RAQAMLI IQTISODIYOT VA AXBOROT TEXNOLOGIYALARI
2023
№4 (12),
oktabr-dekabr
http://dgeconomy.tsue.uz/
ILMIY ELEKTRON JURNAL

WEB SAYTLAR XAVFSIZLIGI, KIBER TAHDIDLAR VA ULARDAN HIMOYA QILISHNING USULLARI

Maxmudov Abbos Sherali o‘g‘li
TDIU “Raqamli iqtisodiyot va axborot texnologiyalari” kafedrasi assistenti
abbos.maxmudov@tsue.uz

Annotatsiya
Ushbu maqolada veb-sayt xavfsizligiga tahdid soluvchi bir nechta kiberhujumlar haqida yoritilgan. Ularning bir-biridan farqlari hamda yillik statistik tahlillari keltirib o‘tilgan. Bundan tashqari, maqolada veb-saytlarni himoya qilishning samarali usullari, jumladan, veb ilovalar uchun xavfsizlik devori, antivirus dasturlari, xavfsizlik siyosati kabi kiberhujumlarni oldini oluvchi amaliy tavfsiyalar keltirilgan. Umuman olganda, maqola veb-sayt xavfsizligining ahamiyati va kiber tahdidlardan himoyalanish usullari haqida keng qamrovli tushunchalarni beradi.

Аннотация
В этой статье рассматриваются несколько кибератак, которые угрожают безопасности веб-сайта. Упоминаются их различия и ежегодный статистический анализ. Кроме того, в статье представлены практические описания эффективных способов защиты веб-сайтов, включая брандмауэры веб-приложений, антивирусное программное обеспечение и политики безопасности для предотвращения кибератак. В целом, статья дает всестороннее понимание важности безопасности веб-сайтов и способов защиты от киберугроз.

Abstract
This article covers several cyber attacks that threaten website security. Their differences and annual statistical analysis are mentioned. In addition, the article provides practical descriptions of effective ways to protect websites, including web application firewalls, antivirus software, and security policies to prevent cyberattacks. Overall, the article provides a comprehensive understanding of the importance of website security and ways to protect against cyber threats.

Калит сўзлар
Kiberjinoyatchi, kiberjinoyat, kibertahdid, malware, ransomware, spyware, pop-up oynasi, DDoS, attacker, SQL injection, Cross-Site Scripting, XSS, firewall

Ключевые слова
Киберпреступник, киберпреступность, киберугроза, вредоносное ПО, программа-вымогатель, шпионское ПО, всплывающее окно, DDoS, атакующий, SQL-инъекция, межсайтовый скриптинг, XSS, брандмауэр.
Keywords
Cybercriminal, cybercrime, cyberthreat, malware, ransomware, spyware, pop-up window, DDoS, attacker, SQL injection, Cross-Site Scripting, XSS, firewall.

Kirish

Bugungi raqamli asrda veb-saytlar kommunikatsiya, portal, tijorat va ma’lumot almashish uchun platforma bo‘lib xizmat qiluvchi biznes va tashkilotlarning muhim tarkibiy qismiga aylandi. Biroq, veb-saytlarga bo‘lgan ishonch ortib borishi bilan bir qatorda, saytdagi muhim sanalgan ma’lumotlarni zararlash, sayt egalarining obro‘siga putur yetkazadigan va hatto moliyaviy yo‘qotishlarga olib keladigan kiber tahdidlar xavfi ortadi. Veb-sayt egalari uchun sayt xavfsizligini birinchi o‘ringa qo‘yish va ularni kiber tahdidlardan himoya qilish choralarini ko‘rish har qachongidan ham muhimroqdir. Maqolada veb-sayt xavfsizligining ahamiyati, veb-saytlar duch keladigan kiber tahdidlarning keng tarqalgan turlari hamda ulardan qanday himoyalanish bo‘yicha na’zariy va amaliy ko‘nikmalar berib o‘tiladi.

Veb-sayt xavfsizligi veb-saytni ruxsatsiz kirish, ma’lumotlarni o‘g‘irlash va boshqa turdagi kiber tahdidlardan himoya qilish uchun ishlatiladigan choralar va usullarni anglatadi.

