10. Suyunbayev, Sh.M. and Butunov, D.B. (2019) “Development of classification of the reasons of losses in the work sorting stations” Journal of Tashkent Institute of Railway Engineers: Vol. 15: Iss. 2, Article 23. Available at: (https://uzjournals.edu.uz/tashiit/vol15/iss2/23).

11. Aripov N., Suyunbaev S., Azizov F., Bashirova A. Method for substantiating the spheres of application of shunting locomotives at sorting stations // E3S Web of Conferences, 2021, 264, 05048. https://doi.org/10.1051/e3sconf/202126405048.

12. Sherzod Jumayev, Sakijan Khudayberganov, Oybek Achilov, Munira Allamuratova. Assessment criteria for optimization of parameters affecting to local wagon-flows at railway sites / E3S Web of Conferences, Vol.264, 05022 (2021). (Scopus) https://doi.org/10.1051/e3sconf/202126405022.

13. Суюнбаев Ш.М., Саъдуллаев Б.А. Выбор рационального варианта организации маневровой работы на станции // Материалы конференции «Приоритетные направления инновационной деятельности в промышленности». – Казань.: ООО «Конверт», 2020. – С. 183–186.

14. Методика тяговых расчетов для маневровой работы, Москва. 1988 г.

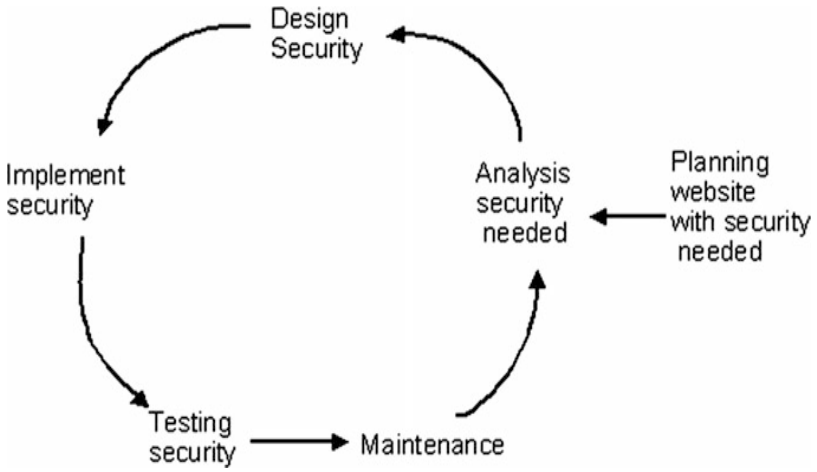
VEB-SAYTLARDA KIBER XAVFSIZLIKNI TA’MINLASH CHORALARI

Olim MIRZAYEV,
PhD, O‘zbekiston Respublikasi madaniyat vazirining madaniyat muassasalari va havaskorlik san’atini rivojlantirish, raqamlashtirish axborot texnologiyalari va ta’lim muassasalari bo‘yicha o‘rinbosari
G‘ayrat MUHAMMADIYEV,
Muhammad al-Xorazmiy nomidagi TATU “Axborot xavfsizligi” fakulteti 2-bosqich magistranti
DOI: https://doi.org/10.47689/978-9943-7818-0-1-pp98-100

Annotatsiya: *Veb-sahifalar gipermatnni uzatish protokoli (HTTP) va shifrlash (HTTP Secure) xavfsizlik mexanizmlaridan foydalanadi. Veb-saytning internet olamidagi roli muhim ahamiyatga ega. Shuning uchun raqamli jinoyatlarning oldini olish uchun veb-saytlarning xavfsizligini ta’minlash talab qilinadi. Jinoyatchilar odamlar bilmagan har qanday vaziyatlarni nishonga olishadi. Ko‘pchilikka ta’sir qiladigan muhim veb-saytlar bank, davlat, savdo va boshqa kabilar uchun xavfsizlik o‘ta muhim. Samarali xavfsizlik dasturi xabardorlik, oldini olish, aniqlash, o‘lchash kabilar xavfni kamaytirish uchun xizmat qiladi. Mukammal xavfsizlik degan narsa yo‘q va qat’iyatli hujumchi mag‘lub bo‘lishi yoki deyarli chetlab o‘tish yo‘lini topishi mumkin.*

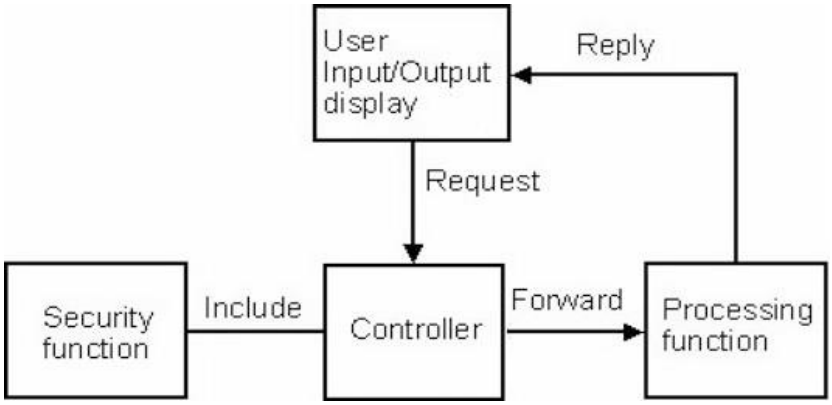
Xavfsizlik maqsadi maxfiylik, yaxlitlik va qulaylik asosida o‘lchanadi.Veb-ilovalar tabiatan xavfsiz emas, chunki u noma’lum foydalanuvchilarga ega bo‘lishga va serverga to‘g‘ridan to‘g‘ri kirish imkon beradi. Hatto xavfsizlik devoridan

