

Soru:

CWE tanımlarında rastgelinen “Seven Pernicious Kingdoms (7PK)” nedir?

Cevap:

Seven Pernicious Kingdoms (7PK) - yani tercümesi ile 7 Zararlı Krallık - uygulama dünyası için bir vulnerability classification'dır (açıklık sınıflandırmasıdır). Bu açıklık sınıflandırmasını oluşturanlar isim olarak biyoloji biliminden yararlanmışlardır. Bu açıklık sınıflandırmasında her bir madde yine biyoloji biliminden ödünç alınan bir terimle, "phyla" adı ile - yani şube adı ile - adlandırılmıştır.

Uygulama dünyasında 7PK (7 Zararlı Krallık) açıklık sınıflandırmasına göre 7 adet phyla (şube) vardır. Bunlar;

1. Input Validation and Representation
2. API Abuse
3. Security Features
4. Time and State
5. Errors
6. Code Quality
7. Encapsulation
- \* Environment

7 Zararlı Krallık açıklık sınıflandırmasına sonradan bir adet daha phyla eklenmiştir. O da sekinci olarak "Environment"tır.

Sonuç olarak yazılımcılar uygulama geliştirirken 7PK (Seven Pernicious Kingdoms / 7 Zararlı Krallık) açıklık sınıflandırmasını oluşturanların önerdiği tavsiyeleri uygulamalıdır. Böylece uygulamalarını saldırılardan koruyabilirler.

Kaynaklar:

<https://cwe.mitre.org/data/definitions/700.html>

<https://vulncat.fortify.com/en>

<https://www.c-sharpcorner.com/article/the-seven-pernicious-kingdoms/>

<https://cwe.mitre.org/documents/sources/SevenPerniciousKingdoms.pdf>

<https://cwe.mitre.org/data/definitions/485.html>