6 –TOM 2 – SON / 2023 - YIL / 15 - FEVRAL

VEB ILOVA ZAIFLIKLARINI ANIQLASH.

Radjabova Madina Shavkatovna
Toshkent axborot texnologiyalari unversitetining "Kiberxavfsizlik va kriminalistika " kafedrasi o'qituvchi-stajyor
Xafizov Shukurullo Fayzullo o'g'li
Qurbonmurodov Diyorbek Ulug'bek o'g'li
Kiberxavfsizlik fakulteti talabalari

Anatatsiya: *Veb ilovalardagi tez-tez uchraydigan zaiflik turlari hissoblangan SQL injection, XSS, LDAP, Command injection zaifliklari to'liq tahlil qilindi. Veb ilovalar zaifliklarini aniqlash uchun foydalaniladigan tijorat va ochiq kodli skanerlar Burp Suite, W3af, Wapiti, Watbo, OWASP Zap va Arachni haqida funksional jihatdan bazi o'rganishlar olib borildi. Veb ilovalardagi zaifliklarni aniqlashda dinamik ilovalar xavfsizligi testi va statik ilovalar xavfsizligi testi o'rganib chiqiladi.*

Kalit so'zlari: *Veb ilova zaifliklari, skaner, Wapiti, Benchmark*

Kirish

Veb-ilovalar kundalik hayotimizning ajralmas qismiga aylandi. Ushbu ilovalarning ko'pchiligida ularning faoliyatiga jiddiy zarar yetkaziadigan veb zaifliklarga ega bo'lishi mumkin. Ushbu holatlar yuzasidan kelib chiqib butun jaxon axborot xafsizligi soha vakillari veb ilovalar xafsizlik chora tadbirlarini ko'rishga turli qarorlar va farmoishlar qo'llashgan. Jumladan, O'zbekiston Respublikasi Prezidentining 2022 yil 28 yanvardagi PF 60-sonli farmoni bilan tasdiqlangan "2022–2026-yillarga mo'ljallangan Yangi O'zbekistonning taraqqiyot strategiyasi to'g'risida"gi 89-maqsad: Fuqarolarning axborot olish va tarqatish erkinligi borasidagi huquqlarini yanada mustahkamlash. Kiberjinoyatchilikning oldini olish tizimini yaratish bo'yicha ustuvor vazifalarni bajarish belgilangan.

Veb ilova zaifliklarni aniqlashga umumiy yondashuvlar

Veb ilovalarini aniqlovchi skanerlarning samaradorligini baholashdan avval veb ilovalar zaifliklari haqida asosiy tushunchaga ega bo'lish juda muhimdir. Ushbu tadqiqot ishida veb-ilovalar zaifligining eng muhim sinov holatlarini amalga oshiradigan OWASP benchmark 2021 versiyasidan foydalanilgan. Har xil turdagi ineksiyalar, sessiyalarni boshqarish va autentifikatsiya buzilishi, saytlararo skriptlash, kirishlarni boshqarishning yetishmovchiligi, saytlararo so'rovlarni soxtalashtirish, xavfsizlikni noto'g'ri sozlash, himoyalanmagan API'lar, hujumdan himoyalanishning yetarli emasligi va ma'lum zaifliklarga ega komponentlardan foydalanishlar va bunga misollar[12]. Biz quyida ba'zi muhim zaifliklarni keltirib o'tamiz:

Cross-site Scripting (XSS) - bu zararli skriptni ilovaga kiritishni o'z ichiga olgan ineksiya hujumi. Ushbu turdagi hujum g'arazgo'y shaxs zararli skriptni brauzer

tomonidagi skript yordamida bir nechta foydalanuvchilarga uzatganda sodir bo'ladi [13]. Agar hujum muvaffaqiyatli bo'lsa, g'arazgo'y shaxs jabrlanuvchining kirish huquqlariga ega bo'ladi. Natijada, agar jabrlanuvchi dastur ichidagi kritik ma'lumotlarga kirish imkoniga ega bo'lsa, bu jiddiy zaiflikdir. Afsuski, bunday hujumlarning muvaffaqiyatli bo'lishiga imkon beruvchi zaifliklar hamma joyda mavjud ekanligi ta'kidlangan. Zaiflik skanerlari saytlararo skriptlarning ba'zi zaifliklarini avtomatik ravishda aniqlashi mumkin bo'lsa-da, turli veb-dasturlar Flash, JavaScript, Silverlight va ActiveX kabi turli interpreterlardan foydalanadi, bu esa avtomatik aniqlashni qiyinlashtiradi. Mirrored or Non-Persistent XSS, ekspluatatsiya veb-ilovaga yuborilganda va keyin uni bajarish uchun maqsadli brauzerda aks ettirilganda sodir bo'ladi. Ushbu hujumni amalga oshirishning eng odatiy usullaridan biri zararli kontentni URL manzilida parametr sifatida taqdim etishdir.

