“KOHA” KİTABXANA İNFORMASİYA İDARƏETMƏ SİSTEMİNDƏ MƏLUMATLARIN MƏXFİLİYİNİN TƏMİN EDİLMƏSİ

Azad İsa oğlu Qurbanov

Riyaziyyat üzrə fəlsəfə doktoru, dosent,
BDU Kitabxanaşünaslıq kafedrası
azadbey@ mail.ru

Açar sözlər: *Koha, məlumat təhlükəsizliyi, məxfilik, kitabxana sistemləri, açıq mənbə proqram təminatı, informasiya təhlükəsizliyi*

Ключевые слова: *Koha, безопасность данных, конфиденциальность, библиотечные системы, программное обеспечение с открытым исходным кодом, информационная безопасность*

Keywords: *Koha, data security, confidentiality, library systems, open source software, information security*

Xülasə: Açıq mənbə kodlu kitabxana informasiya idarəetmə sistemi olan Koha, çevikliyi, qənaətcilliyi və icma əsaslı inkişafı səbəbindən dünyanın bir çox kitabxanalarında uğurla tətbiq edilir. Hər bir kitabxana informasiya idarəetmə sistemi istifadəçilərin şəxsi məlumatlarını saxladığından, məlumatların təhlükəsizliyi və məxfiliyin təmin olunması onlar üçün əsas prioritetdir. Bu səbəbdən məqalədə Koha sisteminin məlumatların qorunması üçün tətbiq etdiyi mexanizmlər araşdırılır, potensial zəifliklər müəyyən edilir və məxfiliyin artırılması üçün strategiyalar təklif olunur. Koha-nın arxitekturası, konfiqurasiya parametrləri və məlumatların qorunması standartlarına uyğunluğu araşdırılmaqla, kitabxana rəhbərlərinə risklərin azaldılması və istifadəçi məxfliyinin məxfiliyinin qorunması üzrə praktik tövsiyələr təqdim olunur.

Резьюме: Koha — это система управления библиотечной информацией с открытым исходным кодом, которая успешно внедрена во многих библиотеках по всему миру благодаря своей гибкости, экономической эффективности и разработке на основе участия сообщества. Поскольку каждая система управления библиотечной информацией хранит персональные данные пользователей, обеспечение безопасности и конфиденциальности данных является для них первостепенной задачей. По этой причине в статье рассматриваются механизмы, реализованные в системе Koha для защиты данных, выявляются потенциальные уязвимости и предлагаются стратегии повышения конфиденциальности. Изучив архитектуру Koha, параметры конфигурации и соответствие стандартам защиты данных, руководители библиотек получают практические рекомендации по снижению рисков и защите конфиденциальности пользователей.

Summary: Koha, an open source library information management system, is successfully implemented in many libraries around the world due to its flexibility, cost-effectiveness and community-based development. Since each library information management system stores users' personal data, ensuring data security and confidentiality is a top priority for them. For this reason, the article examines the mechanisms implemented by the Koha system to protect data, identifies potential vulnerabilities and suggests strategies to increase confidentiality. By examining Koha's architecture, configuration parameters and compliance with data protection standards, practical recommendations are provided to library managers on reducing risks and protecting user privacy.

1. Giriş: Kitabxana informasiya idarəetmə sistemləri istifadəçilərin şəxsi məlumatları, borc tarixi və maliyyə əməliyyatları kimi həssas məlumatların daşıyıcılarıdır. İlk açıq mənbə kodlu Koha

[1], bu məlumatların idarə olunmasında kitabxanalara veb əsaslı interfeys vasitəsilə dəstək verir və MySQL və ya MariaDB verilənlər bazasından istifadə edir, MARC21 və Z39.50 kimi standartlara əməl edir. Lakin Koha-nın açıq mənbə və veb əsaslı arxitekturası məlumatların məxfiliyinin təmin olunmasında xüsusi təhlükəsizlik problemləri yaradır. Bu məqalədə Koha-nın təhlükəsizlik xüsusiyyətləri araşdırılır, zəif cəhətlər qiymətləndirilir və GDPR tələblərinə [2] əməl olunması üçün tədbirlər təklif olunur.

2. **Koha: arxitekturası və təhlükəsizlik xüsusiyyətləri**

Koha veb interfeysli müştəri-server modelində fəaliyyət göstərir və əlaqəli verilənlər bazası ilə dəstəklənir. Əsas təhlükəsizlik xüsusiyyətləri bunlardır [4-5]:

- İstifadəçi autentifikasiyası və girişə nəzarət: Koha rola əsaslanan giriş nəzarətini dəstəkləyir. Bu, administratorlara kitabxana işçiləri üçün icazələri təyin etməyə və istifadəçilərin yalnız öz məlumatlarına çıxışını təmin etməyə imkan verir. LDAP və ya OAuth kimi xarici sistemləri inteqrasiya etməklə iki faktorlu identifikasiya tətbiq edilə bilər.
- Məlumatların ötürülməsinin təhlükəsizliyi: Server və müştərilər arasında məlumat ötürülməsini şifrələmək üçün HTTPS protokolu dəstəklənir.
- Verilənlər bazası təhlükəsizliyi: MySQL/MariaDB bazalarına şifrəli bağlantılar və məhdudlaşdırılmış girişlə konfiqurasiya oluna bilər.
- Audit nəzarəti: Koha istifadəçidavranışlarını tranzaksiya jurnalında qeyd edir ki, bu da inzibatçılara girişləri izləmək və şübhəli davranışları aşkar etmək imkanı verir.

