MASTER VA MA'LUMOTLAR KIRITISH VA XAVFSIZLIK MA'LUMOTLARNI HIMOYA QILISH

Tojimamatov Israiljon Nurmamatovich
Farg'ona davlat universiteti
israiltojimamatov@gmail.com
Rahimaliev Mardonali Zokirzoda
Farg'ona davlat unversiteti talabasi
rahimalievmardonali@gmail.com

Anotatsiya: *Mazkur maqola MASTER vositasi yordamida ma'lumotlarni kiritish shakllarini yaratish va ularni xavfsizligini ta'minlash jarayonlariga bag'ishlangan. Maqolada shakllarning xavfsizligini oshirish uchun kerakli validatsiya va sanitizatsiya jarayonlari, HTTPS protokoli, shifrlash usullari, CSRF va SQL Injection kabi hujumlardan himoya choralariga alohida e'tibor qaratilgan.*

Kalitso'zlar: *MASTER vositasi, ma'lumot kiritish shakllari, xavfsizlik, validatsiya, sanitizatsiya, HTTPS, shifrlash, CSRF, SQL Injection, XSS, foydalanuvchi huquqlari, tizim monitoringi, xavfsizlik choralar, ma'lumotlar himoyasi, foydalanuvchi ma'lumotlari.*

Abstract: *This article is dedicated to the process of creating data input forms using the MASTER tool and ensuring their security. It focuses on necessary validation and sanitization procedures, the HTTPS protocol, encryption methods, and protective measures against attacks such as CSRF and SQL Injection. Special attention is given to how to enhance the security of forms and protect user data effectively. By implementing these techniques, the security of data input forms is reinforced, and potential vulnerabilities are minimized.*

Keywords: *MASTER tool, data input forms, security, validation, sanitization, HTTPS, encryption, CSRF, SQL Injection, XSS, user rights, system monitoring, security measures, data protection, user data.*

Аннотация: *Настоящая статья посвящена процессу создания форм ввода данных с использованием инструмента MASTER и обеспечению их безопасности. В статье рассматриваются необходимые процедуры валидации и санации данных, использование протокола HTTPS, методы шифрования, а также меры защиты от атак, таких как CSRF и SQL Injection. Особое внимание уделено способам повышения безопасности форм и эффективной защите пользовательских данных. Применение этих техник усиливает безопасность форм ввода данных и минимизирует потенциальные уязвимости.*

Ключевыеслова: *Инструмент MASTER, формы ввода данных, безопасность, валидация, санация, HTTPS, шифрование, CSRF, SQL Injection,*

XSS, права пользователей, мониторинг системы, меры безопасности, защита данных, пользовательские данные.

MASTER vositasi foydalanuvchilarga ma'lumotlarni samarali va intuitiv tarzda kiritish imkonini beradi. Shakllarni yaratish jarayoni ko‘plab afzalliklarga ega bo‘lib, ular foydalanuvchi ehtiyojlariga mos keladigan turli shakl turlarini yaratishda yordam beradi. Biroq, shakllar yordamida kiritilgan ma'lumotlar tizimga o‘tkazilayotganda xavfsizlikka alohida e'tibor qaratish zarur. Chunki noto‘g‘ri ma'lumotlar yoki xavfsizlik zaifliklari tizimni zaiflashtirishi va zararli hujumlar uchun imkoniyat yaratishi mumkin. Xavfsizlikka alohida ahamiyat berish, ma'lumotlar xavfsizligini ta'minlash va tizimni himoya qilish uchun zarur choralar ko‘rilishi kerak.

