ISSN 2181-3187

VEB-SAYTLARDA KIBERXAVFSIZLIKNI TA’MINLASH MUAMMOLARI VA YECHIMLARI

Irgasheva Durdona Yakubdjanovna,
Xudoykulov Zarifjon Turakulovich,
Davronova Lola Uktamovna
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari univeristeti
e-mail: uktamovna88@gmail.com

Annotatsiya: Mazkur maqolada veb-saytlarda kiberxavfsizlikni ta’minlash masalalari keng yoritiladi. Tahlil davomida veb-ilovalarga nisbatan amalga oshiriladigan eng keng tarqalgan hujum turlari – saytlararo skriptlash (XSS), SQL in’ektsiyasi, CSRF, zararli dasturlar infiltratsiyasi va zaif autentifikatsiya tizimlari ko‘rib chiqiladi. Shuningdek, ushbu muammolarni bartaraf etish uchun taklif etilgan zamonaviy yechimlar, xususan, WAF texnologiyasi, foydalanuvchi so‘rovlarini real vaqt rejimida filtrlaydigan Python asosidagi middlewarelar, ikki faktorli autentifikatsiya, foydalanuvchi parollari siyosati va xalqaro xavfsizlik standartlari (GDPR va PCI DSS) tahlil qilinadi. Maqolada, shuningdek, xavfsizlikni ta’minlashda xodimlarni o‘qitish, xavfsizlik siyosatini shakllantirish, voqealarga javob berish rejasi va xavfsizlik jarayonlarining doimiy monitoringi kabi tashkiliy yondashuvlar ham muhim omil sifatida baholanadi. Natijada, veb-sayt egalari va ishlab chiquvchilar uchun samarali xavfsizlik strategiyasini ishlab chiqishga yo‘naltirilgan ilmiy-amaliy tavsiyalar shakllantiriladi.

Kalit so‘zlar: Kiberxavfsizlik, veb-sayt xavfsizligi, kiberxavfsizlik tahdidlari, SQL in’ektsiyasi, saytlararo skriptlash (XSS), CSRF hujumi, zararli dastur (malware), Web Application Firewall (WAF), Python middleware, ikki faktorli autentifikatsiya, foydalanuvchi ma’lumotlarini himoya qilish, GDPR, PCI DSS, xavfsizlik siyosati, raqamli xavfsizlik, axborot texnologiyalari, himoyalangan veb-ilovalar

ISSN 2181-3187

Аннотация: В данной статье всесторонне рассматриваются вопросы обеспечения кибербезопасности веб-сайтов. В ходе анализа рассматриваются наиболее распространённые типы атак на веб-приложения, такие как межсайтовое скриптование (XSS), SQL-инъекции, подделка межсайтовых запросов (CSRF), распространение вредоносного программного обеспечения и уязвимости, связанные с слабыми механизмами аутентификации. Также проанализированы современные решения, предложенные для устранения данных угроз, включая технологии WAF (межсетевые экраны веб-приложений), middleware-модули на базе Python, осуществляющие фильтрацию пользовательских запросов в реальном времени, двухфакторную аутентификацию, политику надёжных паролей и соответствие международным стандартам кибербезопасности (GDPR и PCI DSS). Кроме того, акцент сделан на организационных аспектах, таких как обучение сотрудников, формирование политики безопасности, разработка плана реагирования на инциденты и непрерывный мониторинг процессов безопасности. В результате сформулированы научно-практические рекомендации, направленные на разработку эффективной стратегии безопасности для владельцев и разработчиков веб-сайтов.

Ключевые слова: Кибербезопасность, безопасность веб-сайтов, угрозы кибербезопасности, SQL-инъекция, межсайтовое скриптование (XSS), атака CSRF, вредоносное ПО (malware), межсетевой экран веб-приложений (WAF), Python middleware, двухфакторная аутентификация, защита пользовательских данных, GDPR, PCI DSS, политика безопасности, цифровая безопасность, информационные технологии, защищённые веб-приложения

Abstract: This article provides a comprehensive examination of cybersecurity issues in web applications. The analysis focuses on the most common types of attacks against web platforms, including Cross-Site Scripting (XSS), SQL injection, Cross-Site Request Forgery (CSRF), malware infiltration, and weak authentication mechanisms. In response, the article explores modern mitigation strategies such as the

ISSN 2181-3187

implementation of Web Application Firewalls (WAF), Python-based middleware capable of filtering user requests in real time, two-factor authentication systems, secure password policies, and compliance with international cybersecurity standards (GDPR and PCI DSS). Organizational measures are also highlighted, including staff training, the development of security policies, incident response planning, and continuous security process monitoring. Based on these analyses, the paper formulates scientifically grounded and practical recommendations for the development of effective web security strategies for site owners and developers.

