostandart hujumlarni aniqlash imkonini beradi [1, 2].

Veb-ilovalarni himoya qilishda sun’iy intellektdan foydalanish hujumlarni aniqlash va oldini olish jarayonini avtomatlashtirishga, shuningdek xavfsizlik tizimlarining samaradorligini oshirishga imkon beradi.

Sun’iy intellektdan foydalanishning asosiy afzalliklaridan biri bu tizimning o‘zgaruvchan tahdid muhitiga moslashish qobiliyatidir. Kiberjinoyatchilar doimiy ravishda hujumning yangi usullarini ishlab chiqmoqdalar va xavfsizlik tizimlari ular bilan kurashishga tayyor bo‘lishi kerak. Sun’iy intellektdan foydalanish tizimga hujumlarning yangi turlariga tezda moslashish va real vaqtda himoya algoritmlarini yangilash imkonini beradi.

Bundan tashqari, SI anomaliyaga asoslangan hujumlarni aniqlash va oldini olishga yordam beradi. Foydalanuvchilarning g‘ayritabiiy xatti-harakatlari yoki tizimdagi g‘ayrioddiy hodisalar ruxsatsiz kirishga urinish yoki zararli faoliyatni ko‘rsatishi mumkin. Mashinani o‘rganish va SI usullaridan foydalanish tizimga bunday anomaliyalarni avtomatik ravishda aniqlash va hujumlarning oldini olish uchun tegishli choralarni ko‘rish imkonini beradi.

Veb-ilovalarni himoya qilish uchun sun’iy intellektdan foydalanish bir qator imkoniyatlar va afzalliklarni beradi:

- Katta hajmdagi ma’lumotlarni tahlil qilish orqali hujumni aniqlashni avtomatlashtirish va g‘ayritabiiy foydalanuvchi xatti-harakatlarini yoki potensial zararli faoliyatni, shu jumladan SQL inyeksiyasi, saytlararo skript va boshqalarni aniqlash imkonini beradi.

- Hujumlarni yuqori aniqlik va minimal miqdordagi noto‘g‘ri pozitivlar bilan aniqlay oladigan modellarni yaratish hujumlarga javob berish vaqtini qisqartirish va xavfsizlik ma’murlariga yukni kamaytirish orqali ishlash va aniqlik yaxshilash imkonini beradi.

- Sun’iy intellekt yangi ma’lumotlardan saboq olishi va yangi turdagi hujumlarga moslasha oladi, bu esa veb-ilovalarni himoya qilish tizimini doimiy rivojlanayotgan tahdidlar bilan kurashishda yanada moslashuvchan va samarali bo‘lishiga imkon beradi.

- Sun’iy intellekt yangi tahdidlarni bashorat qilish, ishlab chiquvchilar va ma’murlarga kelajakdagi hujumlarning oldini olish choralarini ko‘rish uchun hujumlar hamda zaifliklar haqidagi ma’lumotlarni tahlil qilishiga yordam beradi.

Xulosa

Ushbu maqolada veb-ilovalarga tahdid va hujumlardan himoya qilishning mavjud usullari va vositalari tahlil qilinib, har xil turdagi tahdid va hujumlar, shuningdek, ulardan himoya qilish usullari va vositalari ko‘rib chiqildi. Veb-ilovalarga tahdid va hujumlardan himoya qilishning mavjud usullari va vositalarini tahlil qilish mutlaq xavfsizlikni ta’minlaydigan universal echim yo‘qligini tasdiqlaydi.

Veb-ilovalarni himoya qilish uchun sun’iy intellekt usullaridan foydalanish ko‘plab imkoniyatlar va afzalliklarni taqdim etadi. Ular hujumlarni avtomatik ravishda aniqlash va tasniflash, anomal holatlarni tasniflash, yangi tahdidlarga moslashish, zararli harakatlarning oldini olish uchun kontent va foydalanuvchi xatti-harakatlarini tahlil qilish imkonini beradi.

Kelgusida veb-ilovalarga tahdid va hujumlardan himoya qilishning yangi usullari va vositalarini tadqiq qilish va ishlab chiqishni davom ettirish kerak. Ushbu sohadagi tadqiqotlar DDoS hujumlar, SQL in’eksiyalari, saytlararo skriptlar va boshqalar kabi veb-ilovalarga turli xil hujumlarni aniqlash uchun mashinani o‘qitish algoritmlari, neyron tarmoqlari va boshqa sun’iy intellekt usullaridan foydalanish orqali ijobiy natijalar olish mumkin.

FOYDALANILGAN ADABIYOTLAR

1. Antoni Jaszcz, Dawid Połap. AIMM: Artificial Intelligence Merged Methods for flood DDoS attacks detection: Journal of King Saud University – Computer and Information Sciences, 2022, pp. 8090-8101.
2. Qinghui Liu, Tianping Zhang. Deep learning technology of computer network security detection based on artificial intelligence. Journal of Computers and Electrical Engineering, 2023, pp. 1–10.
3. Odiaga Gloria Awuor. Review of the security challenges in web-based systems: World Journal of Advanced Engineering Technology and Sciences, 2023, 08(02), pp. 204–216.
4. "OWASP Top 10 - 2021: The Ten Most Critical Web Application Security Risks". Open Web Application Security Project. 2021. Retrieved January 11, 2022.
5. Singh N.K., Gupta P., Singh V. and Ranjan R., "Attacks on Vulnerable Web Applications," 2021 International Conference on Intelligent Technologies (CONIT), 2021, pp. 1-5, doi:10.1109/CONIT51480.2021.9498396.
6. Kohei Kubota; Wai Kyi Kyi Oo; Hiroshi Koide, "A New Feature to Secure Web Applications", Eighth International Symposium on Computing and Networking Workshops (CANDARW), 2020, pp. 334-340, DOI: 10.1109/CANDARW51189.2020.00071
7. WASC (Web Application Security Consortium). Retrieved from https://www.webappsec.org/