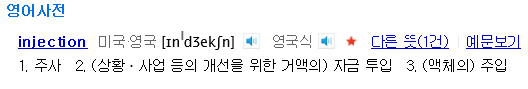
2주차

인잭션(Injection)

1. 주사,주입-문자 그대로 원형에 공격자가 무언가를 주입해서 원하는 결과를 도출 하는 것.
2. html인잭션, sql인잭션
   * html: 각종 폼들로 아웃풋이나 입력이 결정되는경우 등 헤더를 이용해 아웃풋이나 입력이 바뀔수 있는데 이를 이용해 공격 할 수 있다.
   * sql:sql문과 스크립트의 취약점을 이용한 공격

ex)보통 id와 pw값을 비교해 비밀번호가 맞으면 로그인 성공을 시키는데 이때 ‘OR’1’=‘1 같은 비밀번호를 입력하여 비교 쿼리를 항상 트루 값으로 만들어 접속시키는 방법

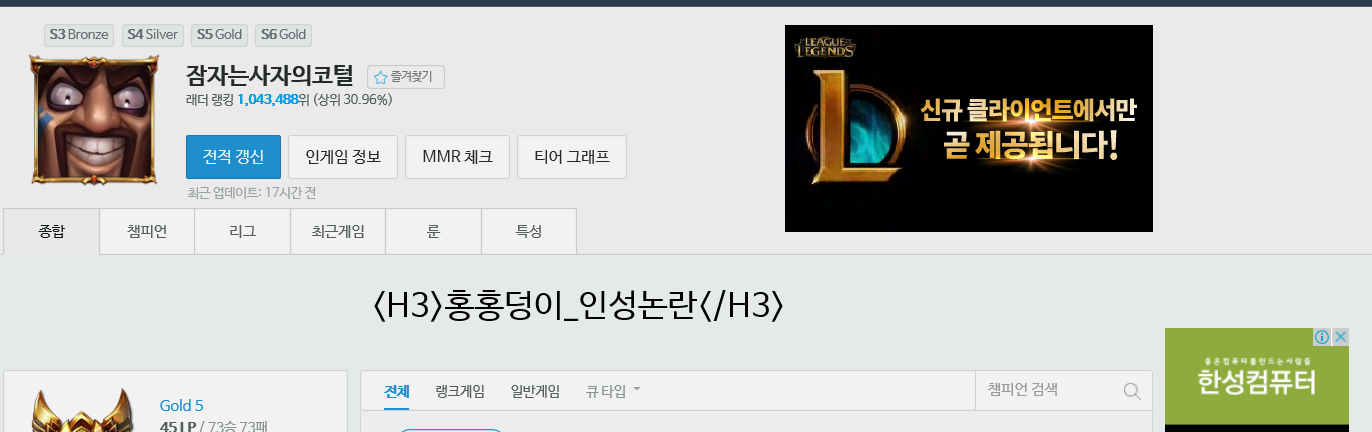


1. HTML인잭션 이란?

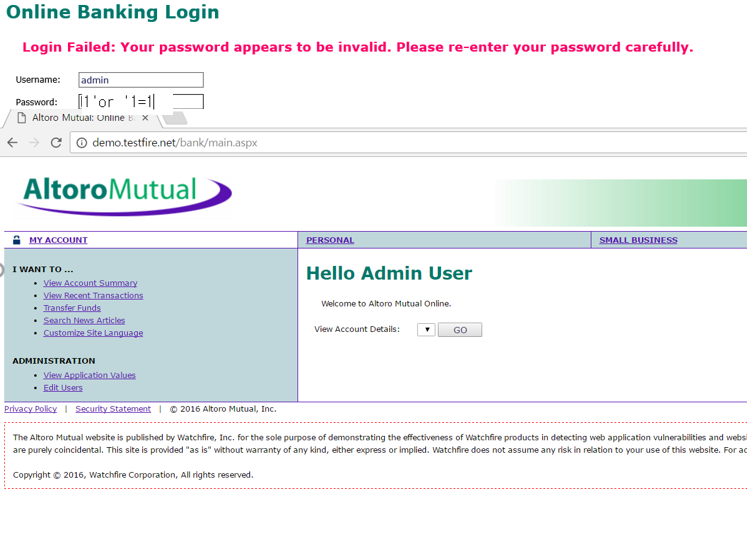
-html은 html이라는 말 자체에서 알 수 있듯이. 텍스트를 이용하여 페이지를 디자인하고 기능을 넣은 것인데.

input type안에 들어가는 정보를 그대로 출력하거나 저장하게 돼있는 코딩의 경우 그 글자 그대로 출력하거나 저장하기 때문에 그 안에 html의 형식을 갖춘 텍스트를 삽입할 경우 문제가 생길수 있다.