Təhlükəsizlik əsasən düzgün konfiqurasiya və server inzibatçılığından asılıdır. Təssüf ki, Koha digər açıq mənbə sistemləri kimi aşağdakı zəifliklərə qarşı həssasdır:

- Yanlış Konfiqurasiya Riski: HTTPS protokolunun aktiv edilməməsi və ya zəif şifrələr kimi səbəblər məlumat sızıntısına səbəb ola bilər.
- Köhnəlmiş proqram təminatı: Koha-nın təhlükəsizlik yeniləmələri cəmiyyət tərəfindən yayımlanır, lakin kitabxanalar tərəfindən gecikdirilmiş tətbiq sistemi təhlükə altında qoya bilər.
- Üçüncü tərəf interfeysləri: Koha ilə inteqrasiya edilən tətbiqlər və xidmətlər (məsələn, ödəniş sistemləri) düzgün yoxlanılmazsa, zəiflik yarada bilər.
- Daxili təhlükələr: Həddindən artıq səlahiyyət verilmiş və ya məlumat təhlükəsizliyi üzrə hazırlıqsız əməkdaşlar məlumatların məxfiliyini poza bilər.

2. Koha-da məxfiliyin təmin edilməsi

Kitabxanalar Koha istifadə edərkən məxfilik, bütövlük və əlçatanlıq (CIA triadası) prinsiplərinə uyğun çoxqatlı informasiya təhlükəsizliyi siyasəti tətbiq etməlidir. Bu siyasət özündə aşağıdakıları ehtiva etməlidir:

1. Texniki tədbirlər. Bunlara aiddir:

- Şifrələmə: Güclü TLS protokolları ilə HTTPS aktiv edilməsi. SSL sertifikatı üçün Let's Encrypt kimi alətlərdən istifadə edilməsi.
- Müntəzəm yeniləmələr: Təhlükəsizlik yenilənmələrinin vaxtında tətbiq edilməsi, həmçinin əməliyyat sisteminin və verilənlər bazasınını yenilənməsi.
- Girişə nəzarət: Ən az səlahiyyət prinsipini tətbiq edilməsi. Güclü və unikal şifrələr istifadə edilməsi. Administratorlar üçün MFA tətbiq edilməsi.
- Ehtiyat nüsxələr və bərpa: Məlumatların şifrəli şəkildə, uzaq məkanda saxlanan ehtiyat nüsxələrini yaradılması.

2. Təşkilati tədbirlər: Bunlara aiddir:

- Əməkdaşların təlimi: İşçilərə məlumatların qorunması, fişinq hücumları və istifadəçi məlumatlarının təhlükəsiz işlənməsi barədə təlimlər keçirmək.
- Təhlükəsizlik siyasətlərin hazırlanması: GDPR və ya 152-FZ kimi qanunlara uyğun məlumat mühafizəsi siyasəti hazırlamaq.

• Audit və Monitorinq: Müntəzəm təhlükəsizlik auditi aparmaq və istifadəçi davranışı qeydlərini analiz etmək.

3. *Qanunvericiliyə uyğunluq:* Koha-nın elastikliyi onu müxtəlif hüquqi tələblərə uyğunlaşdırmağa imkan verir. GDPR-a uyğun olaraq, istifadəçi məmnunluğu və məlumatların minimallaşdırılması təmin edilməlidir. Koha-da borc tarixçəsinin anonimləşdirilməsi və ya məlumatın saxlanma müddətinin məhdudlaşdırılması mümkündür. Azərbaycan qanunvericiliyinə görə, şəxsi məlumatlar ölkə daxilində saxlanılmalıdır, buna görə məlumatlar yerli serverlərə yerləşdirilməlidir.

3. **Nəticə:** Koha güclü bir kitabxana informasiya idarəetmə sistemi olsa da, məlumatların məxfiliyinin təmin edilməsi aktiv tədbirləri tələb edir. Texniki vasitələr, təşkilati siyasətlər və hüquqi tələblərə uyğunluq birləşdirilərək risklər azaldıla və istifadəçi məxfiliyi qoruna bilər. Koha icması davamlı olaraq təhlükəsizlik funksiyalarını gücləndirir və kitabxanalar üçün resurslar təqdim edir. Bunlar vaxtında tətbiq edilməlidir.

Ədəbiyyat

1. Koha (software). (2008). Wikipedia.
2. Information security. (2004). Wikipedia.
3. Federal Law "On Personal Data" No. 152-FZ. (2011). ConsultantPlus.
4. Methods of ensuring information security. (2020). Smart-Soft.
5. Protecting personal data: How to ensure their security in an organization. (2023). CryptoARM.