Elvin Cəsarət oğlu MƏMMƏDZADƏ
Qərbi Kaspi Universiteti
E-mail: elvinmammadzade42@gmail.com

VEB TƏTBİQLƏRDƏ TƏHLÜKƏSİZ AUTENTİFİKASİYANIN TƏMİN OLUNMASINDA OLAN ÇƏTİNLİKLƏR VƏ ONLARIN ARADAN QALDIRLMASI ÜÇÜN GÖRÜLƏN TƏDBİRLƏR

Xülasə

Veb proqramlarının təhlükəsizliyi, xüsusən də autentifikasiyası mexanizmləri kibertəhlükəsizlik sahəsində zaman keçdikcə daha vacib komponentə çevrilmişdir. İnternetə əsaslanan fəaliyyətlər artmaqda davam etdikcə, təhlükəsiz və etibarlı autentifikasiya üsullarına tələbat sürətlə artır. Bu məqalə müasir veb autentifikasiya mexanizmlərini, onların həyata keçirilməsinə xas olan çətinlikləri və onların təhlükəsizliyini və istifadəsini artırmaq üçün potensial strategiyaları araşdırır.

Açar sözlər: veb tətbiqlər, autentifikasiya, veb təhlükəsizliyi, təhdid modeli, autentifikasiya mexanizmləri, çoxfaktorlu autentifikasiya, tək nöqtəli giriş, OAuth, OpenID, OTP, təhlükəsiz məlumat saxlanması

DOI: 10.54414/OQNJ4392

Giriş

Veb tətbiqlərinin yaranması biznes, sosial qarşılıqlı əlaqə, təhsil və əyləncə sahələrində rahatlıq və səmərəliliyin yeni dövrünü asanlaşdırdı. Bununla belə, bu proqramlar, ilk növbədə, həssas məlumat mübadiləsini əhatə etdikdə, müxtəlif təhlükəsizlik təhdidlərinə də meyllidir. Bu təhlükəsizlik problemlərinin əsasında istifadəçilərin şəxsiyyətlərini yoxlamaq və sistem resurslarına giriş icazəsi vermək üçün vacib olan autentifikasiya prosesi dayanır.

Veb Tətbiqlərdə Doğrulama Mexanizmləri

Şifrə əsaslı autentifikasiya: Bu, autentifikasiyanın ən məhşur və geniş istifadə olunan formasıdır. Bu, istifadəçinin unikal identifikator (istifadəçi adı və ya e-poçt) və gizli parol təqdim etməsini nəzərdə tutur. Hər yerdə olmasına baxmayaraq, parol əsaslı autentifikasiya kobud güc hücumlarına (brute-force attack), lüğət hücumlarına və fişinqə qarşı zəiflik kimi çoxsaylı çatışmazlıqlara sahibdir.

İki faktorlu autentifikasiya (2FA): İki faktorlu autentifikasiya istifadəçidən iki növ etimadnamə təqdim etməyi tələb etməklə təhlükəsizliyi artırır. Adətən, bura istifadəçinin bildiyi bir şey (parol) və onlarda olan bir şey (token və ya mobil cihazına göndərilən kod) daxildir. 2FA təhlükəsizliyi əhəmiyyətli dərəcədə yaxşılaşdırsa da, həm də bu prosesi qəlizləşdirir və istifadəçiləri narahat edə bilər.

Çox-Faktorlu autentifikasiya (MFA): MFA ikidən çox autentifikasiya faktorunu əhatə edən 2FA-nın genişləndirilməsidir. O, istifadəçinin özündə olan bir şeyi (biometriya, məsələn, barmaq izləri və ya üz tanıma) daxil etməklə təhlükəsizliyi daha da artırır. MFA-nın qarşısında duran vəzifə təhlükəsizliyin istifadəçi rahatlığı ilə balanslaşdırılmasıdır, çünki o, autentifikasiya prosesinin mürəkkəbliyini əhəmiyyətli dərəcədə artıra bilər.

Tək Nöqtəli Giriş (SSO): SSO istifadəçilərə bir dəfə autentifikasiya etməyə və çoxsaylı əlaqəli, lakin müstəqil proqram sistemlərinə giriş əldə etməyə imkan verir. SSO istifadə qabiliyyətini yaxşılaşdırsa da, hücumçular SSO etimadnaməsini keçə bilsələr, onlar SSO-ya qoşulmuş bütün sistemlərə giriş əldə etmiş olacaqlar.

