ӘОК 004.056+332.1

«АҚЫЛДЫ КӨЛІК» БАҒДАРЛАМАЛЫҚ КЕШЕНІН ІСКЕ АСЫРУДА ҚОЛДАНЫЛАТЫН ҚАЗІРГІЗАМАНҒЫ WEB-ТЕХНОЛОГИЯЛАРДЫҢ ҚАУІПСІЗДІГІН ЗЕРТТЕУ

Нұрғалиқызы Маржан
nurgalikyzy_m@mail.ru
Л. Н. Гумилев атындағы Еуразия ұлттық университеті. Ақпараттық технологиялар факультетінің 1 курс магистранты,Нұр-Сұлтан, Қазақстан
Ғылыми жетекшісі – Қонырханова Асем Адильбекқызы

Аңдатпа: Қазіргі таңда ақпарат әлемі күн санап қарқынды дамып келеді. Дамыған заманда күн сайын жаңа қолданбалар, веб-технологиялар, веб-сайттар, программалық қамтамасыз ету пайда болды. Түрлі ағымдағы веб-қолданбалар - клиенттер мен бизнесті және әртүрлі әкімшіліктерді әртүрлі клиенттерге жіберетін толығымен пайдалы платформа құрылымдары деп те түсінсек болады. Веб сонымен қатар корпоративтік веб-сайттың интернет желісін жақсартуды талап етеді. Аталған құралдар қазіргі кезде нарықта көп болғанымен олардың қаншалықты тиімді екендігін зерттеу, веб-қосымшалардағы қауіпсіздік мәселелерін анықтау өзекті болып отыр. Осыған сәйкес оларға келетін осалдықтар, қауіп түрлерін алдын алу сынды қажетті шараларды іске асыру туындауда. Атап өткендей, көптеген ұйымдарда веб-технологияларды қорғау схемасының қандай да бір түрі немесе оны құру, дамыту әрекеті болғанменен де тиімді генерациялауға қабілетсіз болып жатады. Сондықтан да бұл мақала көптеген қауіпсіздік қатерлері мен шабуылдарына әкелген веб-қосымшалардың маңыздылығын және олардың айналамызда таралуын көрсететін негізгі ақпаратты көрсетуге және веб-технологиялардың қауіпсіздік мәселелерін шешуге, веб-қосымшалардың қауіпсіздіксканерлеу құралдарына жүгінуге бағытталған.

Түйінді сөздер: веб-технологиялар, қауіптер, шабуылдар, веб осалдық сканерлдері,

бағалау, осалдықтар

Кіріспе

Әр жыл сайын веб-негізделген қолданбалар, бүкіл әлемде веб-қосымшалар саны бойынша цифрлар бомаса да, 2020 жылы шамамен 367 миллион домендік атаулар болды. Мысалы, кәсіпорындар өндірісті, капиталды, нұсқауларды және үкіметті үнемдеу үшін операцияларын күшейту және ұлғайту үшін веб-негізделген бағдарламалық жасақтаманы пайдаланады. Атап айтқанда, веб-сайт жарнама берушілерге олардың веб-сайттарына кіретін адамдармен танысуға және байланысуға мүмкіндік береді. Қазіргі заманда онлайн технологиялар маңызды рөлге ие бола отырып, қолданыстағы шешімдерді жаңарту арқылы әдеттегі күнделікті тапсырмаларды автоматтандыруды жүзеге асыруда.

Зерттеу екі негізгі бөлімге бөлінген. Бірінші бөлімде біз веб-қосымшалардың құпиялылығы мен қауіпсіздігіне кепілдік беру үшін енгізілуі тиіс бірқатар қағидаларды қарастырамыз. Екінші бөлімде веб-қосымшалардағы қауіпсіздік қатерлерін талқылаймыз және осындай қауіптерді азайту үшін қауіпсіздік ұсыныстарын көрсетеміз.