Veb-sayt xavfsizligi bir necha sabablarga ko‘ra muhimdir:

- birinchidan, veb-saytlar ko‘pincha kiberjinoyatchilar uchun kerakli nishon bo‘lishi mumkin bo‘lgan shaxsiy ma’lumotlar yoki davlat sirlariga doir ma’lumotlar kabi sirli ma’lumotlarni saqlaydi.
- ikkinchidan, veb-saytga muvaffaqiyatli kiberhujum obro‘ga putur yetkazishi, moliyaviy yo‘qotishlar va qonuniy javobgarlikka olib kelishi mumkin.
- uchinchidan, veb-saytlar ko‘pincha biznes IT infratuzilmasining boshqa qismlariga ulanadi, ya’ni xavfsizlik buzilishi boshqa tizimlar va qurilmalarga tarqalishi mumkin. Umuman olganda, veb-sayt xavfsizligi veb-sayt ma’lumotlari va resurslarining maxfiyligi, yaxlitligi va mavjudligini ta’minlashning muhim jihati hisoblanadi.

Mavzuga oid adabiyotlar tahlili

H. Yulianton, H.L.H.S. Warnars, B. Soewito, F.L. Gaol va E. Abdurachman tadqiqotlariga ko‘ra, veb-saytlardagi zaifliklarni skanerlash ya’ni tekshirish bo‘yicha yechimlar taqdim etilgan. Qolaversa, veb-hujumlarni oldini olish va veb-xavfsizlikni yaxshilash uchun bir nechta ko‘rsatmalar berilgan [3,15].

Muhammad Agreindra Helmiawan olib borgan tadqiqotlarga ko‘ra, veb-sayt xavfsizligi darajasini bilish va xavfsizlikni baholash uchun Open Web Application Security Project 10 (OWASP 10) tizimini qo‘llaydi. Bu tizim veb-saytdagi zaif tomonlarni topish uchun veb-ilovalar xavfsizligiga e’tibor qaratibgina qolmay veb-saytning qo‘shimcha xavfsizlikka bo‘lgan ehtiyojni va veb-sayt xavfsizligi uchun kerakli tavsiyalarni aniqlash uchun oltita sub-domen bilan birga Internet xavfsizligini tahlil qiladi va sinovdan o‘tkazadi [1].

Dr. Rajendra Maurya tadqiqotlariga ko‘ra esa, veb-saytlardagi tahdidlarning evolyutsiyasi hujumning yangi usullarining paydo bo‘lishi hamda simulyatsiya qilingan operatsion tizimlar yoki virtual mashina dasturiy ta’minot muhitlaridan foydalanishga qarshilik qilish bilan bog‘liq bo‘lishi mumkinligi aytiladi. Ushbu tadqiqot hozirgi kibermakonda veb xavfsizlik bilan bog‘liq bo‘lgan bir qancha muammolarni o‘rganadi [2,15].

Justin Hanes tomonidan olib borilgan tadqiqotlarga ko‘ra, web saytda foydalanuvchi autentifikatsiyasi uchun barmoq izlaridan foydalanish tizimini yaratish keltirilgan. Unda, joriy foydalanuvchining barmoq izini skanerlash va uni vakolatli foydalanuvchi bilan bog‘langan barmoq izi bilan solishtirish uchun USB qurilmasiga o‘rnatilgan barmoq izi skaneri orqali amalga oshiriladi [14,17].

A. Abidov tadqiqotlariga ko‘ra, axborot xavfsizligini ta’minlash uchun nosozliklarga chidamli dasturiy ta’minot yaratish usullari va mezonlari tahlil qilingan. Qolaversa, tahdidlar hamda xatoliklar oqibatlarini olidini olish uchun lokalizatsiya, diagnostika va tiklash usullari keng tahlil qilingan bo‘lib, ushbu dasturiy ta’minotlar orqali axborot xavfsizligini ta’minlash mumkin bo‘ladi [11,12].

D.R. Raxmatov bugungi kundagi kiberxavfsizlik muammolari va ularning eng yangi texnologiyalarda yuzaga kelish trendlarini o‘rgandi. Unga ko‘ra, kiberjinoyat kompyuter va internetni qo‘llagan holda shaxsiy ma’lumotlarni o‘g‘irlash, kontrabanda sotish va noto‘g‘ri kodlar bilan operatsiyalarni buzish hollarini oldini olishga qaratilgandir [13].

O. Mirzayev izlanishlariga ko‘ra, Veb-sahifalar gipermatnni uzatish protokoli (HTTP) va shifrlash (HTTP Secure) xavfsizlik mexanizmlaridan foydalangan holda kiberjinoyatlarning oldini olish uchun veb-saytlarning xavfsizligini qisman bo‘lsa ham ta’minlaydi. Lekin veb-saytlarni xavfsizligini oldini olish uchun yanada optimal yechim sifatida samarali xavfsizlik dasturini ishlab chiqishni taklif etadi [9].

