XSS attack

Cross-Site Scripting (XSS) ثغرة

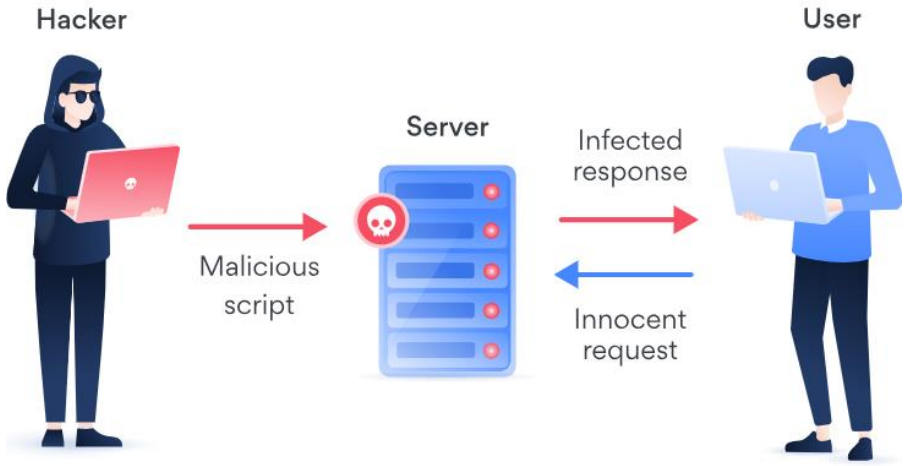
XSS stands for Cross-Site Scripting.
It’s a type of attack where an attacker injects **programming code** into a website, and this code runs directly in the victim’s browser.

What is XSS attack?

شرح ما هو XSS

هو نوع من الهجمات، من خلاله يمكن للمهاجم إدخال أكواد برمجية داخل موقع، والكود يتم تنفيذه في متصفح الضحية.

XSS اختصار لـ Cross-Site Scripting
هجوم إدخال أكواد برمجية عبر المواقع



Executing JavaScript commands in the background without the user knowing, such as stealing their data like login cookies, redirecting users to fake pages, or displaying anything the attacker wants to the user as if it's part of the original website and many other malicious actions.

What Can an Attacker Do with XSS?

ماذا يمكن أن يفعل المهاجم باستخدام XSS

من خلال XSS، المهاجم ممكن:

تنفيذ أوامر جافا سكريبت في الخلفية دون علم المستخدم، مثل سرقة بياناته كبيانات تسجيل الدخول (cookies) أو إعادة توجيه المستخدمين إلى صفحات وهمية، أو عرض أي محتوى يرغب به المهاجم داخل الموقع وكأنه جزء من الموقع الأصلي، وغيرها من الأمور الخبيثة.

How Does XSS Happen?

كيف يحدث هجوم XSS؟

The attack happens when the website uses user input directly in the page output without filtering or sanitizing it.

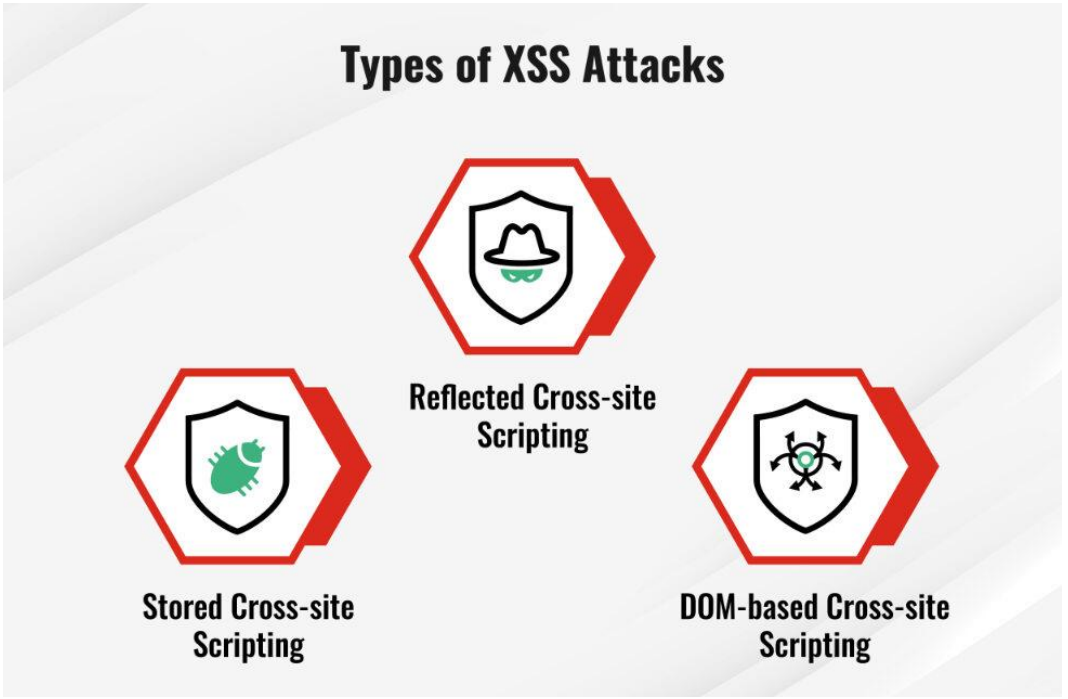
How Does XSS Happen?

