XSS Attack

ما هي ثغرة XSS ؟ تتمثل هذه الثغرة في إدخال سكريبتات خبيثة إلى موقع الويب، مما يتيح للمهاجم تنفيذ أوامر خبيثة على أجهزة الزوار الذين يتفاعلون مع الموقع المصاب. بمعنى آخر، يتم استغلال موقع الويب المصاب كوسيلة لاختراق وإيذاء الزوار الذين يثقون فيه.

: XSSالحماية من

في هذا القسم من المقال سوف نقدم لك (المستخدم العادي) بعض النصائح لتجنب الوقوع في مثل هذا الهجوم بالإضافة لبعض النصائح الخاصة لمطوري المواقع.

بالنسبة للمستخدم:

عدم فتح أي رابط لا تعلم مصدره يمكنك استخدام إضافة [noscript](https://noscript.net/).

أو يمكنك الذهاب الى الاعدادات الخاصة بالمتصفح وتعطيل خيار استخدام javascript .

بالنسبة للمطور:

كمطور ويب تقع عليك مسؤولية حماية المستخدم من المخاطر وليس فقط حماية الموقع

1- يجب التأكد من تطبيق فلاتر مناسبة على جميع حقول الإدخال الخاصة بالموقع

2- يفضل تفعيل httponly flag و إضافته لعدم السماح بقراء ال cookie  عبر اكواد JavaScript

3- تفعيل secure flag لكي لا يتم ارسال ال cookie  إلا عن طريق HTTPS

في النهاية:

لا يوجد نظام آمن بشكل مطلق ولكن يمكننا التخفيف من المخاطر المحتملة ومن المهم جداً نشر التوعية وثقافة [الأمن السيبراني](https://ttech.site/what-is-cyber-security/) على جميع المستويات، كما يجب الإشارة إلى أمر مهم آخر وهو: إن كنت مبرمج أو مطور ويب فهذي النصائح لا تكفي ويجب عليك التوسع بشكل أكبر لمعرفة كل التفاصل الخاصة بهذه الثغرة والاجراءات المضادة لها.