R.A. Xoldarboyev, R.A. Abduvaxobovalarning tadqiqotlariga ko‘ra, xavfsizlik printsiplari, muhim xavfsizlik nazorati va kiberxavfsizlikning eng yaxshi amaliyotlarini o‘z ichiga olgan xavfsizlik asoslarini tushuntiradi. Xavfsizlik dasturlari potentsial zararli dasturlarni foydalanuvchining xatti-harakatlarini tahlil qilish va yangi zararli hujumlarni qanday yaxshiroq aniqlashni o‘rganish mumkinligi aytiladi [10].

Ushbu tadqiqotlardan ko‘rish mumkinki, raqamli dunyoda veb-sayt xavfsizligi muhim ahamiyat kasb etadi. Kiber tahdidlar kundan-kun rivojlanib bormoqda, yangi turdagi kiberhujumlar va zaifliklar paydo bo‘lmoqda. Shu sababli, ushbu tahdidlarni aniqlash va ularni oldin olish uchun samarali strategiyalarni ishlab chiqish uchun doimiy izlanishlar zarurdir.

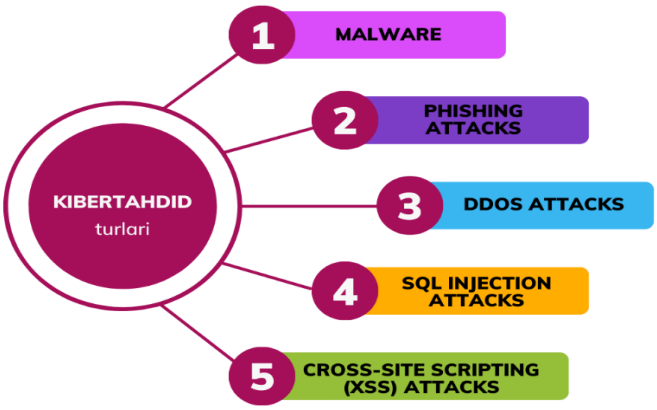
Tadqiqot metodologiyasi

Veb-sayt xavfsizligi, kibertahdidlar va ulardan himoyalanish mavzusida tadqiqot olib borgan bir qancha olimlarning ilmiy izlanishlari va maqolalari tahlil qilindi. Izlanishlar shuni ko‘rsatadiki, veb-saytning xavfsizligi, uni kiberhujumlardan yetarli darajada himoya qilish nafaqat veb-sayt egalari balki barcha raqamlashtirilgan tarmoqlarning kiberhimoyasini ta’minlaydi. Maqolada ayni damdagi top kiber tahdidlar, ularni oldini olish bo‘yicha turli xil amaliy yechimlar taqdim etilgan.

Tahlil va natijalar

Veb-sayt xavfsizligi - sayt ma’lumotlarining kiberjinoyatchilarga ta’sir qilmasligini ta’minlash yoki veb-saytdan biron-bir tarzda ekspluatatsiya qilinishini oldini olish uchun amalga oshirilgan har qanday harakat yoki dastur. Ushbu harakatlar veb-saytdagi maxfiy ma’lumotlar, apparat va dasturiy ta’minotni hozirda mavjud bo‘lgan turli xil hujumlardan himoya qilishga yordam beradi.

Quyida veb-saytlarga xavf soluvchi hozirda keng tarqalgan kibertahdidlarni tahlilini ko‘rish mumkin (1-rasm):



