VEB-ILOVANING XAVFSIZLIK TAHLILI UCHUN MINIMAL GRAFIK MODEL KOMPONENTLARI

Matyoqubov Og‘abek Bahrombek o‘g‘li
Abu Rayhon Beruniy nomidagi Urganch davlat universiteti
Urgench, Uzbekistan
E-mail: ogabekbahrombekogli@gmail.com

Annotatsiya. Maqolada veb-ilovani minimal grafik modeli ko‘rinishida tasvirlash yondashuvi ko‘rib chiqiladi. Bu yerda tugunlar tizimning asosiy komponentlarini, yo‘nalishlar (qirralar) esa ular orasidagi bog‘liqlik va aloqalarni ifodalaydi. Bunday tasvirlash usuli ilovaning xavfsizlik tuzilmasini tahlil qilish, potensial zaifliklar va muhim tugunlarni aniqlash imkonini beradi. Taklif etilgan metod amaliy qo‘llanishga yo‘naltirilgan bo‘lib, bog‘liqliklarni tahlil qilish, arxitekturani vizuallashtirish va axborot xavfsizligi xavflarini baholash kabi vazifalarda qo‘llanishi mumkin.

Kalit so‘zlar. Veb-ilova xavfsizligi, komponentlar grafigi modeli, zaifliklarni tahlil qilish, bog‘liqliklar tahlili, xavf baholash, dasturiy arxitektura, graf nazariyasi, markaziylik ko‘rsatkichlari, CVSS reyting tizimi, ko‘p bosqichli himoya.

Annotation. The article examines the approach of describing a web application in the form of a minimal graphical model. Where the nodes represent the main components of the system, and the directions (edges) represent the connections and connections between them. Such a method of imaging allows you to analyze the security structure of the application, identify potential vulnerabilities and critical nodes.nnotation. The article examines the approach of describing a web application in the form of a minimal graphical model. Where the nodes represent the main components of the system, and the directions (edges) represent the connections and connections between them. Such a method of imaging allows you to analyze the security structure of the application, identify potential vulnerabilities and critical nodes. The proposed method is focused on practical application and can be used in tasks such as dependency analysis, architecture visualization, and information security risk assessment.

Keywords. Web application security, component graph model, vulnerability analysis, dependencies analysis, risk assessment, software architecture, graph theory, centrality indicators, CVSS rating system, multistage protection.

Аннотация. В статье рассматривается подход к изображению веб-приложения в виде минимальной графической модели. Здесь узлы представляют основные компоненты системы, а направления (ребра) представляют связи и связи между ними. Такой метод визуализации позволяет анализировать структуру безопасности приложения, выявлять потенциальные уязвимости и критические узлы.ннотация. В статье

ISSN 3030-3907

рассматривается подход к изображению веб-приложения в виде минимальной графической модели. Здесь узлы представляют основные компоненты системы, а направления (ребра) представляют связи и связи между ними. Такой метод визуализации позволяет анализировать структуру безопасности приложения, выявлять потенциальные уязвимости и критические узлы. Предлагаемый метод ориентирован на практическое применение и может быть использован в таких задачах, как анализ зависимостей, визуализация архитектуры и оценка рисков информационной безопасности.

Ключевые слова. Безопасность веб-приложений, модель компонентного графа, анализ уязвимостей, анализ зависимостей, оценка рисков, архитектура программного обеспечения, теория графов, показатели центрированности, рейтинговая система CVSS, многоуровневая защита.

Kirish

Zamonaviy veb-ilovalar o‘zaro bog‘langan modullar, kutubxonalar va xizmatlar majmuasiga asoslanadi. Bunday ko‘p qatlamli arxitektura funksionallikni oshiradi, biroq xavfsizlik nazoratini murakkablashtiradi. Ko‘pchilik zaifliklar bog‘liqliklarning noaniqligi va aloqalar modelining yo‘qligi sababli yuzaga keladi. Arxitektura tahlilining samarali usullaridan biri — ilovani graf ko‘rinishida ifodalashdir, bunda har bir tugun komponentni, har bir qirra (aloqa) esa ular orasidagi o‘zaro ta’sirni bildiradi. Ushbu maqolada bunday bog‘liqliklarni vizuallashtirish va tahlil qilishni soddalashtiruvchi minimal grafik model taklif etiladi.