OAuth və OpenID: OAuth istifadəçilərə parollar vermədən vebsaytlara və ya proqramlara digər veb-saytlardakı məlumatlarına giriş icazəsi verməyə imkan verən açıq standartdır. Digər tərəfdən, OpenID açıq standart və mərkəzləşdirilməmiş autentifikasiya protokoludur. Bu mexanizmlərin hər ikisi istifadə qabiliyyətini və təhlükəsizliyi artırır, lakin mürəkkəb icra və idarəetmə tələb edir.

Təhlükəsiz Doğrulamanın Tətbiqində Çətinliklər

Təhlükəsizliyin və istifadə imkanının balanslaşdırılması: Təhlükəsiz veb tətbiqinin

autentifikasiyası mexanizmlərinin tətbiqində ən mühüm problemlərdən biri təhlükəsizliyin istifadə imkanları ilə balanslaşdırılmasıdır. Yüksək təhlükəsizlik çox vaxt istifadəçi təcrübəsinə mane ola biləcək daha çox mürəkkəblik deməkdir. Məsələn, MFA üstün təhlükəsizlik təmin etsə də, bir çox addımlar istifadəçiləri məyus edə bilər və ona adaptasiyada çətinliyin yaranmasına səbəb ola bilər.

İstifadəçilərin məlumatlandırılması və davranışı: Hətta ən təhlükəsiz autentifikasiya mexanizmləri belə zəif parollar, etimadnamələrin paylaşılması və ya fişinq hücumlarına aldanmaq kimi as bilikli istifadəçilər hesabına pozula bilər. Buna görə də istifadəçiləri kibertəhlükəsizlik istiqamətində maarifləndirmək mühüm problemdir.

Texniki Mürəkkəblik: SSO, OAuth və OpenID kimi qabaqcıl autentifikasiya mexanizmlərinin tətbiqi texniki cəhətdən mürəkkəb ola bilər. Bu mürəkkəblik səhv konfiqurasiyalara gətirib çıxara bilər və bu, hücumçular tərəfindən istifadə edilə bilən zəiflikləri özündə daşıyır.

Gücləndirilmiş Təhlükəsizlik Strategiyaları: Bu çətinlikləri aradan qaldırmaq üçün aşağıdakı strategiyalar həyata keçirilə bilər:

Risk əsaslı doğrulama:Bu, istifadəçi və ya əməliyyatın qəbul edilən riskinə əsaslanaraq autentifikasiya tələblərinin tənzimlənməsini nəzərdə tutur. Məsələn, pul köçürmələri kimi yüksək riskli əməliyyatlar MFA tələb edə bilər, hesab məlumatlarına baxmaq kimi aşağı riskli əməliyyatlar isə yalnız parol tələb edə bilər.

İstifadəçilərin məlumatlandırılması: İstifadəçiləri təhlükəsiz autentifikasiya haqqında məlumatlandırmaq təhlükəsizliyi əhəmiyyətli dərəcədə yaxşılaşdıra bilər. Buraya istifadəçilərə güclü, unikal parollar yaratmağı öyrətmək və fişinq cəhdlərini tanımaq daxil ola bilər.

Daimi audit və yeniləmə: Audit potensial zəiflikləri müəyyən etmək, istifadəçi davranışını izləmək və müəyyən edilmiş təhlükəsizlik siyasətlərinə uyğunluğu təsdiqləmək üçün autentifikasiya sisteminin müxtəlif aspektlərinin müntəzəm olaraq tədqiqini və təhlilini əhatə edir.

Yeniləmə auditlərin nəticələri, texnologiyada irəliləyişlər, inkişaf edən təhlükə mənzərələri və təşkilatın ehtiyac və ya siyasətlərindəki dəyişikliklər əsasında autentifikasiya sistemində zəruri dəyişikliklərin və təkmilləşdirmələrin edilməsini nəzərdə tutur.

Nəticə olaraq, müntəzəm audit və yeniləmə veb tətbiqinin autentifikasiyasının təhlükəsizliyini qorumaq üçün vacib strategiyalardır. Təşkilatlar autentifikasiya sistemini müntəzəm olaraq yoxlayaraq və təkmilləşdirməklə onun möhkəm, effektiv və zamanla lazımi standartlara və qaydalara uyğun qalmasını təmin edə bilərlər.