Veb zaifliklarni zaiflik skanerlari yordamida aniqlash

Veb-ilovalarda zaifliklar aksariyat holatlarda uchrab turadi. Shu sababli, zaiflik skanerlari ilovalardagi uchrab turuvchi zaifliklarni aniqlash uchun ishlatiladi, shunda ularni minimallashtirish yoki yo'q qilish imkoniyati mavjud bo'ladi. Skanerning aniqligi va samaradorligi har doim ham benuqson emas va hamma skanerlar ham foydalanuvchi uchun qulay bo'lavermaydi [19]. Zaifliklar skanerlari quyidagilarni o'z ichiga oladi:

Burp Suite portSwigger tomonidan ishlab chiqilgan va veb-ilovalardagi zaifliklar va hujum vektorlarini aniqlash uchun axborot xavfsizligi bo'yicha mutaxassislar va penetratsion testerlar tomonidan foydalaniladigan Java-ga asoslangan veb-xavfsizlik tizimidir[20]. Ushbu skaner proksi-server sifatida maqsadli ilovadan kelgan so'rovlar va javoblarni ushlashi va tahlil qilishi mumkin. Bu inyeksiya nuqtasinini qo'lda tanlash imkonini beradi. Cross-site scripting, SQL injection, OS command injection, and file directory traversal kabi zaiflik turlarini aniqlashda foydalaniladi [15].

Web Application Attack and Audit Framework(W3af veb ilovalardagi zaifliklarni aniqlashga yordam beradigan bepul ochiq kodli skaner. Python-ga asoslangan ushbu skaner buyruq qatori interfeysi bilan bir qatorda Grafik foydalanuvchi interfeysini ham taklif etadi. W3af arxitekturasi plagin(veb ilovalarni tezkor ravishda sifatli qurilishida yordam beruvchi dastur kutubxona)larni va asosiy ishchi qismni o'z ichiga olgan ikki qismga bo'linadi. Asosiy qismi ma'lumot almashish uchun ma'lumotlar bazasidan foydalangan holda ulardagi zaifliklarni aniqlash uchun plaginlar tomonidan qo'llaniladigan xususiyatlarni taqdim etadi. Ushbu plaginlar Audit, Grep, Discovery, hujum Mangle, Brute force va Output[21, 20] ga bo'linadi.

Wapiti bepul ochiq kodli veb-ilovaning zaiflik skaneri, u o'zi bilan komandalar interface yordamida ish ko'ra oladigan skaner hissoblanadi. U veb ilovalarini barcha sahifalari bo'ylab zaifliklarini qidiradi va skript zaif ekanligini aniqlash uchun foydali yuklamalarni saytga kiritish uchun ishlatilishi mumkin bo'lgan shakllar va skriptlarni qidiradi va saytga yuklab ko'radi[18]. Wapiti-ning umumiy xususiyatlari orasida skanerlash jarayoniga taluqli matn faylidagi oddiy qator, topilgan zaifliklarning

jiddiyligini farqlash uchun turli usullardagi kodlash va ko'p formatli hisobotlarni yaratishda keng foydalaniladi.

Watabo veb ilovalarni tekshirish uchun ochiq manbali yarim avtomatik skanerdir. Ushbu ruby-ga asoslangan skaner seans boshqaruviga ega, murakkab filtrlash va shaffof proksi-server sifatida ishlash qobiliyatini o'z ichiga oladi.