Shakllarni yaratish jarayonida foydalanuvchi kiritgan ma'lumotlarning to‘g‘riligi va xavfsizligini ta'minlash uchun turli xavfsizlik usullari qo‘llaniladi. Masalan, ma'lumot validatsiyasi, shifrlash, XSS va SQL Injection kabi hujumlardan himoya qilish va foydalanuvchi huquqlarini boshqarish kabi amaliy choralar shakllarning xavfsizligini ta'minlashda muhim ahamiyatga ega. MASTER vositasi yordamida ma'lumot kiritish shakllarini yaratish, tizimdagi ma'lumotlarni to‘g‘ri, samarali va qulay tarzda yig‘ish uchun juda muhim ahamiyatga ega. Ushbu vosita foydalanuvchilarga shakllarni oson va tez yaratish imkonini beradi, bu esa tizimning samaradorligini oshiradi. Shakllar yordamida foydalanuvchilardan kerakli ma'lumotlar kiritilishi mumkin, masalan, ismlar, manzillar, telefon raqamlari, elektron pochta adreslari va boshqalar. Bu ma'lumotlar keyinchalik tizimda saqlanadi va ishlatiladi. Shakllar yaratishda, ularning dizayni va funksionalligi foydalanuvchining ehtiyojlariga mos ravishda ishlab chiqilishi kerak. Bunday shakllar foydalanuvchilarga murakkab ma'lumotlar bilan ishlashni osonlashtiradi, shuningdek, to‘g‘ri va tezkor ma'lumot kiritishni ta'minlaydi.

Bundan tashqari, MASTER vositasida shakl yaratishda xavfsizlikni ta'minlash uchun qo‘llaniladigan bir qator vositalar mavjud. Xavfsizlik, ma'lumotlarni to‘g‘ri saqlash va tizimga hujumlarni oldini olishda asosiy rol o‘ynaydi. Shaklga kiritilgan ma'lumotlar tizimga uzatilayotganda, bu ma'lumotlar xavfsiz bo‘lishi kerak. Masalan, foydalanuvchi kiritgan parollarni saqlashda ular shifrlanishi kerak, bu ma'lumotlarni yomon niyatli shaxslar tomonidan o‘g‘irlanishining oldini oladi. Shuningdek, foydalanuvchi kiritgan ma'lumotlarning sanitizatsiya qilinishi muhimdir. Bu jarayon zararli kodlarning shaklga kiritilishiga yo‘l qo‘ymaydi, bu esa XSS (Cross-site Scripting) va SQL Injection kabi xavfli hujumlarni oldini olishga yordam beradi. Shakllarda foydalanuvchilardan shaxsiy ma'lumotlar so‘ralganida, ularning maxfiyligini saqlash uchun tegishli xavfsizlik choralarini ko‘rish zarur.

MASTER vositasi yordamida shakllar yaratishda, foydalanuvchining ma'lumotlarini olishda yanada yaxshilanishlar qilish mumkin. Misol uchun, shaklga kiritilgan ma'lumotlarni tahlil qilish va ularning yaroqliligini aniqlash uchun avtomatik validatsiya tizimlari ishlatiladi. Bu, foydalanuvchi kiritgan ma'lumotlarni

tezda tekshirib, noto‘g‘ri yoki yaroqsiz kiritilganlarni aniqlash imkonini beradi. Shuningdek, tizimga kiritilgan ma'lumotlarning to‘g‘riligini ta'minlash uchun foydalanuvchidan kiritilgan ma'lumotlarni ikki marta tasdiqlash talab qilinishi mumkin. Masalan, parolni kiritish jarayonida foydalanuvchidan uning takrorlanishi so‘raladi, bu esa kiritilgan ma'lumotlar noto‘g‘ri bo‘lishining oldini oladi. Tizimda ma'lumotlar xavfsizligini ta'minlash uchun shakllarga kiritilgan ma'lumotlar shifrlanadi va faqatgina kerakli ruxsatnomalar bilan ularga kirish mumkin bo‘ladi.

Xavfsizlikka tahdidlardan biri zararli dasturlar (malware) hisoblanadi. Zararli dasturlar, masalan, viruslar, trojanlar, ransomware, spyware va adware tizimga kirib, ma'lumotlarni o‘g‘irlash, zarar etkazish yoki tizimni ishlamaydigan holatga keltirish uchun ishlatiladi. Ular tarmoq orqali yoki foydalanuvchilar tomonidan yuklab olingan fayllar orqali tizimga kirishi mumkin. Zararli dasturlarni aniqlash uchun antivirus dasturlari va zararli kodni tahlil qilish usullari qo‘llaniladi. Antivirus dasturlari foydalanuvchi tizimiga kirgan zararli kodlarni aniqlab, ularni yo‘q qilishga yordam beradi. Biroq, ba'zi zararlilar yangi va ilg‘or usullar bilan tizimga kirishi mumkin, shuning uchun xavfsizlikni ta'minlashda muntazam yangilanish va yangi tahdidlarga tayyor bo‘lish zarur.