Veb Tətbiq Doğrulamasındakı Zəifliklər

Veb tətbiqləri tez-tez autentifikasiya mexanizmlərində çoxsaylı boşluqlarla üzləşirlər, bunlardan bəziləri:

Kobud güc hücumları: Bu tip hücumda hücumçu düzgün parol tapılana qədər bütün mümkün parolları sistematik olaraq yoxlayır. Veb proqramında hesabın bloklanması və ya müəyyən sayda yanlış cəhddən sonra gecikmələr kimi qorunma yoxdursa, o, kobud güc hücumlarına qarşı xüsusilə həssas ola bilər.

Zəif parollar: İstifadəçilər tez-tez zəif, asanlıqla təxmin edilən parollar seçirlər. Bu boşluq geniş yayılmışdır və istifadəçilər güclü parol siyasətlərinə əməl etmədikdə icazəsiz girişə səbəb ola bilər.

Fişinq: Fişinq hücumunda hücumçu istifadəçiləri aldatmaq üçün etibarlı bir qurum kimi maskalanır və onların etimadnamələrini əldə etməyi hədəf alır.

Sessiyanın oğurlanması: İstifadəçi daxil olduqdan sonra veb proqram adətən kukilərdən istifadə edərək sessiyanı saxlayır. Hücumçu bu kukiləri oğurlaya bilsə (məsələn, saytlararası skript və ya ortada adam hücumları vasitəsilə), onlar istifadəçini təqlid edə bilərlər.

Etibarnamənin doldurulması: Etibarnamə doldurma hücumlarında hücumçular istifadəçi hesablarına icazəsiz giriş əldə etmək üçün oğurlanmış hesab etimadnaməsini (adətən məlumatların pozulması nəticəsində) istifadə edirlər. Bu hücum işləyir, çünki istifadəçilər tez-tez eyni parolları bir neçə hesabda təkrar istifadə edirlər.

Təhlükəsiz yaddaş: Tətbiq öz saxlanmış etimadnamələrini lazımi şəkildə qoruya bilmirsə, onlar oğurlana və icazəsiz giriş üçün istifadə edilə bilər.

Etibarlılığı Nisbətən Zəif Çox-Faktorlu Doğrulama Metodları

Çox faktorlu autentifikasiya (MFA) kimi əlavə müdafiə təbəqələri əlavə etməklə veb proqramların təhlükəsizliyi əhəmiyyətli dərəcədə artırmaq olar. Bununla belə, MFA-nın bütün üsulları eyni

dərəcədə təhlükəsiz deyil. Buna misal olaraq aşağıdakı nümunələrə baxaq:

1. SMS əsaslı Birdəfəlik Şifrələr (OTP): MFA-nın ən geniş yayılmış üsullarından biri olan bu mexanizm istifadəçinin qeydiyyatdan keçmiş mobil nömrəsinə birdəfəlik parolun göndərilməsini təmin edir. Bu üsul sadəcə paroldan əlavə təhlükəsizlik səviyyəsini təmin etsə də, onun bir neçə məlum zəifliyi var. Məsələn, hücumçu SİM dəyişdirmə, ortadakı adam hücumları və ya fişinq kimi müxtəlif üsullarla OTP-yə müdaxilə edə bilər. Həmçinin, istifadəçinin telefonu itirilsə və ya oğurlanarsa, telefona girişi olan hər kəs potensial olaraq OTP-ni əldə edə bilər.

2. E-poçt əsaslı OTP-lər və ya Linklər: MFA-nın digər ümumi üsulu istifadəçinin qeydiyyatdan keçmiş e-poçt ünvanına birdəfəlik parol və ya unikal giriş linki göndərməkdir. Burada əsas zəiflik istifadəçinin e-poçt hesabının özünün təhlükəsizliyindədir. E-poçt hesabı ələ keçirilərsə, hücumçu OTP və ya linki asanlıqla əldə edə bilər. Bundan əlavə, e-poçt rabitəsi də ələ keçirilə bilər, xüsusən də şifrələnməsə.

Bu zəifliklərə baxmayaraq, SMS və e-poçt əsaslı MFA üsulları sadəliyi və rahatlığı səbəbindən hələ də geniş istifadə olunur. Onlar istifadəçidən ayrıca proqram yükləməsini və quraşdırmasını tələb etmir və əksər istifadəçilərin artıq istifadə edə biləcəkləri mobil telefonu və e-poçt hesabı var. Bundan əlavə, bu üsulların zəifликləri olsa da, sadəcə paroldan istifadə etməklə müqayisədə onlar hələ də əhəmiyyətli dərəcədə yüksək təhlükəsizlik səviyyəsini təmin edir.

