**🧠 1. Clickjacking Nedir?**

**Clickjacking**, kullanıcıların bir web sayfası üzerindeki buton, form gibi öğelere **farkında olmadan tıklamasını sağlayan bir saldırı tekniğidir**.

📌 Saldırgan, güvenli görünen bir sayfanın üzerine şeffaf bir iframe yerleştirir.  
📌 Kullanıcı, tıkladığını düşündüğü şey yerine arka plandaki zararlı işlem çalışır (örneğin: “beğen” → “parola değiştir”).

**🛠️ 2. Clickjacking Tester Nedir?**

**Clickjacking Tester**, hedef web sitesinin **iframe içine gömülüp gömülemediğini** kontrol eden, genellikle web tabanlı ya da basit HTML/PHP scriptlerle oluşturulmuş bir test aracıdır.

📌 Testin amacı: X-Frame-Options ve Content-Security-Policy (frame-ancestors) başlıklarının doğru yapılandırılıp yapılandırılmadığını kontrol etmektir.

**🎯 3. Ne İşe Yarar?**

| **Özellik** | **Açıklama** |
| --- | --- |
| 🖼️ iframe testi | Site başka bir sayfa içinde gösterilebiliyor mu? |
| 🔒 Güvenlik başlığı kontrolü | X-Frame-Options, CSP başlıklarını kontrol eder |
| 🛡️ Clickjacking savunmasını denetler | Uygulama doğru şekilde korunuyor mu? |
| 🧪 Uygulama seviyesinde test | HTML tabanlı form veya butonlar test edilebilir |

**⚙️ 4. Nasıl Kullanılır? (Manuel Test)**

**✅ Basit HTML test sayfası oluştur:**



**✅ Bu HTML dosyasını bir tarayıcıda aç → Hedef site iframe içinde yükleniyor mu?**

* Eğer **iframe içinde açılmıyorsa**: Güvenlik önlemi vardır ✅
* Eğer **iframe içinde görünüyorsa**: Clickjacking’e karşı savunmasız olabilir ❌

**📋 5. Otomatik Test Aracı Örneği (Kali’de)**

**✅ OWASP Clickjacking Tester (Python)**

**metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.**

**Örnek çıktı:**

**[+] Checking https://targetsite.com...**

**[!] Vulnerable: X-Frame-Options header not set!**

**[+] You can frame this site!**

**🛡️ 6. Clickjacking'e Karşı Güvenlik Başlıkları**

| **Güvenlik Başlığı** | **Açıklama** |
| --- | --- |
| **X-Frame-Options: DENY** | **iframe içine asla yüklenemez** |
| **X-Frame-Options: SAMEORIGIN** | **Sadece aynı domain içinden yüklenebilir** |
| **Content-Security-Policy: frame-ancestors 'none';** | **Daha gelişmiş kontrol sağlar** |

**🧠 7. Kullanım Senaryoları**

* **Web uygulamalarının iframe ile korunup korunmadığını test etme**
* **Pentest / web güvenlik testi öncesi güvenlik başlıklarını analiz etme**
* **OWASP Top 10 kapsamındaki güvenlik açıklıklarına karşı önlem denetimi**
* **Güvenlik duvarı/ayarları test senaryolarında doğrulama**

**🎯 8. Öğrenim Kazanımları**

* **Web uygulamalarında çerçeveleme (framing) kavramını öğrenme**
* **X-Frame-Options ve CSP güvenlik başlıklarının önemini kavrama**
* **Basit HTML ile güvenlik testi yapabilme becerisi**
* **OWASP Top 10 zafiyetlerinden biri olan Clickjacking’i tanıma**