1-rasm. Kibertahdid turlari

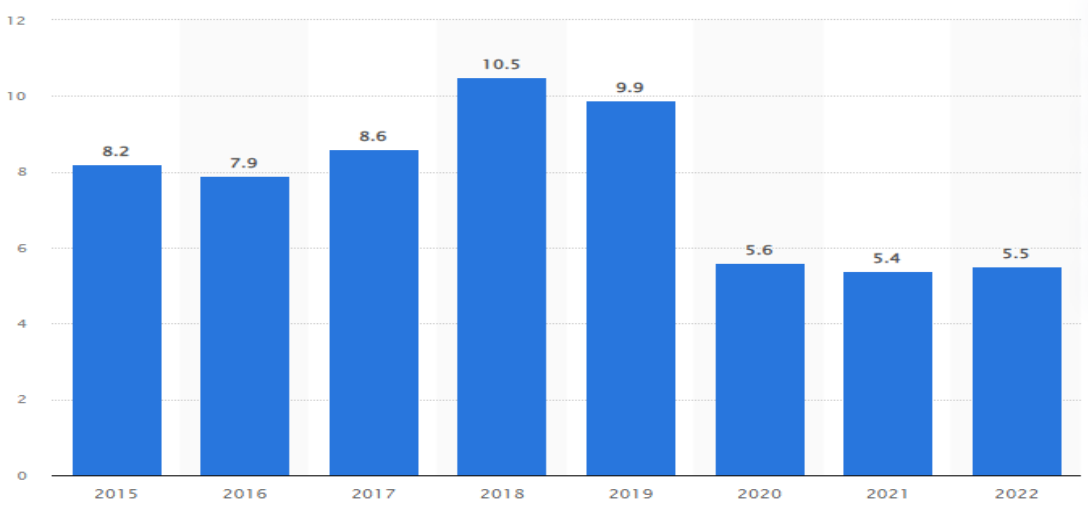
Malware (Ziyon yetkazuvchi dastur): - bu kiberhujum kompyuter tizimi, tarmoq yoki qurilmaga zarar yetkazish uchun mo‘ljallangan har qanday dasturiy ta’minotdir. Kibertahdidning bu turi veb-saytlarni viruslar, spyware (foydalanuvchining kompyuteriga kirib, qurilma va foydalanuvchidan ma’lumotlarni yig‘uvchi va ularning roziligisiz uchinchi shaxslarga yuboruvchi dastur turi), ransomware (bu tizim ekranini qulflash yoki to‘lov to‘lanmaguncha foydalanuvchilarning fayllarini bloklash orqali ularning o‘z tizimiga kirishiga to‘sqinlik qiluvchi yoki cheklovchi dastur turi) va boshqa turli sayt-xavfsizligiga putur yetkazuvchi dasturlar bilan ishlatilishi mumkin.

Phishing attacks (Fishing hujumlari): bu foydalanuvchilarni parollar, kredit karta raqamlari yoki boshqa shaxsiy ma’lumotlar kabi maxfiy informatsiyalarni aldov yo‘li bilan almashish uchun mo‘ljallangan kibertahdid turi sanaladi. Ushbu hujumlar elektron pochta, pop-up oynasi (kompyuter ekran yuzasiga paydo bo‘luvchi dastur oynasi) yoki qonuniy bo‘lganlarga taqlid qiluvchi soxta veb-saytlar shaklida bo‘lishi mumkin.

DDoS (Distributed Denial of Service attacks - DDoS hujumlari): veb-saytlarni trafik oqimi bilan to‘ldirish orqali nishonga oladigan kibertahdidning bir turidir. Bunga veb-sayt infratuzilmasi, dasturiy ta’minoti yoki ilova qatlamidagi zaifliklardan foydalanish orqali erishiladi. DDoS hujumlari odatda botnetlar yordamida amalga oshiriladi, ular attacker tomonidan masofadan boshqariladigan zararlangan kompyuterlar tarmoqlaridir. Botnetlar minglab yoki hatto millionlab buzilgan qurilmalardan iborat bo‘lishi mumkin, bu ularni DDoS hujumlarini amalga oshirish uchun kuchli vositaga aylantiradi.

SQL injection attacks (SQL in’ektsiya hujumlari): tajovuzkorlarga veb-ilovalar ma’lumotlar bazasiga qarshi zararli SQL bayonotlarini bajarishga imkon beruvchi veb-ilovalar xavfsizligi zaifligining bir turi. Bu kiberjinoyatchilarga ma’lumotlar bazasida saqlangan ma’lumotlarni ko‘rish, o‘zgartirish yoki o‘chirish imkonini beradi.

