Cross Site Scripting

간단한 XSS 설명과 예제

J. Hong

XSS 공격이란?

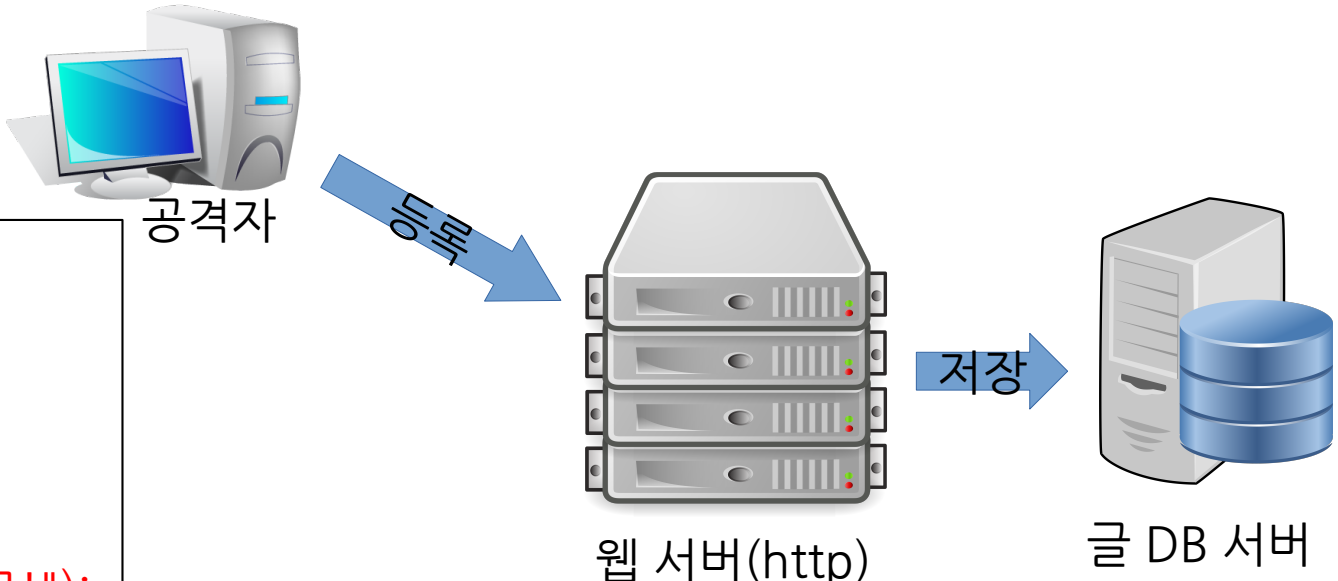
- 공격자가 정상적인 스크립트(또는 코드) 사이에 악성 스크립트를 삽입하는 공격.
- Java Script가 될 수도 있고 다른 코드가 될 수도 있음.

공격 시나리오

1. 취약한 게시판 홈페이지에 공격자가 악성 스크립트가 담긴 글을 등록
2. 악성 스크립트가 포함된 글은 Server의 글 Database에 저장
3. 희생자가 악성 스크립트가 포함된 글을 열람하면 악성 스크립트가 희생자의 컴퓨터에서 실행됨

상세 설명 - 1

- 공격자가 악성 스크립트 삽입된 글 등록



제목:
저를 열어보면 좋은 일이?!

내용:
```
</p>
    <script>
    alert("악성스크립트 실행 완료!");
    </script>
<p>좋은 하루 되세요~
```

상세 설명 - 2

- 웹 서버는 기본 HTML에 해당 글의 제목, 내용을 넣어 동적으로 생성한 웹 문서를 클라이언트로 전송함.

view.html

생성

```
<!DOCTYPE html>
<html lang="kr">
        <head>
                <meta charset="UTF-8">
                <title>게시물 조회</title>
        </head>
        <body>
                <h1>게시물 조회<h1>
                <hr>
                <div id="content_area">
                        <p id='title'></p>
                        <p id='content'></p>
                </div>
        </body>
</html>
```