Onu da qeyd etmək lazımdır ki, MFA metodunun seçimi tez-tez təhlükəsizlik və istifadəyə yararlılıq arasında uyğunlaşmanı nəzərdə tutur. Aparat tokenləri və ya biometrika kimi yüksək təhlükəsizlik üsullarının tətbiqi və istifadəsi daha çətin ola bilər və bütün növ veb proqramlar üçün mümkün və ya zəruri olmaya bilər. Buna görə də, müxtəlif MFA metodlarının zəifliklərindən xəbərdar olmaq vacib olsa da, tətbiqin və onun istifadəçilərinin xüsusi ehtiyaclarına və kontekstinə uyğun olan metodu seçmək daha vacibdir.

Veb Tətbiqin Doğrulanması üçün Təhlükənin Modelləşdirilməsi

Təhdidlərin modelləşdirilməsi potensial təhlükələrin və zəifliklərin müəyyən edilməsini, əlaqəli risklərin qiymətləndirilməsini və müvafiq əks tədbirlərin müəyyən edilməsini əhatə edir. Tez-tez istifadə olunan təhdid modellərinə sadalananlar aiddir: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service və Elevation of Privilege mənasını verən STRIDE-dir.

Bunu veb proqram autentifikasiyası ilə təsvir edək:

Saxtakarlıq - Spoofing: Veb tətbiqinin autentifikasiyası kontekstində saxtakarlıq, etimadnamələrini oğurlamaq və ya təxmin etməklə istifadəçini təqlid edən hücumçuı cəlb edə bilər. Qarşı tədbirlərə güclü parol siyasətləri, 2FA və ya MFA daxil ola bilər.

Müdaxilə - Tampering: Hücumçu tranzit və ya istirahət zamanı identifikasiya məlumatlarına müdaxilə edə bilər. Əks tədbirlərə autentifikasiya məlumatlarının təhlükəsiz ötürülməsi (məsələn, HTTPS) və təhlükəsiz saxlanması da (məsələn, güclü şifrələmə) daxil ola bilər.

Rədd etmə - Repudiation: İstifadəçi hər hansı hərəkəti yerinə yetirdiyini inkar edə bilər. Qarşı tədbirlərə istifadəçi fəaliyyətlərinin qeydiyyatı və auditi daxil ola bilər.

Məlumatın Açığa Çıxması - Information Disclosure: Həssas autentifikasiya məlumatları arzuolunmaz formada açığa çıxa bilər. Müdafiə tədbirlərinə autentifikasiya məlumatlarının təhlükəsiz ötürülməsi və saxlanması, həmçinin saytlararası skriptinq və ya SQL inyeksiyası kimi hücumlara qarşı qorunmalar daxil ola bilər.

Xidmətdən imtina - Denial of Service: Hücumçu, məsələn, tətbiqi autentifikasiya sorğuları ilə doldurmaqla istifadəçilərin autentifikasiyasına mane ola bilər. Müdafiə tədbirlərinə sistemə müraciətlər barədə məhdudlaşdırılmaların tətbiq olunması və DoS hücumlarına qarşı digər qorunmalar daxil ola bilər.

İmtiyazın yüksəldilməsi - Elevation of Privilege: Hücumçu, məsələn, autentifikasiya sistemindəki zəiflikdən istifadə etməklə, olması lazım olduğundan daha yüksək imtiyazlar əldə edə bilər. Müdafiə tədbirlərinə ən az imtiyaz prinsipi və autentifikasiya sisteminin müntəzəm yenilənməsi daxil ola bilər.

Autentifikasiya Mexanizmlərinin Biznesə Təsiri

Doğrulama mexanizmləri bizneslərdə, xüsusən də rəqəmsal məkanda fəaliyyət göstərən müəssisələrdə mühüm rol oynayır. Onlar təşkilatın bir neçə aspektinə əhəmiyyətli təsir göstərir:

1. Təhlükəsizlik: Doğrulama mexanizmlərinin birbaşa təsiri biznesin təhlükəsizlik mövqeyinədir. Giriş icazəsi verməzdən əvvəl istifadəçilərin kimliklərini təsdiq etməklə, autentifikasiya mexanizmləri biznesin resurslarını icazəsiz girişlərdən qoruyur. MFA kimi daha güclü autentifikasiya mexanizmləri baha başa gələn və biznesin nüfuzuna xələl gətirə bilən məlumatların pozulması riskini əhəmiyyətli dərəcədə azaldır.

