**“AZƏRBAYCAN HAVA YOLLARI”**

**QAPALI SƏHMDAR CƏMİYYƏTİ**

**MİLLİ AVİASİYA AKADEMİYASİ**

**Sərbəst iş №1**

**Fakültə:** “Aerokosmik”

**İxtisas:** “İnformasiya Texnologiyaları”

**Fənn:** “Veb sistemləri və texnologiyaları”

**Mövzu:** “Veb proqram kodlarında təhlükəsizlik”

**Qrup:** 2441a

**Tələbə:** Xədicə Qurbanlı

**Müəllim:** Heydərzadə Nübar

**BAKI 2024**

Veb proqramlaşma, internet üzərində işləyən və istifadəçilərə veb tərəfindən təqdim olunan proqramların hazırlanması və inkişafıdır. Bu proses, veb səhifələri, veb tətbiqləri, veb xidmətlər və digər internet məhsullarının yaradılmasını əhatə edir.

Veb proqramlaşmanın əsas məqsədi, istifadəçilərə interaktiv təcrübə təmin etməkdir.

Şirkətlər də veb tətbiqlər vasitəsilə müştərilərlə əlaqə saxlamaq və xidmətlər təklif etmək üçün həmçinin şəxslər şəxsi və ya ticari məqsədlərlə veb səhifələr yaradaraq internetdə məzmun paylaşmaq istəyə bilərlər. Digər tərəfdən, veb tətbiqlər inkişaf etdirilərək online satış platformaları, sosial şəbəkələr və iş idarəetmə sistemləri kimi daha kompleks funksiyonlara malik veb tətbiqləri yaradıla bilər.

Veb proqramlaşdırmanın əsas alətləri HTML (HyperText Markup Language), CSS (Cascading Style Sheets) və JavaScript dilləridir.

1. HTML (HyperText Markup Language): Veb səhifələrin strukturunu təyin edən əsas dildir. Ələmentlər, məzmun bölgüsü, linklər, şəkillər və digər tərkib hissələri təyin etmək üçün istifadə olunur.
2. CSS (Cascading Style Sheets): Səhifələrin görsənimi və stilini tənzimləyən dildir. Rənglər, mənzərələr, tipografiya, bölgülər arası məsafələr, animasiyalar və responsiv düzənləmə kimi görsənən xüsusiyyətləri təyin etmək üçün istifadə olunur.
3. JavaScript: Səhifələrdə interaktivlik və dinamik funksiyaların əlavə edilməsi üçün istifadə olunan proqramlaşdırma dilidir. İstifadəçilərin tətbiqlərlə əlaqəyə keçməsi, formların doğrulanması, animasiyaların yaradılması, məlumatların yüklənməsi və s. kimi funksiyalar JavaScript ilə icra olunur.
4. CSS Frameworks: CSS çərçivələri, hazır şəkildə stil və görünüşü tənzimləmək üçün istifadə olunan qurğulardır. Məsələn, Bootstrap, Foundation, Bulma kimi CSS çərçivələri, responsiv düzənləmə, grid sistemi, naviqasiya çubuğu, düymələr və digər yararlı komponentləri təmin edir.
5. JavaScript Frameworks/Libraries: JavaScript frameworkləri və kitabxanaları, veb tətbiqlərinin inkişafını sürətləndirmək və funksiyonallığını artırmaq üçün istifadə olunur. Məsələn, React, Angular, Vue.js, jQuery kimi frameworklər və kitabxanalar, komponent bazası, məlumat idarəetmə, durğular, API əlaqələri və digər funksiyonallıqları təmin edir.

Veb proqramlaşmanın server tərəfdəki hissəsində, server tərəfində məlumatların işlənməsi, verilənlər bazasına qoşulma, iş tərəfə cavabların hazırlanması və digər server funksiyaları yerinə yetirilir. İşlədilən əsas server tərəf texnologiyaları aşağıdakılardır:

1. Server-Side Programming Languages: Server tərəfdə işlədilən proqramlaşdırma dilləri. Məsələn, Python, Ruby, Java, PHP, Node.js, C# və s. kimi dillər, server tərəfində işləyən kodun yazılması üçün istifadə olunur.
2. Veb Frameworks: Server tərəfdə tətbiqlərin yaradılması və idarə olunması üçün istifadə olunan framework və kitabxanalar. Məsələn, Django (Python üçün), Ruby on Rails (Ruby üçün), Express.js (Node.js üçün), Laravel (PHP üçün) və ASP.NET (C# üçün) kimi frameworklər, veb tətbiqlərinin inkişafını sürətləndirir və funksional təmin edir.
3. Verilənlər Bazası Sistemləri: Server tərəfdə məlumatların saxlanması və işlənməsi üçün istifadə olunan verilənlər bazası sistemləri. Məsələn, MySQL, PostgreSQL, MongoDB, Oracle Database, Microsoft SQL Server və s. kimi verilənlər bazası sistemləri, məlumatların server tərəfində saxlanılmasını və istifadəsinin tənzimlənməsini təmin edir.
4. API (Application Programming Interface): Server tərəfdən tətbiq məlumatların göndərilməsi və qəbul edilməsi üçün istifadə olunan interfeyslər. Məsələn, REST (Representational State Transfer), SOAP (Simple Object Access Protocol), GraphQL və s. kimi protokollar, məlumatların tətbiq arasında mübadiləsi üçün istifadə olunur.
5. Server Configuration and Management Tools: Server tənzimlənməsi, idarə olunması və monitorinqi üçün istifadə olunan alətlər. Məsələn, Apache, Nginx və Microsoft IIS kimi veb serverləri, serverlərin HTTP təşkilatını və digər konfiqurasiya parametrlərini tənzimləmək üçün istifadə olunur.

Veb proqramlaşma, məzmunun dinamikləşdirilməsi, interaktivlik, verilənlər bazası ilə əlaqələrin idarə olunması və təhlükəsizlik prinsiplərinin gözlənilməsi kimi bir çox fəaliyyətləri daxil edir. Təhlükəsizlik prinsiplərinin gözlənilməsi, veb proqramlaşmanın ən əhəmiyyətli aspektlərindən biridir. Bu, server tərəfindəki məlumatların müdafiə edilməsi, hücumlara qarşı qorunma tədbirlərinin gözlənilməsi və məlumatların gizliliyinin və müstəqilliyinin qorunması ilə bağlı tədbirləri əhatə edir. Bu tədbirlərə, güclü autentifikasiya və yetkiləndirmə sistemləri, verilənlər bazasının təhlükəsizliyi, kod təhlükəsizliyi, şifrələmə protokolları və digər təhlükəsizlik tədbirləri aiddir.

Kod təhlükəsizliyi, veb proqramların və tətbiqlərin qorunması üçün əhəmiyyətli bir məsələdir. Veb proqramlarının təhlükəsizliyini təmin etmək, hücumlara, məlumat oğurlanmasına, sistemə girişə və sistem səhvlərinə qarşı qoruma tədbirləri almaq deməkdir.

Veb proqramlarının kod təhlükəsizliyini nəzarət altında saxlamaq, aşağıdakı potensial təhlükələrin qarşısını almağa kömək edir:

1. XSS (Cross-Site Scripting): Veb təhlükəsizliyi ilə əlaqədar ən yayılmış təhlükələrdən biridir. XSS, istifadəçilərə məlumatları təqdim etmək üçün dinamik olaraq yaradılan veb səhifələrindəki təhlükəli kodların yerləşdirilməsi ilə həyata keçirilir. Bu təhlükəli kodlar, istifadəçilərin brauzerində işlənərək məlumatların oğurlanmasına və ya Attackernun məqsədə uyğun kodların icra edilməsinə səbəb ola bilər.

XSS hücumları üçün üç əsas tip tanınır:

1. Stored XSS: Bu növ XSS hücumunda, təhlükəli kodlar veb tətbiqin bazasında saxlanılan məlumatlar vasitəsilə qurbanın brauzerində icra edilir. Müzakirə platformaları, forumlar, şəxsi mesajlaşma səhifələri kimi istifadəçilərin məlumatları paylaşdığı veb tətbiqlər, stored XSS üçün əlverişli olabilir. İstifadəçilər tərəfindən daxil edilən məlumatlar yeterincə filtrlənmədikdən sonra təhlükəli kodlar bazaya yazılaraq, hər hansı bir istifadəçi o məlumatları oxuduqda, kodlar icra olunur.
2. Reflected XSS: Reflected XSS hücumları, Attackernun təhlükəli kodları tərəfdaşa göndərən bir link yaratması ilə həyata keçirilir. Attackernun təhlükəli kodları daxil edə biləcəyi input sahələri, axtarış məlumatları və ya URL parametrləri olabilir. Daha sonra Attackernun tərəfdaşa link göndərməsi və tərəfdaşın bu linkə klik etməsi ilə təhlükəli kodlar qurbanın brauzerində işlənərək icra edilir.
3. DOM-based XSS: Bu növ XSS hücumu, Attackernun təhlükəli kodları JavaScript-in Document Object Model (DOM) strukturunda dəyişikliklər edərək həyata keçirdiyi bir variantdır. Attackernun təhlükəli kodları brauzer tərəfindən işlədilmədən əvvəl DOM-a daxil etməsi ilə hücum həyata keçirilir. DOM-based XSS hücumları ümumilikdə JavaScript-in dinamik olaraq tərtib edilmiş səhifələrində müşahidə olunur.

*XSS hücumlarından qorunmaq üçün aşağıdakı tədbirlər tövsiyə olunur:*

* *İstifadəçi tərəfindən daxil edilən məlumatların düzgün şəkildə filtrlənməsi və təhlükəsizlik prinsiplərinə uyğun olması.*
* *Məlumatların HTML özel simvollarının doğru şəkildə qaytarılması üçün kodun doğru şəkildə yönəldilməsi.*
* *Şifrələrin uyğun şəkildə saxlanılması və qorunması.*
* *HTTP Only flag ilə işarələnmiş cookie-lər.*

1. SQL Injection: Veb tətbiqlərində yayılan bir təhlükələr növüdür. Bu tip hücum, hucümçunun istifadəçi tərəfindən daxil edilən məlumatları manipulyasiya edərək SQL ifadələrini təhrif etməsi ilə həyata keçirilir. Bu sayədə, Attacker verilənlər bazasına giriş edə bilər, məlumatları oxuya və yazmağa qadim ola bilər.

SQL Injection, bir veb tətbiqinin daxil etdiyi məlumatları doğru şəkildə tərtib etmədikdə ortaya çıxır. İnsanlar ümumilikdə veb formaları, axtarış sahələri, URL parametrləri və ya şəxsi hesab məlumatları kimi yerlərdə məlumat daxil edirlər. Ehtimal var ki, bu daxil edilən məlumatları düzgün filtrə etmək üçün etibarlı məsuliyyət daşımayan bir üsul istifadə edilir. Bu, Attackernun məlumatları manipulyasiya etmək və təhlükəli SQL ifadələrini yerləşdirmək üçün bir imkan yaradır.

SQL Injection hücumlarına uyğun olaraq, hucümçu aşağıdakı məqsədləri həyata keçirə bilər:

1. Məlumatların əldə edilməsi: SQL Injection vasitəsilə Attacker, verilənlər bazasındakı məlumatları əldə edə bilər. Bu, istifadəçi hesab məlumatları, kredit kartı məlumatları, şəxsi məlumatlar kimi gizli və əhəmiyyətli məlumatları ehtiva edən verilənlər bazasına giriş etmək deməkdir.
2. Verilənlərin silinməsi və ya dəyişdirilməsi: SQL Injection vasitəsilə Attacker, verilənlər bazasında məlumatları silə, dəyişdirə və ya manipulyasiya edə bilər. Bu, veb tətbiqinin işləməsində səhv vəziyyətlərə, qeyri-müəyyən davranışlara və istifadəçilərə zərər verməyə gətirə bilər.
3. Verilənlərin əlavə edilməsi: Attacker, SQL Injection vasitəsilə verilənlər bazasına yeni məlumatlar əlavə edə bilər. Bu, spam mesajları, zərərli kodlar və ya başqa növ zərərli məlumatların verilənlər bazasında yerləşdirilməsi deməkdir.