كيف يحدث هجوم XSS؟

يحدث الهجوم عندما يتم استخدام البيانات التي يدخلها المستخدم مباشرة داخل صفحة HTML بدون فلترة أو حماية.

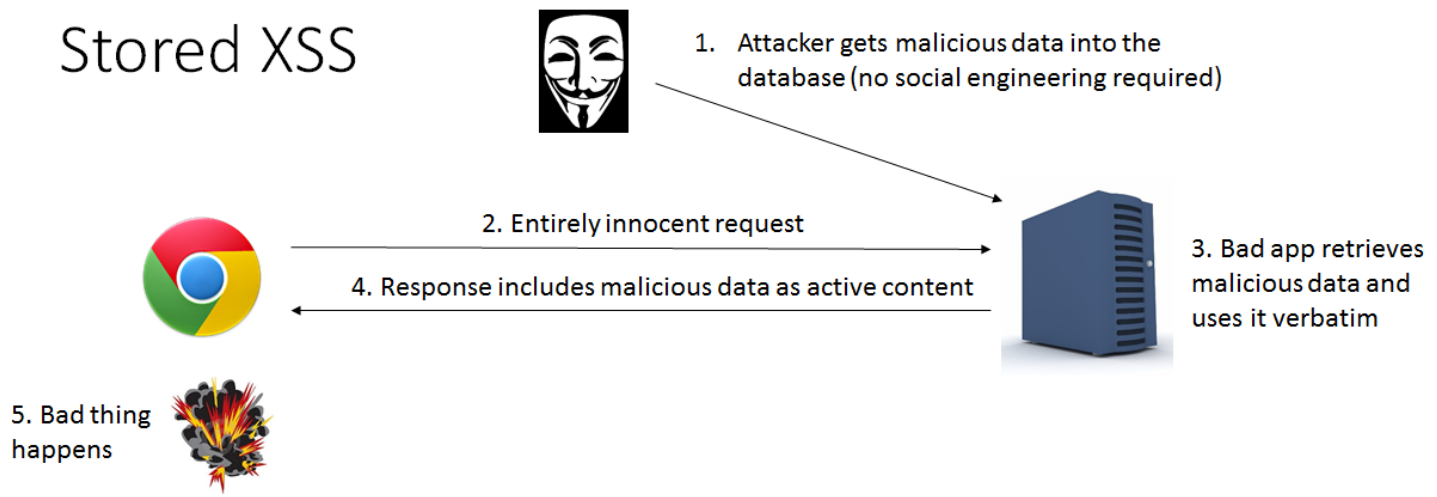
```php
<?php
echo "Hello " . $_GET['name'];
?>
```

```
http://example.com/?name=<script>alert('XSS')</script>
```