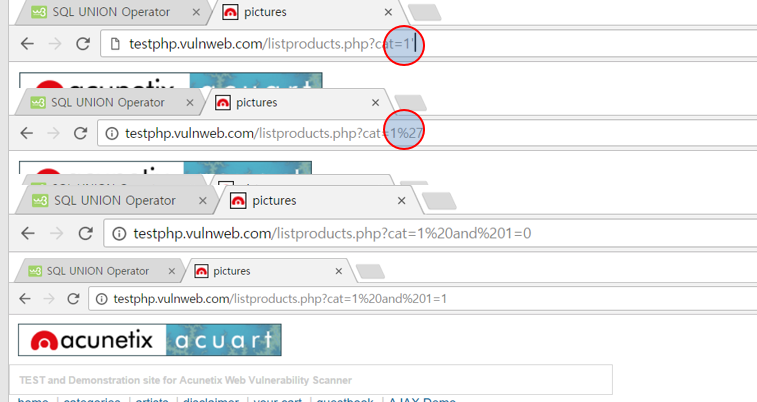
OP.gg에 실습. 잘 막혀있음을 확인 할 수 있다.

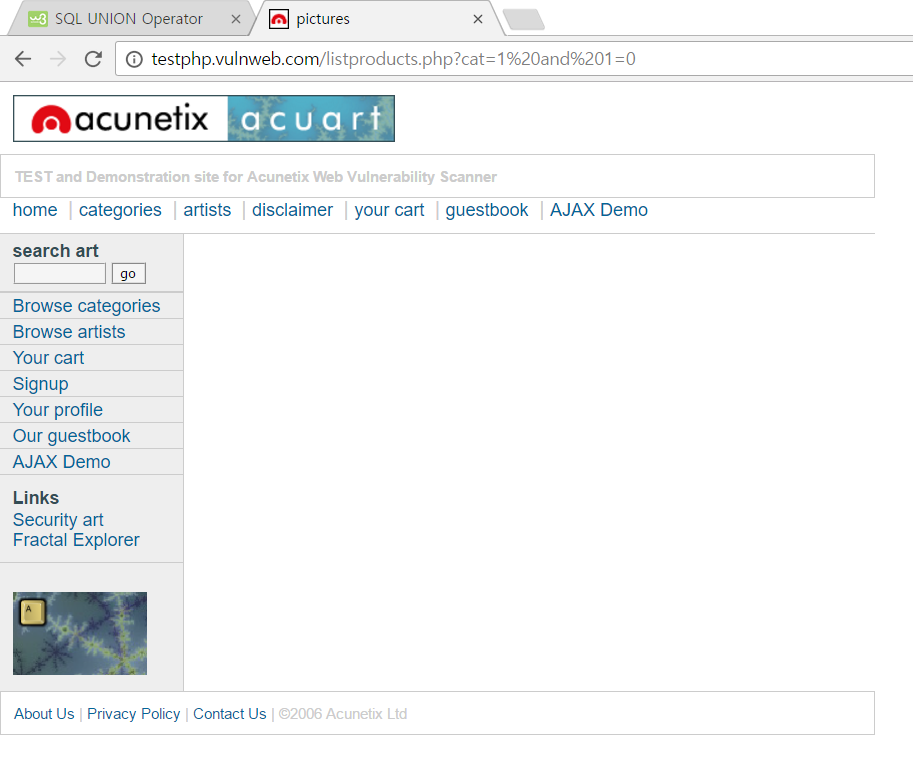


인증 우회 실습 1’or’1’=’1 으로 쿼리 값을 참으로 만듦.