*SQL Injection hücumlarından qorunmaq üçün aşağıdakı tədbirlər tövsiyə olunur:*

1. *Parametrizasiya etmə: Verilənləri tədbiqin SQL ifadəsindən ayrı tutmaq üçün parametrizasiya etmək və parametrləri doğru şəkildə filtrləmək əhəmiyyətlidir.*
2. *Hazır məlumatlardan istifadə etmə: SQL ifadələrinin tərtib edilməsində hazır məlumatları (prepared statements) istifadə etmək, SQL Injection riskini azaldar.*
3. *İstifadəçi tərəfindən daxil edilən məlumatları filtrləmə:*

3. Fayl yükləmə təhlükələri: veb tətbiqlərində yayılan bir təhlükəsizlik boşluğudur. Bu təhlükə, istifadəçilərin veb tətbiqləri vasitəsilə şübhəli və potensial olaraq zərərli faylların yüklənə biləcəyi və icra edə biləcəyi bir imkan yaradır. Attacker, bu boşluqdan istifadə edərək zərərli faylları sistəmə yerləşdirə bilir, istifadəçilərin cihazlarına zarar verə bilir və sistemə çoxalmaq, istifadəçi məlumatlarını əldə etmək və ya başqa növ hücumları həyata keçirmək üçün istifadə edə bilir.

Fayl

yükləmə təhlükələri bir neçə formada gerçəkləşə bilər:

* 1. İcazəsiz fayl yükləmə: Veb tətbiqində, istifadəçilərə icazəsiz şəkildə fayl yükləmək imkanı verilmişdirsə, Attacker bu imkanı istifadə edərək zərərli fayllarını yükləyə bilərlər. Bu fayllar, zərərli kodlar, viruslar, solğun fayllar və ya kötücül hərəkətlər üçün istifadə edilə bilən digər zərərli proqramlar ola bilər.
  2. Fayl adı manipulyasiyası: Attackerlər, yüklənən faylların adlarını manipulyasiya edərək sistemə zərərli fayllar yerləşdirə bilərlər. Məsələn, bir attacker ".exe" uzantısına malik bir faylı ".jpg" kimi göstərə bilər və sistem bu faylı zərərsiz bir şəkildə qəbul edərək icra etməyə başlaya bilər.
  3. Fayl növü doğrulaması: Veb tətbiqləri ümumilikdə yüklənən faylların növünü doğrulamaq üçün bir mexanizma istifadə edir. Attackerlər bu mexanizmanı aşmaq üçün faylın uzantısını manipulyasiya edə bilərlər. Bu, bir attackerin zərərli bir faylı "jpg" olaraq göstərməsinə və sistemə yerləşdirməsinə imkan verir.

*Fayl yükləmə təhlükələrindən qorunmaq üçün aşağıdakı tədbirlər tövsiyə olunur:*

*1. Fayl yükləmə məhdudiyyətləri: Yüklənən faylların təyin edilmiş bir siyahı ilə məhdudlaşdırılması, yükləmə imkanını yalnız təhlükəsiz fayllarla məhdudlaşdırmağa imkan verir.*

*2. Fayl doğrulama: Yüklənən faylların növü, uzantısı və MIME tipi kimi məlumatların doğrulaması, yüklənən faylların etibarlılığını yoxlamağa kömək edir. Bu, zərərli faylların sistemə yerləşdirilməsinin qarşısını alır.*

*3. Fayl təhlükəsizliyi tədbirləri: Yüklənən faylların bir karantinaya alınması, zərərli faylların sistemə daxil olmasını aradan qaldırır. Yüklənən faylların antivirus proqramları və təhlükəsizlik skanerləri ilə yoxlanılması da faydalıdır.*

*4. İcazə və izləmə: İstifadəçilərə yüklənən faylların icazəsi və izləməsi verilməlidir. Böyük faylların yüklənməsi və müəyyən fayl tiplərinin yoxlanılması üçün istifadəçi icazəsini tələb etmək təhlükəsizliyə kömək edir.*

*5. Güncəlləmələr: Veb tətbiqlərinin və serverlərin güncəl olması və təhlükəsizlik yamalarının tətbiq edilməsi əhəmiyyətlidir. Bu, yayılan təhlükəsizlik boşluqlarının qarşısını almağa və fayl yükləmə təhlükələrini azaltmağa kömək edir.*

*6. İstifadəçi təlimatları: İstifadəçilərə fayl yükləmə prosesinin təhlükələri haqqında məlumat vermək və təhlükəsiz yükləmə etmələri üçün təlimat vermək əhəmiyyətlidir. Bu, istifadəçilərin potensial təhlükələrdən qorunmaq üçün daha diqqətli və bilincli olmalarına kömək edir.*

