Veb Mudafie ve Kriptoqrafiya Mutexessisi

Imtahan Telebleri: 30 Sual | 35 Deqiqe | Kecid Heddi: 80%

1. IXTISAS HAQQINDA VE IMTAHANIN EHATE DAIRESI

Muessise seviyyeli TLS 1.3 sifrelemesi, derin CSP siyasetleri, brauzer mense izolyasiyasi ve XSS-e qarsi qabaqcil mudafie uzre pes

2. EHATE OLUNAN ESAS MOVZULAR

* TLS 1.3 kriptoqrafik esaslari ve 0-RTT tekrar hucumlarindan mudafie
* Derin CSP: Nonce, hash ve strict-dynamic siyasetleri
* Cross-Origin Opener Policy (COOP) ve Spectre mudafiesi
* Cross-Origin Embedder Policy (COEP) ve Resource Policy (CORP)
* Permissions-Policy ve brauzer funksiyalarinin mehdudlasdirilmasi
* HSTS Preload telebleri ve subdomenler ucun riskleri

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: Muasir Kriptoqrafiya: TLS 1.3 Memarligi

Qabaqcil gizlilik (Forward Secrecy), kohne sifrelerin legvi ve 0-RTT riskleri.

TLS 1.3 (RFC 8446) kohnelmis ve zeif sifreleme usullarini tamamile legv etdi:
- Statik RSA acar mubadilesi legv edildi: Butun TLS 1.3 baglantilari Perfect Forward Secrecy (PFS) temin eden Ephemeral Diffie-Hellman (ECDHE) teleb edir. Gelecekde serverin gizli acari ogurlansa bele, kecmisde yazilmis melumatlar oxuna bilmez.
- CBC rejimli AES, RC4 ve DES tamamile temizlendi. Yalniz AEAD sifreleri (AES-GCM, CHACHA20-POLY1305) qaldi.
- 0-RTT (Early Data): Qosulmani suretlendirse de, tekrar sorgu hucumlarina (replay) hessasdir. Veziyyet deyisen emeliyyatlarda 0-RTT qadagan edilmelidir.

```
# OpenSSL / Nginx TLS 1.3 Cipher Suite
ssl_protocols TLSv1.3;
ssl_conf_command Ciphersuites TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256;
```

CHAPTER 2: Derin Content Security Policy (CSP)

Tesadufi nonce ve hash-lerle unsafe-inline zeifliyinin aradan qaldirilmasi.

'unsafe-inline' ve ya 'unsafe-eval' saxlayan zeif CSP faktiki olaraq XSS qarsisinda hec bir qoruma temin etmir. Muasir muessise seviyyeli CSP nonce ve ya hash esasli isleyir:
1. Nonce esasli: Her bir HTTP cavabinda kriptoqrafik tesadufi kod yaradilir. Yalniz bu koda malik olan skriptler (<script nonce="...">) ise dusur.
2. strict-dynamic: Nonce ile birge isledildikde etibarli skriptlerin diger kitabxanalari tehlukesiz cagirmasina icaze verir.
3. frame-ancestors: X-Frame-Options-u evez edir ve saytin hansi menselerde yerlesdirile bileceyini deqiq teyin edir.

```
Content-Security-Policy: default-src 'self'; script-src 'nonce-dGVzdDEyMzQ1Ng==' 'strict-dynamic'; object-
```

CHAPTER 3: Menselerarasi Izolyasiya: COOP, COEP ve CORP

Spectre ve XS-Leaks hucumlarina qarsi yaddas serhedlerinin qorunmasi.

Spectre hucumlari zererli kodlarin yaddasdan gizli melumatlari oxumasina serait yaradir. Brauzerler bunun qarsisini almaq ucun Cross-Origin Isolation standartini teqdim etdi:
- Cross-Origin-Opener-Policy (COOP): same-origin teyin edildikde sehifeni ayri bir sistem prosesine ayirir ve window.opener vasitesile hucumlarin qarsisini alir.
- Cross-Origin-Embedder-Policy (COEP): require-corp teyin edilir ki, sehifeye yuklenen butun kenar resurslar icazeli olsun.
- Cross-Origin-Resource-Policy (CORP): same-origin teyin edilerek diger saytlarin sizin gizli fayllarinizi cagirmasini engelleyir.

```
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Embedder-Policy: require-corp
Cross-Origin-Resource-Policy: same-origin
```

CHAPTER 4: Permissions-Policy ve Brauzer Selahiyyetleri

Tehlukeli avadanliq ve sensor API-lerinin mehdudlasdirilmasi.

Permissions-Policy brauzerin guclu avadanliq funksiyalarinin (kamera, mikrofon, geolokasiya, USB) sayt ve iframeler terefinden istifadesine qadaga qoyur. Saytda her hansi XSS zeifliyi yaransa bele, haker istifadecinin kamerasini aca ve ya yerini teyin ede bilmez.

```
Permissions-Policy: camera=(), microphone=(), geolocation=(), payment=(), usb=()
```