VEB SERVERLARDA UCHRAYDIGAN TAHDIDLAR VA ZAIFLIKLAR

Nasrullayev Nurbek Baxtiyorovich
Axborot Texnologiyalari Universiteti
PhD dotsent

Barotova Zahro Akmaljon qizi
Muhammad al-Xorazmiy nomidagi Toshkent
Axborot Texnologiyalari Universiteti
E-mail: zbaratova0402@gmail.com

ANNOTATSIYA

Veb hajmi va adoptatsiyasi kengayib borgani sari, unga bo‘ladigan hujumlar ko‘lami jadal o‘smoqda. Katta buzilishlar va millionlab foydalanuvchi hisob ma’lumotlari haqida doimiy yangiliklar oqimi mavjud. Internetda yirik kompaniyalarning ilovalari ko‘payib borgani sari xavfsizlik masalalariga muhim e’tibor qaratilmoqda. Biroq, ushbu ilovalarning zaif himoyalanmagan nozik jihatlarini ham inobatga olib qo‘yish maqsadga muvofiq. Ushbu maqolada veb serverdagi tahdid va zaiflik masalalari ko‘rib chiqiladi, shu bilan birgalikda veb server xavfsizlik muammolari ham ko‘rib chiqiladi.

Kalit so‘zlar: xavfsizlik, veb server, tahdid, zaiflik, risk.

KIRISH

Veb server - bu fayllarni, veb sahifalarni saqlaydigan, mijozlardan keladigan so‘rovlarni HTTP orqali qayta ishlaydigan, foydalanuvchilarga tarmoq yoki internetga kirish imkonini beruvchi axborot texnologiyalari tizimi. Veb server apparat va dasturiy ta’minotni talab qiladi. Hujumchilar odatda serverga ruxsat olish uchun dasturiy ta’minotdagi ekspluatatsiyalarni nishonga oladilar [1].

Veb brauzer mijozning eng asosiy ilovasi bo‘lib, u foydalanuvchilar uchun veb sahifalarni ko‘rib chiqishning eng samarali usuli hisoblanadi. Hozirgi vaqtda veb brauzerlar ko‘p sonli bozorlarni egallash uchun asosan ko‘rish va ma’lumotlarni yuklab olishdan foydalanadi. Shu bilan birga, u hukumat, korxonalar, elektron tijorat platformasi, ijtimoiy tarmoq va boshqa sohalarni ham qamrab oladi[1]. Veb ilovalarning keng qo‘llanilishi va rivojlanishi bilan uning funksiyasi va interaktivligi ham yaxshilanmoqda [5].

ASOSIY QISM

Terminologiya

Tahdid – bu zaiflikdan foydalanish, qasddan yoki tasodifan zarar yetkazish yoki yo‘q qilish mumkin bo‘lgan har qanday xavf hisoblanadi. Tahdid bu xavfsizlikni buzish ehtimoli bo‘lib, u ruxsatsiz kirish yoki xizmatni rad etishlarni o‘z ichiga oladi. Tahdidlar tizim xavfsizligiga salbiy ta’sir ko‘rsatishi mumkin [2].

Zaiflik – bu tizimning xavfsizligini pasaytiradigan zaiflik yoki nuqson. Tahdid va zaiflik tushunchalarining bir-biridan asosiy farqi shundaki, tizimda tahdid bo‘lishining ehtimoli zaiflik bo‘lish ehtimolidan pastroq bo‘ladi. Zaiflik tizimning istalgan qismida mavjud bo‘lishi mumkin. Misol uchun apparat, dasturiy, tarmoq va server qismlarni keltirish mumkin. Zaifliklar tashqi tajovuzkor, script yoki ba’zi vositalar tomonidan amalga oshiriladi [3].

Risk – bu tahdidning zaiflikdan foydalanib, aktivlarga zarar yetkazishi mumkin bo‘lgan potensial. Riskga yuqoridagi ikkita tushunchaning birgalikda amalga oshirilishi sifatida qarash mumkin [2].