Веб-қосымшалардың қауіпсіздігі

Веб-қосымшаларға арналған қауіпсіздік сынақтары қолданбаның қауіпсіз орындалуын тексеру әдісі болып табылады, яғни сол арқылы ақауларды анықтауға, олардың шабуылға ұшырауына қарсы тұрады. Нәтижесінде веб-қосымшалардың қауіпсіздігін жақсарту мақсатында бірнеше қауымдастықтар пайда болды. Осы қауымдастықтардың ішінде біз OWASP (Ашық веб-бағдарлама қауіпсіздігі жобасы) және WASC (веб-қауіпсіздік консорциумы қолданбасы) сайттарын орналастыра аламыз. WASC классификациясы(Wasc қауіптерін жіктеу) бойынша веб-қосымшалардың қауіпсіздігі 49 қауіптерді жіктеуді ұсынады және оны алты санатқа топтастыруға болады: Аутентификация жеткіліксіз, авторизация жеткіліксіз, клиенттік шабуылдар, пәрменді орындау, ақпараттың ағып кетуі және логикалық шабуыл OWASP классификациясы Барлық ықтимал шабуылдарды сипаттайтын WASC-тен айырмашылығы, Open Web Application Security Project (OWASP) әрбір 3 жыл сайын тек 10 қауіпсіздік тәуекелін қарастырады және веб-қосымшаны ең маңызды қауіптерден қорғауға назар аударуға мүмкіндік береді. Веб-қосымшалардағы алғашқы он осалдықтар тізімі: инъекция, бұзылған аутентификация және сеансты басқару, сайтаралық сценарий (XSS), қауіпсіз тікелей нысан сілтемелері, қауіпсіздік конфигурациясы қате, сезімтал деректер экспозициясы, функция деңгейіндегі қатынасты басқарудың жоқтығы, сайтаралық сұрауды жалған жасау (CSRF), белгілі осалдықтары бар құрамдастарды пайдалану, тексерілмеген қайтабағыттаулар.

Веб-қосымшалардағы қауіпсіздік қатерлері

Біздің зерттеуіміздің осы бөлімінде біз веб-қосымшалар ұшырауы мүмкін ең қауіпті шабуылдар мен осалдықтарды қарастырамыз.

Кесте 1.Веб-қосымшалардағы шабуылдар мен осалдықтар

№	Шабуыл	Жылы	Тәсілдер
1	Buffer Overflow	2019	Буфердің толып кетуі шабуылдаушы бағдарламамен немесе ақпарат өңделгеніне қарамастан көбірек деректерді әдейі беруге тырысқанда пайда болады мұндай шабуыл жүйенің бұзылуына әкелу ықтималдығы басым.
2	Security Misconfiguration	2020	Конфигурацияның бұзылуына байланысты қауіпсіздік мәселесі құрылғының бір немесе бірнеше компоненттері, соның ішінде жүйелер, жақтаулар, қосымшалар серверлері, веб-сервер дұрыс жобаланбаған кезде пайда болады. ДБ сервері, желілік маршрутизатор және платформада қауіпсіз конфигурацияларды анықтап оларды орындаңыз және оларды басқарыңыз.

3	Sensitive Data Exposure	2020	Құпия деректерге пайдаланушы аттары, несие картасының деректері, парольдер және т.б. бағдарлама қауіпсіздігінде қате пайда болғаннан кейін анықталады. Шабуылшы бұл деректерді аша алады және 3 шабуыл нүктесі бар. Біріншісі-ақпараттың ағып кетуімен шабуыл. Екіншісі-шабуылды беру. Үшіншісі-мәліметтер базасын ұрлау.
4	Cross-Site Request Forgery (CSRF).	2021	Бұл белгілі веб-шабуылдар, пайдаланушыны қазіргі уақытта осал веб-қосымшаға негізсіз, шабуылға негізделген HTTP сұрауларын жіберуге шақырады. CSRF-тің негізгі қағидасы-зиянды сұраулар пайдаланушының браузері арқылы веб-қосымшаға жіберіледі, сондықтан пайдаланушының күткен сұраныстарынан өзгеше болмайды.

2020 жылы зерттеушілер веб-қосымшаларға, соның ішінде файлдарды қашықтан біріктіруге ықпал ететін барлық әлсіз жақтарды атап өтті және зерттеушілер қауіпсіздіктің бұзылуына әкелуі мүмкін веб-қосымшаларда көптеген қауіпсіздік осалдықтарын және ену тестілеуін (VAPT) анықтау үшін ашық бастапқы бағдарламалық жасақтаманы қолданды. Қауіпсіздік бұзушылықтары анықталды. VAPT қауіпсіздік тестілеу құралдары қауіпсіздік бұзушылықтарын болдырмау үшін веб-қосымшаларды қорғау үшін өте пайдалы болмақ. 2020 жылы SNEAKERS-ті анықтау ұсынылды. Хакерлер компания туралы ақпаратқа және олар іздеген ақпаратқа қалаусыз қол жеткізе алмайтындай идеялар ұсынылатын осалдықтар бұл құрал веб-осалдықтарды анықтайды және веб-әкімшілендіру, бағалау және веб-осалдықтарды сканерлеу шешімін ұсынады.

