Injection 공격

목 차

01.Injection 공격이란?

Injection의 사전적 의미는 주사, 주입의 의미로 Injection 공격은 공격자의해 신뢰할 수 없는 입력을 프로그램에 주입하도록 하는 공격을 의미하며 이를 통해 해당 프로그램의 실행 과정의 변경을 유도하거나 공격자의 변경 질의를 통해 결과값을 다르게 나오도록 할 수 있다. 다양한 방법으로 악용될 수 있는데 이 공격 방법들은 관리자 권한 획득, 악성코드 전파를 통한 정상적인 서비스 운영 불가, 개인정보와 같은 데이터를 획득, 데이터의 무결성 손실 혹은 전체 시스템 손상 등 악용 범위가 무궁무진한 공격이다.

02.대표적 3가지 Injection 공격 종류

-3가지 대표 공격-

SQL Injection

Injection 공격의 가장 무섭고 대표적 공격이라 할 수 있으며 쉬운 난이도에 비해 굉장한 파괴력을 가지고 있다. 클라이언트의 입력값을 조작하여 서버의 데이터베이스를 공격할 수 있는 공격 기술

Command Injection

웹 애플리케이션에서 시스템 명령어를 실행할 수 있는 함수를 제공하며 사용자 입력값에 필터링이 제대로 이루어지지 않을 경우 공격자가 시스템 명령어를 호출할 수 있는 공격 기술

DLL Injection

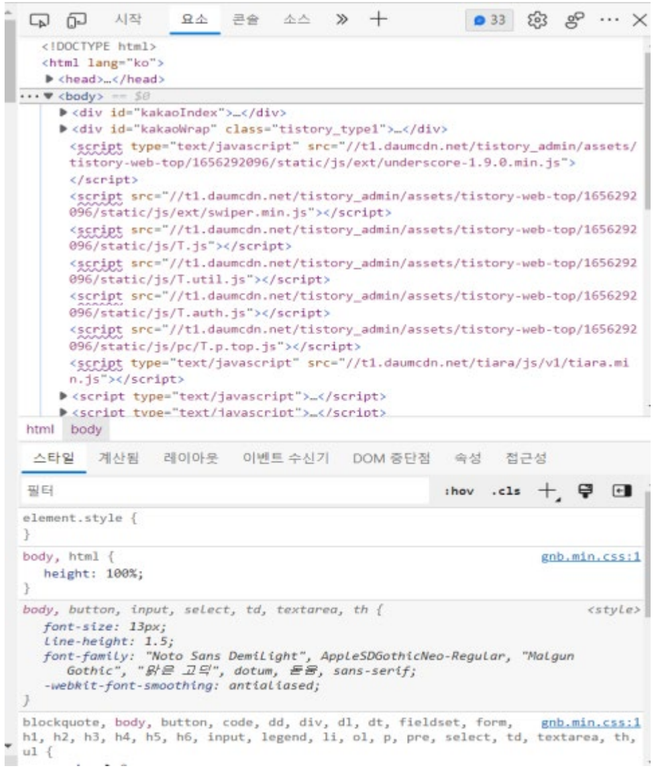
외부 프로그램을 통해 다른 프로그램에 제작자가 의도하거나 예상하지 않은 영향을 미치기 위해 사용하며 다른 프로세스의 주소 공간 내에서 DLL을 강제로 로드시킴으로써 코드를 실행시키는 공격 기술

03.HTML Injection

HTML이란?

HyperText Markup Language

하이퍼텍스트를 가장 중요한 특징으로 하는 마크업이라는 형식을 가진 컴퓨터 프로그래밍 언어



03.HTML Injection

HTML Injection이란?

사용자가 연결을 요청한 페이지에 공격자가 HTML 태그를 삽입하여 의도하지 않은 내용을 보게 하거나 악의적인 사이트에 연결하게 하는 공격 기법이다.

03.HTML Injection

HTML Injection 종류 2가지

1. 반사기법(Rflected)

-Get 방식: URL 형태로 표현하게 되는 방식으로 특정 페이지를 다른 사람에게 접속하게 할 수 있음.

-Post 방식: 값을 body 안에 숨겨서 전송, 사용자가 입력한 값을 바탕으로 작업을 수행

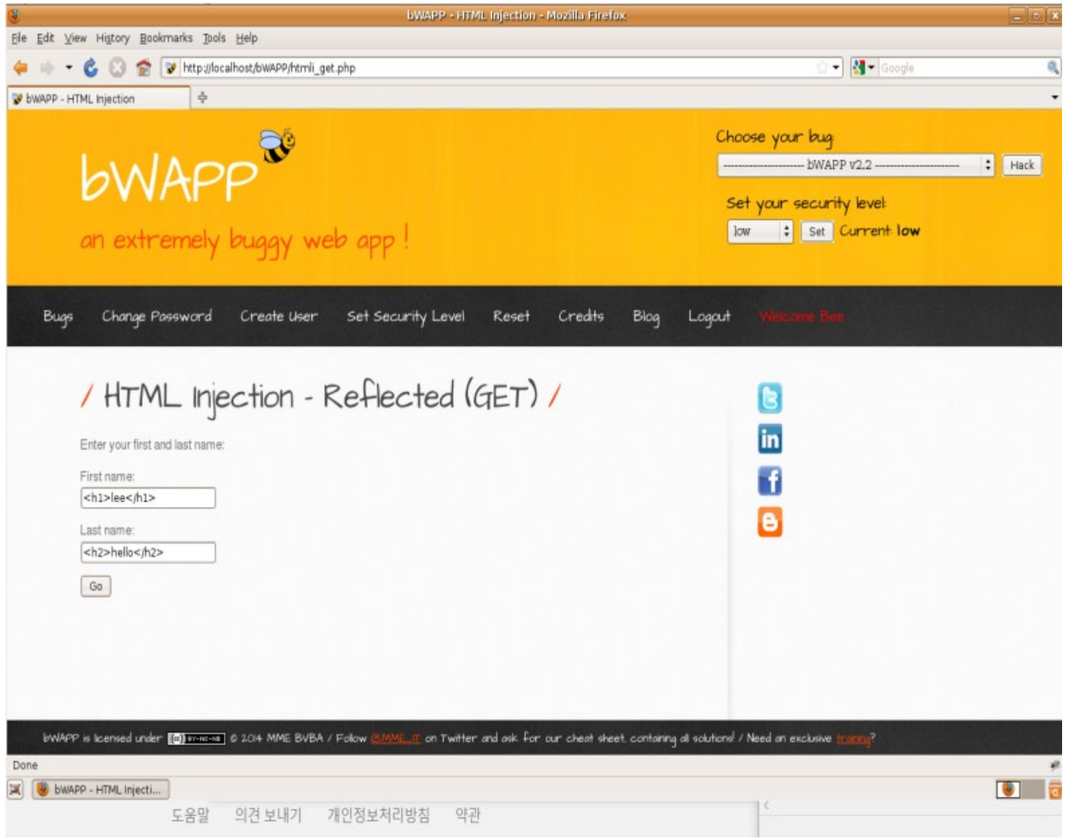
2. 저장기법(Stored)