Turli veb-zaiflik skanerlarining samaradorligi avvalroq baholangan. Biroq, OWASP Benchmark asosidagi OWASP Zed Attack Proxy (ZAP) va Arachni ni o'zaro solishtirish hali amalga oshirilmagan.OWASP benchmarkidan foydalangan holda, ushbu tadqiqot ikkita ochiq manbali va platformalararo skanerlarning samaradorligini taqqoslaydi. Bunda skanerlar yaratilishi funksiyalarga boyligidan qat'i nazar, barcha turdagi testerlar va ishlab chiquvchilarga murojaat qiladi, chunki ulardan foydalanish oson. Natijada, skanerlarning keng doirasi foydalanilishi va xavfsizroq onlayn ilovalar ishlab chiqilishi imkoniyati paydo bo'ladi.

Veb ilovalar zaifliklarini aniqlashning testlash usullari va OWASP texnologiyasi

Hozirgi kunda veb ilovalarning zaifliklarini aniqlash skanerlarida uchta asosiy komponent mavjud. Crawling, fuzzing va scraping bunga misoldir. Dasturchilar va ilovalarni sinovdan o'tkazuvchilar ixtiyorida dastur muammolarini ishga tushirishdan oldin yoki keyin aniqlash uchun bir qator texnologiyalar mavjud. SIXT - Statik ilovalar xavfsizligi testi (SAST- Static Application Security Testing), DIXT - dinamik ilovalar xavfsizligi testi (DAST- Dynamic Application Security Testing) va IIXT - interaktiv ilovalar xavfsizligi testi (IAST- Interactive Application Security Testing) bunga misoldir (IAST).

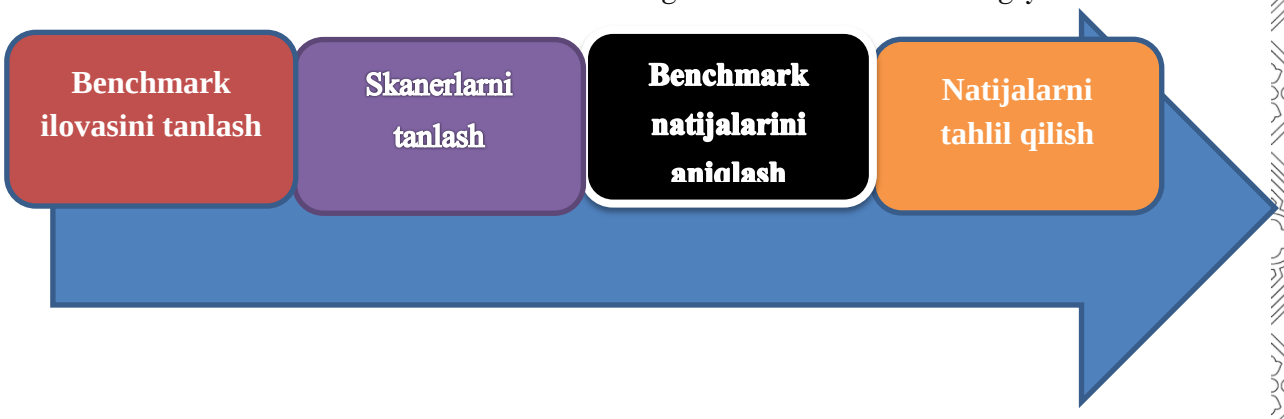
Statik ilovalar xavfsizligi testi (SIXT): faqat inson omili orqali amalga oshirilib dasturning manba kodidagi xatolarni topish uchun kodni tahlil qilish vositasi yordamida amalga oshirilishi mumkin bo'lgan kodga asoslangan veb-ilova sinovidir, buni "Oq quti testi"("White box testing") deb ham atash mumkin.[6]. Biroq, manba kodini tahlil qilish usuli bilan, ayniqsa murakkab dastur kodlari bilan barcha xavfsizlik kamchiliklarini topish qiyin. Bundan tashqari, testlovchi tomonidan ilovaning ichki tuzilishi, dizayni va texnologiyasini bilish ilovadagi kamchiliklarni topishga to'sqinlik qilishi mumkin.

Dinamik ilovalar xavfsizligi testi (DIXT): veb resursning tuzilishi, dizayni va texnologiyasi haqida oldindan ma'lumotga ega bo'lmagan holda dastur zaifliklarini topish jarayoni. Ushbu usul, shuningdek, "Qora quti testi"("Black box testing") va Penetratsiya testi deb nomlanadi. Veb-so'rovlarni o'chirish, qirqish va skanerlash maqsadli ilovalardagi zaifliklarni topish uchun ushbu usulda qo'llaniladigan ba'zi usullardir [7].