Keywords: Cybersecurity, web application security, cybersecurity threats, SQL injection, Cross-Site Scripting (XSS), CSRF attack, malware, Web Application Firewall (WAF), Python middleware, two-factor authentication, user data protection, GDPR, PCI DSS, security policy, digital security, information technology, secure web applications

Veb-ilovalar duch keladigan eng keng tarqalgan tahdid turlaridan biri bu saytlararo skriptlash (XSS – *Cross Site Scripting*) hujumidir. Ushbu turdagi hujumda tajovuzkor foydalanuvchining kiruvchi maydonlari orqali zararli JavaScript kodlarini kiritib, boshqa foydalanuvchilarning brauzerida ushbu kodlar bajarilishini ta’minlaydi. Natijada foydalanuvchi parollari, cookies yoki kredit karta raqamlari kabi nozik ma’lumotlar o‘g‘irlanishi mumkin. Ushbu muammoning yechimlaridan biri sifatida foydalanuvchi tomonidan kiritilgan barcha ma’lumotlarni filtrlash (input validation) va chiqishda (output encoding) xavfsiz kodlash texnologiyalarini qo‘llash taklif etiladi.

Ikkinchi muhim tahdid – bu SQL in’ektsiyasi (SQL Injection) bo‘lib, u veb-ilova ma’lumotlar bazasiga foydalanuvchi tomonidan kiritilgan ma’lumotlar orqali zararli SQL so‘rovlari yuborishga imkon beradi. Ushbu zaiflik orqali tajovuzkor bazadagi ma’lumotlarni o‘zgartirishi, o‘chirishi yoki hatto tizimga to‘liq kirish huquqini qo‘lga kiritishi mumkin. Mazkur muammoni bartaraf etishning asosiy yo‘li bu parametrik

ISSN 2181-3187

so‘rovlardan (prepared statements) va ORM (Object-Relational Mapping) texnologiyalaridan foydalanishdir.

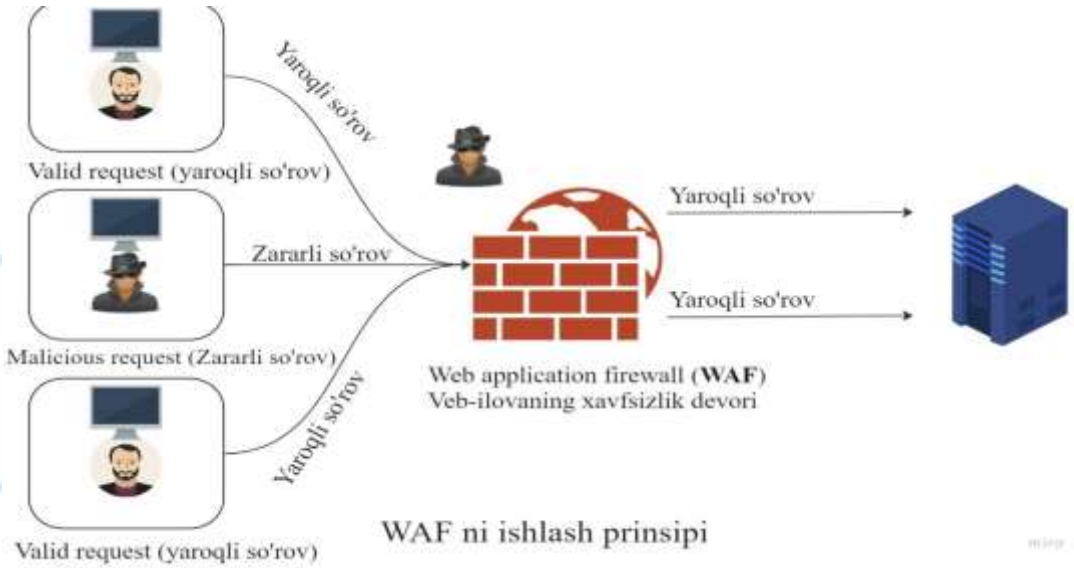
Saytlararo so‘rovlarni qalbakilashtirish (CSRF - Cross-Site Request Forgery) veb-saytlar duch keladigan yana bir kiberxavfsizlik muammosidir. CSRF tajovuzkor autentifikatsiya qilingan foydalanuvchilarni hozirda autentifikatsiya qilingan veb-ilovaga so‘rov yuborishga majburlovchi hujumdir. Bu tajovuzkorga maxfiy ma’lumotlarni o‘girlash yoki veb-sayt nazoratini qo‘lga kiritish imkonini beradi. Ushbu muammoning echimi foydalanuvchi so‘rovlarining haqiqiyligini tekshirish uchun CSRF tokenlaridan foydalanishdir.