2. Uyğunluq: Bir çox sənayelərdə xüsusi autentifikasiya üsulları da daxil olmaqla, müəyyən təhlükəsizlik səviyyələrini tələb edən qaydalar var. Məsələn, Ödəniş Kartı Sənayesi Məlumat Təhlükəsizliyi Standartı (PCI DSS) bizneslərə kart sahibinin məlumat mühitində bütün uzaqdan giriş üçün MFA-i tətbiq etməyi tapşırır. Uyğunsuzluq cərimələrə, o cümlədən cərimələrə və kredit kartı ödənişlərini qəbul etmək qabiliyyətinin itirilməsinə səbəb ola bilər.

3. Etibar və Reputasiya: Güclü autentifikasiya mexanizmlərinin tətbiqi istifadəçi məlumatlarını qorumaq öhdəliyini doğru şəkildə tətbiq etməklə biznesin nüfuzunu artıra bilər. Bu, müştərilərin, tərəfdaşların və maraqlı tərəflərin etibarını qazanmağa kömək edə bilər ki, bu da həssas məlumatların işlənməsinin vacib olduğu sahələrdə xüsusilə dəyərlidir.

4. İstifadəçi Təcrübəsi: Güclü autentifikasiya mexanizmləri təhlükəsizliyi artırsa da, istifadəçi təcrübəsinə də təsir edə bilər. Həddindən artıq mürəkkəb və ya çətin proseslər istifadəçiləri məyus edə və ya onları xidmətdən istifadə etməkdən çəkindirə bilər. Buna görə də, müəssisələr təhlükəsizlik və istifadəyə yararlılıq arasında balans saxlamalıdırlar.

5. Əməliyyat Effektivliyi: Effektiv autentifikasiya mexanizmləri resurslara girişi asanlaşdırır, əməliyyat səmərəliliyini artırır. Məsələn, Single Sign-On (SSO) işçilərə vahid etimadnamələr dəsti ilə çoxsaylı xidmətlərə və ya proqramlara daxil olmaq imkanı verir ki, bu da daxil olmağa sərf olunan vaxtı və hər bir fərdi xidmətə girişin idarə edilməsinə sərf olunan resursları azaldır.

6. Xərc: Autentifikasiya mexanizmlərinin tətbiqi və saxlanması xərclərə də təsir edir. Bunlara ilkin quraşdırma xərcləri, davam edən texniki xidmət xərcləri, istifadəçi dəstəyi ilə bağlı xərclər (məsələn, parol sıfırlamaları) və baş verən hər hansı təhlükəsizlik insidentinin idarə edilməsi ilə bağlı xərclər daxil ola bilər. Bununla belə, güclü autentifikasiya mexanizmlərinin tətbiq edilməməsinin dəyərli məlumatların pozulmasının potensial nəticələrini nəzərə alaraq daha yüksək ola bilər.

Nəticə olaraq, autentifikasiya mexanizmləri biznesin təhlükəsizlik strategiyasının mühüm tərkib hissəsidir. Müəyyən çətinliklər və xərclərlə qarşılaşsalar da, təkmilləşdirilmiş təhlükəsizlik, uyğunluq, etibar, əməliyyat səmərəliliyi və yüksək qiymətli məlumatların pozulması riskinin azaldılması baxımından faydaları onları biznes üçün mühüm investisiya halına gətirir.

Çox-Faktorlu Autentifikasiyanın İstifadəçilərə Təsiri

Çox-Faktorlu autentifikasiyanın (MFA) veb proqramların təhlükəsizliyini əhəmiyyətli dərəcədə artırsa da, son istifadəçilərə də nəzərə çarpan təsirlərə malikdir:

1. Artan mürəkkəblik: MFA autentifikasiya prosesində əlavə addımlar tələb edir, məsələn, SMS və ya e-poçt vasitəsilə göndərilən bir OTP-yə daxil olmaq və ya biometrik autentifikasiya üçün barmaq izini və ya üzü skan etmək kimi. Bu, bəzi istifadəçiləri çaşdıra və ya giriş prosesinin mürəkkəbliyini artıraraq məyus edə bilər.

