ISSN: 3093-9305 VOLUME - 2

JOURNAL OF GLOBAL SCIENTIFIC INNOVATIONS

worldjournal.uz

OWASP TOP 10 ASOSIDA WEB ILOVALARNI PENETRATSION TESTLASH: KOMPLEKS TAHLIL

Nuriddinova Dilnura Sharofiddinovna
"Cyber University" davlat universiteti 1-kurs talabasi
e-mail: ndilnura7@gmail.com
Samarov Sherzod Hamrayevich
"Cyber University" davlat universiteti
"Muhandislik" fakulteti uslubchisi

Annotatsiya. Maqolada web ilovalar xavfsizligini baholashda penetratsion testlash jarayonini OWASP Top 10 freymvorki asosida tizimlashtirish masalasi tadqiq etilgan. Tadqiqotning maqsadi OWASP Top 10 kategoriyalari, nazorat qilinadigan amaliy test va CVSS baholashini yagona metodologik ketma-ketlikka birlashtirish hamda ushbu yondashuvning web ilovalardagi muhim zaifliklarni aniqlashdagi amaliy imkoniyatlarini baholashdan iborat. Tadqiqot izolyatsiya qilingan virtual laboratoriyada, qasddan zaiflashtirilgan web ilova muhitida kulrang quti yondashuvi asosida o'tkazildi. Burp Suite, OWASP ZAP, sqlmap, Nmap va Nikto vositalaridan foydalanilib, aniqlangan holatlar CVSS v3.1 mezonlari bo'yicha baholandi. Natijada olti turdagi zaiflik aniqlandi: ularning uchtasi yuqori, uchtasi o'rta xavf darajasiga mansub bo'ldi. Eng yuqori CVSS ko'rsatkichi SQL in'eksiyasida (8.6), undan keyin IDOR ko'rinishidagi buzilgan kirish nazoratida (8.1) va autentifikatsiya kamchiligida (7.5) qayd etildi. Natijalar avtomatlashtirilgan skanerlashni qo'lda tahlil bilan birlashtirish, xavfsizlik talablarini SDLCning dastlabki bosqichlariga kiritish va penetratsion testlarni muntazam o'tkazish zarurligini ko'rsatadi.

Kalit so'zlar: penetratsion testlash, web ilova xavfsizligi, OWASP Top 10, SQL in'eksiya, XSS, buzilgan kirish nazorati, autentifikatsiya, CVSS, kiberxavfsizlik, DevSecOps.

ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ ВЕБ-ПРИЛОЖЕНИЙ: КОМПЛЕКСНЫЙ АНАЛИЗ НА ОСНОВЕ OWASP TOP 10

Аннотация. В статье исследуется систематизация процесса тестирования на проникновение веб-приложений на основе OWASP Top 10. Цель исследования состоит в объединении категорий OWASP Top 10, контролируемого практического тестирования и оценки CVSS в единую методологическую последовательность и в определении практической эффективности такого подхода. Исследование проведено в изолированной

виртуальной лаборатории на намеренно уязвимом веб-приложении с применением подхода «серого ящика». Использовались Burp Suite, OWASP ZAP, sqlmap, Nmap и Nikto, а выявленные уязвимости оценивались по CVSS v3.1. В результате установлено шесть типов уязвимостей: три высокого и три среднего уровня риска. Наибольший показатель CVSS был зафиксирован для SQL-инъекции (8,6), затем для нарушения контроля доступа типа IDOR (8,1) и недостатков аутентификации (7,5). Результаты подтверждают необходимость сочетания автоматизированного сканирования с ручным анализом, интеграции требований безопасности на ранних этапах SDLC и регулярного проведения тестирования на проникновение.

Ключевые слова: тестирование на проникновение, безопасность веб-приложений, OWASP Top 10, SQL-инъекция, XSS, нарушение контроля доступа, аутентификация, CVSS, кибербезопасность, DevSecOps.

WEB APPLICATION PENETRATION TESTING: A COMPREHENSIVE ANALYSIS BASED ON THE OWASP TOP 10 FRAMEWORK

Abstract. This article examines the systematization of web application penetration testing based on the OWASP Top 10 framework. The study aims to integrate OWASP Top 10 categories, controlled practical testing, and CVSS-based risk assessment into a single methodological sequence and to evaluate its practical effectiveness in identifying critical web application vulnerabilities. The experiment was conducted in an isolated virtual laboratory using a deliberately vulnerable web application and a grey-box testing approach. Burp Suite, OWASP ZAP, sqlmap, Nmap, and Nikto were used, while the identified findings were assessed according to CVSS v3.1. Six vulnerability types were identified: three were rated high risk and three medium risk. The highest CVSS score was recorded for SQL injection (8.6), followed by IDOR-type broken access control (8.1) and authentication weaknesses (7.5). The findings demonstrate the need to combine automated scanning with manual analysis, integrate security requirements into the early stages of the SDLC, and conduct penetration testing on a regular basis.