Веб-бағдарламаның осалдықтары сканерлерінің архитектурасы.

Веб-қосымша сканерлері үш негізгі модульден тұрады: тексеріп шығушы модулі, шабуылдаушы модулі және талдау модулі

Crawling Crawler модулі:

Бұл компонент веб-беттерді, HTML пішіндерінің енгізу өрістері, GET және POST сұрау параметрлері және cookie файлдары сияқты байланысты енгізу векторларын қалпына келтіру және анықтау үшін веб-қосымшаны зерттейді. Сонымен қатар, тексеріп шығушы барлық тексерілген беттердің индекстелген тізімін жасайды. Веб осалдықтарының бар-жоғын анықтау негізінен Crawler сапасына байланысты болып келеді.Егер тексеріп шығу құралы орташа болса, сканерлер осалдықты жіберіп алады деген сөз.

Шабуыл жасаушы (fuzzing):

Бұлдырлау fuzzer деп аталатын құрамдас арқылы жасалады, ол беттердің URL мекенжайларын және бірінші құрамдас тексеріп сосын шыққан кіріс векторларын талдайды, содан кейін алдыңғы қадамда анықталған кіру нүктелеріне ықтимал шабуыл үлгілерін жібереді. Бұл компонент веб-бағдарламаның осалдық сканері тексеретін әрбір жазба және осалдықты іске қосу үшін ықтимал осал мәндерді жасайды; мысалы, XSS осалдығы бар-жоғынтексеру үшін фузер Javascript зиянды кодын енгізуге тырысады.

Талдау модулі:

Бұл модуль fuzzing кезеңінде алынған нәтижелерді, осалдықтардың бар-жоғын анықтау үшін талдауды қарастырады. Егер SQL инъекциясына арналған енгізу сынақтарына жауап ретінде қайтарылған беттер дерекқор қатесі туралы хабарды қамтыса, талдау модулі SQL осалдығы бар екенін анықтайды.

Қорытынды

Веб-қолданбалар қазір біздің өмірімізде аса маңызды рөлді атқарып жатыр. Өйткені біз күн сайын Интернетке қосылған бірнеше веб-қосымшалармен байланысамыз. Зерттеу аясында веб-қосымшаларды қорғауды қарастырдық және жұмыс процесінде олардың қауіпсіздігінде веб-қосымшаларға және олардың тұтынушыларына зиян келтіретін ең зиянды қауіптер мен қауіпсіздік кемшіліктерін қарастырдық. Сонымен қатар веб-

қосымшалардың қауіпсіздігіне баламаларды және зерттеушілердің болашағын қамтитын көптеген зерттеулердің талдауын қарастырдық.

Қолданылған әдебиеттер тізімі

1. R. Jnena, 2013 "Modern Approach for WEB Applications Vulnerability Analysis,"Mohanty, S., Acharya, A. A., Mishra, D. B., & Panda, N. (2019).
2. Security Testing of Web Applications UsingThreat Modeling: A Systematic Review. IJCSMC International Journal of Computer Science and Mobile Computing, 8(1), 50-57
3. Wibowo, R. M., & Sulaksono, A. (2021). Web Vulnerability Through Cross Site Scripting (XSS) Detection with OWASP Security Shepherd. Indonesian Journal of Information Systems, 3(2), 149-159.
4. Awad, M., Ali, M., Takruri, M., & Ismail, S. (2019). Security vulnerabilities related to web-based data. Telkomnika, 17(2), 852- 856.
5. Fredj, O. B., Krichen, M., Hamam, H., & Derhab, A. (2020). An OWASP Top Ten Driven Survey on Web Application Protection Methods.
6. Malekar, V., & Ghode, S. A Review on Vulnerability Assessment and Penetration Testing Open Source Tools for Web Application Security.
7. Darus, M. Y., Omar, M. A., Mohamad, M. F., Seman, Z., & Awang, N. (2020). Web vulnerability assessment tool for content management system. International Journal, 9(1.3).
8. F. Kagorora, J. Li, D. Hanyurwimfura, and L. Camara, 2015 "Effectiveness of Web Application Security Scanners at Detecting Vulnerabilities behind AJAX / JSON,"
9. A. Doupé, M. Cova, and G. Vigna, 2010 "Why Johnny Can’t Pentest: An Analysis of Black-Web Vulnerability Scanners," Proc. 7th Int. Conf. on Detection of Intrusions and Malware, and Vulnerability Assessment, pp. 111-131.