SQL Injection — bu yana bir muhim xavfsizlik tahdidi bo‘lib, veb-applicationlarda ma'lumotlar bazasiga zararli SQL kodlarini yuborish orqali tizimga kirish imkoniyatini yaratadi. SQL Injection hujumlari, tizimga kirgan shaxsning ma'lumotlar bazasini manipulyatsiya qilishiga, foydalanuvchi hisoblarini buzishiga yoki tizimdagi boshqa resurslarga noqonuniy kirishiga olib kelishi mumkin. Ushbu tahdidni aniqlash va oldini olish uchun ma'lumotlar bazasiga yuboriladigan har bir so‘rovni tekshirish va to‘g‘ri parametrik so‘rovlar ishlatish zarur. SQL Injection hujumlarini aniqlashda ma'lumotlar bazasidan noqonuniy kirish va noto‘g‘ri so‘rovlar aniqlanadi.

Cross-Site Scripting (XSS) hujumi, zararli skriptlarni foydalanuvchi brauzeriga yuborish orqali amalga oshiriladi. Ushbu hujum foydalanuvchidan maxfiy ma'lumotlarni o‘g‘irlash, ularning sessiyasini o‘g‘irlash yoki tizimni manipulyatsiya qilishga olib kelishi mumkin. XSS tahdidini aniqlashda, foydalanuvchi kiritgan ma'lumotlarni sanitizatsiya qilish (zararli kodlardan tozalash) va xavfsiz kod yozish amaliyotlariga rioya qilish zarur. XSS hujumlarini aniqlash va oldini olish uchun foydalanuvchi tomonidan kiritilgan barcha ma'lumotlar xavfsiz tarzda qayta ishlanishi va tizimga yuborilishi kerak.

Bundan tashqari, Denial of Service (DoS) va Distributed Denial of Service (DDoS) hujumlari ham tizim xavfsizligiga tahdid soladi. Ushbu hujumlar tizimning resurslarini to‘liq band qilib, uning ishlashini sekinlashtirishi yoki to‘liq ishdan chiqarishi mumkin. DoS hujumi bitta manbadan amalga oshirilsa, DDoS hujumi bir nechta manbalardan amalga oshiriladi, bu tizimni yanada kuchaytirilgan ravishda to‘sib qo‘yadi. DoS/DDoS hujumlarini aniqlashda tarmoq trafigini tahlil qilish va odatdagi trafiga nisbatan noxush o‘zgarishlarni aniqlash uchun maxsus monitoring

vositalari ishlatiladi. Bu hujumlarni oldini olish uchun tarmoqni filtrlar va xavfsizlik devorlari yordamida himoya qilish kerak. Bundan tashqari, Phishing hujumlari orqali tizimlarga zarar yetkazilishi mumkin. Phishing hujumlari, foydalanuvchilarning shaxsiy ma'lumotlarini o‘g‘irlashga qaratilgan soxta xabarlar, veb-saytlar yoki elektron pochta orqali amalga oshiriladi. Foydalanuvchilarni chalg‘itish va ularning login va parollarini olish uchun soxta sahifalar yaratish mumkin. Phishing hujumlarini aniqlashda foydalanuvchilarga soxta elektron pochta yoki veb-saytlarga kirishdan ehtiyot bo‘lishi kerakligi haqida doimiy xabardorlik yaratish zarur. Bundan tashqari, maxsus phishing-tahlil dasturlari va xabarlar filtrlari yordamida ushbu hujumlarga qarshi kurashish mumkin.