Tahdidlar

Veb-server xavfsizligi tahdidlari yoki muammolari quyidagilarni o‘z ichiga oladi:

- Kataloglar bo‘ylab hujumlar;
- DOS (xizmatni rad qilish hujumi);
- Domen nomi tizimini o‘g‘irlash;
- Sniffing;
- Fishing;
- Pharming;
- Buzilishlar;
- Profiling;
- Ruxsatsiz kirish;
- Kodning o‘zgartirilishi;
- Imtiyozlarni oshirish [1].

. Zaifliklar

Veb serverning zaif tomonlari serverga osonlikcha hujum qilish imkonini beradi. Ushbu zaifliklarga quyidagilarni misol qilish mumkin:

- Buzuq sozlamalar (Default settings);
- Operatsion tizim va tarmoqlarning noto‘g‘ri konfiguratsiyasi;
- Operatsion tizim va veb serverlarda baglar:
- Xavfsizlik siyosati va protseduralarining yo‘qligi [1].

Default settings. Foydalanuvchi identifikatori va parollari hujumchi tomonidan osongina taxmin qilinishi mumkin bo‘lgan sozlamalar tushuniladi. Default settings serverda foydalanish mumkin bo‘lgn buyruqlarni ishga tushirish kabi muayyan buyruqlarni bajarishga ruxsat etishni ham ishga tushirishi mumkin [4].

Operatsion tizim va tarmoqlarning noto‘g‘ri konfiguratsiyasi. Agar foydalanuvchida yaxshi parol mavjud bo‘lmasa, foydalanuvchilarga serverda buyruqlarni bajarishga ruxsat beruvchi ba’zi konfiguratsiyalar xavfli bo‘lishi mumkin [5].

Operatsion tizim va veb serverlarda baglar. Operatsion tizim yoki veb server dasturida aniqlangangan xatoliklar yoki baglar tizimga ruxsatsiz kirish uchun yo‘l ochishi mumkin [4].

Xavfsizlik siyosati va protseduralarning yo‘qligi. Antivirus dasturlarini yangilash, operatsion tizim va internetni tiklash kabi xavfsizlik siyosati va protseduralarining yo‘qligi server hujumchilari uchun xavfsizlik teshiklarini yaratishi mumkin.