Veb-ilovani grafik ko‘rinishda tasvirlash uning arxitekturasi va komponentlar o‘rtasidagi o‘zaro aloqalarni tahlil qilish uchun samarali vosita hisoblanadi. An’anaviy dastur kodi tahlilidan farqli ravishda, grafik model tizimni tuzilmaviy darajada idrok etish imkonini beradi — bu yerda asosiy e’tibor bajarilish tafsilotlariga emas, balki ilova qismlari orasidagi bog‘liqliklarga qaratiladi.

Zamonaviy veb-ilovalar ko‘plab elementlardan tashkil topgan: mijoz interfeysi (frontend), server mantiği (backend yoki API), ma’lumotlarni qayta ishlash tizimlari, autentifikatsiya modullari, ma’lumot saqlash tizimlari va tashqi xizmatlar. Ushbu elementlar murakkab bog‘liqlik tarmog‘ini hosil qiladi, bunda bitta komponentdagi o‘zgarish boshqalarning barqarorligi va xavfsizligiga ta’sir ko‘rsatishi mumkin. Shu murakkablikni boshqarish uchun grafik model qo‘llaniladi, bunda tugunlar (nodes) tizim komponentlarini, qirralar (edges) esa ular orasidagi aloqalar va ma’lumot oqimlarini ifodalaydi.

Bunday yondashuv ilova arxitekturasini yo‘nalgan graf (directed graph) sifatida o‘rganish imkonini beradi, bunda qirralar yo‘nalishi chaqiruvlar yoki

ISSN 3030-3907

bog‘liqliklar yo‘nalishini ko‘rsatadi. Masalan, frontend — REST API bilan bog‘lanadi, u esa o‘z navbatida ma’lumotlar bazasi bilan o‘zaro aloqada bo‘ladi. Har bir bunday o‘zaro ta’sir xavfsizlikka tahdid soluvchi potentsial xatolarga sabab bo‘lishi mumkin — masalan, ma’lumot uzatishdagi zaifliklar yoki autentifikatsiya mexanizmlaridagi xatolar.

Mazkur ishda taklif etilayotgan minimal grafik model faqat asosiy yuqori darajadagi komponentlarni (frontend, API, xizmatlar, ma’lumotlar bazalari) va ularning asosiy bog‘lanishlarini qamrab oladi. Ichki past darajadagi chaqiruvlar va yordamchi modullar modeldan chiqarib tashlanadi. Bu yondashuv modelning tahliliy qiymatini saqlagan holda tuzilmani soddalashtirish imkonini beradi.

Nazariy nuqtayi nazardan, ushbu model graf nazariyasi va modulli dasturiy arxitektura tahlili tamoyillariga asoslanadi. Grafikni talqin qilishda foydalaniladigan asosiy ko‘rsatkichlar (metrikalar) quyidagilardan iborat:

- Tugun darajasi (degree) — komponentning boshqa qismlar bilan nechta bog‘lanishga ega ekanligini ko‘rsatadi;
- Markaziylik (centrality) — tugunning ma’lumot uzatishdagi ahamiyat darajasini bildiradi;
- Graf zichligi (density) — tizimning bog‘liqlik darajasini aks ettiradi va arxitektura murakkabligini ko‘rsatadi.

Ushbu metrikalardan foydalanish orqali ilovaning ishlashida markaziy rol o‘ynaydigan, demak eng zaif bo‘lishi mumkin bo‘lgan kritik tugunlarni aniqlash mumkin. Shu tariqa, grafik model nafaqat ilova tuzilmasini vizuallashtirish vositasi, balki uning barqarorligi va ishonchliligini baholash uchun tahliliy instrument sifatida ham xizmat qiladi.