1. Sessiya identifikasiyası və autentifikasiyası: veb proqramlaşdırma sahəsində mühüm məsələlərdir. Bu məlumatlar, istifadəçilərin veb saytlara daxil olma prosesində istifadə olunur. Bu məlumatları doğru şəkildə idarə etmək və təhlükəsizlik tədbirləri almaq, veb təhlükəsizliyinin əsas hissəsidir. Sessiya identifikasiyası, istifadəçinin bir veb saytında başladığı və davam etdiyi sessiyanın unikal bir şəkildə müəyyənləşdirilməsidir. Bu, istifadəçilərin veb sayta giriş etdikdən sonra fəaliyyətlərini izləmək və durumlarını saxlamaq üçün istifadə olunan bir prosesdir. Sessiya identifikasiyası, ümumilikdə istifadəçilərə məxsus unikal bir identifier (şəxsiyyət təsdiq edici) (sessiya ID) yaratmaq üçün cookies və ya URL-lər istifadə edir.

Sessiya identifikasiyası zamanı təhlükələr yarana bilər. Bu təhlükələr aşağıdakıları əhatə edə bilər:

1. Sessiya hacking: Bu, Attackerın etibarsız bir istifadəçi kimi veb sayta daxil olmaq üçün başqalarının sessiya ID-lərini əldə etməsi deməkdir. Bu təhlükə, aşkar edilməsə, Attackerın başqasının hesabına giriş etməsi və hesabın məlumatlarına, xüsusiyyətlərə və gizlilik məlumatlarına çatmağı mümkün edə bilər.

2. Sessiya replay: Bu təhlükə, Attackerın keçmiş sessiya məlumatlarını qeyd edərək və ya yenidən göndərərək istifadəçinin hesabına giriş etməsi deməkdir.

3. Sessiya sübutunun qırılması: Bu, Attackerın sessiya ID-ləri və ya digər məlumatları təhrif edərək istifadəçinin hesabına giriş etməsinə imkan verən təhlükəli işlər nümayiş etdirir.

Autentifikasiya isə istifadəçinin özünü müəyyənləşdirmə prosesidir. Bu proses veb sayta giriş etmək üçün istifadəçinin şəxsiyyətini təsdiq etmək üçün istifadə olunan məlumatları əhatə edir. İstifadəçinin kimliyini doğrulamaq üçün parol, biometrik məlumatlar (parmak izi, yüz təsdiqi kimi), sertifikatlar və ya başqa məlumatlar istifadə oluna bilər.

Autentifikasiya zamanı təhlükələr də yarana bilər. Aşağıdakı nümunələr təhlükələrə misal verə bilər:

1. Zəif parollar: İstifadəçilər tərəfindən asan təxmin edilə bilən və ya təkrarlanan parollar istifadə etmək təhlükə yaradır. Bu, Attackerlərin parolaları aşkar etməsi və hesaba giriş etməsi üçün daha asanlaşdırır.

2. Brute force hücumları: Bu, Attackerlərin hədəf hesabının parolalarını təxmin etmək üçün avtomatik olaraq çoxlu dəfə parolaları sınamaq deməkdir. Zəif parolların istifadəsi halında Attackerlərin hesabın parolalarını təxmin etmək üçün daha az cəhdləri olacaq.

3. Fishing: Bu, Attackerlərin istifadəçiləri məşhur veb saytların, bankaların və ya digər mənbələrin kimi görünən saxta saytlara yönəldərək şəxsi məlumatlarını (parollar, kredit kartı məlumatları kimi) əldə etmək üçün hilələrə başvurmasıdır.

4. Session fixation: Bu təhlükə, Attackerın istifadəçiyə bir sessiya ID təyin etməklə (məsələn, bir URL göndərərək) və istifadəçinin bu ID ilə sayta daxil olmasını təmin edərək istifadəçinin hesabına giriş etməsini mümkün *edir.*