Zararli dastur veb-saytga zarar etkazishi va tashrif buyuruvchilar qurilmalariga tarqalishi, ularning tizimlariga zarar etkazishi yoki ma’lumotlarini o‘girlashi mumkin bo‘lgan yana bir kiberxavfsizlik muammosidir. Ushbu muammoning yechimi zararli dasturlarni skanerlash uchun antivirus dasturidan foydalanish va ruxsatsiz kirishni oldini olish uchun tarmoqlararo ekran xavfsizlik devorlarini ishlatishdir.

Zaif parollar tajovuzkorlarning veb-sayt va uning ma’lumotlariga kirishini osonlashtiradigan yana bir kiberxavfsizlik muammosidir. Kuchli parollardan foydalanish va foydalanuvchilardan kuchli parollarni tanlashni talab qiladigan parol siyosatini qo‘llash muhim. Qo‘shimcha xavfsizlik qatlamini qo‘shish uchun ikki faktorli autentifikatsiyadan foydalanish ham muhimdir.

Veb-saytlarda kiberxavfsizlikni ta’minlashning bir usuli bu veb-ilovalar xavfsizlik devorini (WAF) amalga oshirishdir. WAF kiruvchi trafikni filtrlash va zararli so‘rovlarni bloklash orqali SQL in’ektsiyasi va saytlararo skript kabi hujumlarning oldini olishga yordam beradi. WAF shuningdek, kiruvchi trafikni kuzatishi va qayd qilishi mumkin, bu potentsial hujumlarni aniqlashda foydali bo‘lishi mumkin.

ISSN 2181-3187



1.1 - rasm. WAF ni ishlash prinsipi

Ishonchsiz aloqa veb-saytlar duch keladigan yana bir kiberxavfsizlik muammosidir. Shifrlashdan foydalanmaydigan veb-saytlar tajovuzkorlarga login hisob ma’lumotlari yoki kredit karta raqamlari kabi muxim ma’lumotlarni tutib olishiga ruxsat berishi mumkin. Aloqalarni himoya qilish uchun HTTPS shifrlashdan foydalanish muhimdir.

Quyida Python dasturlash tilidan foydalanilgan holda veb-ilovalarning xavfsizligini ta’minlovchi Web Application Firewall (WAF) tizimini loyihalash va amalga oshirish jarayoni keltirilgan

```
from flask import request, abort
import re

def waf_filter():
    # Ba'zi sahifalarni tekshiruvdan chiqaramiz
    exceptions = ["/login", "/login/callback", "favicon.ico"]
    for exc in exceptions:
        if exc in request.url:
            return

    # Xavfsizlik uchun patternlar
    patterns = {
        "SQL Injection": r"(union|select|from|where|drop|delete|insert|update|--|%27|')",
        "XSS": r"(<script.*?>.*?</script>|javascript:|onerror=|onload=)",
        "Directory Traversal": r"(\.\./|\.\.\\)",
        "Comment or Hash Injection": r"(%23|#)"
    }

    # Tekshiriladigan ma'lumotlar: URL, query string, va forma
    data_to_check = request.url + " " + str(request.args) + " " + str(request.form)

    for name, pattern in patterns.items():
        if re.search(pattern, data_to_check, re.IGNORECASE):
            print(f"[!] {name} bloklandi: {request.url}")
            abort(403)
```

1.2 - rasm. Sodda WAF tizimi

ISSN 2181-3187

1.3 - rasm. Yaratilgan WAF orqali web-sayt xavfsizligini tekshirish

Ushbu dastur kodi ishlab chiqilgan veb-sayt qabul qiladigan so‘rovlarni filter qilishda ishlatiladi.

