Жолтай А.Қ., студент
Абилдаева Г.Б., аға оқытушы
Ә. Сағынов атындағы Қарағанды техникалық университеті

ПАЙДАЛАНУШЫ ДЕРЕКТЕРІНІҢ ҚАУІПСІЗДІГІН ҚАМТАМАСЫЗ ЕТУ ҮШІН ВЕБ-ҚОСЫМШАЛАРҒА КӨП ФАКТОРЛЫ АУТЕНТИФИКАЦИЯ МЕХАНИЗМДЕРІН БІРІКТІРУ

Зерттелетін жобаның өзектілігі: Қазірде интернет, ақпараттық жүйелер дамыған сайын, ақпаратты алу, беру, қолдану, өңдеу өте тез, әрі оңай. Бұл бір жағынан өте жақсы, бірақ кейбір адамдар мұны басқа жағынан да қолданады. Яғни, адамның жеке деректерін деректер базасынан хаккерлік жолмен алып жатады. Ал көп факторлы аутентификация (MFA) жүйеге немесе ресурстарға бірден қол жеткізбес үшін пайдаланушының жеке басын растау үшін екі немесе одан да көп факторларды қамтамасыз етуді талап ететін қауіпсіздік әдісі болып табылады. Бұл тәсіл аутентификация факторларының бірі бұзылған жағдайда да рұқсатсыз қол жеткізу мүмкіндігін азайта отырып, қосымша қорғаныс қабатын қамтамасыз етеді.

Веб-қосымшалар контекстінде көп факторлы аутентификацияны қолдану қажеттілігі желідегі қауіпсіздік қаупінің артуына байланысты. Тек құпия сөзді пайдалану сияқты дәстүрлі аутентификация әдістері фишинг - деректердің бұзылуы сияқты әртүрлі шабуылдарға осал болды. Нәтижесінде, есептік жазбаларды бұзу веб-қосымшаларды пайдаланушылар алдында тұрған негізгі мәселелердің біріне айналды. Бұл мәселенің шешімдерінің бірі-аутентификация процесіне қосымша қауіпсіздік деңгейлерін қосатын көп факторлы аутентификацияны енгізу. Бұл қолданбаға кіруге тырысатын пайдаланушының шынымен кім екенін көруге мүмкіндік береді.

Жобаның мақсаты көп факторлы аутентификацияны енгізу арқылы веб-қосымшалардың қауіпсіздігін жақсарту болып табылады, бұл пайдаланушы деректерін рұқсатсыз кіруден және шабуылдардан қорғауды арттырады. Және де жасаған веб- қосымшаға аутентификацияны енгізіп, пайдаланушылардың деректерін

қауіпсіздікте ұстау. Жаңалығы- бұл көп факторлы аутентификацияның әртүрлі әдістерін біріктіру арқылы веб-қосымшалардың қауіпсіздігін қамтамасыз етудің кешенді тәсілі. Бұл қауіпсіздіктің жоғары деңгейін ғана емес, сонымен қатар аутентификация процесін пайдаланушылар үшін ыңғайлы және икемді етуге мүмкіндік береді.

Жобаның міндеттері: көп факторлы аутентификацияның қолданыстағы әдістері мен технологияларын зерттеу; ағымдағы веб-қосымшалардың қауіпсіздік талаптары мен осалдықтарын талдау; веб-бағдарлама үшін ең қолайлы MFA әдістерін таңдау; таңдалған әдістерге негізделген аутентификация логикасын әзірлеу және біріктіру; пайдаланушыларға аутентификацияның жаңа әдістерін және олардың деректер қауіпсіздігі үшін маңыздылығын үйрету; веб-қосымшада көп факторлы аутентификацияны енгізудің тиімділігі мен нәтижелерін бағалау. Бұл көп факторлы аутентификацияны веб-қосымшалардың, әсіресе пайдаланушылардың жеке деректерін сақтайтын және өңдейтін қауіпсіздік стратегиясының ажырамас бөлігі.

Жобаны зерттеу әдістері: аутентификация түрлеріне байланысты материалдар жинақтау, көп факторлы аутентификация түрлерінің артықшылықтары мен кемшіліктерін зерттеу, веб- қосымшалардағы аутентификацияларды талдау, платформа құрып, оған аутентификация енгізу.