Ularning xususiyatlarini hisobga oladigan bo'lsak, statik ilovalar xavfsizligi testi va dinamik dastur xavfsizligi testi usullari ba'zi zaif va kuchli tomonlarga ega. SIXT DIXTga nisbatan boshqacha yondashuvdan foydalanishi aniq bo'lsa-da, ikkala usul ham bir-birini to'ldiradi.

Tadqiqotlar shuni ko'rsatdiki, DIXT usuli Cross Site Scripting (XSS) zaifliklarini aniqlashda yaxshi ishlashi mumkin, chunki SIXT usulida oddiy aks ettirish o'rniga mijoz tomonidan bajarish (skanerlash) qobiliyati. Shunga qaramay, DIXT usuli log fayliga aniq matn ko'rinishida kiritilgan parol bilan bog'liq zaifliklarni aniqlashda unchalik muvaffaqiyatli emasligi ta'kidlanadi [8], holbuki bu turdagi zaiflikni SIXT usuli bilan yaxshi boshqarish mumkin. [9]. Noto'g'riligiga qaramay, SIXT veb ilovalarini ishlab chiquvchilar tomonidan afzal ko'riladi, chunki u ishlab chiquvchilar guruhiga kodga kerakli o'zgartirishlar kiritish imkonini beradi, chunki kamchiliklar kontseptual darajada aniqlanadi, shu bilan birga loyiha oxirida nuqson aniqlanganda yuzaga kelishi mumkin bo'lgan xarajatlarni kamaytiradi [10].

Veb ilovalar zaiflik skanerlari samaradorligini baholash metodologiyasi



1-rasm Veb zaiflik skanerlarini samaradorligini baholash

Veb-zaiflik skanerlari samaradorligini baholash metodologiyasini ushbu ilmiy tadqiqot davomida bir necha bosqichlarga bo'lish orqali amalga oshiril-di.Ushbu ketma-ketlik quyida rasmda berilgan bo'lib unda asosiy tanlangan veb-zaiflik skanerlarini baholash uchun tegishli usulni tanlash asosiy qismdir. Maqbul usul jarayoni quyidagi rasmda ko'rsatilgan: yani Veb-zaiflik skanerlari samaradorligini baholash metodologiyasi asosiy to'rt qismdan iborat bo'lib unda birinchi navbatda benchmark ilovasini tanlash skanerni tanlash Benchmark natijalarini aniqlash natijalarni tahlil qilish bosqichlaridan iborat.

Benchmark ilovasini tanlash. Benchmark ilovasini tanlash orqali veb ilovlarini zaiflik skanerlarini OWASP mezoni asosida ishga tushuriladi, so'ngra skanerlar olingan natijalar XML fayl ga yoziladi ushbu XML fayl skanerlarni o'zida yeg'uvchi natijalar kartasini shakllantrish uchun ishlailadi. Ushbu olingan natijalar asosida veb ilovalarini zaifliklarini aniqlash skanerlarini baholashda foydalaniladi.

Skanerni tanlash. Ko'pgina oldingi tadqiqotlar tijorat va bepul (ochiq kodli) skanerlarni taqqoslagan bo'lsa-da, bu tadqiqot Arachni va OWASP ZAP, ikkita bepul ochiq kodli skanerlarga qaratilgan. Sinov jarayoni o'zaro tarmoq hozil qiluvchi ikkita kompyuterdan iborat bo'lgan bo'lib, ularning biri hujum qilish uchun ikkinchisi hujumlardan himoya qiluvchi qurbon(victim) dan iborat. Benchmarkingni amalga oshirish uchun OWASP Benchmark, OWASP ZAP va Arachni o'rnatishni barcha

tegishli ilovalar talab qiladi.Chunki, ushbu dasturlar ilmiy tadqiqot davomida o'rganib chiqildi va dasturni tekshirib uning ko'plab funktsiyalari aniqlandi.