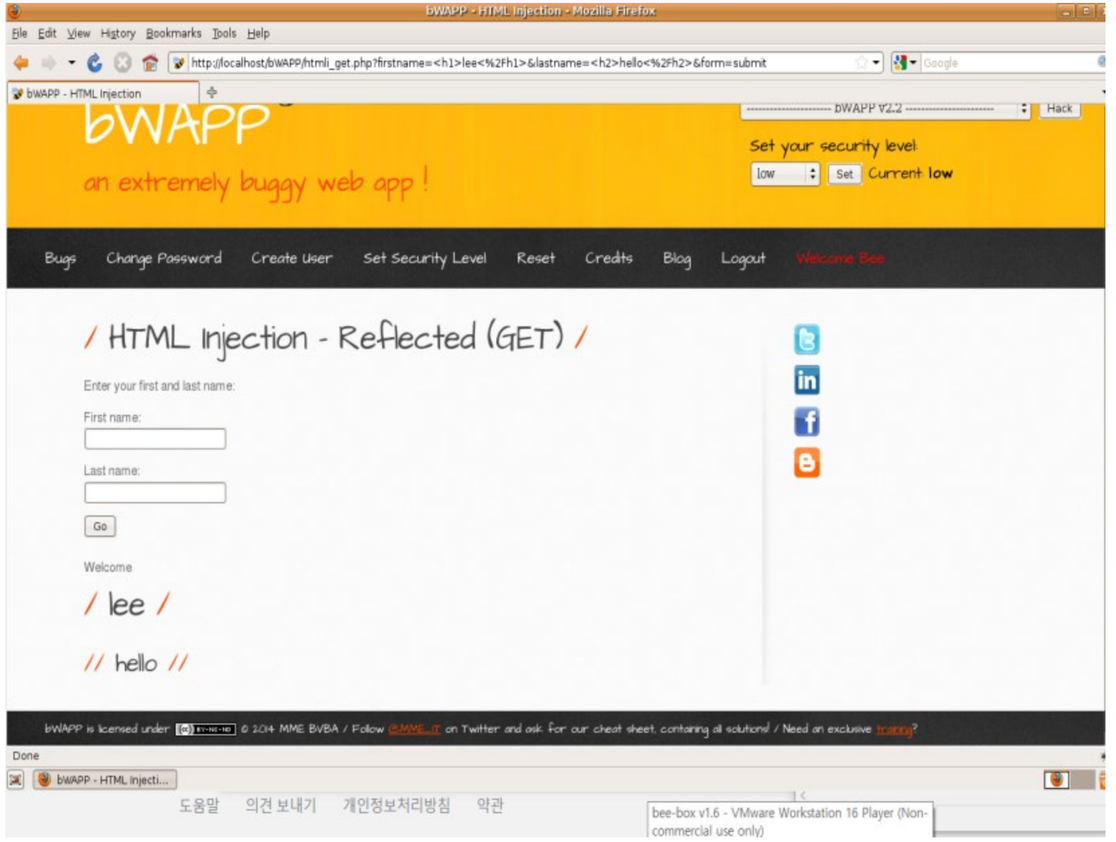
악의적인 HTML 태그를 데이터베이스에 저장하여 저장된 태그 내용을 확인한 사용자의 PC에 HTML 태그가 실행되게 하는 공격기법

04.HTML Injection 공격 실습

실습 환경: Bee-Box

HTML injection - Reflected(Get 방식)





04.HTML Injection 공격 실습

HTML injection - Reflected(Get 방식)

```
<br />
Welcome <h1>lee</h1> <h1>hello</h1>
```

```
%3Ch1%3Elee%3C%2Fh1%3E
%3Ch1%3Ehello%3C%2Fh1%3E
```

05.느낀 점

1

공부 부족

HTML을 공부하다 이를 이용한 해킹 기법을 찾다 Injection 공격에 대해 알게 되었는데 발표 준비를 하면서 기술적 이해와 설명이 부족하다고 느낌(추후에 SQL Injection을 SQL을 학습 후 다시 공부하고 발표할 생각)

2

다양한 경험 필요

웹 개발과 해킹을 제대로 이해하고 학습하려면 다양한 언어와 사례들을 공부하고 직접 적용해야 더 쉽고 자세하게 이해할 수 있을 것 같다고 느낌

Q & A