*Bu təhlükələrin qarşısını almaq üçün bir neçə tədbir vardır:*

* 1. *Güclü parol istifadəsi: İstifadəçilərin güclü, təkrarlanmayan və təxmin edilməsi çətin parollar seçmələri tələb olunmalıdır. Parol qarışıqlığı, uzunluq və rəqəmlər, hərflər və simvolların kombinasiyası ilə artırılmalıdır.*
  2. *İki faktorlu autentifikasiya (2FA): İstifadəçilərin hesabına giriş etmək üçün iki faktorlu autentifikasiya tələb olunmalıdır. Bu, parolun yanında əlavə bir təsdiq məlumatının (məsələn, SMS kodu, mobil tətbiqin təsdiqi kimi) tələb olunması deməkdir.*
  3. *SSL / TLS istifadəsi: SSL (Secure Sockets Layer) və ya TLS (Transport Layer Security) protokolləri, məlumatların şifrələnməsini və mənbənin təsdiq edilməsini təmin edir. Bu, məlumatların göndərilməsi və alınması zamanı təhlükəsizlik tədbirləri göstərir.*
  4. *Sessiya idarəsi: Sessiya idarəsi məsələlərində təhlükəsizlik tədbirləri ətraflı şəkildə nəzərə alınmalıdır. Güclü və təsadüfi sessiya ID-lər yaratmaq, sessiya sübutunun təmin edilməsi və sessiya məlumatlarının təhlükəsiz şəkildə saxlanılması vacibdir.*
  5. *Təcrübəli təhlükəsizlik auditi: Veb təhlükəsizliyini artırmaq üçün təhlükəsizlik auditi və penetrasion testləri, potensial təhlükələri aşkar etmək və düzəltmək üçün əhəmiyyətlidir.*

1. CSRF (Cross-Site Request Forgery): Veb-də əhəmiyyətli bir təhlükədir. Bu təhlükə, Attackerın bir istifadəçinin yetkiləndirilmiş bir veb saytda istənilən əməliyyatı icra etməsi üçün onu dolandırması və təklif etdiyi bir mənbədən istifadəçi adına tətbiq edilən tələbləri veb sayta göndərməsi ilə həyata keçirilir. CSRF hücumu zamanı, Attackerlər istifadəçiləri bir sayta daxil olmaq və saytda avtomatik olaraq bir əməliyyat yerinə yetirmək üçün hədəfə qoyur. Bu hücumların əsas məqsədi, istifadəçinin hesabında dəyişikliklər etmək, məlumatları silmək, ödənişləri icra etmək və ya başqa tələblər yerinə yetirməkdir.

CSRF hücumlarının təhlükələri aşağıdakılar kimi olur:

1. Yetkiləndirilmiş əməliyyatların icrası: Attackerlər, istifadəçinin tarayıcısında oturum açıq olduğu müddətdə, onun adına yetkiləndirilmiş bir əməliyyatı (məsələn, hesabından pul köçürmək) tələb edə bilir. Bu, istifadəçinin qeyri-ixtiyari və ya istəmədən əməliyyatlar icra etməsinə səbəb olur.
2. Hesabın ələ keçirilməsi: Attackerlər, istifadəçinin tarayıcısında oturum açıq olduğu zaman, onun adına hədəfə qoyduqları tələbləri yerinə yetirə bilər və hesabın tam kontrolunu əldə edə bilərlər. Bu, Attackerlərin istifadəçinin hesabında dəyişikliklər etməsini, məlumatları silməsini və ya hesabın tamamilə ələ keçirməsini mümkün edir.
3. Gizli məlumatların oğurlanması: CSRF hücumları, Attackerlərə istifadəçilərin gizli məlumatlarını əldə etmək imkanı verir. Ödəniş məlumatları, şəxsi məlumatlar və digər gizli məlumatlar Attackerlərin əlində olarsa, bu məlumatlar istifadəçilərin maliyyə və şəxsiyyət təhlükəsizliyini təhdid edə bilər.

*CSRF hücumlarından qorunmaq üçün aşağıdakı tədbirlər tövsiyə olunur:*

1. *CSRF token istifadəsi: Veb saytlar CSRF token adlanan və yağışlı tokenləri istifadə edərək istifadəçiləri CSRF hücumlarından qoruyurlar. Bu tokenlər, istifadəçinin tələblərini göndərərkən göndərilməlidir və hər bir tələbə istənilən əməliyyatın yalnız istifadəçinin məhsus tokeni ilə əlaqələndirilməsinə imkan verir.*
2. *SameSite cookies: SameSite cookies, brouzerə göndərilən cookies-lərin istifadəçinin sayt daxilində hər hansı bir əməliyyat yerinə yetirməsi üçün məhdudiyyətlər tətbiq edir. Bu məhdudiyyətlər, yalnız istifadəçinin doğrudan-dolayı tələbə əsaslanan əməliyyatları icra etməsinə imkan verir və istəmədən başqa saytlara tələb göndərməsinə mane olur.*