MODELNI QURISH METODOLOGIYASI

Taklif etilayotgan grafik model veb-ilovaning arxitekturasi va undagi o‘zaro bog‘liqliklarni tahlil qilish asosida quriladi. Asosiy g‘oya — tizim tuzilmasini yo‘naltirilgan graf shaklida ifodalashdan iborat. Bu holda:

- V — tizimdagi komponentlarni ifodalovchi tugunlar to‘plami (nodes),
- E — ularning o‘zaro bog‘lanishlarini ifodalovchi qirralar to‘plami (edges) hisoblanadi.

Bunday ko‘rinish ilovaning tuzilmasini yanada tushunarli tarzda tasvirlash va komponentlar orasidagi bog‘liqliklarni formal tahlil qilish imkonini beradi. Minimal model quyidagi 4 ta asosiy elementdan tashkil topadi:

ISSN 3030-3907

1-jadval

Tugun xavfini baholash

Element	Tavsif	Misol
Tugun (Node)	Tizim komponenti: modul, kutubxona, servis, mikroxizmat, API yoki ma'lumotlar bazasi	AuthService, Database, Frontend, LoggerService
Qirra (Edge)	Komponentlar orasidagi bog'liqlik yoki murojaat yo'nalishi	AuthService → Database
Bog'liqlik turi	Tugunlar orasidagi aloqaning tabiati: kod importi, API chaqiruvi, SQL so'rovi, xabar almashinuvi va h.k.	import, REST call, SQL query
Atributlar	Xavfsizlik tahlilida ishlatiladigan qo'shimcha ma'lumotlar	version=1.2, CVE-2024-1234, risk_level=high

Komponentlarning xavf darajasini aniqlash uchun quyidagi formula qo'llaniladi:

$$R(node) = CVSS \times C(node)$$

bu yerda:

- CVSS — *Common Vulnerability Scoring System* bo'yicha zaiflik bahosi (0 dan 10 gacha),
- C(node) — tugunning grafdagi markaziylik ko'rsatkichi (*centrality*), ya'ni u butun tizimdagi ahamiyatini bildiradi.

Natijada, markaziyligi yuqori va zaifligi kuchli tugunlar eng xavfli hisoblanadi va ular xavfsizlik auditida ustuvor tekshiruv obyektlari bo'lishi lozim. Yaratilgan grafik model quyidagi imkoniyatlarni beradi:

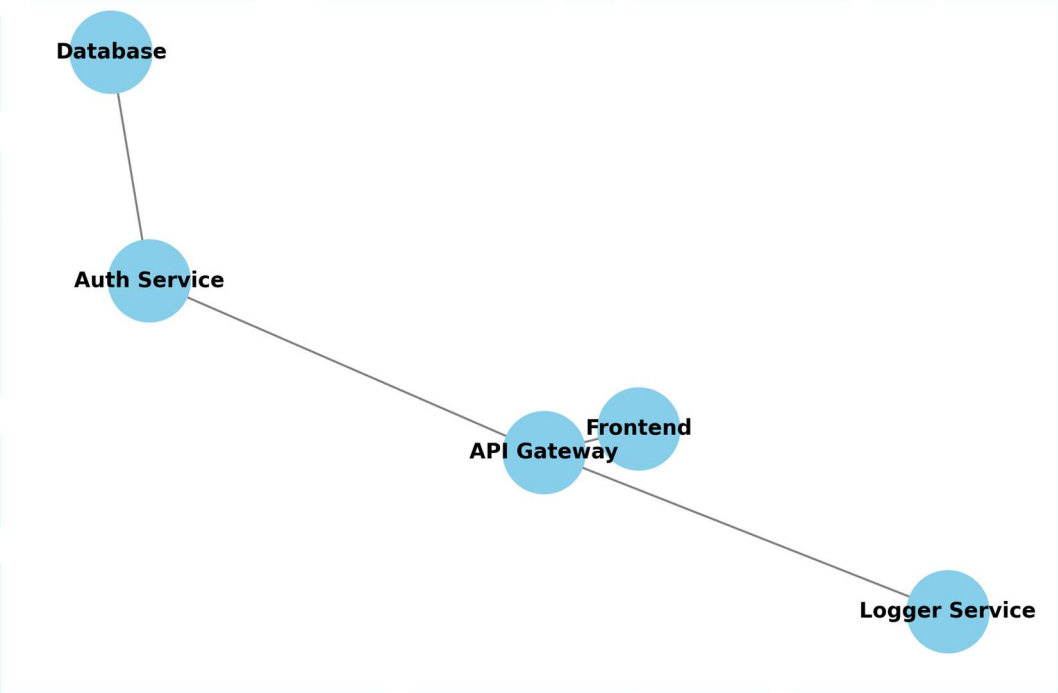
- tizimdagi xavf to'planayotgan nuqtalarni aniqlash;
- xavfli zanjirlarni (masalan, himoyasiz API yoki eskirgan kutubxona orqali) kuzatish;
- arxitektura tuzilmasini vizual ko'rinishda ifodalash, bu esa dasturchilar va axborot xavfsizligi mutaxassislari uchun tushunarliroq tahlil imkonini yaratadi.