+

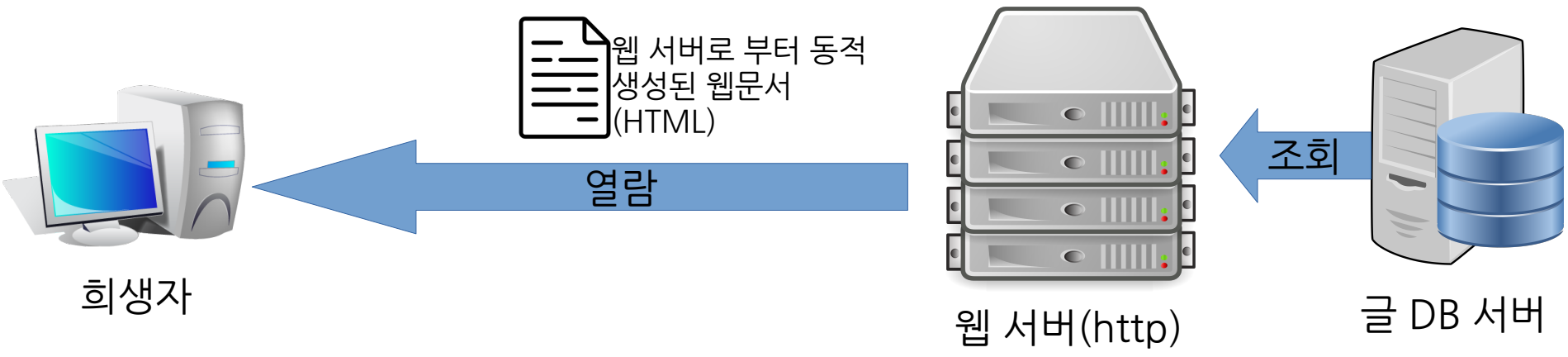
제목:
저를 열어보면 좋은 일이?!

내용:

```
</p>
        <script>
        alert("악성스크립트 실행 완료!");
        </script>
<p>좋은 하루 되세요~
```

상세 설명 - 3

- 희생자가 악성 스크립트 포함된 글 열람



상세 설명 - 4

- 공격자가 등록한 글의 내용은 코드로 취급되어 희생자의 컴퓨터에서 실행됨

```
<!DOCTYPE html>
<html lang="kr">
	<head>
		<meta charset="UTF-8">
		<title>게시물 조회</title>
	</head>
	<body>
		<h1>게시물 조회<h1>
		<hr>
		<div id="content_area">
			<p id='title'>저를 열어보면 좋은 일이?!</p>
			<p id='content'></p>
				<script>
					alert("악성스크립트 실행 완료!");
				</script>
			<p>좋은 하루 되세요~</p>
		</div>
	</body>
</html>
```

XSS 공격의 경우

```
<!DOCTYPE html>
<html lang="kr">
	<head>
		<meta charset="UTF-8">
		<title>게시물 조회</title>
	</head>
	<body>
		<h1>게시물 조회<h1>
		<hr>
		<div id="content_area">
			<p id='title'>저를 열어보면 좋은 일이?!</p>
			<p id='content'>좋은 하루 되세요~</p>
		</div>
	</body>
</html>
```

