# Testing for HTML Injection (HTML Enjeksiyonu Testi)

## Summary (Özet)

HTML enjeksiyonu, bir kullanıcı bir giriş noktasını kontrol edebildiğinde ve hassas bir web sayfasına rastgele HTML kodunu enjekte edebildiğinde ortaya çıkan bir enjeksiyon güvenlik açığı türüdür. Bu
güvenlik açığı, kurbanı taklit etmek için kullanılabilecek bir kullanıcının oturum çerezlerinin açıklanması gibi birçok sonuç doğurabilir veya daha genel olarak saldırganın kurbanlar tarafından
görülen sayfa içeriğini değiştirmesine izin verebilir.

Bu güvenlik açığı, kullanıcı girişi doğru bir şekilde sterilize edilmediğinde ve çıktı kodlanmadığında ortaya çıkar. Bir enjeksiyon, saldırganın bir kurbana kötü amaçlı bir HTML sayfası göndermesine izin verir. Hedeflenen tarayıcı, (güven) meşru parçalarının sayfasının kötü amaçlı bölümlerinden ayırt edemeyecek ve sonuç olarak tüm sayfayı kurbanın bağlamında ayrıştıracak ve yürütecektir.

HTML içeriği oluşturmak için kullanılabilecek çok çeşitli yöntem ve nitelikler vardır. Bu yöntemler güvenilmez bir girdi sağlanıyorsa, HTML enjeksiyonu güvenlik açığı riski yüksektir. Örneğin, kötü amaçlı HTML kodu ile enjekte edilebilir `innerHTML` JavaScript yöntemi, genellikle kullanıcı tarafından eklenen HTML kodunu oluşturmak için kullanılır. İpler doğru şekilde sterilize edilmezse, yöntem HTML enjeksiyonunu etkinleştirebilir. Bu amaç için kullanılabilecek bir JavaScript fonksiyonudur `document.write()` . .

Aşağıdaki örnek, sayfa bağlamında dinamik HTML oluşturmak için geçerli olmayan bir girdinin kullanılmasını sağlayan bir savunmasız kod parçasını gösterir:

```
var userposition=location.href.indexOf("user=");
var user=location.href.substring(userposition+5);
document.getElementById("Welcome").innerHTML=" Hello, "+user;
```

Aşağıdaki örnek, savunmasız kodu kullanarak gösterir `document.write()` Fonksiyon:

```
var userposition=location.href.indexOf("user=");
var user=location.href.substring(userposition+5);
document.write("<h1>Hello, " + user +"</h1>");
```

Her iki örnekte de, bu güvenlik açığı:

`http://vulnerable.site/page.html?user=<img%20src='aaa'%20onerror=alert(1)>`

Bu giriş, kötü amaçlı kullanıcı tarafından HTML bağlamında eklenen keyfi JavaScript kodunu yürütecek sayfaya bir resim etiketi ekleyecektir.

## Test Objectives (Test Hedefleri)

- HTML enjeksiyon noktalarını belirleyin ve enjekte edilen içeriğin ciddiyetini değerlendirin.

## How To Test (Nasıl Test Edilir)

Aşağıdaki DOM XSS egzersizini göz önünde bulundurun
http://www.domxss.com/domxs/01_Basics/06_jquery_old_html

HTML kodu aşağıdaki komut dosyasını içerir:

```
<script src="../js/jquery-1.7.1.js"></script>
<script>
function setMessage(){
   var t=location.hash.slice(1);
   $("div[id="+t+"]").text("The DOM is now loaded and can be manipulated.");
}
$(document).ready(setMessage  );
$(window).bind("hashchange",setMessage)
</script>
<body>
   <script src="../js/embed.js"></script>
   <span><a href="#message" > Show Here</a><div id="message">Showing M
   div></span>
   <span><a href="#message1" > Show Here</a><div id="message1">Showing
   </div>
   <span><a href="#message2" > Show Here</a><div id="message2">Showing
```

```
    /div>
  </body>
```

HTML kodu enjekte etmek mümkündür.