SurfaceScan Academy

Resmi Tedris Beledcisi ve Imtahan Proqrami

Ixtisas Kodu: CFSAA

Tetbiq ve Infrastruktur Tehlukesizliyi Auditoru

Imtahan Telebleri: 35 Sual | 40 Deqiqe | Kecid Heddi: 80%

1. IXTISAS HAQQINDA VE IMTAHANIN EHATE DAIRESI

Hucum sethinin kompleks auditi: SRI xetleri, CORS sizmalari, .git/.env ifsasi, tehlukeli baza/idareetme portlari ve CMS zeifliklerini

2. EHATE OLUNAN ESAS MOVZULAR

* Subresource Integrity (SRI) ve CDN hucumlarindan mudafie
* CORS xetalari, Origin eks olunmasi ve melumat sizmasi
* Hessas fayl ifsasi: /.git/HEAD, /.env, /backup.sql, /composer.json
* Tehlukeli aciq portlar: Verilenler bazasi (3306, 5432, 6379, 27017) ve Idareetme (3389, 23)
* CMS muhafizesi: WordPress XML-RPC, istifadeci ifsasi ve daxili API qorunmasi
* Kiber tehdid kesfiyyati, domen reputasiyasi ve qara siyahilar

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: Subresource Integrity (SRI) ve Techizat Zenciri Mudafiesi

CDN xidmeti sindirildiqda sayta zererli kod daxil edilmesinin qarsisinin alinmasi.

Muasir saytlar kenar CDN-lerden kitabxanalar (jQuery, Bootstrap ve s.) yukleyirler. Eger hemin CDN sindirilarsa, o skripti cagiran butun saytlarda haker kodu icra olunur.

Subresource Integrity (SRI) brauzere yuklenen faylin hash-ini (SHA-384) yoxlamagi tapsirir. Eger faylda bir bayt bele deyisdirilibse, brauzer hemin skriptin icrasini qeti qadagan edir.

Mutleq integrity hash-i crossorigin="anonymous" ile birge istifade edilmelidir.

```
<script
  src="https://cdnjs.cloudflare.com/ajax/libs/lodash.js/4.17.21/lodash.min.js"
  integrity="sha384-H6MmXflB4yB9J1kM2oB1M4I+gqY6K6v9a4c1D0b2e8="
  crossorigin="anonymous">
</script>
```

CHAPTER 2: CORS Tehlukesizliyi ve Tez-tez Edilen Xetalar

Icazesiz domenlerin melumatlari oxumasinin ve sessiyalarin ogurlanmasinin qarsisi.

CORS brauzerin Same-Origin siyasetini yumsaldaraq basqa domenlerin API-den melumat oxumasina icaze verir. En tehlukeli xetalar:

1. Gelen Origin-i birbasa tesdiqleyib Access-Control-Allow-Credentials: true vermek. Bu zaman internetdeki istenilen sayt istifadecinin daxilindeki sexsi melumatlari oxuya bilir.

2. Zeif regex yoxlanisi (mes: "example.com" yazmaqla hakerin "attacker-example.com" saytina icaze vermek).

3. "null" menseyine icaze vermek (bu, sandbox iframeler terefinden asanliqla sui-istifade edilir).

```
# Secure Express.js CORS handler
const ALLOWED_ORIGINS = new Set(['https://app.example.com', 'https://admin.example.com']);
app.use((req, res, next) => {
  const origin = req.headers.origin;
  if (ALLOWED_ORIGINS.has(origin)) {
    res.setHeader('Access-Control-Allow-Origin', origin);
    res.setHeader('Access-Control-Allow-Credentials', 'true');
  }
  next();
});
```

CHAPTER 3: Hessas Fayl Ifsasi ve Kesfiyyat Riskleri

Aciq .git melumatlari, .env fayllari ve baza nusxelerinin temizlenmesi.

Hakerler hucumdan evvel avtomatik skanerlerle yuzlerle gizli unvani yoxlayirlar:
- /.git/HEAD: Saytin butun kecmis kod tarixcesini, gizli acarlari ve daxili fayllari ifsa edir.
- /.env ve ya /config.json: Baza sifrelerini, AWS ve Stripe acarlarini aninda hakere teqdim edir.
- /wp-json/wp/v2/users: WordPress-in daxili idareci adlarini ifsa ederek hedefli sifre sindirma hucumlarina yol acir.

```
# Nginx rule: Block all hidden dotfiles and sensitive backups
location ~ /\.(?!well-known) {
  deny all;
  return 404;
}
location ~* \.(env|git|sql|bak|yml|yaml|ini|log|conf)$ {
  deny all;
  return 404;
}
```

CHAPTER 4: Verilenler Bazasi ve Idareetme Portlarinin Qorunmasi

Baza portlarinin (MySQL, Postgres, Redis, Mongo) ve idareetmenin qorunmasi.

Verilenler bazasi ve ya idareetme portlarini birbasa aciq internete qoymaq en boyuk tehlukesizlik xetalarindandir:
- MySQL (3306), PostgreSQL (5432), MongoDB (27017): Ransomware botlari aciq bazalara girib melumatlari silir ve sifreleyerek pul teleb edir.
- Redis (6379): Cox vaxt sifresiz qalir; hakerler servere daxil olub birbasa root huququ elde edirler.
- RDP (3389) ve Telnet (23): Sifre sindirma hucumlari ile serverin ele kecirilmesine sebeb olur.
Helli: Butun xidmetler yalniz 127.0.0.1 unvanina baglanmali ve firewall (UFW) ile qorunmalidir.

```
# Ubuntu UFW Firewall rules
ufw default deny incoming
ufw default allow outgoing
ufw allow 22/tcp
ufw allow 80/tcp
ufw allow 443/tcp
ufw enable
```

© 2026 SurfaceScan · CFSAA Certification Curriculum