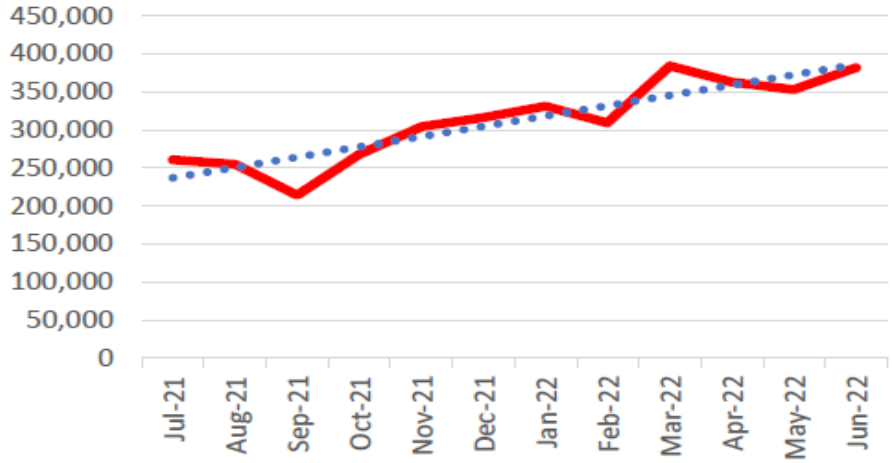
Cross-Site Scripting (XSS) attacks (Saytlararo skript hujumlari): kibertahdidning bir turi bo‘lib, attackerlar boshqa foydalanuvchilar tomonidan ko‘riladigan veb-sahifaga zararli kodni kiritishlari orqali hujum uyushtiradilar. Bu kiberjinoyatchilarga boshqa foydalanuvchilardan login hisob ma’lumotlari yoki seans cookie-fayllari kabi maxfiy ma’lumotlarni o‘g‘irlash imkonini beradi. XSS hujumlari ko‘pincha veb-ilova tomonidan to‘g‘ri tozalanmagan qidiruv maydonchalari yoki sharhlar bo‘limlari kabi kirish maydonlariga zararli kodni kiritish orqali amalga oshiriladi. Foydalanuvchi sahifani ko‘rganida, zararli kod o‘z brauzerida bajariladi, bu attackerga o‘z sessiyasiga kirish va uni boshqarish imkonini beradi.



2-rasm. Butun dunyo bo‘ylab malware kiberhujumlarining soni (mlrd)

Malware kibertahdid turi orqali amalga oshirilgan hujumlar 2022-yilda butun dunyo bo‘ylab 5,5 milliardga yetdi, bu esa avvalgi yilga nisbatan 2% ga oshganligini bildiradi. Eng ko‘p kiberhujumlar esa 2018-yilda qayd etilgan ya’ni 10,5 milliard (2-rasm) [4].

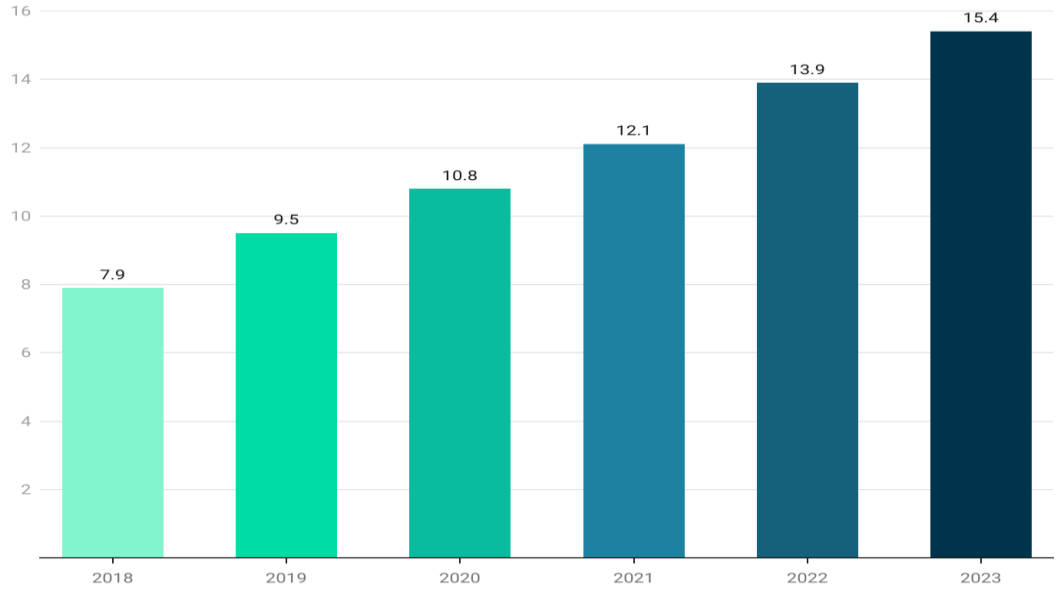
Statistik tahlillarga qaraganda, APWG (Phishing Activity Trends Report) talqiniga ko‘ra, 2022-yilning ikkinchi choragida jami 1 097 811 ta fishing hujumlari uyushtirilgan (3-rasm).