2. Potensial gecikmələr: Əlavə autentifikasiya addımları da gecikmələrlə nəticələnə bilər. Məsələn, SMS və ya e-poçt vasitəsilə OTP qəbulunda gecikmə ola bilər və ya istifadəçi biometrik skanerin qurulmasına əlavə vaxt sərf etməli ola bilər.

3. Əlavə Qurğulardan və ya Məlumatlardan Asılılıq: Bəzi MFA metodları istifadəçilərdən əlavə cihazlara və ya məlumatlara çıxışın olmasını tələb edir. Məsələn, istifadəçinin bir OTP almaq üçün mobil telefonu olmalı və ya təhlükəsizlik sualının cavabını yadda saxlamalı ola bilər.

İstifadəçi dostu MFA üçün strategiyalar

Bu çətinliklərə baxmayaraq, MFA-i daha istifadəçi dostu etmək üçün həyata keçirilə bilən bir neçə strategiya var:

1. Risk əsaslı autentifikasiya: Bu yanaşma müəyyən bir hərəkətin qəbul edilən riskinə əsasən tələb olunan autentifikasiya səviyyəsini tənzimləyir. Məsələn, hesab məlumatlarına baxmaq

yalnız parol tələb edə bilər, əməliyyat etmək isə əlavə autentifikasiya tələb edə bilər.

2. Prosesi sadələşdirin: MFA prosesi mümkün qədər sadə və sadə olmalıdır. Məsələn, OTP tələb olunarsa, o, dərhal çatdırılmalı və istifadəçilər onu asanlıqla daxil edə bilməlidirlər.

3. İstifadəçi Təhsili: İstifadəçilər MFA-in əhəmiyyəti və ondan necə səmərəli istifadə etmək barədə məlumatlandırılmalıdır. Bu, quraşdırma prosesi zamanı aydın təlimatlar, həmçinin davamlı dəstək və resursları əhatə edə bilər.

4. İstifadəçi üçün əlverişli MFA metodlarından istifadə: Mümkün olduqda, istifadəçilər üçün asan olan MFA metodlarından istifadə edin. Məsələn, biometrik autentifikasiya çox istifadəçi dostu ola bilər, çünki istifadəçidən heç nə yadda saxlamağı və ya əlavə cihaza girişi tələb etmir.

5. Etibarlı Qurğuları Yadda Saxlayın: Etibarlı cihazları xatırlamaqla, istifadəçilərdən hər dəfə daxil olanda MFA tələb olunmur, ancaq onlar və ya başqası yeni cihazdan daxil olmağa çalışdıqda.

6. Sadələşdirilmiş Bərpa Prosesi: İstifadəçilər autentifikasiya faktoruna girişi itirdikdə (telefonu itirmək və ya təhlükəsizlik suallarını unutmaq kimi) sadə və təhlükəsiz bərpa prosesini təmin edin.

Bu strategiyaları həyata keçirməklə, MFA-nı daha çox istifadəçi dostu etmək, bununla da yüksək səviyyəli təhlükəsizliyi qorumaqla, istifadəçinin qəbulunu və qəbulunu təşviq etmək mümkündür.

Nəticə

Veb tətbiqi təhlükəsizliyi sahəsində autentifikasiya mexanizmləri icazəsiz giriş və həssas məlumatların qorunmasında mühüm rol oynayır. Ənənəvi parol əsaslı sistemlərdən tutmuş çoxfaktorlu autentifikasiya və tək nöqtəli giriş kimi qabaqcıl prosedurlara qədər əhatə edən bu mexanizmlər təhlükəsizlik üstünlükləri və potensial zəifliklərin vəhdətini yaradır.

Bu autentifikasiya mexanizmləri, güclü tərəflərinə baxmayaraq, kobud güc hücumları, fişinq, sessiyanın oğurlanması və etimadnamənin doldurulması kimi kiber təhlükələrə qarşı toxunulmaz deyildir. Beləliklə, təşkilatların hərtərəfli təhdid modelləşdirməsini, müntəzəm auditi və ardıcıl sistem yeniləmələrini əhatə edən təhlükəsizliyə proaktiv yanaşmanı qəbul etməsi vacibdir.