XSS 공격 코드가 없는 정상적인 HTML코드

상세 설명 - 5

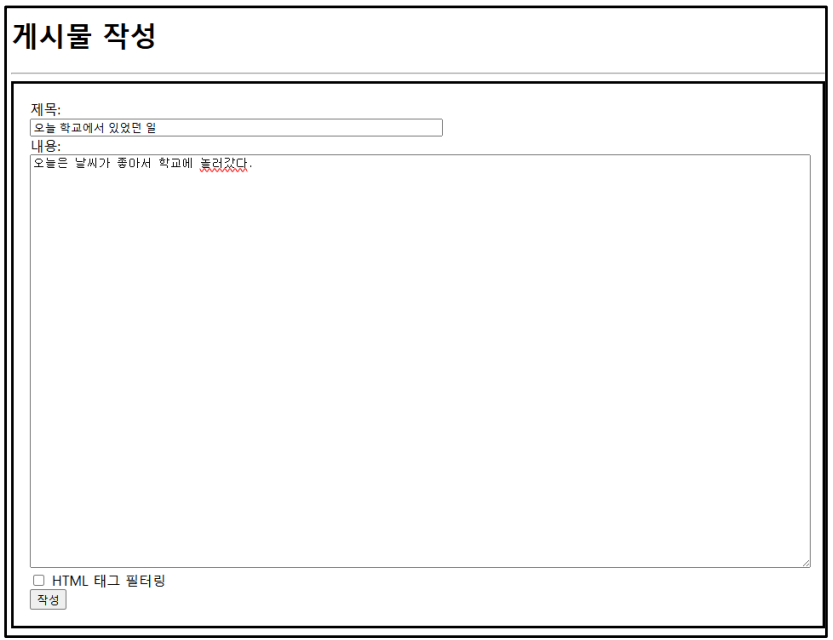
- 예제의 경우 팝업 창 하나 띄우는 게 전부지만 공격자가 의도한 코드를 원격 환경에서 실행되게 할 수 있다는 점에서 충분히 위협적임.
- 예방하기 위해서는 사용자의 입력을 신뢰해서는 안됨. 유저가 입력한 글에서 HTML에 사용되는 <, >, &, ; 등의 특수 문자를 HTML Entity로 치환하거나 제거하여 위협을 완화함.

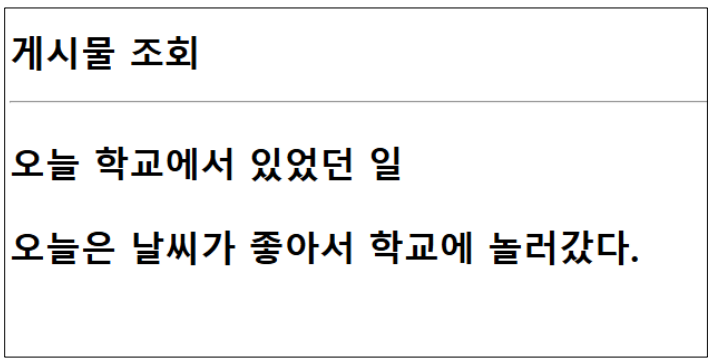
상세 설명 - 6

- 예시로는 간단한 공격을 보였지만 기상천외한 방법으로 필터링을 우회할 수 있음.