Keyingi bosqichda veb-ilova xavfsizligini yanada takomillashtirish maqsadida, foydalanuvchi tomonidan yuborilayotgan barcha HTTP so‘rovlarini real vaqt rejimida tahlil qilib, ularni oldindan belgilangan xavfsizlik me’zonlari asosida filtrlash mexanizmini joriy etish nazarda tutiladi. Jumladan, agar so‘rov mazmunida Cross-Site Scripting (XSS) yoki SQL Injection turidagi zararli kiritmalar aniqlansa, tizim ushbu so‘rovga javob qaytarmasligi va tegishli IP-manzilni avtomatik ravishda qora ro‘yxatga (blacklist) kiritishi ko‘zda tutiladi. Bunday yondashuv foydalanuvchining tajovuzkor harakatlarini dastlabki bosqichda aniqlash va ularni samarali tarzda bloklash imkonini beradi.

Ushbu funksional imkoniyatni amalga oshirish uchun Python dasturlash tilining keng tarqalgan veb-ilova freymvorki bo‘lgan Djangodan foydalaniladi. Django arxitekturasida bunday xavfsizlik logikasi odatda middleware komponenti orqali tashkil etiladi. Middleware — bu veb-server va ilova orasida joylashgan oraliq dasturiy ta’minot moduli bo‘lib, u kiruvchi HTTP/HTTPS so‘rovlarini va chiquvchi javoblarni oldindan tahlil qilish, o‘zgartirish yoki nazorat qilish imkonini beradi. Mazkur komponent xavfsizlik, autentifikatsiya, kirish nazorati, log yuritish, seanslarni boshqarish kabi global vazifalarni bajarishga xizmat qiladi va tizimga yuqori darajadagi xavfsizlik qatlamini integratsiyalashda muhim vosita hisoblanadi.

Shunday qilib, ushbu yondashuv asosida ishlab chiqilgan WAF tizimi nafaqat xavfsizlik tahdidlarini aniqlash, balki ularni real vaqt rejimida bartaraf etish imkoniyatini beradi, bu esa veb-ilovaning umumiy ishonchliligini va foydalanuvchi ma’lumotlarining yaxlitligini ta’minlashda muhim omil bo‘lib xizmat qiladi.

ISSN 2181-3187

```python
import re
from django.http import HttpResponse

class WAFMiddleware:
    def __init__(self, get_response):
        self.get_response = get_response

        # Oldindan belgilangan xavfsizlik qoidalari
        self.rules = {
            "SQL Injection": r"(union|select|from|where|drop|delete)",
            "Cross-Site Scripting (XSS)": r"(<script>|javascript:)"
        }

    def __call__(self, request):
        # Xavfsizlik qoidalari asosida kiruvchi so'rovni filtrlang
        for rule_name, rule_pattern in self.rules.items():
            if re.search(rule_pattern, request.path, re.IGNORECASE):
                return HttpResponse(f"Blocked request due to {rule_name} attack")

        # Keyingi o'rta dastur yoki ko'rish funksiyasini chaqiring
        response = self.get_response(request)
        return response
```

1.4 - rasm. Mukammal WAF ni yaratish

```python
MIDDLEWARE = [
    # ...
    'path.to.WAFMiddleware',
    # ...
]
```

1.5-ram. WAF ni o‘rta dasturlar qatoriga qo‘shish

Yaratgan middleware ni settingsdagi qolgan middlewarelar qatoriga qoshib qoyiladi.

