



DOM XSS



# Target Information



الهدف من الفحص كان موقع عام  
الدومين المستخدم في الشرح:

<https://example.com>

نوع الفحص: **Web Application Security Testing**

# Reconnaissance Phase



في البداية قمت بأخذ الدومين example.com  
بدأت بعملية Recon على الموقع  
قمت بتصفح وفحص جميع الصفحات الممتاحة

# Identifying Potential Entry Points



أثناء الفحص لاحظت وجود صفحة تحتوي على **Search functionality** الغريب أن صفحة البحث لم تحتوي على **Parameters** ظاهرة في الـ **URL** هذا الشيء أعطاني احتمال وجود **hidden parameters**

# Parameter Discovery using Arjun



قمت باستخدام أداة Arjun لتخمين  
بعد عملية الفحص، تم اكتشاف Parameter غير موثق  
اسم الـ :Parameter  
**action\_**

# Parameter Testing



قمت بأخذ ال **Parameter** المكتشف  
بدأت باختباره باستخدام عدة **Payloads**  
الهدف كان التأكد هل يتم عكس الإدخال في الصفحة أم لا

# XSS Payload Injection



أثناء الاختبار، قمت بتجربة عدة XSS Payloads نجح في التنفيذ:  
أحد الـ XSS Payloads نجح في التنفيذ:

```
<img src=x onerror=alert(1)><"
```

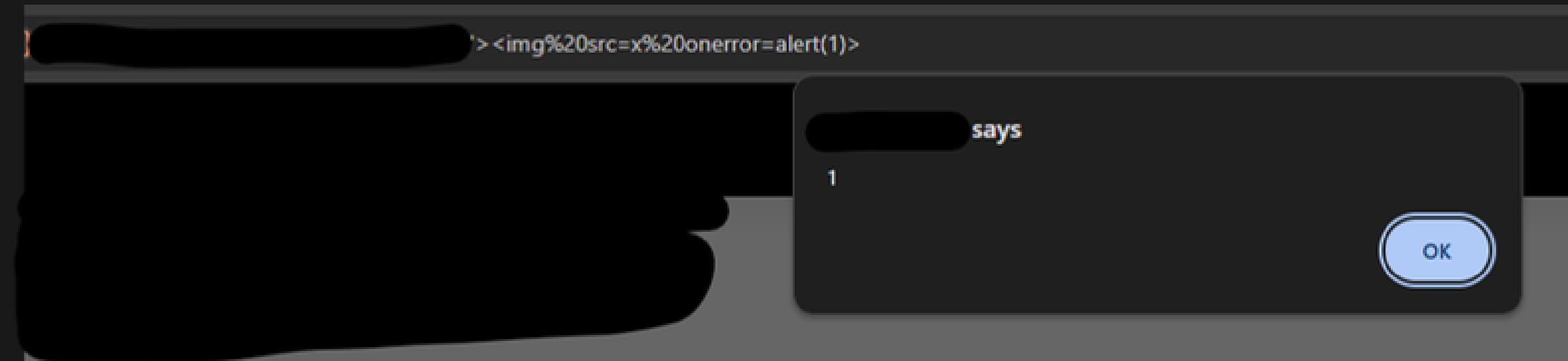


اضافة في المتصفح سوف تساعدك: [Hack-Tools](#)

# DOM XSS Confirmation



تم تنفيذ JavaScript داخل المتصفح بنجاح  
ظهرت نافذة alert بدون أي تفاعل إضافي من المستخدم  
**هذا يؤكد وجود DOM XSS vulnerability**





DOM XSS