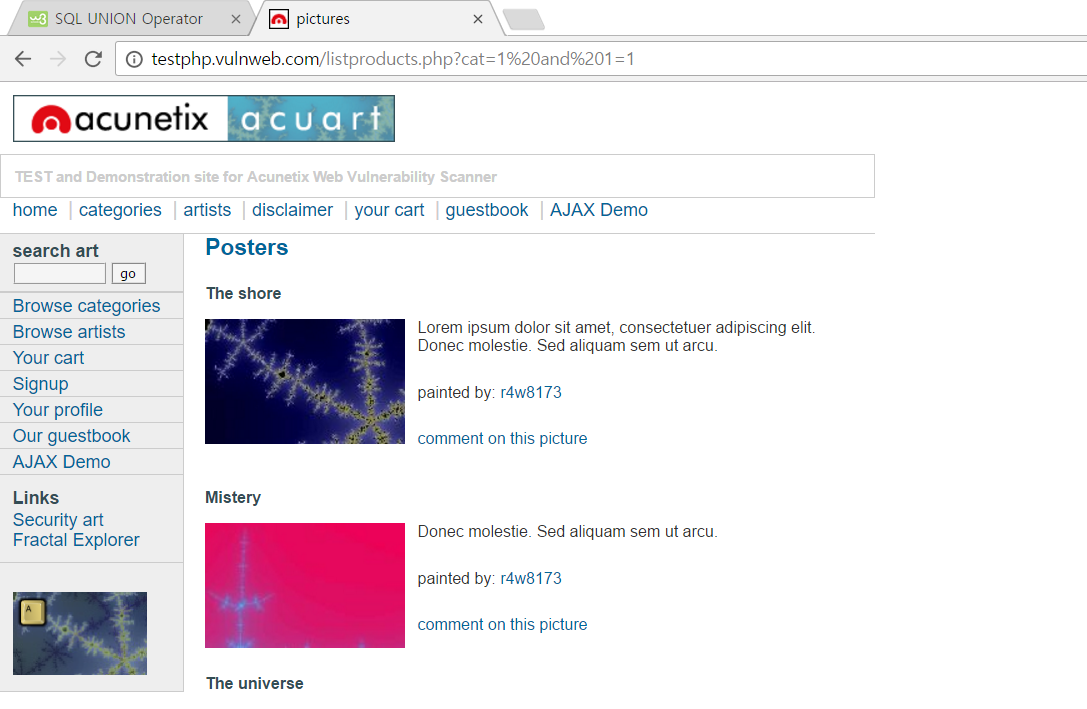


쿼리가 안될경우 파라미터로 가능한지 확인하는 과정





-쿼리 1=0이 거짓이기에 아무런 페이지도 호출되지 않음



-쿼리 1=1이 되기 때문에 호출됨 따라서 이 페이지에선 파라미터를 이용하여 뭔가 쿼리를 전달한다는 것을 알 수 있음.

SQL인잭션

* SQL 인젝션은 코드 인젝션의 한부분으로 클라이언트의 입력값을

조작하여 서버의 데이터 베이스를 공격할 수 있는 공격방식

* 공격이 쉬운데 비해 파괴력이 크다
* 인젝션의 경우 테스트를 통해 발견하긴 힘들지만

스캐닝툴이나 코드 검증절차를 거치면 보통 쉽게 발견된다.

논리적 에러를 이용한 인잭션 기법

1. OR연산을 이용
   1. Id값을 TEST\_ID로 주고 비밀번호를 ‘test’or’1’=‘1’을 입력하면
   2. select \* from member where id =‘TEST\_ID’ and bPass\’test’or’1’=‘1’; 위와같은 쿼리가 전달이 되고
2. 주석문을 이용한 admin 로그인
   1. 주석문을 이용해 뒤에것을 무시하는 기법
      1. ex1. select\* from member where bid=‘admin’ and bPass=‘test’or’1’=‘1’
      2. ex2. select\* from member where bid=‘admin’ –and bPass=‘’
      3. select\* from member where bid=‘admin’

위의 1번을 2번으로 바꾸면 bPass는 무시되어 3번처럼 변하고 비밀번호 없이 바로 로그인이 가능하다.

에러 기반의 SQL인잭션이 가능한지 여부는 특수문자를 입력해 보아 에러발생여부를 보면 알 수 있다. 주석처리시 – 이후 ; 세미콜론이 붙지 않는데 왜 쿼리문이 돌아가는지 이해가 가지않음.

3. 두개 이상의 쿼리를 이용하는 Union SQL Injection

유니언은 2개이상의 쿼리를 요청하여 결과를 얻는 연산자로 공격자는 이를 악용하여 원래의 요청에 한 개의 추가 쿼리를 삽입하여 정보를 얻어내는 방식이다.

ex) <http://www.site.com/news.php?id=5> union all select 1 , table\_name ,3 from information\_schema.tables

4. 쿼리 가능엽를 이용하는 Blind SQL Injection

악의적인 문자열 삽입 대신 쿼리결과에 따라 정보를 취득하는 기법이다.

-> 에러가 없는 사이트에서는 위의 기법들을 사용 할 수 없기때문에 정상적인 방법으로 수행

쿼리가 수행된다면 취약점이 없다고 볼 수 있으나 쿼리가 수행되지 않는다면 공격가능성은 있다고 볼 수 있다.

5. 저장 프로시저를 이용하는 Stored Procedure SQL Injection

저장 프로시저

6.타임 기반의 Blind SQL Injection

쿼리결과를 특정 시간만큼 지연시키는 방법을 이용

ex) URL+ AND SLEEP(5) 이라고 했을때 5초의 지연이 발생한다고 하면 쿼리가 제대로 들어가고 있다는 뜻이므로 취약점이 있다고 판단가능 만약 수행되지않고 빈 페이지만을 즉시 제공한다면 사용하는 DB가 MySQL이 아니라는 것을 유추해 볼 수 있다.