# SurfaceScan Academy

Resmi Tedris Beledcisi ve Imtahan Proqrami

**Ixtisas Kodu: CWSF**

## Veb Tehlukesizliyi Esaslari

Imtahan Telebleri: 25 Sual | 25 Deqiqe | Kecid Heddi: 80%

### 1. IXTISAS HAQQINDA VE IMTAHANIN EHATE DAIRESI

Muasir veb sifrelemesi, temel HTTP tehlukesizlik basliqlari, DNS muhafizesi ve avtomatlasdirilmis hucumlardan qorunma uzre resm

### 2. EHATE OLUNAN ESAS MOVZULAR

* SSL/TLS sifreleme elaqesi ve sertifikatlar
* HTTP Strict Transport Security (HSTS) is prinsipi
* Temel tehlukesizlik basliqlari (X-Frame-Options, X-Content-Type-Options)
* Cookie tehlukesizlik atributlari (HttpOnly, Secure, SameSite)
* Temel DNS tehlukesizliyi: CAA ve SPF-e giris
* Ifsa olunmus server fayllari ve aciq riskli portlar

**Imtahan Qaydalari ve Kocurmeye Qarsi Tehlukesizlik Sistemi:**

* Duzgun cavablar yalniz server terefinde saxlanilir ve brauzere gonderilmir.
* Suallar ve variantlar her namized ucun tesadufi ardicilliqla qarisdirilir.
* Imtahan zamani vaxt nezareti aparilir ve pencere deyismesi qeyde alinir.

## CHAPTER 1: SSL/TLS ve Sebeke Sifrelemesi

### Sifrelemenin oturulen melumatlari nece qorumasi ve sertifikatlarin is prinsipi.

Transport Layer Security (TLS) veb brauzerler ve serverler arasindaki melumat mubadilesini sifreleyir. Muasir tehlukesizlik standartlari TLS 1.3 ve ya guclu sifrelerle (ECDHE) TLS 1.2 teleb edir. TLS olmadiqda, araliq sebekeler (ictimai Wi-Fi, provayderler) sifreleri, sessiya acarlarini ogurlaya ve sehifenin mezmununu deyisdire biler (MitM hucumlari). Sertifikatlar etibarli CA terefinden verilmeli ve vaxtinda yenilenmelidir. Muddeti cemi 1 deqiqe bele bitmis sertifikatlar brauzerde qirmizi tehluke xeberdarligi cixarir.

```
# Nginx SSL Configuration
ssl_protocols TLSv1.2 TLSv1.3;
ssl_prefer_server_ciphers off;
ssl_ciphers "ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256";
```

## CHAPTER 2: HTTP Strict Transport Security (HSTS)

### HTTPS baglantisinin mecbur edilmesi ve SSL-strip hucumlarinin qarsisinin alinmasi.

Sayt HTTPS desteklese bele, istifadeciler cox vaxt brauzerde http:// yazir ve ya sifrelenmemis linklere klikleyirler. Hakerler SSL-strip hucumu ile baglantini adi HTTP-ye sala bilerler. HSTS basligi brauzere gosterilen muddetde (max-age) hec vaxt sifrelenmemis HTTP baglantisi etmemeyi emr edir. SurfaceScan-da A+ bali almaq ucun max-age en azi 31,536,000 saniye (1 il) olmali ve includeSubDomains parametrini saxlamalidir.

```
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
```

## CHAPTER 3: Esas HTTP Tehlukesizlik Basliqlari

### X-Frame-Options, X-Content-Type-Options ve Referrer-Policy basliqlari.

Tehlukesizlik basliqlari brauzer mudafiesini aktivlesdirmek ucun HTTP cavabinda gonderilen gosterislerdir:
1. X-Frame-Options: DENY ve ya SAMEORIGIN teyin edilir ki, sayt iframe icinde gizledilerek istifadeci klikleri ogurlanmasin (Clickjacking).
2. X-Content-Type-Options: nosniff teyin edilir ki, brauzer faylin tipini (MIME) texmin etmesin ve yuklenmis sekli skript kimi icra etmesin.
3. Referrer-Policy: strict-origin-when-cross-origin teyin edilir ki, linklerdeki gizli tokenler kenar saytlara sizmasin.

```
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Referrer-Policy: strict-origin-when-cross-origin
```

© 2026 SurfaceScan · CWSF Certification Curriculum

## CHAPTER 4: Cookie Muhafizesi: HttpOnly, Secure ve SameSite

**XSS ve CSRF vasitesile sessiya ogurlanmasinin qarsisinin alinmasi.**

Sessiya cookie-leri istifadeci hesabinin acaridir. Eger ogurlanarsa, haker sifresiz daxil ola biler:

- HttpOnly: JavaScript-in (document.cookie) cookie-ye catmasini qadagan edir ve XSS zamani sessiyanin ogurlanmasini engelleyir.
- Secure: Brauzerin cookie-ni yalniz sifrelenmis HTTPS ile gondermesini temin edir.
- SameSite=Lax ve ya Strict: Kenar saytlardan gelen sorgularda cookie-nin gonderilmesini mehdudlasdirir ve CSRF hucumlarini zerersizlesdirir.

```
Set-Cookie: session_id=xyz789; Path=/; Secure; HttpOnly; SameSite=Lax
```

## CHAPTER 5: Ifsa Olunmus Fayllar, Git Qovluqlari ve Aciq Portlar

**Hakerler istifade etmemisden evvel kesfiyyat zeifliklerinin askarlanmasi.**

Hakerler avtomatik aletlerle daimi olaraq /.env ve /.git/HEAD kimi hessas fayllari axtarirlar. Aciq .env fayli verilenler bazasi sifrelerini ve API acarlarini sizdirir. Aciq .git qovlugu ise layihenin butun menbe kodunun berpa edilmesine imkan verir. Hemcinin verilenler bazasi portlari (MySQL 3306, PostgreSQL 5432, Redis 6379, MongoDB 27017) ve idareetme portlari (RDP 3389, Telnet 23) hec vaxt aciq internete cixarilmamali, yalniz yerli (localhost) ve ya VPN daxilinde saxlanmalidir.

```
# Apache .htaccess: Deny access to hidden files and .env
<FilesMatch "^(\.git|\.env|\.yml|composer\.json)">
  Order allow,deny
  Deny from all
</FilesMatch>
```