PHP ve Web Güvenliği Ezber Kartları

Kartlarda bulunan bilgiler PHP ve web güvenliği konusunda giriş seviyesinde olup, günümüze sıklıkla karşımıza çıkan güvenlik açıklarını ve bunlarla ilgili en çok kullanılan PHP komutlarını özet olarak içermektedir.

Kartlarda bulunan güvenlik açıkları türleri, komutlar ve terimler üzerine detaylı şekilde araştırma yapılması önerilir.

SQL Injection

SQL cümleciklerinin içine sızarak veritabanı üzerinde beklenenin dışında - kötü amaçlı - işlemler yapılması.

XSS
Cross-site Scripting

Yazılıma ait kod içine sızarak istemci veya sunucu tarafında - kötü amaçlı - kodlar çalıştırma.

CSRF / XSRF
Cross-site Request Forgery

Ziyaretçinin rızası dışında başka bir web sitesine otomatik istekte bulundurtma ve istekten dönen bilgileri (çerezler gibi) alma.

mysql_real_escape_string

[SQL Injection]

Değişken (metin) içindeki SQL cümlecikleri için özel anlam ifade eden sembolleri süzerek güvenli hale getirir.

htmlspecialchars	*[Cross-site Scripting]* Değişken (metin) içindeki HTML için özel anlam ifade eden sembolleri süzer.
strip_tags	*[Cross-site Scripting]* Değişken (metin) içindeki HTML ayraçlarını süzer.
filter_input	*[SQL Injection, Cross-site Scripting]* Kullanıcı tarafından girilmiş verileri (formdan gelen veriler gibi) istenilen kurala göre süzer veya doğrular.
filter_var	*[SQL Injection, Cross-site Scripting]* Değişkenleri istenilen kurala göre süzer veya doğrular.