Keywords: penetration testing, web application security, OWASP Top 10, SQL injection, XSS, broken access control, authentication, CVSS, cybersecurity, DevSecOps.

KIRISH

Raqamli xizmatlarning kengayishi bilan web ilovalar bank, elektron tijorat, davlat xizmatlari, ta'lim va korporativ axborot tizimlarining asosiy interfeysiga aylandi. Ularning Internet orqali doimiy ochiq bo'lishi va ko'p sonli foydalanuvchilar

bilan ishlashi hujum yuzasini kengaytiradi. Shu sababli web ilova xavfsizligi dasturiy mahsulotning qo'shimcha funksiyasi emas, balki uning ishonchliligi, ma'lumotlar maxfiyligi va xizmatlarning uzluksizligini belgilovchi asosiy talab sifatida qaralishi lozim.

Penetratsion testlash vakolatli va oldindan belgilangan doirada real hujumchi xatti-harakatlarini modellashtirib, tizimdagi zaifliklarning amalda ekspluatatsiya qilinish ehtimoli va oqibatlarini baholash imkonini beradi. Zaifliklarni avtomatik skanerlashdan farqli ravishda pentest aniqlangan kamchilikning haqiqiy xavfini kontekstda tekshiradi. NIST SP 800-115 xavfsizlikni testlashni rejalashtirish, o'tkazish, natijalarni tahlil qilish va tuzatish choralariga bog'langan boshqaruv jarayoni sifatida ko'radi [7]. Penetratsion testlash bo'yicha amaliy adabiyotlarda ham razvedka, zaifliklarni aniqlash, ekspluatatsiya va hisobot bosqichlarining uzviyligi ta'kidlanadi [5, 6, 8, 12].

OWASP Foundation tomonidan ishlab chiqilgan OWASP Top 10 web ilovalarda eng muhim xavf kategoriyalarini tizimlashtiradi [1]. Web Security Testing Guide testlash uchun amaliy yo'nalishlarni [2], Application Security Verification Standard esa ilovalar xavfsizligini tekshirish uchun verifikatsiya talablarini beradi [3]. Ushbu manbalar bir-birini to'ldirsa-da, risk kategoriyasi, amaliy laboratoriya tekshiruvi va CVSS asosidagi ustuvorlashtirishni bitta izchil tajriba modeli doirasida namoyish qilish alohida metodologik ahamiyatga ega.

O'zbekiston Respublikasining 'Kiberxavfsizlik to'g'risida'gi Qonuni kiberxavfsizlikni ta'minlashning huquqiy asoslarini belgilaydi [11]. Shu nuqtai nazardan, penetratsion testlash faqat texnik tajriba sifatida emas, balki ruxsat, test doirasi, axborotga ehtiyotkor munosabat va natijalarni mas'uliyatli hujjatlashtirishni talab qiladigan boshqariladigan xavfsizlik jarayoni sifatida o'tkazilishi lozim.

Mazkur tadqiqotdagi ilmiy-amaliy muammo shundan iboratki, OWASP kategoriyalarini bilishning o'zi web ilova xavfsizligini to'liq baholash uchun yetarli emas: zaiflikni aniqlash, uni xavfsiz laboratoriya sharoitida tasdiqlash, xavf darajasini yagona mezon bo'yicha baholash va bartaraf etish ustuvorligini belgilash bir-biriga bog'langan jarayon sifatida tashkil etilishi kerak. Shu sababli tadqiqotning maqsadi OWASP Top 10 asosidagi penetratsion testlash metodologiyasini nazorat qilinadigan tajriba orqali sinash, aniqlangan zaifliklarni CVSS v3.1 bo'yicha baholash va olingan natijalar asosida web ilovalarni ishlab chiqish hamda ekspluatatsiya qilish jarayoni uchun amaliy tavsiyalar ishlab chiqishdan iborat.

