Click Jacking چیست و چگونه از سرقت کلید در ASP.NET جلوگیری کنیم؟ (نسخه PDF)

با استفاده از تکنیک Click Jacking می توان کلیک های یک وب سایت را دزدید. این تکنیک با استفاده از ویژگی z-index در تگ های DIV و IFrame پیاده سازی می شود. یعنی یک سایت تقلبی را بر روی سایت واقعی بگـذاریم و با این کار تراکنش های سایت اصـلی را تخریب کنیم یا بدزدیم. خوب چه جوری این طوری شد؟ سایت تقلبی صـفحه سایت اصـلی را در IFrame خودش باز می کند و سایت اصـلی را در پشت زمینه قرار می دهد و خاصیت transparency آن را با false مقداردهی می کند. با اسـتفاده از این مکانیزم، سایت تقلبی بازدیدکننده های سایت اصلی را ناخواسته مجبور می کند که با استفاده از اطلاعات سایت تقلبی به فعالیت در سایت اصلی بپردازند.

تکنیک سرقت کلیک

در ادامه دو مرحله برای پیاده سازی click jacking را معرفی می کنیم:

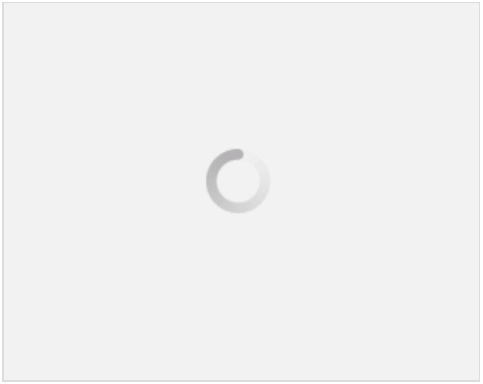
۱. برای ویژگی z-index سایت اصلی یک مقدار پایین را در نظر بگیرید (مثلا ۵).
۲. برای ویژگی z-index سایت تقلبی یک مقدار بالاتر را در نظر بگیرید (مثلا ۱۰).

```
<html>
<body>
<iframe src="http://www.microsoft.com" allowtransparency="false" style="float; position: absolute;
left: -5px; top: 12px; width: 731px; background: white; height: 259px; z-index: 5;
margin-top: 0px;" border="0" frameborder="0" scrolling="no"/>

<div style="position:absolute; left:0px; top:0px; width: 250px; height: 200px; background:white; z-index:10">

<h1>Click Jacking</h1>

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



مفهوم ساده ای است. سایت تقلبی بر روی سایت اصـلی قرار می گیرد، به طوری که هر کاری که روی سایت تقلبی انجام دهیـد، رویدادهای (event) سایت اصلی را فعال می کند. با این روش سایت تقلبی تراکنش های بی اعتبار را ایجاد می کند و در اصطلاح می گوییم که سایت اصلی در برابر click-jacking یا دزدی کلیک خطرپذیر است.

سناریوی واقعی

تصور کنیـد که یک فروشـگاه کتاب اینترنتی داریم. یک سایت دیگر هم دقیقا با این اطلاعات وجود دارد که تنها تفاوت آن در این است که کاربران را مجبور می کند که تراکنش خاصی را انجام دهند. در این سناریو یک سایت واقعی داریم که برای هر کتاب یک دکمه "خرید" دارد و یک سایت تقلبی داریم که به جای دکمه "خریـد" دکمه "اهدا" را دارد. البته توجه داشـته باشـید که دکمه اهدا رویداد خاصـی را ندارد و زمانی که کاربر دکمه تقلبی اهدا را فشار می دهد، در واقع دکمه خرید در سایت اصـلی که z-index کمتری دارد را فعال می کند. به همین راحتی هکرها از سایت تان سوء استفاده می کنند.

راه حل هایی برای Click Jacking

راه حل های زیر برای معماری .NET هسـتند اما هر تکنولوژی راه حل هایی برای این مشکل دارد. با استفاده از X-frame-option که بسیار قدرتمند است، می توانیم سایت هایمان را در برابر سوء استفاده های click jacking مقاوم کنیم.

سه راه حل داریم:

راه حل ۱:

کد زیر را در فایل Global.asax از web application بنویسید

```
Void Application_BeginRequest(object sender, EventArgs e)
{
 This.Response.Header[“X-Frame-Options”] = “DENY”;
}
```

در اینجا لازم است به یک نکته اشاره کنم که ممکن است با خطای زیر مواجه شوید:

```
Error: This operation requires IIS integrated pipeline mode”
```

راه حل ۲. این کد برای همه روش های احراز هویت کار می کند

```
Void Application_BeginRequest(object sender, EventArgs e)
{
 HttpContext.Current.Response.AddHeader(“x-frame-options”, “DENY”);
}
```

راه حل ۳. مستقیما می توانیم x-frame-options را دستکاری کنیم و این محدودیت را ایجاد کنیم.

مادامی که سایت ها در برابر click jacking خطرپذیر هستند، هکرها می توانند با استفاده از Cross Site Scripting یا همان XSS یک کاربر را فریب دهند تا لینک های نامربوط را کلیک کنند. با استفاده ازIIS می توانید هدر X-Frame-Optionsرا بفرستید.

۱. IIS را باز کنید (با استفاده از دستور inetmgr).
۲. فولدر سایت را باز کنید و بر روی سایتتان کلیک راست کنید و وارد Properties شوید.
۳. وارد تب Http Header شوید.
۴. به قسمت Custom Header بروید.
۵. روی Add کلیک کنید.
۶. داخل Custom Header Name این عبارت را تایپ کنید:

```
X-Frame-Options Custom Header Value: “DENY”
```

۱. اگر سایتی در یکی از زیرمجموعه ها داشته باشید، IIS از شما می پرسد که آیا می خواهید که این تنظیمات بر روی آن ها هم اعمال شود یا نه.
۲. OK را فشار دهید و با استفاده از دستور iisreset آن را ریست کنید.

نویسنده: پویا فضلعلی

منبع: انجمن تخصصی فناوری اطلاعات ایران

مطلب اصلی