Man-in-the-middle (MITM) hujumi, tarmoqda uzatilayotgan ma'lumotlar orasida oraliq sifatida turib, foydalanuvchi va server o‘rtasidagi aloqani tahlil qilish yoki manipulyatsiya qilish orqali amalga oshiriladi. MITM hujumlarini aniqlash uchun tarmoq trafigini shifrlash va HTTPS protokolini ishlatish zarur. Bu, foydalanuvchining va serverning o‘rtasidagi aloqalarni himoya qiladi va ma'lumotlarning o‘g‘irlanishining oldini oladi.

Xavfsizlik tahdidlarini aniqlashning yana bir muhim usuli - bu tizimni doimiy ravishda monitoring qilishdir. Tarmoqda va tizimda yuz berayotgan barcha jarayonlarni kuzatish, zararli faoliyatni aniqlash va unga tezda javob berish imkonini beradi. Intrusion Detection Systems (IDS) va Intrusion Prevention Systems (IPS) tizimlari zararli harakatlarni aniqlashda va oldini olishda yordam beradi. Ushbu tizimlar tizimga kirgan har bir faoliyatni tahlil qilib, xavfli faoliyatni aniqlaydi va tizimni himoya qiladi.

MASTER vositasi yordamida xavfsiz shakllar yaratish, tizimni himoya qilish va foydalanuvchi ma'lumotlarini saqlashda muhim ahamiyatga ega. Shakllar tizimga ma'lumot kiritishning asosiy usuli bo‘lib, ular foydalanuvchi bilan o‘zaro aloqada bo‘lgan barcha jarayonlarda ishlatiladi. Shakllar yordamida foydalanuvchilardan shaxsiy yoki tijorat ma'lumotlari olinishi mumkin, shuning uchun shakllarni yaratishda ularning xavfsizligini ta'minlash juda muhimdir. Xavfsiz shakl yaratishning asosiy maqsadi — foydalanuvchi ma'lumotlarini himoya qilish, tizimga zararli kirishlarning oldini olish va ma'lumotlar bazasini manipulyatsiya qilishni oldini olishdir. MASTER vositasida shakllar yaratishda qo‘llaniladigan xavfsizlik choralarini ko‘rib chiqamiz.

Shakllarda foydalanuvchi ma'lumotlarini to‘g‘ri yig‘ish va saqlash uchun birinchi navbatda, ma'lumotlarni validatsiya qilish zarur. Validatsiya, foydalanuvchi tomonidan kiritilgan ma'lumotlarning to‘g‘ri va qonuniyligini tekshirishni anglatadi. MASTER vositasida shakl yaratishda, har bir maydon uchun aniq validatsiya qo‘llanilishi kerak. Masalan, telefon raqami yoki elektron pochta manzilini kiritishda, ularning formatlari avtomatik tekshiriladi. Bunda, faqatgina yaroqli ma'lumotlar tizimga uzatiladi, bu esa noto‘g‘ri yoki zararli ma'lumotlarning kirishining oldini

oladi. Validatsiya nafaqat shaklni to‘ldirishda, balki server tomonida ham amalga oshirilishi zarur. Bu ikki bosqichli validatsiya ma'lumotlarning to‘g‘riligini yanada mustahkamlaydi.

Shakllarni xavfsiz qilishning yana bir muhim jihati — ma'lumotlarni sanitizatsiya qilish. Sanitizatsiya jarayoni, foydalanuvchidan olingan ma'lumotlarni zararli kodlardan tozalashni ta'minlaydi. Masalan, foydalanuvchi shaklga zararli JavaScript yoki SQL kodlarini kiritishi mumkin, bu esa XSS (Cross-Site Scripting) yoki SQL Injection hujumlariga olib kelishi mumkin. Shaklga kiritilgan har bir ma'lumotni sanitizatsiya qilish, ushbu xavfli kodlarni aniqlash va ularni tizimga yuborilmasdan oldin tozalash imkonini beradi. MASTER vositasida shakl yaratishda ma'lumotlarni sanitizatsiya qilishda maxsus funktsiyalarni qo‘llash va kirishdagi ma'lumotlarni tahlil qilish zarur. Bu holat tizimni xavfsiz holatda ushlab turadi va ma'lumotlar xavfsizligini ta'minlaydi.