Types of XSS Attacks

انوع هجمات XSS



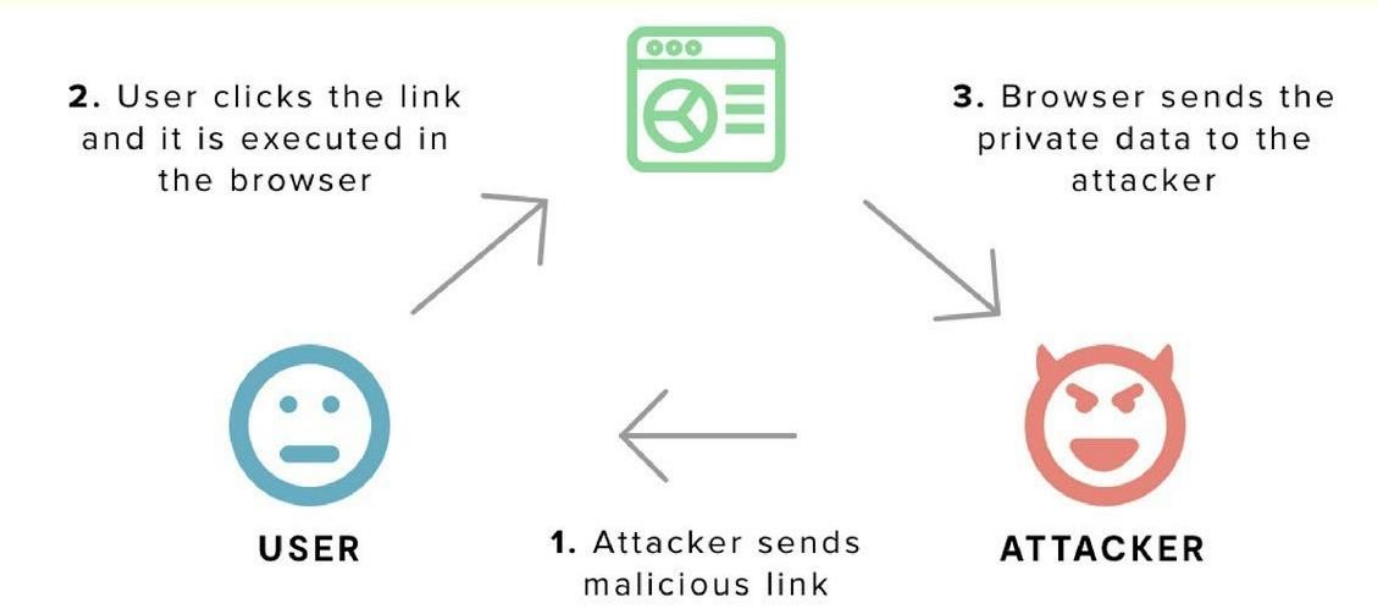
Stored XSS attack

شرح الهجوم Stored XSS

It happens when the malicious code is stored in the database or on the server, and whenever any user visits the page, the code gets executed automatically. It is dangerous because it affects all users who visit the infected page.

Stored XSS (الهجوم المخزن)

يحدث عندما يتم حفظ الكود الضار في قاعدة بيانات أو على الخادم،
وعند زيارة أي مستخدم للصفحة، يتم تنفيذ الكود تلقائيًا.
خطير لأنه يؤثر على جميع المستخدمين الذين يزورون الصفحة المصابة.



Reflected Cross-site Scripting

شرح Reflected XSS

An attack where the attacker places malicious code inside a link and sends it to the victim. When the victim opens the link, the code runs directly in their browser.

هجوم عن طريق وضع كود ضار داخل رابط، ثم إرساله للضحية.
وعندما يفتح الضحية الرابط، يتم تنفيذ الكود داخل متصفحه مباشرة.

DOM Based XSS: An attack where the malicious code is executed directly in the victim's browser through JavaScript on the page. The payload does not go to the server; instead, it is handled on the client side using the DOM.

It happens when JavaScript on the page reads data from the URL or page elements without proper filtering, and then injects it back into the page in a dangerous way.

DOM-based XSS attack

DOM Based XSS شرح

هذا نوع من الهجوم يحدث داخل متصفح المستخدم، عندما يقوم الجافاسكربت بمعالجة البيانات القادمة من الرابط أو الصفحة بدون فلترة أو حماية صحيحة.

Example - مثال

How Does XSS Happen?

كيف يحدث هجوم XSS؟

```php
<?php
echo "Hello " . $_GET['name'];
?>
```

```
http://example.com/?name=<script>alert('XSS')</script>

<img src=x onerror="alert('You have been hacked')">
```

How to Prevent XSS?

كيف نحمي موقعنا من XSS؟

Avoid displaying user input directly in the page. Always make sure it is safe or turned into plain text before showing it.

تجنب الطباعة المباشرة داخل الصفحة لأي بيانات يدخلها المستخدم، إلا بعد التأكد من معالجتها أو تحويلها لنص عادي.

How to Prevent XSS?

كيف نحمي موقعنا من XSS؟