**Bir saldırganın index.php?sayfa=../../../../etc/passwd şeklinde bir istek göndermesindeki temel teknik amaç nedir?**

- [x] ../ karakterlerini kullanarak mevcut çalışma dizininden üst dizinlere çıkıp hassas sistem dosyalarını okumak.
- [ ] index.php dosyasının include() fonksiyonunu kullanarak uzak bir sunucudan zararlı bir PHP betiği çalıştırmak.
- [ ] etc/passwd dosyasının adını kullanarak sunucudaki parola karmalarını (hash) doğrudan ele geçirmeye çalışmak.
- [ ] '../../' karakterlerini bir SQL sorgusuna enjekte ederek veritabanı yapısı hakkında bilgi toplamaya çalışmak.
- [ ] %00 (Null Byte) karakteriyle birlikte kullanarak .php uzantısını atlatıp dosya yükleme zafiyetini tetiklemek.

2. MULTIPLE CHOICE • 2 mins • 1 pt

**Bir "Kalıcı XSS" (Stored XSS) saldırısının "Yansıyan XSS" (Reflected XSS) saldırısından temel teknik farkı nedir?**

- [ ] Kalıcı XSS, saldırı kodunu URL parametresi içinde gönderir ve yalnızca o URL'ye tıklayan kurbanı etkiler.
- [x] Kalıcı XSS, saldırı kodunu veritabanına (örn. bir yorum olarak) kaydeder ve o sayfayı görüntüleyen herkesi etkiler.
- [ ] Kalıcı XSS, sunucuda eval() benzeri bir fonksiyonu tetiklerken Yansıyan XSS yalnızca echo fonksiyonunu tetikler.
- [ ] Kalıcı XSS, yalnızca POST metodu ile çalışırken Yansıyan XSS saldırısı yalnızca GET metodu ile çalışabilir.
- [ ] Kalıcı XSS, htmlspecialchars() fonksiyonunu atlatabilirken Yansıyan XSS bu fonksiyon tarafından kolayca engellenir.

3. MULTIPLE CHOICE • 2 mins • 1 pt

**Bir SQL Enjeksiyonu saldırısında ' OR '1'='1' -- şeklindeki bir ifadenin (payload) kullanılmasının teknik amacı nedir?**

- [ ] UNION SELECT komutuyla birleştirerek sorguya yetkisiz sütunlar ekleyip başka tablolardan veri çekmektir.
- [ ] WAITFOR DELAY komutunu tetikleyerek veritabanı sunucusunun yanıtını geciktirip zamanlama saldırısı yapmaktır.
- [x] WHERE koşulunu mantıksal olarak her zaman doğru (true) hale getirip parola kontrolünü etkisiz bırakmaktır.
- [ ] -- karakterlerini kullanarak sorgunun geri kalanını yorum satırı yapıp LIMIT gibi kısıtlamaları kaldırmaktır.
- [ ] OR anahtar kelimesini kullanarak veritabanı sürümünü ve adını öğrenmek için hata mesajları üretmektir.

4. MULTIPLE CHOICE • 2 mins • 1 pt

**OS Komut Enjeksiyonu (OS Command Injection) saldırısının temel çalışma prensibi aşağıdakilerden hangisidir?**

- [ ] Sunucuda include('pages/' . $sayfa) gibi bir kodu sömürerek php://filter ile sunucu dosyalarını okumaktır.
- [ ] <script>alert(1)</script> gibi bir kodu HTML içine enjekte ederek kurbanın tarayıcısında JavaScript çalıştırmaktır.
- [ ] (uid=*) gibi bir LDAP filtresini enjekte ederek Active Directory gibi dizin servislerindeki tüm kayıtları listelemektir.
- [x] 8.8.8.8 ; ls -la gibi ; veya && karakterlerini kullanarak uygulamanın çalıştırdığı shell komutuna yeni komut eklemektir.
- [ ] ' OR 1=1 gibi bir ifadeyi SQL sorgusuna ekleyerek veritabanı seviyesinde kimlik doğrulama işlemini atlamaktır.

5. MULTIPLE CHOICE • 2 mins • 1 pt

**Bir web uygulamasında RFI (Remote File Inclusion) zafiyetinin başarılı bir şekilde sömürülmesi için gereken en kritik sunucu yapılandırması nedir?**

- [ ] Sunucunun open_basedir direktifinin PHP'nin sadece belirli dizinlere erişimini kısıtlamamış olması gerekmektedir.
- [ ] Sunucunun magic_quotes_gpc ayarının On konumunda olması ve tırnak işaretlerini otomatik olarak escape etmesi gerekmektedir.
- [ ] Sunucunun bir "Web Application Firewall" (WAF) tarafından korunmuyor olması ve gelen GET isteklerini filtrelememesi gerekmektedir.
- [ ] Sunucunun register_globals direktifinin On konumunda olması ve GET parametrelerini doğrudan değişken olarak ataması gerekmektedir.