Veb-ilova komponentlarining o'zaro bog'liqligini tushunarli shaklda ifodalash uchun grafik tasvirlash (vizuallashtirish) usuli qo'llaniladi. Ushbu yondashuv tizimning tuzilmasini vizual ko'rinishda ko'rsatib, foydalanuvchiga komponentlar o'rtasidagi aloqalar va ularning rolini tezda aniqlash imkonini beradi.

Grafdagi tugunlar (nodes) — bu ilovaning asosiy qismlari (masalan, frontend, API gateway, autentifikatsiya servisi, ma'lumotlar bazasi), qirralar (edges) esa ular orasidagi o'zaro bog'lanishlarni bildiradi. Har bir qirra ma'lumot oqimi yoki chaqiruv yo'nalishini ifodalaydi. Masalan, Frontend foydalanuvchi so'rovlarini API Gateway ga uzatadi, u esa navbatdagi bosqichda Auth Service orqali Database bilan aloqa o'rnatadi.

ISSN 3030-3907

Quyidagi rasmda veb-ilova komponentlarining minimal graf ko‘rinishidagi modeli keltirilgan. Bu modelda asosiy modullar va ular orasidagi bog‘liqliklar ifodalangan.



Rasm 1 - Veb-ilova komponentlari grafigi.

Rasmdagi tugunlar — tizim qismlarini, qirralar esa ular orasidagi aloqa yo‘nalishini bildiradi.

Ushbu model yordamida arxitektura quyidagi jihatlar bo‘yicha tahlil qilinadi:

- Markaziy tugunlarni aniqlash: eng ko‘p bog‘lanishga ega komponentlar;
- Ma’lumot oqimining yo‘nalishini tahlil qilish: foydalanuvchi so‘rovlaridan boshlab, ichki servislar orqali bazaga borish yo‘li;
- Zaif bog‘lanishlarni aniqlash: himoyasiz API yoki autentifikatsiya xizmatlaridagi potensial xavfli bog‘lanishlar.

Grafik tasvirlash arxitektura tahlilini intuitivroq qiladi va xavfsizlik auditi jarayonida muhim komponentlarni tezda aniqlashga yordam beradi. Shu tarzda qurilgan vizual model keyingi bosqichlarda xavf tahlili, graf metrikalari (centrality, degree) va avtomatlashtirilgan monitoring uchun asos bo‘lib xizmat qiladi.

NATIJALAR

Grafik model aniqlash mumkin. Ushbu tahlilning asosiy afzalligi shundaki, u tizimdagi xavflarni faqat alohida komponent darajasida emas, balki butun arxitektura kontekstida baholash imkonini beradi.

Grafdagi har bir tugun (komponent) o‘zining markaziylik darajasi (centrality) va zaiflik ko‘rsatkichlari (CVE, CVSS) orqali baholanadi. Markaziyligi yuqori bo‘lgan tugunlar ko‘plab boshqa komponentlar bilan bog‘langan bo‘lib, ular orqali tizimning katta qismi ishlaydi. Shu sababli, bunday tugunlardagi har qanday zaiflik — butun tizim xavfsizligiga jiddiy tahdid tug‘diradi.