3-rasm. 2021-2022 yil oy kesimida fishing hujumlarining soni [5]

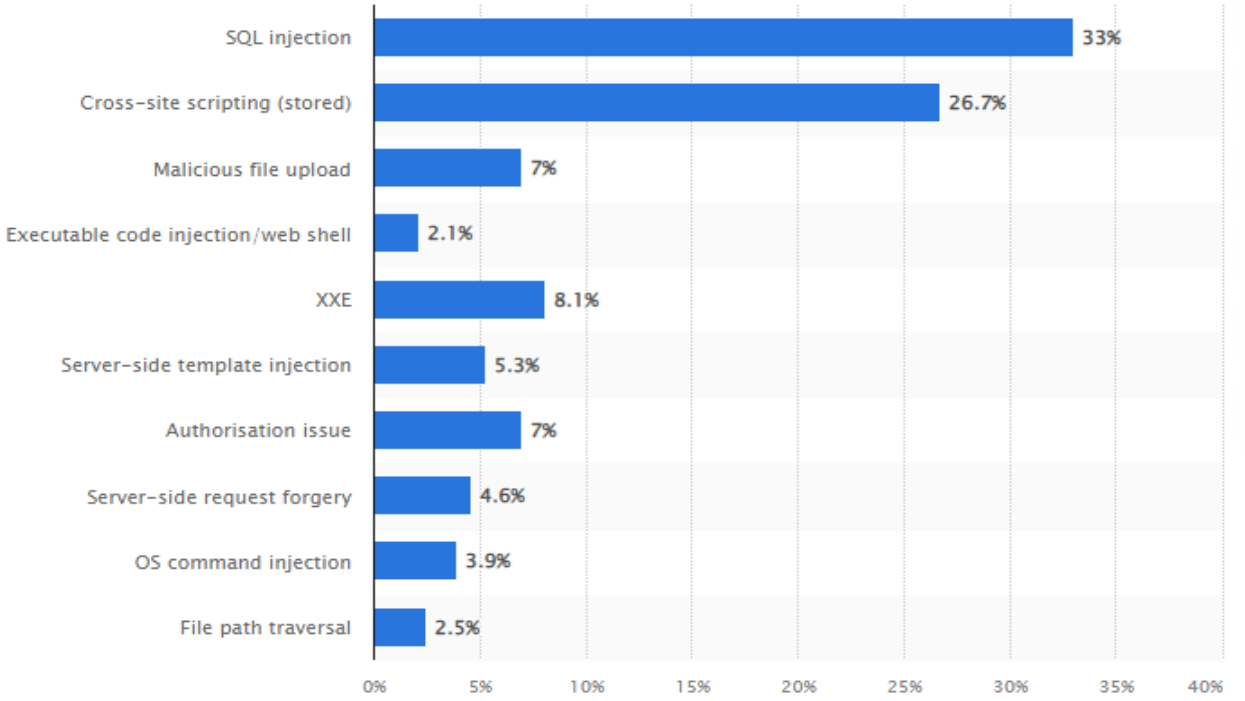
Cisco kompaniyasining [6] olib borgan izlanishlariga ko‘ra, 2018-2023 yillarda DDoS kiberhujumlari sonini tahmin qilingan (4-rasm). Unga ko‘ra, 2022-yilda 13 900 000 ta kibertahdidlar tahmin qilingan bo‘lsa, real ko‘rsatkichda bu juda yuqori

ya’ni 26 796 000 ta qayd etilgan [7,8]. O’sish sur’ati to‘rtinchi chorakda sekinlasha boshlagan va dekabrga kelib, hujumlar 53% ga kamaygan.



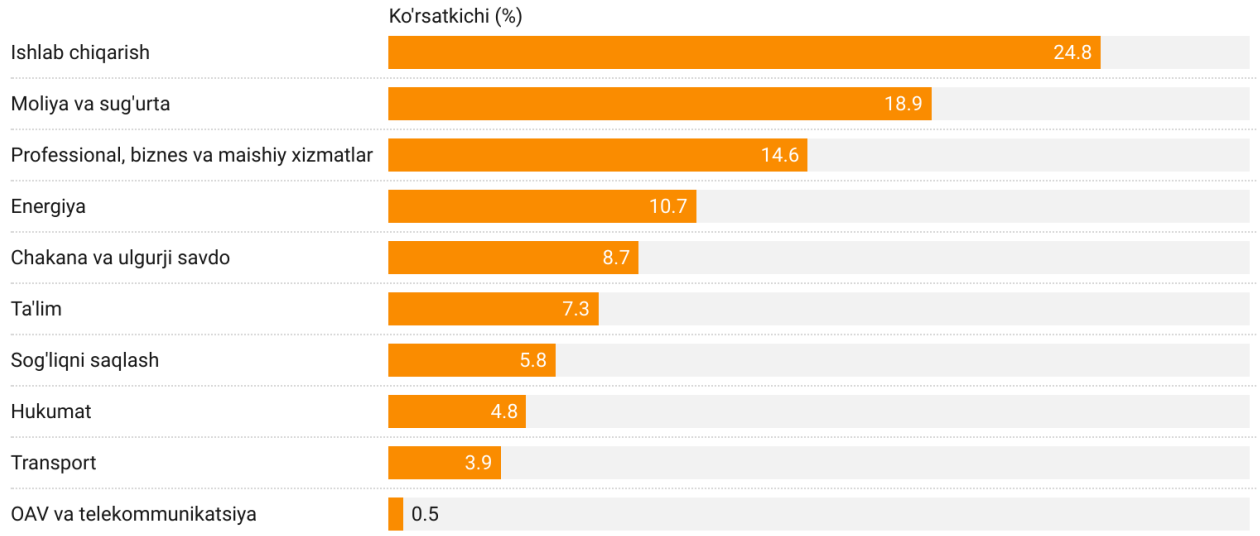
4-rasm. Dunyo bo‘ylab DDoS hujumlarining soni [6]

