“AZƏRBAYCAN HAVA YOLLARI” QAPALI SƏHMDAR CƏMİYYƏTİ MİLLİ AVİASİYA AKADEMİYASİ

Sərbəst iş №6

Fakültə: “Aerokosmik”

İxtisas: “İnformasiya Texnologiyaları”

Fənn: “Veb sistemləri və texnologiyaları”

Qrup: 2441a

Tələbə: Ələkbərov Emil

Müəllim: Heydərzadə Nübar

2024

Veb proqramları kodları

Veb proqram kodları, internet üzərində yerləşən veb saytlarının hazırlanması üçün yazılmış proqramlaşdırma dilindəki kodlar deməkdir. Bu kodlar, istifadəçilərin veb saytlarında interaktiv olaraq məlumatları daxil etmələrini, məlumatları dəyişmələrini və digər funksiyaları icra etmələrini təmin edir. İnternetin dinamikliyini və funksionalını təmin etmək üçün proqram kodları olmazsa, veb saytları yalnız statik məlumatlar göstərə bilərlər. Veb proqram kodları müxtəlif proqramlaşdırma dillərində yazıla bilər. Ən çox yayılmış olanlar arasında HTML, CSS, JavaScript, PHP, Python, Ruby, Java, ASP.NET və daha bir çoxu sayıla bilər. Günümüzdə işləyən veb saytlarının çoxunun bir neçə proqramlaşdırma dili və ya framework-dan istifadə etdiyini görmək mümkündür.

Aşağıda veb saytın proqramında istifadə olunan bəzi geniş yayılmış proqram dillərinin xüsusiyyətləri:

1. HTML (HyperText Markup Language):

- Veb səhifənin strukturu və məzmununu təyin edir.
- Başlıqlar, mətn bölmələri, şəkillər, linklər kimi əsas HTML elementləri ilə işlənir.

2. CSS (Cascading Style Sheets):

- Veb səhifələrinin görünüşünü və stili təyin edir.
- Rənglər, mənalar, arxa planlar, böyüklüklər, sətirlər kimi görsənən xüsusiyyətləri təyin edir.

3. JavaScript:

- Veb səhifələrində interaktivlik və dinamik funksiyalar əlavə edir.
- İstifadəçilərin məlumat daxil etməsi, düymələrə basması və s.

4. PHP:

- Sunucu-tərəfli bir proqramlaşdırma dilidir və veb saytlarının funksionalını təmin edir.
- Məlumat bazaları ilə əlaqə yaratmaq, form məlumatlarını işləmək, dinamik səhifələr yaratmaq kimi funksiyaları icra edir.

Veb proqramlar kodlarının təhlükəsizliyi

Veb proqram kodlarının təhlükəsizliyi, veb saytlarının proqramlarını müxtəlif təhlükə faktorlarından qorunması xidmətlərin və ya mənbələrin sağlamlığının təmin edilməsi deməkdir. Bu, etibarlılığa və mümkün təhlükələrin azaldılmasına nail olmaq üçün bir neçə tədbirin görülməsi zəruridir.

Bu tədbirlər aşağıdakıları əhatə edir:

- Verilənlərin qorunması: İstifadəçi məlumatları (ad, soyad, e-poçt, şifrələr kimi) saxlanılırkən end-to-end şifrələmə tətbiq edilməli, məlumatlar gizli və təhlükəsiz saxlanılmalıdır.

- **SQL injection və digər təhlükələrə qarşı qorunma:** SQL injection və digər hücumlardan qorunmaq üçün daxili verilənlərin doğrulanması, istifadəçi "input"-larında sərt təhlükəsizlik yoxlamaları və parametrizasiya kimi tədbirlər tətbiq edilməlidir.

- **Cross-Site Scripting (XSS) hücumlarına qarşı müdafiə**: XSS hücumlarına qarşı, mətnləri sıxılaşdırmaq, "input"-ları yoxlamaq, və ya məlumatları kodlaşdırmaq kimi tədbirlər alınmalıdır.

- **Cross-Site Request Forgery (CSRF) hücumlarından qorunma**: CSRF hücumlarından qorunmaq üçün, istifadəçilərdən gələn HTTP istək növləri CSRF tokenləri ilə təsdiqlənməlidir.

- **Açıq mənbəli (open source) və ya Framework-lərdən faydalanma:** Laravel, Django, Ruby on Rails kimi təhlükəsizlik prinsipləri ilə inkişaf etmiş və açıq mənbəli framework-lərdən istifadə etmək təhlükəsizliyi artırır.

- **Yenilik(Güncəllik):** Veb proqram kodlarının və tətbiq olunan framework-lərin güncəl olması, mövcud təhlükəsizlik açıqlarının referans olunması və düzəlməsi üçün əhəmiyyətlidir.

- **Log izləmə və audit:** Server loglarının monitorinqi, giriş nöqtələrinin izlənməsi və auditlər, potensial təhlükələri və hücumları tanımağa kömək edir.

- **Fayl yükləmə təhlükəsizliyi:** İstifadəçilərin veb sayta fayl yükləməsi mümkündür və bu faylların təhlükəsizlik müddətində olması əhəmiyyətlidir. Yüklənən faylların növü və həcmi yoxlanılmalı, düzgün bir şəkildə işlənməlidir. Faylların həcmi limitlənməli və təhlükəli faylların avtomatik olaraq ləğv olması zəruri olmalıdır.

- **Mənbələrin təhlükəsizliyi:** Saytlarda istifadə olunan mənbələr (şəkillər, JavaScript faylları, kimi) də təhlükəsizlik riskinə gətirib çıxarır. Bu mənbələr özündə potensial təhlükələr ola bilər və bu səbəbdən istifadə olunan mənbələrin

təhlükəsizliyi yoxlanılmalıdır. Mənbələrin HTTPS protokolu ilə gələrək şifrələnmiş olması və etibarlı təhlükəsizlik sertifikatlarına malik olması əhəmiyyətlidir.

- **İki mərhələli doğrulama:** İstifadəçilərin giriş prosesini gücləndirmək və hesablarının daha təhlükəsiz olmasını təmin etmək üçün iki mərhələli doğrulama tətbiq edilə bilər. Bundan başqa SMS kodları, e-poçt doğrulamaları və ya autentifikasiya tədbirləri kimi əlavə doğrulama mərhələləri olmalıdır.

Bu tədbirlər veb proqram kodlarının təhlükəsizliyini artırmağa kömək edir və istifadəçilərin məlumatlarını və saytın funksiyalarını qoruyur. Təhlükəsizlik, müvafiq standartlara və yaxud təşkilatın özünəməxsus təhlükəsizlik tələblərinə əsaslanmalıdır.