예제

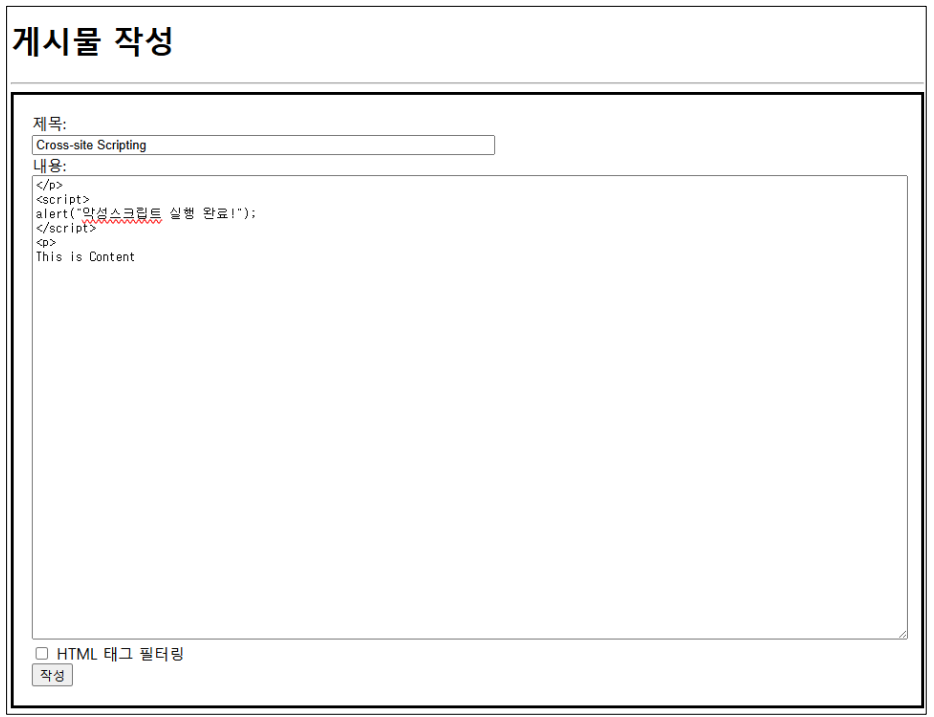
- 제목, 내용을 입력하면 새 창을 열어 다시 보여주는 간단한 예제

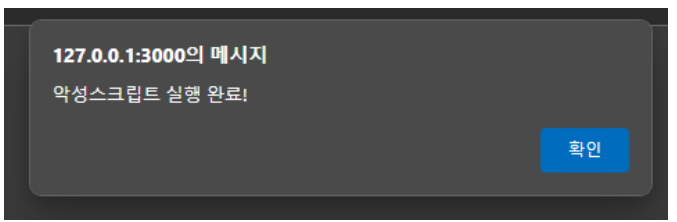




예제

- 사용자 입력을 RAW하게 출력하기 때문에 취약.

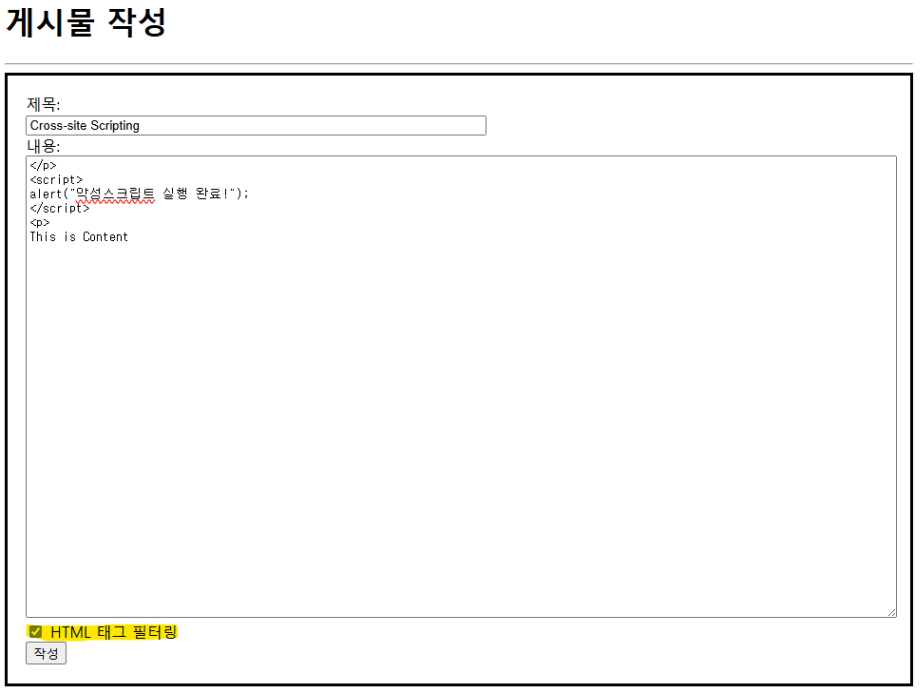


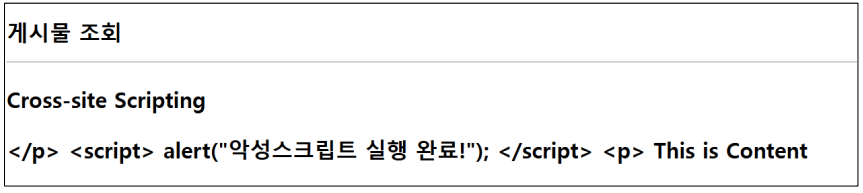


공격자가 입력한 글이
스크립트로써 실행되어
팝업창이 나온다.

예제

- 체크박스를 체크하면 단순한 필터링을 실시함.





필터링에 의해 HTML Entity로 치환되었기 때문에 코드로 인식되어 실행되지 않고 그대로 출력.

감사합니다.