2022-yilda global miqyosda veb-ilovalar uchun asosiy kibertahdidlar SQL in’ektsiya turi bo‘lib 33 foizni tashkil qilgan bo‘lsa, internetdagi muhim zaifliklarning 26,7 foizi saytlararo skriptlar (XSS) hujumlari bilan bog‘liq (5-rasm).



5-rasm. 2022 yildan boshlab butun dunyoda veb-ilovalar uchun turlari bo‘yicha muhim zaifliklarning tarqalishi [4]

2022 yilda ishlab chiqarish sohasi dunyoda yetakchi tarmoqlar orasida kiberhujumlarning eng yuqori ulushiga ega bo‘ldi. Ushbu yil davomida ishlab chiqarish kompaniyalariga kibertahdidlar umumiy hujumlarning qariyb 25 foizini tashkil qilgan (6-rasm).



6-rasm. Kiberhujumlarning sohalar bo‘yicha umumiy statistikasi [4]

Statistik tahlillar shuni ko‘rsatadiki, yuqorida ta’kidlangan kiberhujumlarning barcha turlarida kutilganidan ko‘p hujumlar sodir bo‘lgan. Bu hujumlardan himoyalanish uchun birinchi navbatda qanday himoyalanish vositalari borligi, himoyalanishda nimalarga e’tibor berish kerakligini o‘rganish maqsadga muvofiq bo‘ladi.

Quyida kiber tahdidlarni chetlab o‘tish va veb-saytni himoya qilishning amaliy usullari keltirilgan:

Veb ilovalar uchun xavfsizlik devori (web application firewall - WAF) - bu veb-ilovalarni himoya qiluvchi dasturiy yoki apparatga asoslangan xavfsizlik devori. U veb-sayt serveri va ma’lumotlar havolasi o‘rtasida bog‘lovchi vazifasini bajaradi. Texnik jihatdan, u server va brauzer orasidagi o‘tadigan barcha ma’lumotlarni o‘qiydi.

Aksariyat zamonaviy WAF lar kichik oylik abonent to‘lovi evaziga bulutga asoslangan bo‘lib, “plug-and-play” xizmati sifatida taqdim etiladi. Bulutli xizmat asosan serveringiz oldida o‘rnatiladi va barcha kiruvchi trafik uchun kanal vazifasini bajaradi. Veb-ilovaning xavfsizlik devorlari barcha xakerlik urinishlarini to‘xtatib, o‘rnatilgandan so‘ng, spamlar va zararli botlar kabi kiruvchi trafikning boshqa shakllarini filtrlash orqali to‘liq xotirjamlikni ta’minlaydi.

Antivirus dasturlari - Zararli dasturlardan va boshqa viruslardan himoya qilishning birinchi yo‘nalishlaridan biri bu tarmoqqa ulangan barcha qurilmalarga antivirus dasturlarini o‘rnatishdir. Antivirus dasturi zararli fayllarni tizimga o‘rnatilishini aniqlay oladi va oldini oladi va so‘nggi ta’riflarni kiritish uchun uni muntazam yangilab turish kerak.

Xavfsizlik siyosati - Tarmoqqa hujum qilish xavfini kamaytirishning uchinchi usuli bu xavfsizlik siyosatini amalga oshirishdir. Xavfsizlik siyosati tarmoqdagi barcha qurilmalar viruslar va zararli dasturlardan himoyalanganligini va foydalanuvchilar kuchli parollardan foydalanayotganligini ta’minlashga yordam beradi. Ushbu qoidalar, shuningdek, ba’zi tarmoq mintaqalariga kirishni va foydalanuvchi imtiyozlarini cheklashi mumkin.