foydalanilgan bo‘lsa ham, unda ochiladigan portlar bo‘lishi foydalanuvchilarga serverga ulanishga imkon beradi. Veb-sayt yaratish qo‘shimcha qatlamlar, ya’ni apparat, ulanish va dastur kabi ba’zi kombinatsiyalarni birlashtiradi va barcha qismlar himoyalangan bo‘lishi kerak. Yetarlicha xavfsiz kod yozish orqali himoya qilish yaxshiroqdir. Hujumchilar har doim hujum qilish uchun eng zaif tomonni qidiradilar, lekin ular veb-saytni tark etadilar, agar u yetarlicha xavfsiz bo‘lsa va boshqa zaif veb-saytlarni qidirishadi. Qilinishi kerak bo‘lgan birinchi narsa xavfsizlikda hech qachon faqat bitta himoya usuliga tayanmaslikdir. Chunki u muvaffaqiyatsiz bo‘lsa, u yerda zaxira bo‘lmaydi. Mijozlar tizimga kirishi va foydalanilgan protokollarni, so‘rovlar sanasi va vaqtini, domen nomlarini tekshirish orqali so‘rovlarga javob beradigan kompyuterlarni, shuningdek, URL-so‘rovining mazmunini kuzatishi mumkin. 1-rasmda ko‘rsatilgan usulga ko‘ra sikl hech qachon tugamaydi, bu degani xavfsizlik har doim yangilanishi kerak bo‘lgan abadiy ishdir. Hujum metodologiyasi ko‘p qatlamlarga ega va veb-saytlarning xavfsizligini amalga oshiradiganlar ushbu hujum usullaridan xabardor bo‘lishlari kerak. Hujumchining zaif qismi bo‘lsa, har bir qatlam darajasini chetlab o‘tishi mumkin.Shuning uchun xavfsizlik funksiyasi barcha qatlam darajalarini himoya qilishi kerak. Hujumchilar xatolarni va ushbu tizimning zaif tomonlarini qidiradilar, topilgan xatolardan so‘ng qo‘lda yoki avtomatik yondashuv yordamida (bot kompyuterdan foydalangan holda) kraker hujum qila boshlaydi. Shundan so‘ng kraker ,odatda, zombi kompyuteridan foydalanish va IP-manzilini yashirish orqali shaxsiyatini himoya qilish uchun mudofaa rejimini yaratadi.



1-rasm. Xavfsiz dasturiy ta’minotni ishlab chiqish usuli.

Quyida veb-saytga xavfsizlik funksiyasini qanday joylashtirish sintaksisi keltirilgan:



2-rasm. Xavfsizlik diagrammasini joylashtirish.

Kiritilgan sintaksis quyidagicha: include(“../function/security.php”); Xavsizlikni ta’minlash kodi ko‘plab filtrlash va tekshirish funksiyalaridan iborat. Nomi "Filtr($text)" bo‘lgan funksiya MySQL inyeksiyasi va XSS hujumi uchun matnni filtrlash uchun foydalanadi. “DOScheck()” funksiyasining vazifasi DoS hujumidan himoya qilishdir, u foydalanuvchi IP-so‘rovini aniqlash orqali ishlaydi va agar so‘rov chegaradan oshib ketgan bo‘lsa, uni bloklaydi. “CSRF($funksiya)” funksiyasi yuridik shaklni o‘tkazib yuboradigan CSRF hujumining oldini olish uchun ishlaydi. Eng yaxshi xavfsizlik usuli hujumning qanday ishlashini va qanday sodir bo‘lishini tushunishdir.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI:

1. Козлов Д.Д., Петухов А.А. «Методы обнаружения уязвимостей в web-приложениях» / Программные системы и инструменты: тематический сборник ф-та ВМиК МГУ им. Ломоносова N 7. П/р Л.Н. Королева. М.: Издательский отдел ВМиК МГУ. Изд-во МАКС Пресс, 2006 г.

2. Бармен Скотт. Разработка правил информационной безопасности. М.: Вильямс, 2002. – С. 208. – ISBN 5-8459-0323-8, ISBN 1-5787-0264-X.

3. Межсайтовый_скриптинг http://ru.wikipedia.org/wiki/Межсайтовый_скриптинг.

4. Защита от SQL injection и XSS (функция secureInner Data) http://n3info.blogspot.com/2013/05/sql-injection-xss-secureinnerdata.html.

5. XSS атака сайта и способы защиты. Как сделать и проверить XSS уязвимость http://consei.ru/xss-ataka-sajta-i-sposoby-zashhity/.