**HTML5sec**, web uygulamalarına yönelik modern saldırı tekniklerini içeren, HTML5 özellikleri üzerinden gerçekleştirilebilecek güvenlik açıklarını sergileyen bir **referans ve test platformudur**. Kendi başına bir araçtan çok, HTML5 tabanlı saldırı vektörlerini örnekleriyle sunan bir “**pentest destek sayfası**” olarak değerlendirilir.

Genellikle XSS, Clickjacking, Local Storage Abuse, WebSocket Hijacking gibi tarayıcı tabanlı saldırıların denenmesi ve gözlemlenmesi için kullanılır.

**Bu Platformun Özellikleri Nelerdir?**

* **XSS Payload Testleri**: HTML5 ile gerçekleştirilebilecek birçok XSS varyasyonunu gösterir.
* **Clickjacking ve IFrame Bypass Testleri**: Tarayıcı güvenlik ayarlarını aşan teknikleri içerir.
* **Web Storage Manipülasyonları**: localStorage ve sessionStorage suistimalleri test edilebilir.
* **JavaScript URI Testleri**: Zararlı link ve yönlendirme teknikleri içerir.
* **Sandbox Bypass**: HTML5 sandbox özelliğinin nasıl aşılabileceğini örneklerle gösterir.
* **Educational (Eğitim Odaklı)**: Gerçek sistemlere zarar vermez; örnekler yalnızca test amaçlıdır.
* **Offline veya Online Kullanım**: GitHub’dan indirip kendi sisteminizde çalıştırabilirsiniz.

**HTML5sec Platformunu Kali Linux’a Kurma ve Kullanma Adımları**

**Adım 1: Gerekli Paketlerin Kurulumu**

Herhangi bir web sunucusu (örneğin Python HTTP server) ile çalışabileceği için yalnızca Git ve Python yeterlidir:

“sudo apt update

sudo apt install git python3 -y”

**Adım 2: HTML5sec Reposunu Klonlayın**

“git clone https://github.com/cure53/HTML5sec.git

cd HTML5sec”

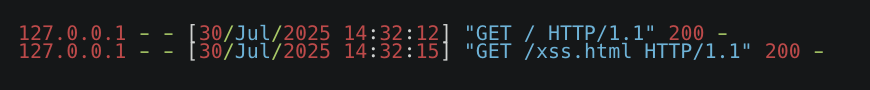
Bu adımda tüm saldırı senaryoları ve örnek HTML dosyaları sisteminize indirilmiş olur.

**Adım 3: Basit Web Sunucusu ile Sayfaları Yayınlayın**

Python 3 ile bulunduğunuz klasörü bir HTTP sunucusu gibi yayınlayın:

“python3 -m http.server 8080”

Bu komut, http://localhost:8080 adresinde tüm HTML5sec örneklerini tarayıcıdan görüntülemenizi sağlar.

****

**Adım 4: Tarayıcıdan Arayüze Erişin**

Tarayıcıya şunu yazın: <http://localhost:8080>

Açılan sayfada:

* xss.html
* iframe-bypass.html
* web-storage.html
* sandbox-escape.html

gibi dosyaları tıklayarak her saldırı örneğini test edebilirsiniz.

**Adım 5: Örnek XSS Senaryosunu Gözlemleme**

Açılan xss.html dosyasında şunlar olabilir:

“<script>alert('XSS')</script>”

Tarayıcıda bu dosya açıldığında bir uyarı kutusu belirir. Bu, HTML5 ile oluşturulmuş klasik bir **stored XSS** örneğidir.

metin, yazı tipi, ekran görüntüsü içeren bir resim

Açıklama otomatik olarak oluşturuldu

**Kullanım Senaryoları**

| **Amaç** | **Dosya** |
| --- | --- |
| DOM tabanlı XSS | xss-dom.html |
| Sandbox kaçış testi | sandbox-escape.html |
| iframe bypass | iframe-bypass.html |
| WebStorage manipülasyonu | web-storage.html |
| JavaScript URI abuse | javascript-uri.html |