TADQIQOT METODOLOGIYASI

Tadqiqot nazariy tahlil va nazorat qilinadigan laboratoriya tajribasini birlashtirgan amaliy-eksperimental yondashuv asosida olib borildi. Nazariy bazani OWASP Top 10:2021 [1], OWASP Web Security Testing Guide [2], OWASP ASVS [3], NIST SP 800-115 [7] hamda CVSS v3.1 spetsifikatsiyasi [9] tashkil etdi.

Ushbu manbalar test obyektlarini tanlash, tekshiruv ketma-ketligini belgilash va aniqlangan zaifliklarni xavf darajasi bo'yicha baholash uchun metodik asos sifatida foydalanildi.

Amaliy sinov Internetdan ajratilgan, izolyatsiya qilingan virtual laboratoriyada qasddan zaifliklar joylashtirilgan o'quv web ilovasi ustida o'tkazildi. Test real uchinchi tomon tizimlariga qaratilmadi. Asosiy yondashuv sifatida kulrang quti (grey-box) modeli tanlandi: testerga cheklangan ichki ma'lumot va oddiy foydalanuvchi darajasidagi kirish berildi. Bu usul tashqi hujumchi sharoitiga yaqinlikni saqlagan holda autentifikatsiya va avtorizatsiya mexanizmlarini chuqurroq tekshirish imkonini berdi.

Test jarayonida Burp Suite Community Edition HTTP/HTTPS so'rovlarini tahlil qilish uchun, OWASP ZAP avtomatlashtirilgan dinamik tekshiruv uchun, sqlmap SQL in'eksiya alomatlarini tasdiqlash uchun, Nmap xizmatlar va ochiq portlarni aniqlash uchun, Nikto esa web server konfiguratsiyasidagi ma'lum kamchiliklarni aniqlash uchun qo'llanildi. Avtomatlashtirilgan natijalar yakuniy xulosa sifatida qabul qilinmay, qo'lda tekshirish bilan qayta tasdiqlandi.

Tajriba olti bosqichda tashkil etildi: (1) test doirasi va ruxsat etilgan usullarni belgilash; (2) razvedka; (3) skanerlash; (4) aniqlangan zaifliklarni laboratoriya doirasida tasdiqlash; (5) oqibat va xavf darajasini baholash; (6) natijalarni hisobot ko'rinishida tizimlashtirish. Har bir topilma OWASP Top 10 kategoriyasiga moslashtirildi va CVSS v3.1 bazaviy balli bilan baholandi [9].

Tadqiqotning muhim cheklovi shundaki, tajriba qasddan zaiflashtirilgan bitta laboratoriya ilovasida o'tkazilgan. Shu sababli olingan natijalar real ishlab chiqarish tizimlaridagi zaifliklar tarqalish darajasini statistik jihatdan ifodalamaydi. Ular, avvalo, taklif etilgan test ketma-ketligining amaliy qo'llanishini ko'rsatishga xizmat qiladi.

NATIJALAR

Nazorat qilinadigan test natijasida OWASP Top 10:2021 tasnifining bir nechta kategoriyalariga mos keluvchi olti turdagi zaiflik aniqlandi. CVSS v3.1 bo'yicha ularning uchtasi yuqori, uchtasi o'rta xavf darajasiga mansub bo'ldi. Eng

yuqori bazaviy ball SQL in'eksiyasida — 8.6, IDOR ko'rinishidagi buzilgan kirish nazoratida — 8.1 va autentifikatsiya kamchiligida — 7.5 qayd etildi. Natijalar 1-jadvalda umumlashtirilgan.

1-jadval. Amaliy testda aniqlangan asosiy zaifliklar

Aniqlangan zaiflik	OWASP Top 10 kategoriyasi	CVSS bazaviy ball	Potensial ta'sir
SQL in'eksiyasi (login formasi)	A03: Injection	8.6 — Yuqori	Ma'lumotlar bazasiga ruxsatsiz kirish xavfi
Buzilgan autentifikatsiya	A07: Identification and Authentication Failures	7.5 — Yuqori	Hisob ma'lumotlarini egallash va seans xavfsizligining buzilishi
Saqlanuvchi XSS (izoh formasi)	A03: Injection	6.1 — O'rta	Foydalanuvchi seansiga va brauzer kontekstiga ta'sir
Buzilgan kirish nazorati (IDOR)	A01: Broken Access Control	8.1 — Yuqori	Boshqa foydalanuvchi ma'lumotlariga ruxsatsiz kirish
Noto'g'ri xavfsizlik sozlamalari	A05: Security Misconfiguration	5.8 — O'rta	Server va tizim haqida ortiqcha texnik ma'lumot oshkor bo'lishi
Eskirgan komponentlar	A06: Vulnerable and Outdated Components	6.5 — O'rta	Ma'lum zaifliklardan foydalanish xavfining ortishi

Manba: muallif tomonidan izolyatsiya qilingan laboratoriya tajribasi natijalari asosida tuzilgan.