Bundan əlavə, bu mexanizmlərin tətbiqi bizneslər üçün əhəmiyyətli nəticələrə malikdir və təkcə təhlükəsizliyə deyil, həm də sənaye standartlarına uyğunluğa, istifadəçi etibarına, əməliyyat səmərəliliyinə və istifadəçi təcrübəsinə təsir göstərir. Çətinlik möhkəm təhlükəsizlik və istifadəçi rahatlığı arasında düzgün tarazlığı saxlamaqdan ibarətdir - bu tarazlıq əldə edildikdə təhlükəsiz və istifadəçi dostu rəqəmsal mühitlə nəticələnir.

İnkişaf etdikcə, daha təhlükəsiz və effektiv autentifikasiya üsullarının axtarışının diqqət mərkəzində qalacağı aydındır. Texnologiya inkişaf etdikcə və kibertəhlükə mənzərəsi inkişaf etdikcə, veb proqramların təhlükəsizliyinə yanaşmalarımız da elə olmalıdır. Təhlükəsizliyi prioritetləşdirməyə davam etməklə, eyni zamanda son istifadəçi təcrübəsini nəzərə alaraq, müəssisələr daha təhlükəsiz və daha etibarlı rəqəmsal gələcək qura bilərlər.

ƏDƏBİYYAT SİYAHISI:

1.W. E. Burr, D. F. Dodson, and W. T. Polk. Electronic authentication guideline. In Recommendations of the National Institute of Standards and Technology, NIST SP 800-63, Version 1.0.2, April 2006.

2.W. E. Burr, D. F. Dodson, and W. T. Polk. Electronic authentication guideline. In Recommendations of the National Institute of Standards and Technology, NIST SP 800-63, Version 1.0.2, April 2006.

3.Grassi, P.A.; Fenton, J.L.; Newton, E.M.; Perlner, R.A.; Regenscheid, A.R.; Burr, W.E.; Richer, J.P.; Lefkovitz, N.B.; Danker, J.M.; Choong, Y.Y.; et al. NIST Special Publication 800-63B. Digital Identity Guidelines: Authentication and Lifecycle Management; Technical Report; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2017.

4. Gunson, N.; Marshall, D.; Morton, H.; Jack, M. User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. Comput. Secur. 2011, 30, 208–220.

5.https://blogs.sap.com/2022/04/28/frictionless-authentication-in-practice-and-benefits-for-business/

6. A new risk-based authentication management model oriented on user's experience

M Sepczuk, Z Kotulski - Computers & Security, 2018 - Elsevier

Эльвин Джасарат МАМЕДЗАДЕ
Западно-Каспийский университет
E-mail: elvinmammadzade42@gmail.com

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОЙ АУТЕНТИФИКАЦИИ В ВЕБ-ПРИЛОЖЕНИЯХ И ШАГИ, КОТОРЫЕ МОЖНО ПРЕДПРИНЯТЬ ДЛЯ ИХ ПРЕОДОЛЕНИЯ

Резюме

Безопасность веб-приложений, в частности механизмы аутентификации пользователей, становится все более важным компонентом в сфере кибербезопасности. Поскольку деятельность в Интернете продолжает расширяться, спрос на безопасные и надежные методы аутентификации резко возрос. В данной статье рассматриваются современные механизмы аутентификации в Интернете, проблемы, присущие их реализации, и потенциальные стратегии повышения их безопасности и удобства использования.

Ключевые слова: веб-приложения, аутентификация, веб-безопасность, модель угроз, механизмы аутентификации, многофакторная аутентификация, единый вход, OAuth, OpenID, одноразовый пароль, незащищенное хранилище

Elvin Jasarat MAMMADZADA
Western Caspian University
E-mail: elvinmammadzade42@gmail.com

ENSURING SECURE AUTHENTICATION IN WEB APPLICATIONS AND THE STEPS THAT CAN BE TAKEN TO OVERCOME THEM

Abstract

Web applications' security, specifically user authentication mechanisms, has become an increasingly crucial component in the cybersecurity landscape. As Internet-based activities continue to proliferate, the demand for secure and reliable authentication methods has skyrocketed. This paper explores contemporary web authentication mechanisms, the inherent challenges in implementing them, and potential strategies for enhancing their security and usability.

Keywords: web applications, authentication, web security, threat model, authentication mechanisms, multi-factor authentication, single sign-on, OAuth, OpenID, OTP, Insecure Storage

Daxil olub: 12.05.2023