Xavfsizlikni buzish turlari

Kategoriyasi	**Ta’rifi**
DoS	DoS hujumlarida hujumchi kompaniyaning serverlariga katta miqdordagi ma’lumot so‘rovlarini yuboradi. Ushbu hujum maqsadi veb serverlarni ortiqcha yuklash va qonuniy foydalanuvchilar uchun veb saytlarni yaroqsiz holatga keltirishdir. Ushbu turdagi xavfsizlik buzilishi veb saytlar orqali daromad oladigan kompaniyalar uchun muhim ahamiyatga ega. Biroq, ushbu hujumning oqibatlari kamdan-kam hollarda maxfiy ma’lumotlarning yo‘qolishiga olib keladi [2].
Mijoz ma’lumotlariga ruxsatsiz kirish	Ushbu turdagi hujumda mijoz ma’lumotlariga kirish huquqiga ega bo‘ladilar. Bu jismoniy holatlarda, ya’ni noutbukni, hardni, zaxira turlarini o‘g‘irlash yoki kompaniya tarmog‘iga elektron tarzda kirish orqali amalga oshiriladi. Kompaniya tarmog‘ida mijoz ma’lumotlari, ya’ni ismlar, manzillar, tug‘ilgan sanalar, kredit karta ma’lumotlari, ijtimoiy xavfsizlik raqamlari, tibbiy yozuvlar, onlayn xaridlar va boshqalar bo‘lishi mumkin. Ushbu turdagi hujumlar asosan huquqbuzarlik sifatida qabul qilinadi va mijozlarning ishonchlariga ta’sir ko‘rsatishi mumkin.
Hodim ma’lumotlariga ruxsatsiz kirish	Ushbu turdagi xavfsizlik buzilishi mijoz ma’lumotlariga ruxsatsiz kirishga o‘xshaydi. Shu kabi strategiyalardan foydalangan holda, tajovuzkor hodimlarning maxfiy ma’lumotlari, ismlar, ijtimoiy xavfsizlik raqamlari, ish haqi haqida ma’lumot va hokazolarga kirish huquqiga ega bo‘lishi mumkin. Biroq bunday hujumlarning ko‘lami kamroq [3].
Kompaniya ma’lumotlariga ruxsatsiz kirish	Kompaniya ma’lumotlari yangi samolyot dizayni, operatsion tizim manba kodi, yangi film yoki kompyuter o‘yinining bir qismi, kompaniyaning boshqa hisobot va hujjatlari bo‘lishi mumkin. ma’lumotlarning maxfiylik darajasiga qarab, ushbu xavfsizlik sathi buzilishi kompaniyaning raqobatbardosh ustunligiga va mavjudlilik darajasiga sezilarli darajada zarar yetkazishi mumkin [6].
Veb saytni o‘zgartirish /Buzilishlar	Ushbu hujumlarda hujumchining maqsadi kompaniya veb serverlariga kirish huquqiga qaratilgan bo‘ladi. Shundan so‘ng, hujumchi veb sayt logotipi, xabarlarini yoki materiallarini o‘zgartirishi, yoki barcha fayllarni va veb saytni butunlay o‘chirishi mumkin. DoS hujumiga o‘xshab, veb sayt o‘zgartirishlari veb sayt mavjudligi orqali daromad oladigan kompaniyalar uchun muhim hisoblanadi [6].

XULOSA

Veb tajovuzkor shaxslarga foydalanuvchilarning maxfiy ma’lumotlari va resurslarini monetizatsiya qilishga urinish va hujumlar uyushtirish uchun asosiy nishonga aylandi. Ushbu maqolada turli xil veb serverlar xavfsizligi va zaifliklari tavsiflab berildi. Shuningdek, veb server zaifliklari ro‘yxati bayon qilindi va ta’rif berildi. Veb serverlar xavfsizlik funksiyalarini amalga oshirish orqali hujumlarning oldini olishiga qaramay, zaifliklarning mavjudligi veb serverlarga bo‘ladigan hujumlarning ko‘lamini oshirish imkonini beradi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI: (REFERENCES)

1. Amadi E.C., Onebunne F. C. Analysis Of Web Server Security Challenges. Iheukwumere O. Federal University Of Technology, Owerri. emmanuel.amadi@futo.edu.ng. International Journal For Research In Advanced Computer Science And Engineering. June 2016
2. Garcia-Valls, M.; Calva-Urrego, C.; García-Fornes, A. Accelerating smart eHealth services execution at the fog computing infrastructure. Future Gener. Comput. Syst. 2020, 108, 882–893. [CrossRef]
3. Monostori, L. Cyber-physical production systems: Roots, expectations and R&D challenges. Procedia CIRP 2014, 17, 9–13.
4. Garcia-Valls, M.; Dubey, A.; Botti, V. Introducing the new paradigm of Social Dispersed Computing: Applications, Technologies and Challenges. J. Syst. Archit. 2018, 91, 83–102. [CrossRef]
5. Schagen, N.; Koning, K.; Bos, H.; Giuffrida, C. Towards automated vulnerability scanning of network servers. In Proceedings of the 11th European Workshop on Systems Security, Porto, Portugal, 23 April 2018.
6. Linxuan Song and Marisol García-Valls. Improving Security of Web Servers in Critical IoT Systems through Self-Monitoring of Vulnerabilities. Beijing University of Posts and Telecommunications, Beijing 100876, China; 2018213147@bupt.cn 2 Universitat Politècnica de València, 46022 Valencia, Spain Correspondence: mgvalls@dcom.upv.es. 2 july 2022