Veb-ilovalar xavfsizligini ta’minlashda inson omili muhim strategik ahamiyat kasb etadi. Xususan, axborot xavfsizligiga oid xavf-xatarlarni oldindan aniqlash va ularning oldini olishda xodimlarni muntazam o‘qitish va ularda raqamli savodxonlikni oshirish zaruriy chora-tadbirlardan biridir. Xodimlar, ayniqsa, kuchli parol siyosatini amalda qo‘llash, fishing (phishing) hujumlarini aniqlash, shaxsiy va korporativ

ISSN 2181-3187

ma’lumotlarni xavfsiz boshqarish, hamda ijtimoiy muhandislik (social engineering) tahdidlariga qarshi immunitetni shakllantirish bo‘yicha amaliy ko‘nikmalarga ega bo‘lishlari lozim. Ushbu maqsadlarda xavfsizlikka oid eng yaxshi amaliyotlar (best practices) asosida ishlab chiqilgan treninglar, seminarlar va test sinovlari tashkil etilishi tavsiya etiladi.

Bundan tashqari, har qanday kiberxavfsizlik hodisasiga nisbatan tezkor va muvofiqlashtirilgan chora ko‘rish imkonini beruvchi voqealarga javob rejasining (Incident Response Plan, IRP) mavjud bo‘lishi zarur. Ushbu reja voqea sodir bo‘lgan vaziyatda uning oldini olish, sabablari va zaiflik manbalarini aniqlash, zararni kamaytirish, zarur holatda huquqni muhofaza qiluvchi organlar va manfaatdor tomonlar bilan aloqa o‘rnatish kabi bosqichlarni o‘z ichiga olishi kerak. Bundan tashqari, hodisa natijasida ko‘rilgan zarar va ko‘rilgan choralar tahlili asosida tizimni takomillashtirish bo‘yicha takliflar ishlab chiqilishi lozim.

Umuman olganda, veb-ilovalarni himoyalashda kirishni nazorat qilish (access control), Web Application Firewall (WAF) tizimlari, ma’lumotlar zaxiralash siyosati (backup strategy), xodimlar tayyorgarligi va voqealarga javob mexanizmlarini integratsiyalash orqali kiberxavflarning salbiy ta’sirini sezilarli darajada kamaytirish mumkin. Bu borada veb-sayt egalari, ishlab chiquvchilar va axborot xavfsizligi mutaxassislari o‘zaro hamkorlikda faoliyat yuritishlari, tahdidlarning evolyutsion xarakterini hisobga olgan holda proaktiv va adaptiv xavfsizlik yondashuvlarini tatbiq etishlari lozim.

Faqat tizimli, kompleks va uzluksiz yondashuv orqaligina veb-ilovalarning yaxlitligini, foydalanuvchi ma’lumotlarining maxfiyligini hamda ishonchlilik darajasini yuqori pog‘onaga ko‘tarish mumkin. Shu nuqtai nazardan, kiberxavfsizlik yagonalikda amalga oshiriladigan, texnologik vositalar bilan inson resurslarini integratsiyalovchi uzluksiz strategik jarayon sifatida qaralishi lozim.

Shuni ta’kidlash kerakki, kiberxavfsizlik bir martalik tuzatish emas, balki doimiy monitoring, sinov va takomillashtirishni talab qiladigan doimiy jarayondir. Xavfsizlik choralari muntazam ravishda yangilanishi va o‘zgaruvchan tahdid

ISSN 2181-3187

landshaftiga moslashtirilishi kerak. Xavfsizlik siyosatlari, protseduralari va amaliyotlarini ularning samarali va dolzarb bo‘lishini ta’minlash uchun muntazam ravishda ko‘rib chiqish va yangilab turish juda muhimdir.

Veb-sayt kiberxavfsizligining yana bir muhim jihati bu qoidalar va standartlarga rioya qilishdir. Sanoatga qarab, amal qilinishi kerak bo‘lgan turli xil qoidalar va standartlar bo‘lishi, Evropa Ittifoqidagi umumiy ma’lumotlarni himoya qilish to‘grisidagi nizom (GDPR) yoki kredit karta ma’lumotlari bilan ishlaydigan tashkilotlar uchun to‘lov kartalari sanoati ma’lumotlar xavfsizligi standarti (PCI DSS). Ushbu qoidalar va standartlarga rioya qilish nafaqat qonuniy muvofiqlikni ta’minlaydi, balki kiberxavfsizlik choralarini kuchaytirishga yordam beradi.