Зерттеудің теориялық негіздері:

- Ғылыми мақалалар;
- Интернеттегі жазбалар;
- Аутентификациясы бар веб- қосымшалар;

Жұмыстың теориялық және практикалық маңыздылығы

Аутентификация түрлерін талдай отырып, веб- қосымшаға арналған тиімді аутентификация әдісін таңдап, оны қосымшаға орнату. Жеке бас деректерін қауіпсіздікте ұстауды барлық пайдаланушы отыратын веб- қосымшаларда орнықтырудың маңызын көрсету.

1. Көп факторлы аутентификация. Қауіпсіздік қатерлері және MFA қажеттілігі. MFA негізгі әдістері мен технологияларын, олардың артықшылықтарын, кемшіліктерін және веб-қосымшалар контекстінде қолданылуын толығырақ қарастырайық:

1. SMS-кодтар: пайдаланушыға SMS арқылы бір реттік аутентификация коды жіберіледі, оны жеке басын растау үшін енгізу керек; пайдалану оңай, ұялы телефондардың кең таралуы. Бірақ SMS-ті беріп қою осалдығы, хабарламаларды жеткізудің кешігуі, ұялы телефон мен байланыс желісінің болуына тәуелділік.

2. Аутентификаторлар: пайдаланушы мобильді құрылғыда бір реттік құпия сөздерді немесе аутентификация кодтарын жасау үшін қолданбаны пайдаланады. SMS кодтарына қарағанда қауіпсіз әдіс, байланыс желісіне тәуелділіктің болмауы, желіден тыс пайдалану мүмкіндігі. Бірақ қосымшаны орнату қажеттілігі, мобильді құрылғының қол жетімділігіне қатысты мәселелер туындайды. Веб-қосымшаларға қол жетімділіктің қауіпсіздігін қамтамасыз ету үшін тиімді, әсіресе жоғары қорғаныс қажет болған жағдайда.

3. Биометриялық сәйкестендіру: пайдаланушының саусақ ізі, бетті немесе дауысты тану сияқты бірегей физиологиялық немесе мінез-құлық сипаттамаларын пайдалану. Қауіпсіздіктің жоғары деңгейі, есте сақтаудың немесе қосымша құрылғыларды киюдің қажеті жоқ. Техникалық шектеулер (мысалы, жүйені алдау мүмкіндігі), дәлдік пен тану жылдамдығында мәселелер болуы мүмкін. Пайдаланушы құрылғыларында немесе кіріктірілген веб-камераларда арнайы сенсорларды қолдайтын веб-қосымшаларда ғана қолдануға болады.

2. Веб-қосымшаларда MFA қолдану.

Көп факторлы аутентификацияны (MFA) веб-қосымшаларға біріктіру процесі мұқият жоспарлау мен енгізуді қажет етеді. Мұнда MFA-ны қолданыстағы немесе жаңа веб-қосымшаларға біріктіру кезінде орындалатын негізгі қадамдарды көрсетемін.

Ең бірінші қауіпсіздік талаптарын талдау. Яғни, веб-қосымшаға қажетті қауіпсіздік деңгейін анықтау және кездесетін қауіпсіздік тәуекелдерін бағалау. Пайдаланушы деректерін өңдеуге және сақтауға қатысты заңнамалық талаптар мен реттеулерді қарастыру керек.

Екінші, MFA әдістерін таңдау. MFA-ның әртүрлі әдістері мен технологияларын зерттеп, қолданба мен аудиторияға сәйкес келетінін таңдау. Пайдаланушыларға ыңғайлылықты, іске асыру және қолдау шығындарын және әр әдіс ұсынатын қауіпсіздік деңгейін ескеру қажет.

Қосымшаға MFA интеграциясы таңдалған әдістерін қолдайтын аутентификация логикасын жасау және іске асыру. SMS провайдерлері, аутентификация қолданбалары немесе биометриялық жүйелер сияқты API және MFA қызметтерін қолданбаға біріктіру керек.

Тестілеу және жөндеу: Барлық аутентификация әдістерінің дұрыс және қауіпсіз жұмыс істейтініне көз жеткізу үшін MFA интеграциясын тексереміз.Табылған мәселелерді шешіп, пайдаланушыларға арналған аутентификация процесі біркелкі және қажетсіз қиындықтарсыз өтетініне көз жеткіздік.