SQL in'eksiyasi login shaklidagi foydalanuvchi kiritmalarini qayta ishlashdagi kamchilik orqali aniqlandi. Server javoblaridagi xatolik belgilari dastlabki indikator sifatida kuzatildi va zaiflik maxsus test vositasi yordamida laboratoriya doirasida tasdiqlandi. Mazkur holat A03: Injection kategoriyasiga mos kelib, 8.6 CVSS balli bilan tajribadagi eng yuqori xavf ko'rsatkichini oldi. Ushbu natija foydalanuvchi kiritmalarini ishonchli manba sifatida qabul qilmaslik, parametrli so'rovlardan foydalanish va server tomonida tekshiruvni majburiy tashkil etish zarurligini ko'rsatadi [1, 2].

Kirish nazorati bo'yicha testda foydalanuvchi obyektining identifikatorini o'zgartirish orqali boshqa foydalanuvchi ma'lumotlariga kirish imkonini beruvchi IDOR holati qayd etildi. U A01: Broken Access Control kategoriyasiga tegishli bo'lib, 8.1 CVSS balli bilan yuqori xavf darajasida baholandi. Shuningdek,

autentifikatsiya mexanizmidagi kamchilik 7.5 ball bilan yuqori xavf sifatida qayd etildi. Bu ikki holat identifikatorni bilishning o'zi resursga kirish huquqini bermasligi va har bir so'rovda server tomonida avtorizatsiya tekshiruvi bajarilishi kerakligini ko'rsatadi.

Saqlanuvchi XSS, xavfsizlik sozlamalaridagi kamchiliklar va eskirgan komponentlar o'rta xavf guruhiga kirdi. XSS holatida foydalanuvchi kiritgan kontentni yetarli tozalash va chiqishda kodlash mexanizmlarining yo'qligi kuzatildi. Konfiguratsiya kamchiligi server haqida ortiqcha texnik ma'lumotlarning ochilishiga, eskirgan komponentlar esa ma'lum zaifliklar mavjud bo'lishi ehtimolining oshishiga olib kelishi mumkin. Shu tariqa, tajribada aniqlangan xavflar bitta texnik sababga emas, balki kiritmalarni qayta ishlash, autentifikatsiya, avtorizatsiya, konfiguratsiya va komponentlarni boshqarish kabi turli qatlamlarga taqsimlandi.

MUHOKAMA

Olingan natijalar OWASP Top 10 freymvorkidan penetratsion testning yakuniy chek-listi sifatida emas, balki xavf kategoriyalarini tizimlashtiruvchi boshlang'ich model sifatida foydalanish samarali ekanini ko'rsatdi. Tajribada A01, A03, A05, A06 va A07 kategoriyalariga oid holatlarning aniqlanishi web ilova xavfsizligi kirish nazorati, ma'lumotlarni qayta ishlash, konfiguratsiya va identifikatsiya kabi bir-biridan farqli qatlamlarning birgalikdagi holatiga bog'liqligini namoyon etdi [1].

Natijalar avtomatlashtirilgan skanerlashning imkoniyatlari bilan bir qatorda uning chegaralarini ham ko'rsatadi. OWASP ZAP va boshqa vositalar dastlabki indikatorlarni tez aniqlashga yordam beradi, biroq resurslararo avtorizatsiya yoki biznes mantiqiga bog'liq kamchiliklar ko'pincha kontekstni tushunadigan qo'lda tekshiruvni talab qiladi. OWASP WSTG ham web ilovani testlashda turli test texnikalarini birgalikda qo'llash zarurligini ko'rsatadi [2]. Demak, avtomatlashtirish testerning tahliliy bahosini almashtirmaydi, balki uni to'ldiradi.

Tajribaning yana bir muhim natijasi zaifliklarni faqat mahsulot tayyor bo'lgandan keyin aniqlash yetarli emasligidir. ASVS kabi verifikatsiya talablaridan loyihalash va ishlab chiqish bosqichlarida foydalanish [3], xavfsiz kodlash standartlarini joriy etish va CI/CD jarayonlariga SAST hamda DAST tekshiruvlarini qo'shish zaifliklarni erta aniqlash imkonini beradi. Bu yondashuv xavfsizlikni SDLCning oxirgi nazorat nuqtasidan uzluksiz DevSecOps jarayoniga o'tkazadi.