GDPR (General Data Protection Regulation) - umumiy ma’lumotlarni himoya qilish qoidalarini anglatadi. Bu 2018-yil 25-mayda kuchga kirgan Yevropa Ittifoqining (Yevropa Ittifoqi) reglamentidir. GDPR kompaniya va tashkilotlar Yevropa Ittifoqi fuqarolarining shaxsiy ma’lumotlarini qanday himoya qilishi kerakligi haqidagi qoidalarni belgilaydi. Bu shaxslarga shaxsiy ma’lumotlari ustidan ko‘proq nazorat qilish imkonini beradi va kompaniyalardan ma’lumotlar amaliyoti bo‘yicha shaffof bo‘lishini talab qiladi.

1.6 - rasm. *GDPR* - umumiy ma’lumotlarni himoya qilish qoidalari

GDPRga muvofiq, shaxsiy ma’lumotlar shaxsni aniqlash uchun ishlatilishi mumkin bo‘lgan ism, manzil, elektron pochta manzili yoki IP manzili kabi har qanday

ISSN 2181-3187

ma’lumotlarni o‘z ichiga oladi. Nizom kompaniyaning qayerda joylashganidan qat’i nazar, Yevropa Ittifoqi fuqarolarining shaxsiy ma’lumotlarini qayta ishlovchi har qanday kompaniya yoki tashkilotga nisbatan qo‘llaniladi.

GDPRning asosiy talablaridan ba’zilari quyidagilardan iborat:

– shaxsiy ma’lumotlardan foydalanish uchun jismoniy shaxslardan aniq rozilik olish;

– jismoniy shaxslarga shaxsiy ma’lumotlariga kirish va ularni o‘chirish huquqini ta’minlash;

– shaxsiy ma’lumotlarni himoya qilish uchun tegishli xavfsizlik choralarini qo‘llash;

– 72 soat ichida ma’lumotlarning buzilishi haqida hokimiyatga va zarar ko‘rgan shaxslarga xabar berish;

– ma’lumotlarni himoya qilish bo‘yicha ishlarni nazorat qilish uchun ma’lumotlarni himoya qilish bo‘yicha xodimni (DPO) tayinlash.

GDPRga rioya qilmaslik 20 million yevro yoki kompaniyaning global yillik daromadining 4 foizigacha, qaysi biri kattaroq bo‘lsa, katta miqdorda jarimaga olib kelishi mumkin.

PCI DSS (Payment Card Industry Data Security Standard.) - to‘lov kartalari sanoati ma’lumotlar xavfsizligi standartini anglatadi. Bu Visa, Mastercard, American Express va Discover kabi yirik kredit karta kompaniyalari tomonidan to‘lov kartalari bilan operatsiyalarni amalga oshirishda karta egasining nozik ma’lumotlarini himoya qilishni ta’minlash uchun yaratilgan xavfsizlik standartlari to‘plamidir.

1.7 - rasm. Yevropa to‘lov tizimini nazorat standarti

ISSN 2181-3187

PCI DSS to‘lov kartasi tranzaksiyalarini qabul qiladigan yoki qayta ishlovchi har qanday tashkilot uchun amal qiladi. Ushbu kredit karta kompaniyalari PCI DSSga rioya qilishni talab qiladi va ularga rioya qilmaslik jarima va boshqa jazolarga olib kelishi mumkin.

PCI DSS standartining asosiy 12 talabi (Payment Card Industry Data Security Standard Requirements)

PCI DSS standarti kredit/debet kartalari bilan ishlovchi barcha tashkilotlar tomonidan rioya qilinishi lozim bo‘lgan xavfsizlik choralarining majmuasidir. Standart karta egasi ma’lumotlarining maxfiyligi, yaxlitligi va mavjudligini ta’minlashga qaratilgan quyidagi 12 asosiy talablardan iborat:

1. Tarmoq xavfsizligini ta’minlash: Karta egasi ma’lumotlarini tashqi tahdidlardan himoya qilish uchun xavfsizlik devorlari (firewalls) konfiguratsiyasini ishlab chiqish, sozlash va doimiy ravishda yangilab borish zarur.

2. Standart parollar va sozlamalardan voz kechish: Ishlab chiqaruvchi tomonidan berilgan standart parollar va xavfsizlik parametrlaridan foydalanishni taqiqlash, ularning o‘rniga maxsus sozlangan, kuchli autentifikatsiya tizimlarini joriy etish talab etiladi.