Shakllar xavfsizligini ta'minlashda HTTPS protokolini ishlatish ham muhimdir. HTTPS, HTTP protokolining xavfsiz versiyasi bo‘lib, ma'lumotlarni shifrlash orqali tarmoqda ma'lumotlarning o‘g‘irlanishini oldini oladi. Agar shakl foydalanuvchidan maxfiy ma'lumotlar, masalan, parol yoki bank kartasi raqamini so‘rasa, bu ma'lumotlar shifrlanmagan holda uzatilmasligi kerak. HTTPS protokoli yordamida, foydalanuvchi kiritgan barcha ma'lumotlar xavfsiz tarzda uzatiladi, va bu foydalanuvchining shaxsiy ma'lumotlarini himoya qiladi. Shakl yaratishda HTTPS protokolining mavjudligini tekshirish, tizim xavfsizligini yanada mustahkamlaydi.

Shifrlash texnologiyasi shakllarda kiritilgan maxfiy ma'lumotlarni saqlashda yana bir muhim xavfsizlik chorasi hisoblanadi. Foydalanuvchi ma'lumotlarini saqlashda ular shifrlanishi kerak, ayniqsa, parollar va kredit kartalari kabi maxfiy ma'lumotlar. Shifrlash, kiritilgan ma'lumotlarni tizimda saqlashni xavfsiz qiladi va agar tizimda ma'lumotlar o‘g‘irlangan taqdirda, ularni tushunib bo‘lmaydi. MASTER vositasida shakl yaratishda ma'lumotlar shifrlashini qo‘llash, tizimga zararli kirishlarni oldini olish uchun juda muhimdir.

Shakllar yaratish va ularni xavfsiz qilishda, doimiy yangilanish va monitoring zarur. Shakllarning xavfsizligi va tizimning himoyasi doimiy ravishda tekshirilishi kerak. Yangi tahdidlar va hujum turlariga qarshi himoya qilish uchun xavfsizlikni yangilab borish va tizimni optimallashtirish zarur. MASTER vositasida shakl yaratish va xavfsizlikni ta'minlash jarayonida doimiy monitoring va test qilish orqali tizimning zaif joylarini aniqlash mumkin.

Xulosa

MASTER vositasi yordamida xavfsiz shakllar yaratish, ma'lumotlar xavfsizligini ta'minlash va tizimni himoya qilish uchun juda muhimdir. Shakllar foydalanuvchi bilan tizim o‘rtasidagi ma'lumot almashinuvi uchun asosiy vosita bo‘lib, ularning xavfsizligini ta'minlash orqali ko‘plab zararli hujumlar, shu jumladan SQL Injection, XSS, CSRF va DDoS hujumlari oldini olinishi mumkin. Shakllarda foydalanuvchi

kiritgan ma'lumotlarni validatsiya qilish, sanitizatsiya qilish, HTTPS protokoli orqali shifrlash, shuningdek, ma'lumotlarni shifrlash va foydalanuvchi huquqlarini boshqarish kabi xavfsizlik choralarini qo‘llash tizimni himoya qiladi.

FOYDALANILGAN ADABIYOTLAR:

1. Koller, M. (2019). *Mastering Database Design: Understanding the Theory of Relational Databases*. Wiley.
2. Ghosh, A., & Gupta, R. (2021). *Secure Web Application Development with Master Tool*. Springer.
3. Allen, J. H. (2020). *Web Application Security: Exploitation and Protection Techniques*. Pearson.
4. Kumar, R., & Singh, A. (2018). *Principles of Secure Database Management Systems*. Elsevier.
5. Rouse, M. (2020). *SQL Injection Prevention: A Comprehensive Guide*. O'Reilly Media.
6. Jackson, B. (2017). *Cross-Site Scripting and SQL Injection: Threats and Prevention*. Wiley-Blackwell.
7. Arapoglou, A., & Dimitriadis, G. (2021). *Web Application Firewalls: Techniques and Tools*. McGraw-Hill.
8. Anderson, S. L. (2019). *Introduction to Cyber Security for Web Applications*. CRC Press.
9. Martinez, D., & Perez, M. (2020). *Cybersecurity for Web Forms and Applications*. Elsevier.