Shu bilan birga, ushbu tadqiqot natijalarini real web ilovalardagi zaifliklar tarqalishining empirik statistikasi sifatida talqin qilish mumkin emas. Test muhiti ataylab zaiflashtirilgan va bitta laboratoriya ilovasi bilan chegaralangan. Bundan tashqari, API xavfsizligi, mikroservislar, konteyner infratuzilmasi va bulutli konfiguratsiyalar alohida sinov predmeti bo'lmagan. Kelgusi tadqiqotlarda OWASP

API Security Top 10 [4] bilan integratsiyalashgan test modeli, zamonaviy REST/GraphQL APIlar va konteynerlashtirilgan muhitlarda xuddi shu metodologiyani tekshirish maqsadga muvofiq.

XULOSA

Tadqiqot OWASP Top 10 asosidagi penetratsion testlashni nazorat qilinadigan laboratoriya muhitida bosqichma-bosqich qo'llash web ilovadagi muhim xavf nuqtalarini tizimli aniqlash va ularni CVSS mezonlari bo'yicha ustuvorlashtirish imkonini berishini ko'rsatdi. Tajribada olti turdagi zaiflik aniqlanib, ularning uchtasi yuqori va uchtasi o'rta xavf darajasida baholandi. SQL in'eksiyasi, IDOR ko'rinishidagi buzilgan kirish nazorati va autentifikatsiya kamchiligi eng yuqori xavf ko'rsatkichlariga ega bo'ldi.

Olingan natijalar asosida web ilovalar xavfsizligini kuchaytirish uchun OWASP Top 10 va ASVS talablarini ishlab chiqish jarayoniga integratsiya qilish, avtomatlashtirilgan tekshiruvlarni qo'lda testlash bilan birlashtirish, kirish nazorati va autentifikatsiyani server tomonida qat'iy tekshirish, komponentlarni muntazam yangilash hamda har bir muhim yangilanishdan so'ng qayta xavfsizlik testini o'tkazish maqsadga muvofiq. Penetratsion testlash bir martalik tekshiruv emas, balki zaifliklarni boshqarish va DevSecOps jarayonining takrorlanuvchi elementi sifatida tashkil etilgandagina barqaror natija beradi.

Mazkur tadqiqotning amaliy ahamiyati OWASP kategoriyalari, laboratoriya tasdig'i va CVSS baholashini bitta izchil metodologik zanjirga birlashtirishidadir. Kelgusida ushbu modelni API, mikroservis va konteynerlashtirilgan muhitlarga tatbiq etish, shuningdek avtomatlashtirilgan tahlil natijalarini ekspert bahosi bilan solishtirish orqali metodologiyaning qo'llanish chegaralarini kengaytirish mumkin.

FOYDALANILGAN ADABIYOTLAR RO'YXATI

[1] OWASP Foundation. OWASP Top 10:2021 — The Ten Most Critical Web Application Security Risks. OWASP, 2021.
[2] OWASP Foundation. OWASP Web Security Testing Guide (WSTG) v4.2. OWASP, 2020.
[3] OWASP Foundation. OWASP Application Security Verification Standard (ASVS) v4.0.3. OWASP, 2021.
[4] OWASP Foundation. OWASP API Security Top 10:2023. OWASP, 2023.
[5] Stuttard, D., Pinto, M. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. 2nd ed. Wiley, 2011.
[6] Weidman, G. Penetration Testing: A Hands-On Introduction to Hacking. No Starch Press, 2014.
[7] National Institute of Standards and Technology. NIST SP 800-115: Technical Guide to Information Security Testing and Assessment. 2008.

[8] Engebretson, P. The Basics of Hacking and Penetration Testing. 2nd ed. Syngress, 2013.
[9] FIRST. Common Vulnerability Scoring System v3.1: Specification Document. Forum of Incident Response and Security Teams, 2019.
[10] PortSwigger. Web Security Academy — Learning Materials on Web Vulnerabilities. 2023.
[11] O'zbekiston Respublikasining 2022-yil 15-apreldagi O'RQ-764-son 'Kiberxavfsizlik to'g'risida'gi Qonuni.
[12] Kim, P. The Hacker Playbook 3: Practical Guide to Penetration Testing. 2018.