6. MULTIPLE CHOICE • 2 mins • 1 pt

Preview Edit

**Aşağıdakilerden hangisi eval() gibi fonksiyonların kullanıcı girdisiyle beslenmesi sonucu ortaya çıkan "Sunucu Taraflı Kod Enjeksiyonu" (Server-Side Code Injection) saldırısına bir örnektir?**

- [x] hesapla.php?q=10 * 5 ; system('whoami') girdisini eval() fonksiyonuna göndererek sunucuda PHP kodu çalıştırmaktır.
- [ ] profil.php?id=1' UNION SELECT 1,2,user,pass girdisini göndererek SQL veritabanından kullanıcı parolalarını çekmektir.
- [ ] arama.php?term=<img src=x onerror=alert(1)> girdisini göndererek arama sonuç sayfasında XSS saldırısı yapmaktır.
- [ ] index.php?sayfa=../../boot.ini girdisini göndererek sunucudaki sistem dosyalarının içeriğini okumaya çalışmaktır.
- [ ] ldap.php?user=(objectClass=*) girdisini göndererek LDAP sunucusundaki tüm nesnelerin listesini çekmeye çalışmaktır.

7. MULTIPLE CHOICE • 2 mins • 1 pt

**Bir LDAP Enjeksiyonu saldırısı, temelde hangi teknik zafiyeti sömürerek bilgi sızdırmaya veya kimlik doğrulamayı atlamaya çalışır?**

- [ ] Kullanıcıdan alınan veriyi doğrudan SQL sorgusuna ekleyerek veritabanı sunucusunun mantığını manipüle etmektir.
- [x] Kullanıcıdan alınan veriyi (*, | & gibi) filtrelemeden LDAP sorgu filtresine ekleyerek sorgu mantığını bozmaktır.
- [ ] Kullanıcıdan alınan veriyi system() fonksiyonuna vererek sunucunun işletim sisteminde keyfi komutlar çalıştırmaktır.
- [ ] Kullanıcıdan alınan veriyi include() fonksiyonuna vererek sunucudaki yerel dosyaları okumak veya çalıştırmaktır.
- [ ] Kullanıcıdan alınan veriyi şifresiz port 389 üzerinden göndererek ağdaki trafiği dinleyen saldırganlara yakalanmaktır.

8. MULTIPLE CHOICE • 2 mins • 1 pt

**Web uygulamalarında XSS (Cross-Site Scripting) saldırılarını önlemenin en etkili ve standart yolu aşağıdakilerden hangisidir?**

- [ ] Kullanıcıdan alınan tüm verileri veritabanına kaydetmeden önce strip_tags() fonksiyonundan geçirip tüm HTML etiketlerini silmektir.
- [ ] Kullanıcıdan alınan veriyi addslashes() fonksiyonundan geçirerek tırnak işaretlerini (') etkisiz hale getirip SQLi'yi de engellemektir.
- [x] Kullanıcıdan alınan veriyi HTML içine basmadan önce htmlspecialchars() gibi fonksiyonlarla özel karakterleri (<, >) kodlamaktır.
- [ ] Content-Security-Policy (CSP) başlığını kullanmayarak tarayıcının tüm kaynaklardan (inline, external) kod çalıştırmasına izin vermektir.
- [ ] Gelen tüm GET isteklerini POST isteklerine çevirerek zararlı kodun URL üzerinden taşınmasını tamamen engellemektir.

9. MULTIPLE CHOICE • 2 mins • 1 pt

**SQL Enjeksiyonu saldırılarına karşı en sağlam ve tavsiye edilen savunma yöntemi aşağıdakilerden hangisidir?**

- [ ] Gelen tüm kullanıcı girdilerindeki OR, SELECT, UNION gibi tehlikeli SQL anahtar kelimelerini filtrelemek veya engellemektir.
- [ ] Web sunucusunu düşük yetkili bir kullanıcı (örn. www-data) ile çalıştırarak veritabanı erişimini kısıtlamaktır.
- [ ] mysql_real_escape_string() gibi eski fonksiyonları kullanarak kullanıcıdan gelen özel karakterleri (') escape etmektir.
- [x] Kullanıcı girdisini SQL sorgusuyla birleştirmek yerine "Parametreli Sorgular" (Prepared Statements) kullanarak veriyi koddan ayırmaktır.
- [ ] Kullanıcı girdisini HTML'e basmadan önce htmlspecialchars() fonksiyonuyla zararlı olabilecek karakterleri kodlamaktır.

10. MULTIPLE CHOICE • 2 mins • 1 pt

**Bir saldırganın, LFI zafiyetini RCE'ye (Uzaktan Kod Çalıştırma) yükseltmek için "Log Zehirleme" (Log Poisoning) tekniğini kullanmasının adımları nelerdir?**

- [ ] php://filter/read=convert.base64-encode/resource=config.php komutuyla konfigürasyon dosyasını Base64 olarak okumaktır.
- [ ] ../../etc/shadow dosyasını okuyup elde ettiği parola kamalarını (hash) çevrimdışı araçlarla kırmaya çalışmaktır.
- [ ] http://evil.com/shell.php adresini include() fonksiyonuna vererek allow_url_include ayarını sömürmektir.
- [ ] admin' OR 1=1 -- gibi bir SQL kodunu log dosyasına yazdırıp veritabanı bağlantısı üzerinden RCE denemektir.
- [x] User-Agent gibi bir HTTP başlığında PHP kodu gönderip log dosyasına yazdırmak, sonra LFI ile o log dosyasını include() etmektir.