3. Saqlanayotgan ma’lumotlarni himoyalash: Karta egasining shaxsiy ma’lumotlari (PAN, CVV) saqlanayotgan holatda ishonchli shifrlash algoritmlari orqali himoyalanishi kerak.

4. Tarmoqlar orqali uzatilayotgan ma’lumotlarni shifrlash: Ochiq va umumiy tarmoq infrastrukturasi (masalan, Internet) orqali uzatilayotgan ma’lumotlar kuchli kriptografik usullar bilan shifrlanishi shart.

5. Antivirus va antimalware vositalarini joriy etish: Tizimlar va serverlar malware tahdidlaridan himoyalanishi uchun litsenziyalangan antivirus dasturlari o‘rnatilishi va ularning muntazam ravishda yangilanishi lozim.

6. Xavfsiz tizimlar va dasturiy ta’minotni ishlab chiqish va qo‘llab-quvvatlash: Tashkilot tomonidan ishlab chiqilgan yoki ishlatilayotgan barcha ilova va

ISSN 2181-3187

tizimlar xavfsizlik me’zonlariga muvofiq ishlab chiqilishi, testdan o‘tkazilishi va xavfsiz tarzda ekspluatatsiya qilinishi kerak.

7. Ma’lumotlarga kirish huquqlarini cheklash: Karta egasi ma’lumotlariga faqat xizmat doirasida zarur bo‘lgan holatdagina kirish imkoniyati berilishi, ya’ni prinsipial jihatdan "bilishi zarur" (need-to-know) yondashuvi qo‘llanishi lozim.

8. Yagona identifikatsiyalovchi belgilarni qo‘llash: Har bir foydalanuvchiga noyob identifikator (ID) tayinlash orqali tizimga kirish nazoratini aniqlashtirish talab qilinadi.

9. Jismoniy kirishni nazorat qilish: Karta egasining ma’lumotlari saqlanadigan qurilmalar va serverlarga jismoniy kirishni qat’iy nazorat qilish, kirish yozuvlarini yuritish talab etiladi.

10. Kirish faoliyatini monitoring qilish va yozib borish: Tarmoqdagi barcha resurslar va karta egasi ma’lumotlariga kirish faoliyati log fayllar orqali doimiy monitoring ostida bo‘lishi shart.

11. Xavfsizlik tizimlarini sinovdan o‘tkazish: Tashkilot xavfsizlik siyosatiga muvofiq tarzda tizimlar va ilovalarni muntazam ravishda zaifliklarga tekshirish, pentesting (penetration testing) va xavfsizlik auditi o‘tkazishi lozim.

12. Axborot xavfsizligi siyosatini yuritish: Xavfsizlik siyosatini ishlab chiqish, uni yangilab borish va xodimlar o‘rtasida targ‘ib qilish – tashkilotda xavfsizlik madaniyatini shakllantirish uchun zaruriy choradir.

PCI DSS muvofiqligi odatda o‘z-o‘zini baholash so‘rovnomalari va tashqi malakali xavfsizlik baholovchilari (QSA) tomonidan tekshirishlar kombinatsiyasi orqali baholanadi. Talab qilinadigan baholash darajasi tashkilotning tranzaksiya hajmiga va boshqa omillarga bog‘liq. PCI DSS muvofiqligi bir martalik harakat emas, balki doimiy jarayondir, chunki standart yangi tahdidlar va zaifliklarga moslashish uchun rivojlanadi. Tashkilotlar muvofiqlikni ta’minlash uchun xavfsizlik nazoratini muntazam ravishda ko‘rib chiqishlari va yangilashlari kerak.

PCI DSS standarti karta egasi ma’lumotlarining maxfiyligi, yaxlitligi va mavjudligini himoya qilish uchun mo‘ljallangan. Standartga rioya qilish orqali

ISSN 2181-3187

tashkilotlar ma’lumotlarning buzilishi, firibgarlik va boshqa xavfsizlik hodisalari xavfini kamaytirishi mumkin. PCI DSS ga muvofiqlik nafaqat kredit karta kompaniyalari tomonidan talab qilinadi, balki tashkilotlarga ham foyda keltiradi. Bu mijozlar ishonchini oshirishi, obro‘siga putur etkazish xavfini kamaytirishi va rioya qilmaslik natijasida moliyaviy jazolardan qochishi mumkin.