Benchmarkni natijalari. Veb ilovlar zaifliklarini aniqlovchi skanerlar OWASP mezoni asosida ishga tushurilgandan so'ng, skanerlardan olingan natijalar XML fayl ga yoziladi ushbu XML fayl skanerlarni o'zida yeg'uvchi natijalar kartasini shakllantrish uchun ishlailadi. Ushbu olingan natijalar asosida veb ilovalarini zaifliklarini aniqlash skanerlarini baholashda foydalaniladi.

Veb ilovalarining zaiflik skanerlarini samaradorligini baholashning meyoriy xuquqiy asoslari

Veb ilovalarining zaifliklarini aniqlashdagi meyoriy xuquqiy asoslar quyidagilardan iborat:

1. Tomonlar(Veb ilovalarini sinovdan o'tkazuvchi tashkilot sinovni amalga oshirtrishga talabgor tashkilotlar) o'rtasidakelishuv bitmiga roziligini bildiruvchi meyoriy xuquqiy hujjatlarni tayyorlaniladi.
2. Veb ilovalarini sinovdan o'tkazuvchi tashkilot sinovni amalga oshirish davomida ushbu sinovni amalga oshirishga talabgor tashkilotga tegishli malum turdagi manbalarni yo'qotilishiga javobgarlikni o'z zinmasidan soqit qiladi.
3. Sinovdan o'tkazilayotgan veb ilovasi mavjud parollar va user informatsiyalari veb ilovalarini sinovdan o'tkazilayotgan tashkilot tomonidan sir saqlash kelishuvi asosida ish olib boriladi.
4. Veb ilovalarini sinovdan o'tkazuvchi tashkilot sinovni amalga oshirish davomida topilgan zaifliklarni e'lon qilmaslik va tarqatmaslik javobgarligini o'z zinmasiga oladi.

FOYDALANILGAN ADABIYOTLAR:

1. O'zbekiston Respublikasi Prezidentining Farmoni, 2022 — 2026-yillarga mo'ljallangan yangi O'zbekistonning taraqqiyot strategiyasi to'g'risida. 2022-yil.
2. Core_Security. (2018). What is Penetration Testing Available: https://www.coresecurity.com/content/penetration-testing
3. T.Laskos. (2017). Arachni Apllication Security Scanner Framework.
4. INFOSEC_Institute. (2016). The History of Penetration Testing.
5. OWASP. (2016). Fuzzing. Available: https://www.owasp.org/index.php/Fuzzing
6. Z. T. Watson_ C., "Automated-threat-handbook," 2016.
7. A. C. Barus, D. I. P. Hutasoit, J. H. Siringoringo, and Y. A. Siahaan, "White box testing tool prototype development," in 2015 International Conference on Electrical Engineering and Informatics (ICEEI), 2015, pp. 417-422.
8. S. Xu, L. Chen, C. Wang, va O. Rud, "A comparative study on black-box testing with open source applications," 2016 IEEE/ACIS International Conference on

Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), 2016, pp. 527-532.

9. Information Security Stack Exchange. (2017). Effectiveness of Interactive Application Security Testing.

10.P. E. Black, "Static Analyzers in Software Engineering.pdf," National Institute of Standards and Technology2009.

11.Skoussa. (2018, January). What do SAST, DAST, IAST and RASP mean to developers.

12.Y. Wang and J. Yang, "Ethical hacking and network defense: Choose your best network vulnerability scanning tool," in Proceedings - 31st IEEE International Conference on Advanced Information Networking and Applications Workshops, WAINA 2017, 2017, pp. 110-113.

13.OWASP. (2017). OWASP Top Ten Project. Available: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#tab=OWASP_Top_1 0_for_2017_Release_Candidate_1

14.OWASP. (2016). Cross Site Scripting. London

15.PortSwigger_Ltd. (2018, 2018). SQL injection.

16.R. K., "A benchmark approach to analyse the security of web frameworks," Master, Computer Science, Radboud University Nijmegen, Nijmegen, Netherlands, 2014.

17.Infosec_Institute. (2018). File-Inclusion Attack.

18.M. El, E. McMahon, S. Samtani, M. Patton, and H. Chen, "Benchmarking vulnerability scanners: An experiment on SCADA devices and scientific instruments," in 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), 2017, pp. 83-88.

19.PENTESTGEEK. (2018). WHAT IS BURP SUITE. Link: https://www.pentestgeek.com/what- is-burpsuite