ISSN 3030-3907

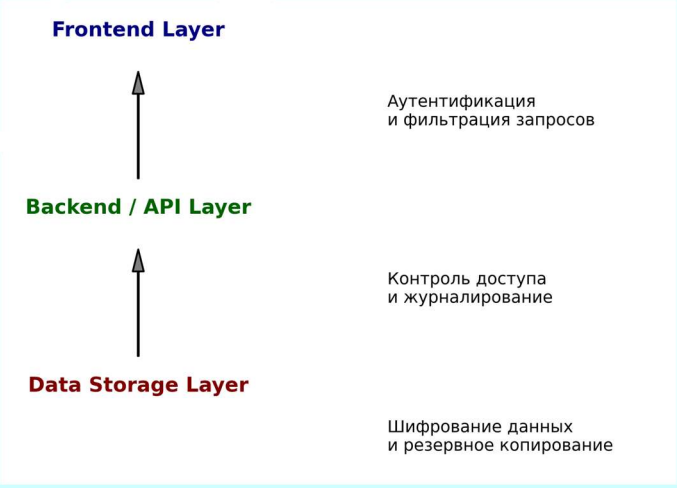
Masalan, API Gateway tuguni Frontend, Auth Service va boshqa servislar bilan bevosita aloqada bo‘lishi mumkin. Agar aynan shu modulda zaiflik mavjud bo‘lsa, hujumchi unga kirish orqali boshqa barcha bog‘langan komponentlarga ta’sir o‘tkazishi ehtimoli yuqori.

Shuning uchun xavfsizlik tahlili bosqichida quyidagi jarayonlar amalga oshiriladi:

1. Markaziy tugunlarni aniqlash: eng ko‘p bog‘lanishga ega va ma’lumot oqimining markazida joylashgan komponentlar topiladi.
2. Zaifliklarni xaritalash: har bir tugun uchun mos CVE (Common Vulnerabilities and Exposures) yozuvlari tekshiriladi.
3. Risk ko‘rsatkichini hisoblash: har bir komponent uchun R(node)=CVSS×C(node)R(node) = CVSS \times C(node)R(node)=CVSS×C(node) formulasi bo‘yicha xavf bahosi aniqlanadi.
4. Risk darajasi bo‘yicha ustuvorlikni belgilash: yuqori xavfli tugunlar (masalan, CVSS > 7.0 va C(node) > 0.5) birinchi navbatda ko‘rib chiqiladi.

Veb-ilovaning arxitekturasi odatda uchta asosiy xavfsizlik qatlamidan iborat: Frontend, Backend/API va Data Storage. Har bir qatlam o‘zining himoya mexanizmlariga ega bo‘lib, ular birgalikda ilovaning yaxlit xavfsizlik tizimini shakllantiradi.

Quyidagi rasmda bu qatlamlarning o‘zaro bog‘liqligi va ularga xos xavfsizlik funksiyalari ko‘rsatilgan:



Rasm 2 - Veb-ilovaning xavfsizlik darajalari.

Har bir qatlamda alohida himoya mexanizmlari ishlaydi:

- Frontend Layer — foydalanuvchi so‘rovlarini autentifikatsiya qilish va filtrdan o‘tkazish. Bu bosqichda XSS, CSRF, va input injection kabi hujumlarning oldi olinadi.
- Backend / API Layer — kirish huquqlarini nazorat qilish, token asosidagi autentifikatsiya va jurnallashtirish (logging) amalga oshiriladi. Ushbu qatlamda so‘rovlarning haqiqiyligini va ularning manbasini tekshirish muhim.

ISSN 3030-3907

• Data Storage Layer — ma’lumotlarni shifrlash, zaxira nusxalarini yaratish va ruxsatsiz kirishlardan himoya qilishni ta’minlaydi.

Bu qatlamlar birgalikda vertikal xavfsizlik modelini shakllantiradi, ya’ni hujum bir bosqichni yenggan taqdirda ham keyingi qatlam uni to‘xtatadi. Shu tarzda tizimda ko‘p bosqichli himoya (multi-layer defense) konsepsiyasi amalga oshadi.