Shuni ta’kidlash kerakki, PCI DSS bilan muvofiqlik umumiy xavfsizlik strategiyasining faqat bir jihati hisoblanadi. Tashkilotlar xavflarni baholash, xodimlarni o‘qitish, hodisalarga javob berishni rejalashtirish va xavfsizlik nazoratini muntazam ravishda sinovdan o‘tkazish va monitoringini o‘z ichiga olgan xavfsizlikka kompleks yondashuvni qo‘llashlari kerak.

Bundan tashqari, xosting provayderlari va kontentni yetkazib berish tarmoqlari (CDN) kabi uchinchi tomon xizmatlari ham kiberxavfsizlikka xavf tug‘dirishi mumkin. Uchinchi tomon provayderlarini tekshirish va ularning tegishli xavfsizlik choralari mavjudligini ta’minlash muhimdir.

Xulosa

Mazkur maqolada veb-saytlar va veb-ilovalarda uchraydigan asosiy kiberxavfsizlik muammolari – XSS, SQL in’ektsiyasi, CSRF hujumlari, zararli dasturlar va zaif autentifikatsiya tizimlari tahlil qilindi. Ularni bartaraf etish uchun input/output filtrlash, parametrik so‘rovlar, CSRF tokenlar, shuningdek WAF tizimlaridan foydalanish zarurligi asoslandi. Django asosida yaratilgan middleware orqali real vaqtli monitoring va IP-manzillarni avtomatik bloklash mexanizmi samarali yechim sifatida ko‘rsatildi. Shuningdek, xodimlar raqamli savodxonligini oshirish, voqealarga javob rejasini ishlab chiqish va xalqaro standartlar (GDPR, PCI DSS)ga muvofiqlikni ta’minlash veb-xavfsizlikning ajralmas jihatlari sifatida baholandi. Xulosa qilib aytganda, veb-sayt xavfsizligini ta’minlash integratsiyalashgan texnik, tashkiliy va huquqiy choralarni talab etadi hamda bu jarayon uzluksiz monitoring va takomillashtirishga asoslanishi lozim.

ISSN 2181-3187

Foydalanilgan adabiyotlar

1. OWASP Foundation. *OWASP Top Ten Web Application Security Risks*, 2023. https://owasp.org/www-project-top-ten
2. PCI Security Standards Council. *Payment Card Industry Data Security Standard (PCI DSS) v4.0*, 2022. https://www.pcisecuritystandards.org
3. European Union. *General Data Protection Regulation (GDPR), Regulation (EU) 2016/679*, Official Journal of the European Union, 2016.
4. Django Software Foundation. *Django Middleware Documentation*. https://docs.djangoproject.com
5. Stallings, W. *Network Security Essentials: Applications and Standards*. 6th Edition, Pearson, 2016.
6. Anderson, R. *Security Engineering: A Guide to Building Dependable Distributed Systems*. 3rd Edition, Wiley, 2020.
7. Scarfone, K., Souppaya, M. *Guide to Intrusion Detection and Prevention Systems (IDPS)*. NIST SP 800-94, 2007.
8. Alsmadi, I., Karabatis, G. *Information Fusion for Cyber-Security Analytics*. Springer, 2019.
9. Beznosov, K., Kruchten, P. *Towards Agile Security Assurance for Web Applications*. Springer, 2012.
10. Gollmann, D. *Computer Security*. 3rd Edition, Wiley, 2011.
11. Ferreira, A., Cruz-Correia, R., Oliveira-Palhares, E. *How to break access control in a controlled environment*. Computers & Security, 2009.
12. SANS Institute. *Defending Web Applications Security Essentials (SEC-522)*. https://www.sans.org
13. Shostack, A. *Threat Modeling: Designing for Security*. Wiley, 2014.
14. Mitropoulos, S., Karakoidas, V., Spinellis, D. *Countering Code Injection Attacks: A Unified Approach*. Information Management & Computer Security, 2006.
15. IBM X-Force. *Threat Intelligence Index 2023: Insights into the Global Threat Landscape*. https://www.ibm.com/security/data-breach/threat-intelligence