XSS

크로스 사이트 스크립팅(XSS)는 웹 애플리케이션의 취약점을 이용하여 악성 스크립트를 삽입하여 사용자의 브라우저에서 실행되게 하는 공격이다. 이를 통해 공격자는 사용자의 정보를 탈취하거나, 세션을 탈취하거나, 악성 행동을 유도할 수 있다. XSS는 웹 해킹의 대표적인 공격 중 하나로, 웹 애플리케이션의 보안에 큰 위험을 야기할 수 있다.

XSS 공격의 세 가지 유형

1. **Stored XSS (영구적 XSS)**: 악성 스크립트가 서버에 저장되어 사용자가 해당 페이지를 방문할 때 실행된다. 예를 들어, 사용자의 댓글이나 게시글에 악성 스크립트가 삽입되어 저장되고, 이후 다른 사용자가 해당 페이지를 열면 스크립트가 실행된다.
2. **Reflected XSS (반사적 XSS)**: 악성 스크립트가 사용자의 입력과 함께 서버로 전송되며, 서버에서 해당 입력을 바로 응답으로 반환할 때 발생한다. 공격자는 피해자에게 악성 링크나 메시지를 보내고, 피해자가 해당 링크를 클릭하거나 메시지를 열면 스크립트가 실행된다.
3. **DOM-based XSS**: Document Object Model(DOM)을 조작하여 발생하는 XSS 공격이다. 악성 스크립트가 웹 페이지의 DOM을 변경하여 웹 페이지의 동작을 조작하거나 사용자의 정보를 탈취한다.

XSS 공격 보안 대책

1. **입력 검증 및 필터링**: 사용자의 입력값을 검증하고 허용되지 않은 스크립트 코드를 제거하거나 이스케이프하여 처리해야 한다.
2. **출력 이스케이프**: 웹 페이지에서 동적으로 생성되는 내용을 출력할 때는 반드시 적절한 이스케이프 함수를 사용하여 스크립트 실행을 방지해야 한다.

3. **HTTP 헤더 설정**: Content Security Policy (CSP) 헤더를 사용하여 허용되는 스크립트 리소스의 출처를 제한할 수 있다.
4. **세션 보안 강화**: 사용자 세션을 안전하게 관리하고 쿠키 속성을 설정하여 스크립트 실행을 제한할 수 있다.
5. **웹 보안 테스트**: 웹 애플리케이션을 정기적으로 보안 테스트하고 XSS 취약점을 찾아내고 수정해야 한다.