XULOSA

Ushbu tadqiqotda veb-ilova komponentlarini tahlil qilish uchun minimal grafik model asosida yondashuv taklif etildi. Mazkur model veb-ilovaning murakkab arxitekturasini soddalashtirilgan, lekin tahliliy jihatdan foydali shaklda ifodalashga imkon beradi.

Grafik yondashuv yordamida tizimdagi asosiy komponentlar (frontend, API, ma’lumotlar bazasi) va ularning o‘zaro bog‘liqliklari aniqlanadi. Har bir tugun va qirra ma’lum atributlarga ega bo‘lib, ular asosida xavfsizlik holatini baholash mumkin. Shu orqali dastur arxitekturasidagi markaziy nuqtalar, ya’ni tizim uchun eng muhim va ayni paytda eng zaif komponentlar ajratib olinadi.

Taklif etilgan metodologiya nafaqat tahlilni soddalashtiradi, balki xavfsizlikni boshqarishning yangi, graf asosidagi ko‘p bosqichli yondashuvini shakllantiradi. Veb-ilova xavfsizlik qatlamlari — Frontend, Backend/API va Data Storage — bir-birini to‘ldiruvchi himoya tizimlari sifatida baholandi. Bu esa hujumlarni turli bosqichlarda to‘xtatish imkonini beruvchi ko‘p darajali himoya (defense in depth) tamoyilini amalda qo‘llashga xizmat qiladi.

Yakuniy natijada, ishlab chiqilgan model:

• ilovaning arxitektura tuzilmasini vizual va tahliliy jihatdan ifodalaydi;
• komponentlar orasidagi xavf darajasini miqdoriy baholash imkonini beradi;
• xavfsizlik mutaxassislari uchun ustuvor risklarni aniqlash va ularni kamaytirish strategiyasini ishlab chiqishda yordam beradi.

Kelgusida ushbu modelni yanada rivojlantirish maqsadida, uni grafik ma’lumotlar bazalari (Neo4j, ArangoDB) bilan integratsiya qilish, hamda mashina o‘rganish algoritmlari orqali avtomatik zaiflik aniqlash tizimiga aylantirish istiqbollari mavjud.

FOYDALANILGAN ADABIYOTLAR

1. OWASP Foundation, *“OWASP Top 10: The Ten Most Critical Web Application Security Risks,”* 2024.
2. National Institute of Standards and Technology (NIST), *“National Vulnerability Database (NVD),”* 2024.
3. ISO/IEC 27001:2022 — *Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems Requirements*, ISO, 2022.

ISSN 3030-3907

4. D. E. Knuth, *The Art of Computer Programming*, Vol. 1–3. Addison-Wesley, 2011.
5. Neo4j Graph Data Science Team, *"Graph Data Science Manual,"* Neo4j Documentation, 2023.
6. Snyk Ltd., *"Open Source Security Report,"* 2024.
7. A. Zolotukhin, "Graph-Based Vulnerability Analysis of Software Dependencies," *IEEE Access*, vol. 11, pp. 44812–44825, 2023.
8. A. H. Madaminov, "Hybrid Traffic Filtering and Anomaly Detection Model for Next-Generation Networks," *USBEREIT Conference Proceedings*, IEEE, 2024.
9. M. Newman, *Networks: An Introduction*, Oxford University Press, 2018.
10. R. Pastor-Satorras and C. Castellano, "Topological Vulnerability of Complex Networks," *Nature Physics*, vol. 18, pp. 67–76, 2022.
11. S. T. Ahmed, "Dependency Graphs for Secure Software Architecture Analysis," *Springer Journal of Information Security*, vol. 32, no. 4, pp. 611–628, 2023.
12. OWASP, *"Kali Linux Tools and Best Practices for Penetration Testing,"* Offensive Security, 2024.
13. J. Scott and M. Carr, *Cybersecurity Risk Assessment Using Graph-Theory Metrics*, Elsevier, 2023.
14. U. Shadmanov and F. Jumaniyozov, *"Information Security Models for Web Systems,"* TUIT Press, 2023.
15. S. G'ANIYEV, M. KARIMOV, K.TASHEV, *"Axborot xavfsizligi"* «ALOQACHI» nashriyoti, 2008

ISSN 3030-3907