Stored XSS

주관적으로 생각했을 때 가장 간단한 공격 기법이다.

Stored XSS는 악성 스크립트가 서버 내에 DB, 파일 등의 형태로 저장되어 있다.

이렇게 말하면 이해가 잘 안될 수도 있는데 ,

대표적인 예를 들어보자.

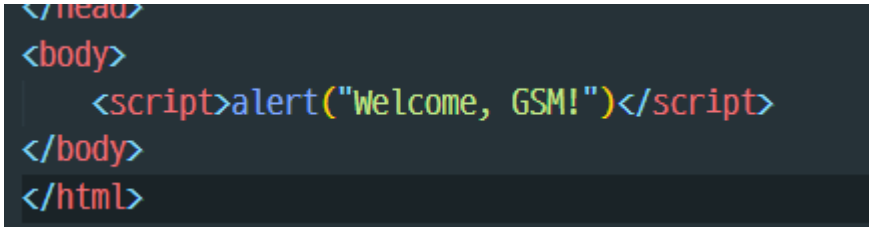
게시판

어느 한 서버의 게시판 서비스에 글을 게시한다고 가정하자.

게시글을 작성 할 때 평범한 게시글을 작성했을 때와 악성 스크립트를 적은 게시글을 비교해 보자.

평범한 게시글을 열람 했을 때 HTML 코드

악성 스크립트를 적은 게시글을 열람 했을 때 HTML 코드



이런 식으로 스크립트 태그를 이용하여 공격하는 식이 일반적이다.

이렇게 단순한 취약점인데도 불구하고, 이런 취약점이 발생하는 서버가 많다.

대응책

대응책은 대표적인 예로 필터링이 있다.

간단하게 알아보면, <, >와 같은 태그 기호를 막는 것과,

<script>자체를 필터링 하는 방법이 있다.

하지만 이 방법 또한 <sc<script>ript>alert(1)</sr<script>ipt> 와 같이 우회하는 방법이 있다.

소규모 서버를 운영하면 저 정도 필터링만으로 충분하겠지만,

대규모 서버를 운영한다면 여러가지 필터링을 걸어놔야 할 필요성이 있는 것 같다.