Monitor faoliyati - tarmoqdagi faoliyatni kuzatish muhim sanaladi. Kuzatuv jurnallari va boshqa ma’lumotlar shubhali faoliyatni tezda aniqlashga zamin yaratadi,

bu esa xavfsizlik xodimlariga potentsial tahdidlarni tekshirish va yumshatish choralarini ko‘rishga imkon beradi.

Xulosa

Xulosa qilib aytganda, kibertahdidlar tobora murakkablashib borayotgan va keng tarqalgan bugungi raqamli asrda veb-sayt xavfsizligi juda muhim hisoblanadi. Ushbu maqolada kiberhujumlarning beshta asosiy turlari, ularning yillar kesimida va sohalar bo‘yicha umumiy tahlillari olib borildi va ulardan himoyalanishning usullari haqida hamda ularni qo‘llash orqali veb-saytga kiberhujum xavfini sezilarli darajada kamaytirish mumkinligi ko‘rsatildi. Shuni yodda tutish kerakki, veb-sayt xavfsizligi doimiy jarayon bo‘lib, paydo bo‘ladigan tahdidlarga qarshi turish uchun doimiy monitoring va takomillashtirishni talab qiladi.

Adabiyotlar ro‘yxati

1. Muhamad Agreindra Helmiawan, Yanyan Sofiyan, Esa Firmansyah, Fathoni Mahardika, Irfan FadilAgun Guntara “Analysis of Web Security Using Open Web Application Security Project 10” The 8th International Conference on Cyber and IT Service Management (CITSM 2020) On Virtual, October 23-24, 2020.
2. Rajendra Maurya (CCNA, CEH, CISSP) “Research Challenges and Issues in Web Security” www.hackingmadeeasy.com, www.rajendramaurya.in, www.voaservices.com.
3. H. Yulianton, H.L.H.S. Warnars, B. Soewito, F.L. Gaol va E. Abdurachman “Web security and vulnerability: a literature review” Journal of Physics: Conference Series 1477 (2020) 022028 doi:10.1088/1742-6596/1477/2/022028.
4. https://statista.com
5. https://apwg.org/trendsreports/
6. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html
7. https://www.infosecurity-magazine.com/blogs/2022-ddos-yearinreview/
8. https://www.a10networks.com/blog/5-most-famous-ddos-attacks/
9. Olim Mirzayev “Veb-saytlarda kiber xavfsizlikni ta’minlash choraları” “Актуальные вопросы развития инновационно-информационных технологий на транспорте” АВРИИТТ-2021 I-Республиканская научно-техническая конференция (Ташкент, 24-25 ноября 2021 года).
10. Xoldarboyev R.A., Abduvaxobova R.A. “Kiberxavfsizlik" Science and Education" Scientific Journal / Impact Factor - 3.567 (SJIF) July 2022 / Volume 3 Issue 7 www.openscience.uz / ISSN 2181-0842.
11. Abidov A. Diagnostics Of The State And Recovery Of Real Time Systems Performance. The 6th International Conference on Future Networks & Distributed Systems (ICFNDS ‘22), December 15, 2022, Tashkent, TAS, Uzbekistan. - DOI{10.1145/3584202.3584237}.
12. Abidov A.A., Mirzaaxmedov D.M. Анализ современных угроз информационной безопасности. «Raqamli iqtisodiyot va axborot texnologiyalari» elektron jurnali // 2022 йил, maxsus son-1. 8-13 б. http://dgeconomy.tsue.uz/jurnal/.

13. Raxmatov D.R. Kiber xavfsizlik muammolari va ularning eng yangi texnologiyalarda yuzaga kelish trendlarini o‘rganish // “Axborot kommunikatsiya texnologiyalari va dasturiy ta’minot yaratish” XV ilmiy-amaliy konferensiya 2020y.
14. Justin Hanes “Website Security” US20130067545A1 Patent citations.
15. R.E. Prez-Guzmn, Y. Salgueiro-Sicilia, and M. Rivera, “Communication systems and security issues in smart microgrids,” in 2017 IEEE Southern Power Electronics Conference (SPEC), pp. 1-6, Dec. 2017.
16. M.Z. Gunduz and R. Das, “Analysis of cyber-attacks on smart grid applications,” in 2018 International Conference on Artificial Intelligence and Data Processing (IDAP), pp. 1-5, Sept. 2018.
17. C. Lopez, A. Sargolzaei, H. Santana, and C. Huerta, “Smart Grid Cyber Security: An Overview of Threats and Countermeasures,” Journal of Energy and Power Engineering, vol. 9, July 2015.