Пайдаланушы сеанстарын басқару: Рұқсатсыз кіруді болдырмау үшін MFA пайдалану кезінде пайдаланушы сеанстарын басқару әдістерін қарастыру керек. Белгілі бір әрекетсіздік кезеңінен кейін немесе құрылғыны немесе пайдаланушының орнын ауыстырған кезде автоматты түрде шығу функцияларын іске асырамыз.

Практикалық бөлім: Медициналық платформаға да аутентификация науқастардың жеке деректерін қауіпсіздікте сақтауда өте қажет. Және заңнамаға сәйкес адамның жеке ақпараттарын құпияда ұстау қажет. Мен жасап жатқан бұл веб-қосымшаға ыңғайлы аутентификация тәсілі деп бір реттік құпия сөзді аутентификаторды таңдадым. Себебі, адамдарға бұл ыңғайлы. Басқа тәсілдердің байланысқа және техникалық ақауларға тәуелділігін ескердім. Тіркелу жүйесі. Пайдаланушы веб- қосымшаға алғаш кіргенде өзінің қолданатын есімін және парольді ұйымдастырады. Бұл жерде қалай жазылу керектігі жөнінде сипаттамалар пайдаланушыға көмекке келеді. Парольді екі қайтара жазу арқылы адамның жүйеге кіретін құпия сөзді дұрыс жазғанын тексеру мақсатында құрылған. Кіру жүйесі. Пайдаланушы тіркелу кезінде жазған есім мен құпия сөзді жазу арқылы бірден веб- қосымшаға кіріп, қолдана береді.

Қорытынды

Веб-қосымшаларға көп факторлы аутентификацияны (MFA) енгізу деректердің қауіпсіздігін қамтамасыз етуде және рұқсатсыз кіруден қорғауда шешуші рөл атқарады. Зерттеу барысында біз MFA-ның негізгі принциптері мен түсініктерін, әртүрлі әдістер мен технологияларды және оларды веб-қосымшаларға біріктіру процесін қарастырдым.

MFA қосымша аутентификация қабаттарын қосу арқылы веб-қосымшалардың қауіпсіздігін жақсартудың тиімді құралы болып табылады. MFA-ның әртүрлі әдістерінің артықшылықтары мен кемшіліктері бар және белгілі бір әдісті таңдау қауіпсіздік пен ыңғайлылық талаптарына байланысты болуы керек. MFA-ны веб-қосымшаларға біріктіру мұқият жоспарлауды қажет етеді.

Қорытындылай келе, MFA-ны веб-қосымшаларға біріктіру деректердің қауіпсіздігі мен пайдаланушылардың мүдделерін қорғаудың маңызды қадамы болып табылады. Бұл саланы одан әрі дамыту веб-әзірлеу саласында қауіпсіздіктің жоғары деңгейін қамтамасыз ете отырып, одан да сенімді және ыңғайлы аутентификация құралдарын жасауға ықпал ететін болады.

Пайдаланылған әдебиеттер тізімі

1. Надейкина В.С, Лагуткина Т.В. Анализ способов реализации системы многофакторной аутентификации. Журнал аты: Научный результат, 2022
2. Логиновский О,Коваль М., Шинкарев А. Применение метода идеальной точки для поиска наилучшего способа аутентификации в корпоративных информационных системах. Журнал аты: Научный результат, 2022
3. https://www.anti-malware.ru/analytics/Technology_Analysis/Multi-factor-authentication-AMLive-2024
4. https://kk.internetdaybook.com/10649151-what-is-authentication

Зарлық Р., Алдаш Д., Тұрдалы Б., студенттер
Турсумбаева А.Ф., оқытушы
С.Сейфуллин атындағы Қазақ агротехникалы зерттеу университеті КеАҚ

ФИЗИКАЛЫҚ БЕЛСЕНДІЛІКТІ БАҚЫЛАУҒА АРНАЛҒАН WEB-ҚОСЫМШАНЫ ӘЗІРЛЕУ

Жобаның мақсаты:

Заманауи технологиялар пайдаланушылардың денсаулығы мен жайлылығына күтім жасауда шешуші рөл атқарады. Бұл саладағы инновациялық бағыттардың бірі-физикалық белсенділікті